Pla d'adequació a l'Esquema Nacional de Seguretat en un Ajuntament.

Alumne: Juan Antonio Vera Nieto

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

Área: Sistemas de Gestión de la Seguridad de la Información

Consultor: Arsenio Tortajada Gallego
Centre: Universitat Oberta de Catalunya - UOC

Data Lliurament: 28/12/2020

FITXA DEL TREBALL FINAL

Títol del treball:	*Pla d'adequació a l'Esquema Nacional de Seguretat en un Ajuntament.*
Nom de l'autor:	*Juan Antonio Vera Nieto*
Nom del consultor:	*Arsenio Tortajada Gallego*
Data de lliurament (mm/aaaa):	*12/2020*
Àrea del Treball Final:	*Sistemes de gestió de la seguretat de la informació*
Titulació:	*Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)*

Resum del Treball (màxim 250 paraules):

Aquest treball fi de màster descriu els objectius, l'abast, planificació i resultats d'un projecte d'adequació d'un ajuntament a l'Esquema Nacional de Seguretat.

El capítol 1 es justifica la necessitat de d'assegurar la informació i serveis d'un Ajuntament, i es fa una introducció al Esquema Nacional de Segureta (ENS).

El capítol 2 es fa una comparativa de similituds i diferències entre l'ENS i la ISO27001, i la possible adaptació de l'Ajuntament a les dues normatives aprofitant l'esforç realitzat dins del pla d'adequació.

El capítol 3 es descriu l'Ajuntament d'estudi, la seva activitat i es realitza un anàlisi diferencial amb l'ENS i la ISO27001 per tal de trobar les mancances.

El capítol 4 es dedica a presentar el sistema documental que suportarà tota la normativa del SGSI, així com el redactat de la política de seguretat, indicadors de gestió i la declaració d'aplicabilitat (entre d'altres).

El capítol 5 trobem una anàlisi de riscos molt detallat amb l'eina PILAR, que ens mostrarà el grau d'exposició dels actius identificats del nostre ajuntament .

Com a resultat d'aquest anàlisi, es proposen uns projectes de millora al capítol 6 que hauran de millorar la seguretat.

Finalment, es presentarà a la part final possibles línies de treball posteriors a aquest TFM.

Abstract (in English, 250 words or less):

This final master's thesis describes the objectives, scope, planning and results of a project to adapt a city council to the National Security Scheme.

Chapter 1 justifies the need to ensure the information and services of a City Council, and makes an introduction to the National Security Scheme (ENS).

Chapter 2 makes a comparison of similarities and differences between the ENS and ISO27001, and the possible adaptation of the City Council to the two regulations taking advantage of the effort made within the adaptation plan.

Chapter 3 describes the study City Council, its activity and carries out a differential analysis with the ENS and ISO27001 in order to find the shortcomings.

Chapter 4 is dedicated to presenting the document system that will support all ISMS regulations, as well as the wording of the security policy, management indicators and the declaration of applicability (among others).

In Chapter 5 we find a very detailed risk analysis with the PILAR tool, which will show us the degree of exposure of the identified assets of our city council.

As a result of this analysis, in Chapter 6 some improvement projects are proposed that will need to improve security.

Finally, possible lines of work after this TFM will be presented at the end.

Paraules clau (entre 4 i 8):

SGSI. ENS, ISO27001, PILAR, ANÀLISI RISCOS

Índex

Índex de taules

Índex de figures

1. Introducció

1.1 Context i justificació del Treball

CONTEXT DEL TREBALL

Totes les organitzacions (independentment de la seva mida) i del seu tipus (sigui pública o privada) han de recollir, processar, emmagatzemar i transmetre informació fent servir mitjans electrònics, físics i orals (amb converses i presentacions, per exemple) [1]. I això és així atès que actualment ja ningú pot dubtar que un dels actius més importants per a qualsevol organització és la informació amb la que treballa.

De fet, aquesta informació i el conjunt de serveis que es troben desenvolupats al voltant (o gràcies a la seva existència) és la base del que anomenem *Societat de la Informació,* i que es basa en posar la informació en el centre de tot per poder realitzar les activitats de qualsevol organització. Per tant, podem assegurar sense por a equivocar-nos que la *Informació* (més concretament, la seva gestió i explotació) s'ha convertit en quelcom fonamental i estratègic per a qualsevol organització d'avui en dia.

Però no podem considerar la informació com un concepte aïllat dins del món a on ens trobem, atès que la informació com a tal no té valor si no és possible obtenir *coneixement* de les dades gràcies a una explotació de la mateixa. Dins d'aquest escenari ens podrem trobar des de l'organització més petita que gestiona una petita base de dades de clients, fins a les grans corporacions a on es gestionen terabytes d'informació, coincidint totes en un factor comú: necessiten la informació per poder realitzar les seves activitats i aconseguir els objectius que com a organització s'han fixat (o els hi han fixat, com ja veurem posteriorment, mitjançant normatives dins d'un marc regulatiu que han de seguir).

Per tant, aquesta explotació de la informació es traduirà en una *cartera de serveis* que oferirà l'organització, serveis que al prestar-se fent servir les TIC i prenent com a element primordial la informació que disposa l'organització, formarà part de l'ecosistema global que ens trobem dins d'allò que es coneix i anomenem com *Societat de la Informació.*

Val a dir que la prestació de serveis telemàticament no és un concepte nou, atès que la mateixa xarxa d'Internet es va crear originàriament per connectar ordinadors i intercanviar informació entre ells. La diferència principal que podem trobar entre aquella època i l'actual és el valor que té la informació (i els serveis) que son prestats a la xarxa: serveis com *e-commerce*, banca per internet, serveis governamentals, etc ... són

prestats fent servir les TIC, adquirint aquesta prestació de serveis un gran valor econòmic que és d' interès per organitzacions *ciber-criminals.*

Per tant, i resumint l'exposat, actualment ens trobem en un context a on totes les organitzacions ofereixen serveis de gran interès econòmic a través d'Internet i que tenen com a valor (o actiu) principal la informació que gestionen, i que aquesta informació (i seus serveis associats amb ella) ***necessita d'una protecció contínua*** per evitar qualsevol incident que puguin posar en perill els objectius de les organitzacions. I és justament amb la necessitat d'una protecció contínua d'aquests serveis i informació a on hem d'abordar una aproximació metòdica en la realització d'aquesta protecció, no podent deixar a la improvisació les decisions relacionades a proporcionar aquesta seguretat. És en aquesta protecció contínua i en l'aproximació sistemàtica a la mateixa a on haurem de definir un procés de gestió de la seguretat dins de les organitzacions, procés com el definit a la norma ISO27001:2013, o de l'Esquema Nacional de Seguretat, com veurem posteriorment.

SOCIETAT DE LA INFORMACIÓ I SECTOR PÚBLIC

Com hem pogut veure, les organitzacions necessiten protegir-se dels possibles incidents de seguretat que puguin malmetre els seus serveis o comprometre la informació de que disposen. D'aquesta manera es podrà impulsar la Societat de la Informació al poder permetre als ciutadans i empreses fer servir les eines TIC d'una manera més eficient, àgil, i sobretot segura en la prestació dels seus serveis. Tots aquests avantatges que proporciona la Societat de la Informació (eficiència, reducció de costos, flexibilitat, etc), i que les empreses i organitzacions privades s'estan beneficiant ja fa temps, han d'arribar també a les organitzacions del sector públic. Els Estats reconeixen la necessitat de poder oferir també els seus serveis fent servir les eines TIC, i aprofitar-se també dels avantatges d'aquest nou paradigma. De fet, la *Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans* [2] *als Serveis Públics* (ara ja derogada per la llei 39/2015 i la 40/2015) ja deixa en l'exposició de motius

«És en aquest context en el qual les administracions s'han de comprometre amb la seva època i oferir als seus ciutadans els avantatges i possibilitats que la societat de la informació té, assumint la seva responsabilitat de contribuir a fer realitat la societat de la informació. Els tècnics i els científics han posat en peu els instruments d'aquesta societat, però la seva generalització depèn, en bona mesura, de l'impuls que rebi de les administracions públiques. Depèn de la confiança i seguretat que generi en els ciutadans i depèn també dels serveis que ofereixi»

Per tant, els diferents tipus d'organitzacions que conformen el sector públic es troben oferint també serveis fent servir les TIC i, per tant,

formen ja part de la Societat de la Informació, compartint amb la resta d'organitzacions les avantatges que proporciona, però també els perills als que s'està sotmès dins d'aquest nou entorn.

Per tot això, és necessari també a les AAPP una aproximació sistemàtica i metòdica per tal de protegir els serveis i la informació que hi estan oferint. Podem arribar a dir que, fins i tot, la protecció que han d'oferir les AAPP ha de ser superior en moltes situacions a la protecció que poden oferir altres organitzacions de la mateixa mida. Això és justifica pel tipus especial de serveis que hi ofereixen (salut, atenció social, etc) amb el què es treballa, en moltes ocasions, amb informació especialment protegida.

És per tot això que es va aprovar el Reial Decret 3/2010 [3] que regula **l'Esquema Nacional de Seguretat.** Es tracta d'una norma d'obligat compliment per part de tot el sector públic que es sustenta en principis internacionals de seguretat de la informació, i que tracta la protecció de la informació, els sistemes i els serveis. El ENS contempla i exigeix la gestió continuada de la seguretat, per la qual cosa cal aplicar un sistema de gestió. De fet, l'ENS contempla la seguretat com un procés integral (art. 5), i la reavaluació periòdica (art. 9). També fa aparèixer un nou procés de seguretat dins de les AAPP, procés que s'ha d'organitzar i implementar (art. 12), que necessitarà d'una millora contínua (art. 26), entre d'altres.

Per satisfer els esmentats principis bàsics i requisits mínims es pot aplicar un model de tipus PCDA aplicat en processos de gestió de seguretat, processos com el que tenim a la norma UNE ISO / IEC 27001:2013.

Per tant, tot i que podria semblar excessiu aplicar la norma ISO27001 (que és opcional per a qualsevol organització, sigui pública o privada) a les AAPP al existir l'obligatorietat de l'ENS, podem considerar que:

1. L'ENS necessita d'un SGSI per a poder gestionar el nou procés de seguretat.
2. La norma ISO27001 defineix el procés d'implantació i gestió d'un SGSI d'una manera verificada i contrastada per l'experiència de molts anys en el sector.
3. L'estàndard ISO27001:2013 proporciona una acreditació reconeguda i acceptada internacionalment de bones pràctiques en seguretat de la informació.
4. El conjunt de controls de la ISO27001 requereix (especificats a la ISO27002) son en molts casos els mateixos (o comparables) als que necessita l'ENS, de manera que es podria aprofitar el treball realitzat en el desplegament de la ISO27001 també en el desplegament de l'ENS (i a l'inrevés).
5. La certificació ISO2001:2013 és basa en l'aplicació de millora contínua PDCA o cicle de Deming, que és també un requeriment per a l'Esquema Nacional de Seguretat.

Tal i com podem veure, tant la ISO27001:2013 com l'ENS realitzen una aproximació similar als processos de seguretat de la informació: un procés sistemàtic i gestionat de seguretat que asseguri la informació i els actius més importants de l'organització. A més, com ja veurem, l'ENS necessita d'un gestor de seguretat de la informació (en les seves categories mitjana i alta), i l'estàndard ISO27001:2013 compleix amb aquest objectiu.

1.2 Objectius del Treball

Per tant, i després de l'exposat, aquest treball descriurà el pla d'implementació i adequació a l'Esquema Nacional de Seguretat (ENS), amb la implementació d'un SGSI basat en la norma ISO27001:2013 en un ajuntament. Es realitzarà aquesta adequació per tal de poder cobrir la necessitat d'un SGSI (tal i com requereix l'ENS), i farem servir la norma ISO27001:2013 per ser un estàndard de prestigi i reconegut internacionalment

Per tant aquest treball descriurà el pla d'implementació i adequació a la norma ISO27001:2013 en un ajuntament, així com de l'Esquema Nacional de Seguretat d'obligat compliment. Es realitzarà aquesta doble adequació buscant els següents objectius:

1. Implantar un SGSI basat en la norma ISO27001:2013 reconeguda internacionalment. Aquesta norma, tot i no se necessària per les AAPP, ens servirà per poder posar en marxa el SGSI que necessitarà l'ENS.

2. Adequar-nos a l'Esquema Nacional de Seguretat fent servir el treballs que es desenvolupen per a la implantació del SGSI. En aquest sentit, s'anirà revisant a cada aspecte de les implantacions les diferències que existeixen a cada model i s'aniran implementar els controls necessaris (si fos oportú, com ja veurem amb la declaració d'aplicabilitat) en cadascuna de les certificacions.

Tot i que sembla que el nou Reial Decret - Llei 12/2018 seguretat de les xarxes i sistemes d'informació afecta només a sectors crítics, la transposició de la Directiva NIS de la UE que ha realitzat l'estat Espanyol ha ampliat el seu àmbit d'aplicació i podria ser que les administracions públiques haguessin d'implementar algunes de les mesures de protecció que hi apareixen. En aquest sentit, sembla clar que la UE es recolza en els estàndards internacionals de seguretat i que, tot i que està previst el desplegament de les mesures a implementar dins del nou Esquema Nacional de Seguretat, podem

assegurar que no es tractaran de mesures que no existeixen a la sèrie ISO27000 i que, per tant, la realització de la implementació d'un SGSI basat en la ISO27001:2013 ens acostarà a un possible futur grau de compliment.

Com a objectius secundaris, podem distingir:

1. Anàlisi de les diferents metodologies que es segueixen en la ISO27001 i l'ENS.
2. Anàlisi de similituds i diferències dels dos models de seguretat.
3. Estudi de noves metodologies diferents a les proposades per tal d'implementar el projecte dins d'un termini de temps ajustat.
4. Desenvolupar una gestió documental

1.3 Enfocament i mètode seguit

L'enfocament que es seguirà en aquest treball serà un enfocament basat en fases o etapes a on s'aniran entregant resultats ben definits al final de cada etapa. Per tant, l'aproximació serà semblant a les que es realitzen en les metodologies àgils de gestió de projectes, a on es realitzaran entregues parcials però complertes en diferents fases o interaccions.

Es partirà de la situació inicial de l'ajuntament, i es compararà amb la situació objectiu que l'ENS estableix. Seguidament s'implantarà un sistema gestor documental que haurà de suportar tot el desplegament de polítiques i normatives que acompanyaran al nostre SGSI. Això inclourà la definició de la política de seguretat, així com definició de rols i responsabilitats, declaració d'aplicabilitat, entre d'altres. Es realitzarà una anàlisi i gestió de riscos fent servir la metodologia *MAGERIT v3 [*4] fent servir l'eina de suport PILAR. Com a resultat d'aquesta anàlisi, s'identificaran els possibles projectes de millora que permetin reduir el risc detectat per sota del risc acceptable de l'ajuntament i es finalitzarà amb l'execució d'una auditoria per veure el grau de compliment un cop acabat

1.4 Planificació del Treball

Aquest treball es planificarà en les següents fases:

Fase 1: Situació inicial: Contextualització, objectius i anàlisi diferencial.
Temps necessari: 8 dies Introducció al Projecte. Enfocament i selecció de l'ajuntament que serà objecte d'estudi. Definició dels objectius del Pla Director de Seguretat i Anàlisis diferencial de l'empresa amb respecte a l'ENS.

Fase 2: Sistema de Gestió Documental
Temps necessari: 12 dies Elaboració de la Política de Seguretat. Declaració de l'aplicabilitat i documentació del SGSI

Fase 3: Anàlisis de riscos
Temps necessari: 20 dies 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.

Fase 4: Proposta de projectes
Temps necessari: 15 dies 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.

Fase 5: Auditoria de Compliment de l'ENS.
Temps necessari: 7 dies Avaluació de controls, maduresa i nivell de compliment.

Fase 6: Presentació de Resultats i entrega de Informes
Temps necessari: 5 dies Consolidació dels resultats obtinguts durant el procés d'anàlisis. Realització dels informes i presentació executiva a Direcció. Entrega del projecte final.

1.5 Breu sumari de productes obtinguts

El resultat del projecte serà la política de seguretat que establirà les directrius i principis de l'ajuntament en la gestió i protecció de la seva informació i serveis, així com un conjunt de normatives (un cos normatiu) que indicarà com es realitza la protecció per a totes les mesures de seguretat que requereix l'ENS. També s'obtindrà un conjunt de projectes a implementar per tal de desenvolupar les proteccions que les diferents normatives regulen.

1.6 Breu descripció dels altres capítols de la memòria

Al capítol 2 repassarem els principis de l'Esquema Nacional de Seguretat, la seva motivació, principis i objectius. També es realitzarà un repàs de l'estàndard ISO27001:2013 i de la seva relació amb l'ENS.

Al capítol 3 es centra en la fase 1 i es realitza la descripció inicial de l'ajuntament i el seu context. S'analitza les diferents categories de sistemes que descriu l'ENS i es realitza l'anàlisi diferencial en funció de la que es determina per l'ajuntament.

El capítol 4 es centra en la fase 2 i s'estableix la gestió documental del sistema. Es defineixen la política de seguretat, defineixen rols, i es descriu el document d'aplicabilitat.

El capítol 5 es realitza l'anàlisi de riscos. Es fa l'inventari d'actius existents dins de l'abast definit en el pla director i es realitza l'anàlisi de riscos associats. S'introdueix en l'ús de l'eina PILAR com a suport a l'anàlisi de riscos.

Dins del capítol 6 podrem trobar la llista de projectes identificats, amb els seus objectius, i estimació de recursos necessaris.

Si examinem el capítol 7 trobarem una auditoria final per veure el resultat de tot el procés que ens dirà si podem o no certificar el nostre sistema dins del marc regulador de l'Esquema Nacional de Seguretat.
Finalment, al capítol 8 es dedica a la realització de l'informe final i la presentació de les conclusions d'aquest treball.

2. ENS i ISO27001:2013

2.1. Esquema Nacional de Seguretat

Com ja hem comentat anteriorment, la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als Serveis Públics [2] va ser la primera llei a nivell estatal a on es redacta un «*les administracions públiques* ***hauran de fer servi****r mitjans electrònics per desenvolupar les seves funcions»* en contraposició al «l*es administracions públiques* ***podran fer*** *servir mitjans electrònics» per desenvolupar les seves funcions* (tal i com deia l'art. 45 de l' exinta Llei 30/1992, de 26 de Règim Jurídic de les Administracions Públiques i de Procediment Administratiu Comú (*LRJAPPAC*)).

Però tal i com deia la Llei 11/2007, es necessita donar garanties a tots els participants (ciutadans, empreses i administracions) en la nova prestació de serveis telemàtics que la llei indicava. Per tal donar aquestes garanties, la Llei 11/2007 indicava que es desenvoluparien via reial decrets dos estàndards d'obligat compliment per les administracions públiques:

- Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica. l'Esquema Nacional de Seguretat
- Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.

Val a dir que, tot i que la llei 11/2007 i la llei 30/1992 han estat derogades per la nova llei 39/2015 i 40/2015, és a la mateixa llei 39/2015 a on s'indica que contínua sent necessari (i, per tant, obligatori) l'aplicació de tant de l'ENI com de l'ENS.

L'ENI (o Esquema Nacional d'Interoperabilitat) te com a objectiu fixar el format d'intercanvi d'informació entre els participants de qualsevol intercanvi dins de l'administració electrònica per tal de poder garantir el flux d'informació. Com és evident, l'estudi d'aquest estàndard queda fora de l'abast d'aquest treball.

La finalitat de l'Esquema Nacional de Seguretat (a partir d'ara ENS) és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures per garantir la seguretat dels sistemes, les dades, les comunicacions, i els serveis electrònics, que permeti als als ciutadans ia les administracions públiques, l'exercici de drets i el compliment de deures a través d'aquests mitjans. Per tant, i com ha havíem comentat en la introducció, és d'obligat compliment per a qualsevol organització dins del sector públic.

L'ENS té aplicació en tots els sistemes, dades, comunicacions i serveis electrònics que permeten exercir els drets i obligacions per part dels ciutadans, empreses i administracions. Això és un dels trets que diferencia a l'ENS de la ISO27001:2013, atès que la primera ens indica a què conjunts de sistemes s'ha

d'aplicar. En canvi, la segona, al no ser obligatòria i de caràcter més genèric no ens limita al conjunt de sistemes a aplicar (dependrà d'allò que l'interessi a l'organització certificar el seu SGSI).

L'ENS s'articula en base a uns principis que hauran de regir tot el seu desplegament:

- **Seguretat integral:** La gestió de la seguretat ha de ser un procés integral a on es considerin els elements tècnics, humans, materials i organitzatius. No es poden realitzar accions puntuals, sinó que tot ha de formar part d'un procés global de seguretat. Té especial rellevància la formació del personal per prendre consciència de que la seguretat és un procés que afecta a tot, a tots, i és un procés més de l'administració.

- **Gestió de riscos:** Per tal de protegir a l'organització, hem conèixer què volem protegir (allò que és valuós per l'organització en la consecució dels seus objectius), i de què (els riscos als que poden estar sotmesos). Per tal de poder complir aquestes tasques, es necessitarà una ***anàlisi de riscos*** (que detectarà les amenaces que poden malmetre els nostres actius), ***i la gestió d'aquests riscos*** (el procés en que gestionarem aquestes amenaces per tal reduir els riscos dins d'un nivell acceptable). Típicament podrem gestionar el riscos aplicant contramesures per tal de mitigar o baixar el risc fins a un nivell acceptable, eliminar l'amenaça (prescindint del servei, per exemple) o transferir-lo a un tercer (externalització del servei, contractant pòlisses d'assegurances, etc).

  Per tal de poder fer-ho, ENS aconsella fer servir la metodologia *MAGERIT* [4] (formada per tres llibres principalment), juntament amb l'eina *PILAR* [5] que ens servirà per la realització d'aquesta gestió de riscos.

- **Prevenció, reacció i recuperació:** D'aquesta manera podem classificar les mesures de seguretat que podem aplicar i que l'ENS ens ofereix dins del seu catàleg. Tindrem algunes que podran prevenir la materialització d'una amenaça (control d'accés, per exemple), d'altres que ens permetran reaccionar (antivirus, per exemple) o recuperar-nos (còpies de seguretat de la informació).

- **Línies de defensa**: S'aplica el concepte de tenir diferents capes de defensa per tal de poder protegir el sistema. Així combinarem diferents mesures (organitzatives, físiques i tècniques) en la consecució del mateix objectiu. Per exemple, tindrem una normativa que indicarà clarament la prohibició d'accés a personal no autoritzat, locals tancats a personal no autoritzat, així com usuaris i contrasenyes només per al personal autoritzat.

- **Reavaluació periòdica**: Aquest és, potser, el factor més determinant. La seguretat de la informació s'ha d'estar avaluant periòdicament, i no s'ha de considerar com una acció puntual. Ha de formar part de l'organització

com un procés bàsic de la mateixa i, com a tal, ha de ser un procés susceptible de millora contínua. En aquest sentit és a on podem abraçar el procés que ens presenta el model ISO27001:2013, un procés que s'emmarca dins del model PDCA.

Tot i que podríem entrar en detall en la concepció que es va seguir en la concepció de l'ENS, ens limitarem només a explicar que en tot el procés de la implantació de l'ENS hi ha un actor que juga un paper fonamental en l'acompanyament i assessorament per a totes les administracions públiques. Ens referim al CNI (Centre Nacional d'Intel·ligència) i, concretament, al CCN (Centre criptològic Nacional, depenent del CNI). I és que, tal i com diu el mateix art 29.1, RD 3/2010, «*Per al millor compliment del que estableix l'Esquema Nacional de Seguretat, el Centre Criptològic Nacional, en l'exercici de les seves competències, elaborarà i difondrà les corresponents guies de seguretat de les tecnologies de la informació i les comunicacions.*». Això a la pràctica consisteix que el CCN s'encarrega de la publicació d'un conjunt de documents, guies i instruccions tècniques de suport a la implantació de l'ENS per part de les AAPP. És important tenir present aquest fet atès que, com no pot ser d'altra manera, es faran servir aquestes guies en la implementació de l'ENS dins d'aquest TFM. De fet, tota la sèrie de documents CCN-STIC-800 [6] es troba dedicada a l'Esquema Nacional de Seguretat.

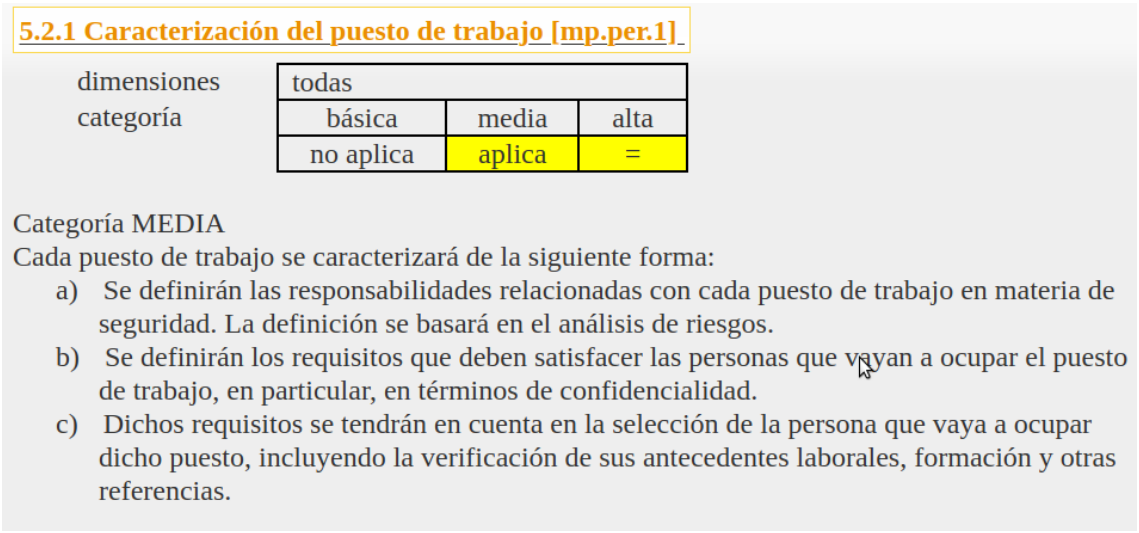
En definitiva, i tal com s'indiquen en la introducció de tots els documents de la sèrie CNN-STIC-800, la sèrie de documents CCN-STIC s'elabora per a complir les la feina encarregada al Centre Criptològic Nacional (tal i com ho reflecteix l'Esquema Nacional de Seguretat), establiment un marc de referència en aquesta matèria que serveixi de suport perquè el personal de la Administració dugui a terme la seva difícil, i de vegades, ingrata tasca de proporcionar seguretat als sistemes de les TIC sota la seva responsabilitat. Aquesta darrera afirmació (la ingrata tasca de proporcionar seguretat als sistemes TIC) té un significat molt rellevant atès que l'administració pública (i el personal que hi treballa) mai han tingut una tradició de treball segur en termes de seguretat TIC i, per tant, resultarà imprescindible el recolzament de l'alta direcció, així com la formació i conscienciació en termes de seguretat a tot el personal (recordem, es tracta d'un procés integral, que ha d'afectar a tota l'organització i no només un conjunt de mesures tècniques a implementar).

2.1.2 ENS: Categoria dels sistemes i mesures de seguretat

Un cop hem presentat què és l'ENS i en quins principis es fonamenta, haurem de parlar de l'aproximació que hem de seguir en la seva aplicació. Dins de l'annex II del RD 3/2010 podem trobar el conjunt de mesures que haurem d'aplicar al nostre sistema per tal de poder acreditar el nostre compliment. Si revisem l'annex II, podem observar que el conjunt de mesures es troben organitzades en tres grans grups.

Figura 1: Mesures de seguretat recollides a l'ENS

Analitzant qualsevol de les mesures, ens podem trobar que existeixen 3 columnes per a cada mesura amb el noms de BAIXA, MITJANA i ALTA.



5.2.1 Caracterización del puesto de trabajo [mp.per.1]

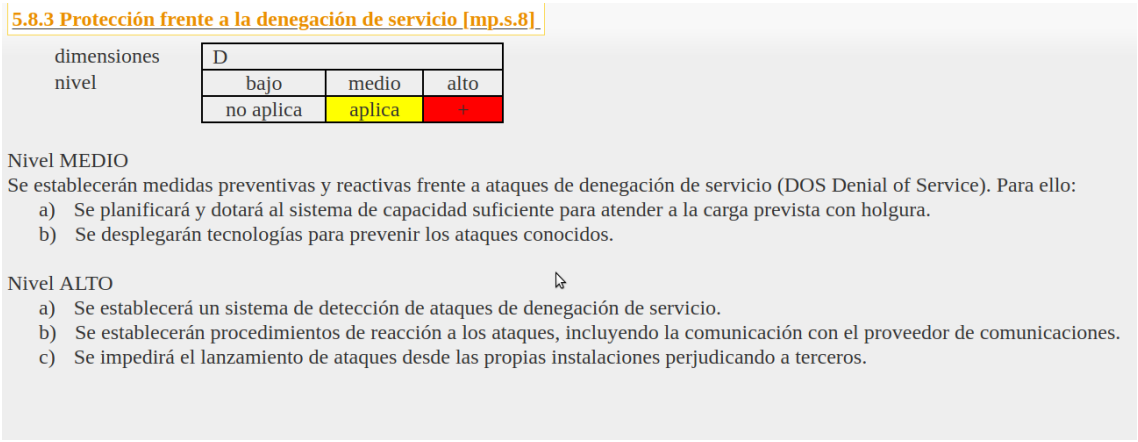
dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA
Cada puesto de trabajo se caracterizará de la siguiente forma:

a) Se definirán las responsabilidades relacionadas con cada puesto de trabajo en materia de seguridad. La definición se basará en el análisis de riesgos.
b) Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad.
c) Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar dicho puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias.

Figura 2: Exemple de control mp.per.11

(font: https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1128)



5.8.3 Protección frente a la denegación de servicio [mp.s.8]

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	+

Nivel MEDIO
Se establecerán medidas preventivas y reactivas frente a ataques de denegación de servicio (DOS Denial of Service). Para ello:
a) Se planificará y dotará al sistema de capacidad suficiente para atender a la carga prevista con holgura.
b) Se desplegarán tecnologías para prevenir los ataques conocidos.

Nivel ALTO
a) Se establecerá un sistema de detección de ataques de denegación de servicio.
b) Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.
c) Se impedirá el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

Figura 3: Exemple de control mp.s.8

(font: https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1164)

El concepte de categoria, tal i com descriu l'art 43, «***modularà l'equilibri entre la importància de la informació que gestiona, els serveis que presta i l'esforç de seguretat requerit, en funció dels riscos a què està exposat, sota el criteri del principi de proporcionalitat»*.** És per tant una manera de no sobreprotegir un actiu que no tingui un gran impacte la materialització d'una amenaça, o no protegir adequadament un actiu que sí que és veritablement important.

Per a poder categoritzar el nostre sistema, s'haurà d'aplicar els criteris que s'indiquen a la guia *CNN-STIC803- ENS Valoració de sistemes.* En aquesta guia, bàsicament, es plasma d'una manera més extensa el contingut de l'annex I del RD 3/2010 a on es descriu el procediment a seguir.

Per a cada servei i informació s'haurà de valorar quina importància té en funció dels següents criteris de seguretat:

- Disponibilitat [D]. Aquesta criteri indica que l'actiu es troba disponible quan es necessari. Per tant, per poder valorar-lo, haurem de respondre a la pregunta de «què passa si l'actiu no es troba disponible quan és necessari» ?.
- Integritat [I]: L'actiu no ha estat alterat de manera no autoritzada. Llavors, ens haurem de preguntar «quina importància té que l'actiu hagi estat alterat de manera no autoritzada» ?.
- Confidencialitat[C]: La informació no es posa a disposició, ni és coneguda per part de persones o processos no autoritzats. Haurem de respondre a «quines conseqüències té que l'informació hagi estat coneguda per algú no autoritzat ?».
- Traçabilitat [T]: Aquesta qualitat indica que es pot conèixer qui o què, i quan s'ha fet una determinada acció. Per tant, «quina importància tindria no poder identificar qui o què ha executat una acció?».
- Autenticitat [A]: És la propietat que ens garanteix que algú és qui diu què és, o que podem garantir d'on provenen unes dades. Per tant, «quina

importància tindria que el remitent o destinatari d'un actiu no fos qui diu què és?».

A més a més, el Reglament (EU) 2016/679 (conegut com RGPD) també obliga a realitzar un anàlisis dels tractaments que es realitzin per tal de poder escollir de manera proporcionada el conjunt de mesures que els protegeixin.

Específicament, la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, que és la transposició al cos normatiu de l'Estat Espanyol del RGPD, indica a la seva disposició primera que *«L'Esquema Nacional de Seguretat inclourà les mesures que s'hagin d'implantar en cas de tractament de dades personals per evitar la seva pèrdua, alteració o accés no autoritzat, adaptant els criteris de determinació de el risc en el tractament de les dades al que estableix l'article 32 de l' Reglament (UE) 2016/679».*

Per tant, i tenint en compte que qualsevol Ajuntament realitza tractament amb dades de caràcter personal, sembla evident que es necessitarà poder inventariar els nostres actius i categoritzar-los de l'Ajuntament *MISTIC* per tal de donar resposta al detall del conjunt de controls que l'ENS ens obliga a implementar, ja sigui per l'aplicació de la 39/2015, com per la *LOPD-GDD*.

CATEGORITZACIÓ DE SISTEMES

Per donar una visió global de l'impacte que ha tingut l'ENS, i del treball que comporta la seva adequació, exposarem els criteris que s'han de seguir per poder categoritzar un actiu.

Com ja hem vist abans, haurem de categoritzar cada dimensió de l'actiu, de manera que tindrem que per un actiu determinat, tindrem categoritzades com BAIX,MITJÀ o ALT cadascuna de les seves dimensions. Un cop que tenim categoritzades cadascuna de les dimensions, obtindrem la categoria resultant de l'actiu com la categoria més alta de totes les dimensions de seguretat de l'actiu. És a dir, que si un actiu «servidor 1» té com a resultat aquesta categorització:

	D	**I**	**C**	**T**	**A**
servidor01	M	B	M	M	B

Taula 1: Exemple de categorització d'un servidor

El nostre actiu *servidor1* serà categoritzat com 'M', i s'hauran d'aplicar el conjunt de mesures de tipus mitja presents a l'annex II del RD 3/2010.

A més a més, la categoria més alta d'un actiu marcarà la categoria del nostre sistema d'informació i, per tant, el nivell del conjunt de mesures que s'haurà

d'aplicar al conjunt d'actius presents en el nostre sistema d'informació. Això vol dir, en l'exemple que estem descrivint, que el fet de tenir l'actiu *servidor01* categoritzat com a 'M' implicarà que tot el nostre sistema sigui categoritzat com 'M'.

Per no estendre més aquest apartat, inclourem algunes taules amb els criteris que s'han de seguir per determinar la categoria per a cada dimensió de seguretat i actiu.

CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE INFORMACIÓN Y SERVICIOS					
		No Adscrito (N/A)	**BAJO**	**MEDIO**	**ALTO**
Disposición legal o administrativa		COM.DIS.N No existe ninguna disposición legal que condicione su nivel.	COM.DIS.B Por disposición legal o administrativa: ley, decreto, orden, reglamento...	COM.DIS.M Por disposición legal o administrativa: ley, decreto, orden, reglamento...	COM.DIS.A Por disposición legal o administrativa: ley, decreto, orden, reglamento...
Perjuicio Directo al ciudadano		COM.PER.N No supone ningún perjuicio directo al ciudadano	COM.PER.B Algún perjuicio al ciudadano	COM.PER.M Daño importante, aunque subsanable al ciudadano	COM.PER.A Grave daño, de difícil o imposible reparación al ciudadano
Incumplimiento de una Norma	**Legal**	COM.LEG.N No implica incumplimiento de una norma jurídica	COM.LEG.B Incumplimiento formal leve de una norma jurídica, de carácter subsanable	COM.LEG.M Incumplimiento material de una norma jurídica, o incumplimiento formal no subsanable	COM.LEG.A Incumplimiento grave de una norma jurídica
	Regulatoria	COM.REG.N No implica incumplimiento de normativa de un regulador	COM.REG.B Implica incumplimiento de normativa de un regulador	COM.REG.M Implica sanción significativa de un regulador	COM.REG.A Implica sanción grave de un regulador y/o pérdida de licencia de operar
	Contractual	COM.CON.N No implica incumplimiento de una obligación contractual	COM.CON.B Incumplimiento leve de una obligación contractual	COM.CON.M Incumplimiento material o formal de una obligación contractual	COM.CON.A Incumplimiento grave de una obligación contractual
	Interna	COM.INT.N No implica incumplimiento de normativa interna	COM.INT.B Incumplimiento leve de una norma interna	COM.INT.M Incumplimiento material o formal de una norma interna	COM.INT.A Incumplimiento grave de una norma interna

Taula 2: Criteris per establir categories de serveis i informació (1/2)

CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE INFORMACIÓN Y SERVICIOS				
	No Adscrito (N/A)	**BAJO**	**MEDIO**	**ALTO**
Pérdidas económicas	COM.ECO.N No implica pérdidas económicas	COM.ECO.B Pérdidas económicas apreciables (inferior a un 4% del presupuesto anual de la organización)	COM.ECO.M Pérdidas económicas importantes (igual o superior a un 4% e inferior a un 10% del presupuesto anual de la organización)	COM.ECO.A Pérdidas económicas o alteraciones financieras significativas (igual o superior a un 10% del presupuesto anual de la organización)
Reputación	COM.REP.N No implica daño reputacional	COM.REP.B Daño reputacional apreciable con los ciudadanos o con otras organizaciones	COM.REP.M Daño reputacional importante con los ciudadanos o con otras organizaciones	COM.REP.A Daño reputacional grave con los ciudadanos o con otras organizaciones
Protestas	COM.PRO.N No se prevé que pueda desembocar en protestas.	COM.PRO.B Múltiples protestas individuales.	COM.PRO.M Protestas públicas (alteración del orden público)	COM.PRO.A Protestas masivas (alteración seria del orden público)
Delitos	COM.DEL.N No facilitaría la comisión de delitos ni dificultaría su investigación.	COM.DEL.B Favorecería la comisión de delitos	COM.DEL.M Favorecería significativamente la comisión de delitos o dificultaría su investigación.	COM.DEL.A Incitaría a la comisión de delitos, constituiría en sí un delito, o dificultaría enormemente su investigación.

Taula 3: Criteris per establir categories de serveis i informació (2/2)

CRITERIOS PARA TIPOS DE INFORMACIÓN CON DATOS PERSONALES EN FUNCIÓN DEL TIPO		
BAJO	**MEDIO**	**ALTO**
PRI.TIP.B Datos de carácter personal con carácter general.	PRI.TIP.M Incluye datos de carácter personal: a) Relativos a la comisión de infracciones administrativas. b) Aquellos cuyo funcionamiento se rija por el artículo 29 de L.O. 15/1999, de 13 de diciembre. c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias. d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros. e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social. f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos. Datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y libertades fundamentales, incluidos: • Origen étnico o racial (RGPD, art. 9). • Opiniones políticas (RGPD, art. 9). • Convicciones religiosas o filosóficas (RGPD, art. 9). • Afiliación sindical (RGPD, art. 9). • Datos genéticos (RGPD, art. 9). • Datos biométricos dirigidos a identificar de manera unívoca a una persona física (RGPD, art. 9). • Datos relativos a salud (RGPD, art. 9). • Datos relativos a la vida sexual u orientaciones sexuales (RGPD, art. 9). • Condenas e infracciones penales (RGPD, art. 10).	

Taula 4: Criteris per establir categories d'informació amb dades de caràcter personal

CRITERIOS PARA TIPOS DE INFORMACIÓN CON DATOS PERSONALES EN FUNCIÓN DEL TRATAMIENTO				
	N/A	BAJO	MEDIO	ALTO
Cantidad considerable de datos personales			PRI.CAN.M Operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala (RGPD, 91)	
Importante riesgo para los derechos y libertades de los interesados			PRI.DER.M Operación de tratamiento que entraña un alto riesgo para los derechos y libertades de los interesados, en particular cuando esta operación hace más difícil para los interesados el ejercicio de sus derechos (RGPD, 91)	
Evaluación sistemática y exhaustiva de aspectos personales			PRI.ASP.M Operación de tratamiento para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas (RGPD, 91)	
Control de zonas de acceso público a gran escala			PRI.ACC.M Operaciones de control de zonas de acceso público a gran escala, en particular cuando se utilicen dispositivos optoelectrónicos (RGPD, 91)	

Taula 5: Criteris per establir categories d'informació amb dades de caràcter personal en funció del tractament

2.2 ISO2001:2013

L'ISO 27001 és una norma internacional de Seguretat de la Informació que pretén assegurar la confidencialitat, integritat i disponibilitat de la informació d'una organització i dels sistemes i aplicacions que la tracten. Aquest estàndard ha estat desenvolupat per l'Organització Internacional de Normalització (ISO: "*International Organization for Standardization*") i per la Comissió Electrotècnica Internacional (IEC: "*International Electrotechnical Commission*").

La norma defineix de manera genèrica, independentment del tipus d'organització com es planifica, implanta, verifica i controla un Sistema de Gestió de Seguretat de la Informació, a partir de la realització d'una anàlisi de riscos i de la planificació i implantació de la resposta als mateixos per a la seva mitigació. És a dir, qualsevol empresa o organització pot desplegar un SGSI seguint aquest estàndard. La norma ISO27001 especifica com s'hauria d'abordar tots els aspectes de l'estructura organitzativa, les polítiques i la planificació de les activitats, responsabilitats, pràctiques, procediments, processos i recursos que han de permetre la gestió del procés de seguretat de la informació.

Finalment, la norma ISO27001 és una norma certificable que permet que un auditor extern i independent pugui certificar que una determinada organització disposa d'un procés de gestió de la seguretat de la informació dins de la seva organització, i que aquest procés és conegut i reconegut a nivell internacional per seguir unes bones pràctiques en el disseny i gestió.

2.2.1 Família ISO27000. Norma ISO 27002

La norma ISO27001 (que és la norma certificable), pertany de fet a una família de normes conegudes com la família ISO27000. Farem una petita descripció de cadascuna d'elles [7].

- 27000. Defineix conceptes i vocabulari que surten en els diferents estàndards de la sèrie de normes ISO 27000.

- 27001. Conté les especificacions per a implantar un sistema de gestió de la seguretat de la informació. Té l'origen en la BS 7799-2:2002, a la qual substitueix. És la norma certificable.

- 27002. És el codi de bones pràctiques per a la gestió de la seguretat de la informació. Té l'origen en la BS 7799 (part 1) i l'ISO-IEC 17799.

- 27003. És una guia d'implementació dels SGSI, de l'ús del model PDCA i dels requisits de les diferents fases d'aquest model. Té l'origen en l'annex B de la norma BS 7799:2 i en la sèrie de documents publicats per BSI al llarg dels anys amb recomanacions i guies d'implantació.

- 27004. Especificació de les mètriques i tècniques de mesura aplicables per a determinar l'eficàcia d'un SGSI i dels controls que hi estan relacionats. Aquestes mètriques s'usen fonamentalment per a mesurar els components de la fase do del cicle PDCA.

- 27005. Estableix les directrius per a gestionar el risc en matèria de seguretat de la informació. Dóna suport als conceptes generals especificats en la norma ISO-IEC 27001 i s'ha dissenyat per a ajudar a aplicar satisfactòriament la seguretat de la informació basada en un enfocament de gestió de riscos. La publicació d'aquesta norma revisa i retira les normes ISO-IEC TR 13335-3:1998 i ISO-IEC TR 13335-4:2000.

- 27006. Especifica els requisits i proporciona una guia per a acreditar entitats d'auditoria i certificació de sistemes de gestió de seguretat de la informació.

- 27007. Representa una guia d'auditoria d'un SGSI.

- 27017. Representa un codi de bones pràctiques, similar a la ISO 27002 però amb mesures de seguretat de la informació específiques enfocades a la provisió i l'ús de serveis cloud.

- 27018. Representa un codi de bones pràctiques, similar a la ISO 27002 i ISO 27017, però amb mesures de seguretat específiques enfocades a la protecció d'informació personal en entorns cloud.

- 27032. Representa un codi de bones pràctiques, similar a la ISO 27002 però amb mesures de seguretat específiques enfocades a la ciberseguretat.

Com podem comprovar, la família 27000 contempla en els seus diferents documents els diferents aspectes necessaris per gestionar un SGSI, però per al nostre treball TFM ens fixarem en una norma especialment: la ISO27002.

Norma ISO 27002

La norma ISO 27002, codi de bones pràctiques per a gestionar la seguretat de la informació, és un estàndard de seguretat de la informació a tot el món i proporciona informació dels controls de seguretat per protegir la informació i la tecnologia de la informació. Els procediments per implementar realment els controls de seguretat corresponen a l'organització i variarà segons l'entorn físic i tècnic. Així, la norma ISO27002 recollirà un seguit de controls classificats en diferents dominis d'aplicació, que han d'assegurar la implantació d'un SGSI que ens permeti gestionar la seguretat mitjançant mesures organitzatives (definició de polítiques, normatives, etc ...) i tècniques.

2.3. Diferències i similituds ISO2001:2013 i Esquema Nacional de Seguretat. Combinació de ENS-ISO27001.

Tot i que totes dues normes s'ocupen d'assegurar la seguretat de la informació, es poden trobar les següents diferències [8][9][10]:

Concepte	ISO/IEC 27000	ENS
Tipus de norma	**Norma voluntària** (només s'exigeix per organitzacions que operen en alguns àmbits: exemple: sistemes d'informació dels organismes pagadors i de coordinació dels fons europeus agrícoles han d'estar certificats de conformitat amb la norma ISO / IEC 27001.	Norma **obligatòria** per totes les AAPP
Abast	Cada organització pot escollir l'àmbit d'aplicació del SGSI	Obligatori tots els sistemes que prestin serveis a ciutadania(exemple: RRHH no seria d'aplicació, tot i que el podríem aplicar-ho també).
Categorització	No hi han categories.	Depenent de l'impacte de les amenaces sobre les dimensions dels actius es classifiquen en BAIX, MITJÀ i ALT.
Controls	Norma ISO27002 defineix un major número de controls a aplicar: 114 controls => El resultat serà el document d'aplicabilitat	Depenent de la categoria, s'aplicaran un conjunt de mesures de seguretat a l' Annex II: 75.
Modulació aplicació mesures	Sota criteri de l'auditor.	Regulat en funció dels tipus d'actius i els nivells de seguretat requerits-
Aproximació gestió de riscos	La norma ISO27001:2013 segueix una aproximació a riscos.	L'ENS es basa en la gestió de riscos, encara que només és obligatori en sistemes de categoria MITJA i ALTA.
Auditories	Exigeix la realització d'auditories periòdiques	Exigeix auditoria bianual en sistemes categoria MITJA i ALTA

Taula 6: Comparativa normes ISO27001 vs ENS

Si ens fixem en les diferències observades a la taula anterior podem concloure que els dos sistemes no son tan diferents i que, de fet, podríem aprofitar la implantació del model obligat per l'ENS per poder també assolir la certificació de la nostre organització amb la norma ISO27001.

De fet, aquesta idea queda lluny de ser una quimera i ja han començat a redactar-se documents, articles, etc. en aquesta línia de pensament. De fet, i com no podria ser d'altre manera, fins i tot podríem aplicar el treball desenvolupat en l'aplicació de l'ENS per poder realitzar part de l'adequació necessària al RGPD, sobretot en la seva avaluació de riscos necessària en les Avaluació d'Impacte en els tractament de dades personals (tot i que no existeix una translació directa i que serà necessària l'ampliació de l' Annex II de l'ENS per tal de poder fer servir la mateixa norma).

Però si ens fixem en la comunió ISO27001-ENS, podem citar dues guies que ens han d'orientar en la consecució del doble objectiu de certificació ENS i ISO27001.

- *CCN-STIC 825 - ESQUEMA NACIONAL DE SEGURIDAD CERTIFICACIONES 27001 [8]*
- *CCN-STIC-852 - Aplicación del ENS en organismos pagadores [11]*

La guia CCN-STIC 825 està dedicada a analitzar si amb una certificació ISO27001 podem arribar a estar certificats amb ENS. Realitza una revisió de cada mesura de l'ENS i la compara amb cada control de la ISO27002, afegint comentaris sobre la necessitat d'adaptar el control implementat per tal de poder complir amb la mesura de l'Annex II de l'ENS.

Per un altre banda, la guia CCN-STIC-852 es situa en l'altre banda. Tot i que la guia sembla que sigui només d'aplicació al organismes pagadors, ens serveix atès que aquest tipus d'organismes estan obligats per la UE a tenir la certificació ISO27001. En aquest cas, si tenim en compte que poden haver-hi organismes pagadors públics que estan obligats a complir amb l'ENS, la guia es pregunta quines mesures i controls addicionals a l'ENS hauria de complir per assolir la certificació ISO27001.

Serà en aquesta segona línia a on centrarem el nostre treball per tal de poder intentar que podem començar a desplegar els esforços per tal que la nostre organització d'estudi pugui assolir les certificacions ENS i ISO27001.

Com ja veurem, tot i que podem aprofitar els resultats dels treballs que es desenvolupen, en ocasions haurem de duplicar o «transformar» algun dels documents necessaris a les certificacions. Ens estem referint sobretot al document de aplicabilitat, atès que aquest document es refereix als controls i mesures que l'organització considera que s'han d'aplicar i, com ja hem vist, son diferents per les dues normes.

Per acabar aquest apartat, es mostrarà molt breument unes taules extretes del document *CCN-STIC-852 - Aplicación del ENS en organismos pagadores* que indica quin és l'esforç addicional de les mesures implantades en l'ENS per tal de que tinguin equivalència amb ISO27001.

Nivel	Comentario
0	Cubierto. Los requisitos contemplados en el cuerpo normativo de ISO/IEC 27001 se cubren en el ENS
1	Parcialmente cubierto. Los requisitos contemplados en el cuerpo normativo de ISO/IEC 27001 se cubren de forma parcial en el ENS. Deberá realizarse un esfuerzo adicional de implantación de alguna medida adicional para cumplir con el requisito correspondiente.
2	No cubierto. Los aspectos contemplados en el cuerpo normativo ISO/IEC 27001 no se cubren en los artículos ni en las medidas de seguridad del Anexo II del ENS. Deberán implantarse todas las medidas adicionales necesarias para cumplir con el requisito correspondiente.

Taula 7: Nivell de cobertura ENS amb ISO27001:2013

Cláusula	Requisito ISO/IEC 27001	Artículo / Medida ENS	Esfuerzo
4	**Contexto de la organización**		
4.1	Compresión de la organización y su contexto	Artículo 43 Anexo I	1
4.2	Necesidades y expectativas de las partes interesadas	Artículo 43 Anexo I	1

Cláusula	Requisito ISO/IEC 27001	Artículo / Medida ENS	Esfuerzo
4.3	Alcance	Ley 40/2015 Artículo 1 Artículo 3	0
4.4	Sistema de gestión de seguridad de la información (SGSI)	Artícul o5 [org.1] [org.2] [org.3] [op.pl.2]	1

		Anexo III	
5	**Liderazgo**		
5.1	Liderazgo y compromiso	Artículo 12	0
5.2	Política	Artículo 10 Artículo 11 Artículo 12 [org.1]	0
5.3	Roles, responsabilidades y autoridades	Artículo 10 [org.1]	0
6	**Planificación**		
6.1	Procesos de apreciación y tratamiento de riesgos de seguridad de la información	Artículo 6 Artículo 7 Artículo 13 [op.pl.1]	1
	Declaración de Aplicabilidad	Artículo 27 Anexo II	0
6.2	Objetivos de seguridad de la información	Artículo 4 [org.1]	1
7	**Soporte**		
7.1	Recursos	[op.pl.2] [op.mon.2]	1
7.2	Competencia	Artículo 14 Artículo 15 [mp.per.4]	1
7.3	Concienciación	Artículo 5 [mp.per.3]	0
7.4	Comunicación	Artículo 24 [op.exp.7]	1
7.5	Información documentada	[org.1] [org.2] [org.3] [op.pl.2]	1
8	Operación		

Cláusula	Requisito ISO/IEC 27001	Artículo / Medida ENS	Esfuerzo
8.1	Planificación y control operacional	Artículo 5 Artículo 7 Artículo 40	0
8.2	Resultados de las apreciaciones de riesgos	Artículo 13 [op.pl.1]	0
8.3	Resultados del tratamiento de riesgos	Artículo 13	1
9	**Evaluación del desempeño**		

9.1	Seguimiento, medición, análisis y evaluación	Artículo 9 Artículo 20 [op.mon.2]	0
9.2	Auditoría interna	Artículo 34 Anexo III	1
9.3	Revisiones por la dirección	Anexo III	1
10	**Mejora**		
10.1	No conformidad y acciones correctivas	Artículo 7 Artículo 34 Anexo III	1
10.2	Mejora continua	Artículo 24 Artículo26	0

Taula 2.8: Esforç a dedicar en assolir cobertura ENS-ISO27001

3. FASE 1: Context de l'organització, objectius i anàlisi diferencial.

3.1 Context de l'organització

L'organització amb la que es basarà aquest treball es un Ajuntament d'una mida mitjana que presta un conjunt de serveis cap a la ciutadania que vol assegurar. L'ajuntament és conscient de que els serveis que presta son importants per la ciutadania, i que el resultat de la seva prestació repercuteix en el benestar de la ciutadania. Aquest Ajuntament manifesta la voluntat que té de prestar aquests serveis amb les màximes garanties en termes de seguretat de la informació i és per això que enceta un projecte d'implantació d'un SGSI. També, i no podem oblidar, vol assegurar el compliment del marc regulatiu i lleis a que està sotmès com Administració Pública, i coneix i reconeix que el compliment de l'ENS és obligació legal.

L'organització que analitzem es defineix amb els següents paràmetres:

MISSIÓ

La missió de l'Ajuntament és servir i treballar per a construir una comunitat basada en el bé comú, i en el desenvolupament de les persones que viuen i treballen al municipi.

VISIÓ

Tenim una visió de servei públic que ens obliga a la millora contínua de serveis i polítiques que oferim a la ciutadania. Volem generar oportunitats de futur i de progrés social, econòmic i que la ciutadania se senti orgullosa de viure al nostre municipi.

VALORS

- La sinceritat, confiança i dedicació plena que dicta les actuacions del tot el personal de l'Ajuntament.
- La responsabilitat, eficàcia i eficiència en l'administració dels recursos públics.
- Governança basada en les persones i destinades a les persones.
- Cohesió, civisme i convivència

Per tal de poder contextualitzar més el cas d'estudi, podem analitzar el context a nivell de municipi i de recursos disponibles

TERRITORI

En la realització d'aquest treball hem escollit l'Ajuntament MISTIC que disposa d'una població de 40.000 habitants, en una superfície de 8 km^2. És un ajuntament que per la seva mida en termes de població es considera prou gran i madur com per no ser beneficiari dels ajuts que proporciona la Diputació, així que haurà de contar amb els seus recursos propis per dur a terme el projecte.

A més, aquest municipi es troba envoltat d'altres que li dupliquen o tripliquen la població, ocasionant una pressió en la demanda de serveis del municipi que estudiem al sentir-se obligat a prestar els mateixos serveis que municipis més grans i amb més recursos de l'entorn.

PRESSUPOST

Aquest ajuntament disposa d'un pressupost anual de 40.000.000 €, tot i que només es destina 200.000 € al departament TIC de l'ajuntament. Això, sens dubte, podrà condicionar el ritme de desenvolupament de les diferents fases del pla director, així com el desplegament dels possibles projectes que se'n derivin.

OFICINES MUNICIPALS

L'ajuntament disposa de les següents oficines municipals:

- Edifici E00: És l'edifici principal. Es troba a a la plaça de la Vila i és on treballen la majoria dels treballadors municipals. Aquí podrem trobar treballadors, la direcció política (alcalde, regidors) i tècnica dels diferents departaments (caps de departament, servei, etc.). A l'edifici principal trobarem la única Oficina Atenció al Ciutadà a on es poden realitzar tràmits i gestions presencials.

- Edifici E01: Edifici on es troben un part dels treballador de serveis socials.

- Edifici E02: Edifici on es troben un altre part dels treballador de serveis socials.

- Edifici E03: Edifici on es troben les oficines de la brigada municipal.

- Edifici E04: Edifici on es troba la policia local.

- Edifici E05: Edifici on es troba una part important dels treballadors del departament de promoció econòmica.

A banda d'això, podrem trobar diferents equipaments culturals (casals, poliesportius) disseminats per tot el municipi.

INFRAESTRUCTURA TIC

Si ens fixem una mica més en detall en la infraestructura TIC de que disposa l'Ajuntament podem trobar:

Programari

- **Ofimàtica:** Els ordinadors personals tenen Windows 10 com a sistema operatiu, i l'eina Microsoft Office 2019 com a eina ofimàtica. També disposen de diferents navegadors d'internet.

- **ERP municipal:** A nivell global es fa servir un ERP proporcionat per una empresa que s'executa en un servidor d'aplicacions JBOSS, Aquest ERP proporciona:

  - Padró d'habitants
  - Gestió de tributs/recaptació.
  - Comptabilitat
  - Registre electrònic

- **Administració electrònica:** Podem trobar un conjunt d'aplicacions desplegades en diferents servidors TOMCAT's i que implementen la part més operativa de l'Administració Electrònica. Aquí ens podem trobar:

  - Portal de seu electrònica (amb carpeta ciutadana inclosa)
  - Gestor d'expedients (amb signatura electrònica)

- **Programari d'infraestructura:** Amb aquest nom ens referim al programari que sustenta la infraestructura de les operacions de l'Ajuntament. Per tant, estem parlant del programari que autentica usuaris en els inicis de sessió (Windows amb Active Directory), servidors de fitxers (programari SAMBA), correu electrònic (postfix), servidor DNS, etc .

CPD

Aquest ajuntament disposa de tots els seus sistemes TIC en un CPD situat a la segona planta del edifici principal E00, situat a la plaça de la Vila. Aquest conté els servidors Linux i Windows

que donen servei a l'ajuntament de MISTIC . Disposa de SAI i accés per porta amb clau, finestres de vidre i sistemes de refrigeració amb aire condicionat.

Maquinari

Podem trobar-nos diferent tipus de maquinari:

- **Ordinadors personals**

  L'Ajuntament disposa d'un conjunt de 200 ordinadors personals amb Microsoft Windows 10 i Microsoft Office.

- **Impressores**

  L'Ajuntament disposa de 15 equips multifunció amb capacitats d'impressió A3,A4, escàner, etc.

- **Servidors**

  L'Ajuntament disposa de 4 servidors HP amb programari de virtualització. Tots els serveis que es presten es fa mitjançant tècniques de virtualització

- **Màquines virtuals**

  L'Ajuntament desplega tots els seus serveis TIC mitjançant la virtualització en diferents màquines virtuals (un total de 20 VM). Totes les màquines virtuals es troben desplegades entre els 4 servidors físics anteriors. Aquestes màquines implementen servidors Windows, servidors de fitxers Linux, TOMCAT, JBOSS, Oracle, etc .. que proporcionen els serveis del pogramari ERP, i la resta de serveis com gestor d'expedients, seu electrònica, etc ..

  Finalment fer notar que també proporcionen els serveis de còpies de seguretat, usuaris, compartició de carpetes, servidors DHCP, etc ..

- **Sistema d'emmagatzematge**

  L'Ajuntament disposa de dos cabines redundants de discos SATA per suportat tota la infraestructura de discos. Es troben configurades en RAID6.

- **Xarxa**

    - Tots els ordinadors i servidors es troben connectats a una xarxa LAN.
    - Tots els edificis municipals es troben connectats amb FO pròpia.
    - Aquesta xarxa de FO es concentra a l'edifici principal E00. En aquest edifici tindrem centralitzat tot l'accés a Internet de la resta d'edificis. L'ajuntament disposa de 2 tallafocs i diferents encaminadors. La connectivitat a Internet la proporciona VODAFONE amb una connexió de FO de 100Mbps.

Personal

Distingirem entre 5 col·lectius, atesa la funció diferenciada que tenen:

- Personal d'oficis: Personal bàsicament de la Brigada Municipal (fusters, electricista, etc ..). No fan servir mitjans electrònics. Aproximadament 10 persones.

- Policia Local: Bàsicament agents i caporals. Alguns d'ells fan servir eines ofimàtiques en la redacció d'atestats i connexió a Internet. Aproximadament 70 persones, distribuïdes en 3 torns.

- Funcionaris tramitadors de l'OAC: Unes 12 persones que es dediquen a l'atenció presencial en la única Oficina d'Atenció de que es disposa. La seva atenció consisteix en el registre de la sol·licitud i l'inici de l'expedient administratiu amb el ciutadà present físicament.

- Funcionaris: Agruparem aquí a la resta de funcionaris de l'organització. Son funcionaris que pertànyen a altres departaments i que son personal administratiu, tècnics i caps de servei. Parlem d'uns 100 usuaris.

- Personal TIC: Personal del departament TIC de l'Ajuntament. Ens trobem un departament amb un cap de departament, 3 tècnis mitjans i un operador. 5 persones en total.

ESTRUCTURA ORGANITZATIVA

L' Ajuntament es troba governat pel ple municipal format per 21 regidors, sent un dels regidors l'alcalde del municipi. L'ajuntament té els següent òrgans de govern:

- Alcalde/President de l'organització.

- Regidors. Aquí ens trobem a tots els regidors de l'Ajuntament dels diferents partits polítics.
- Junta de govern: Format per l'alcalde i els regidors que prenen les decisions de govern.
- Regidories: La funció de govern es divideix en diferents àrees o regidories, cadascuna governades per un regidor per delegació de l'alcalde. Cada regidor pot tenir una o més regidories a càrrec. Aquestes regidories es tradueixen en serveis i/o departaments.
- Departaments: De caràcter més operatiu, podem trobar:

    - Serveis socials
    - Promoció Econòmica
    - Activitats ciutadanes (cultura, esports)
    - Recursos Humans
    - Departament TIC
    - Oficina Atenció Ciutadana
    - Territori

Al següent diagrama podem veure l'estructura en departaments en la que es troba dividit l'ajuntament.

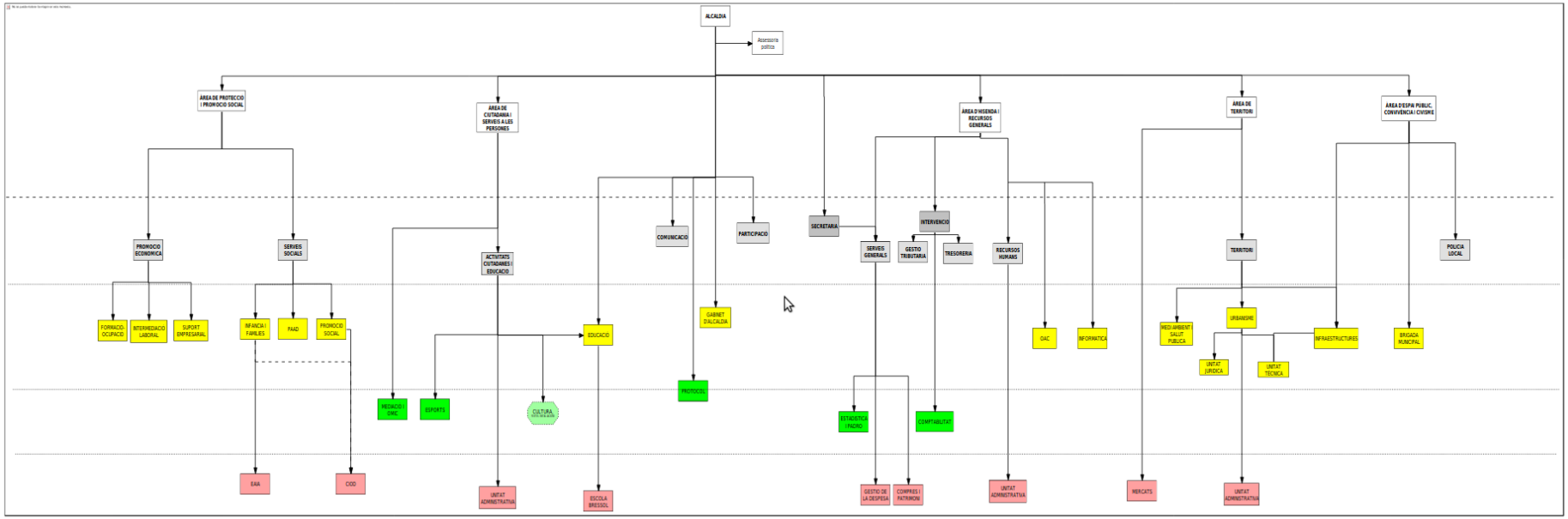


Figura 4: Organigrama de l'Ajuntament

Com s'ha comentat, a nivell gerencial, l'Ajuntament és governat pel Ple Municipal, que està format pel conjunt de regidors que han estat escollits en les eleccions municipals. El Ple està presidit per l'Alcalde, que delega les funcions en els regidors que formen part del govern, que s'organitzen en regidories per tal de poder executar les diferents competències municipals que li son obligades per la llei de bases del règim local.

Aquest tipus d'organització a on els regidors poden canviar cada quatre anys pot ocasionar que projectes de gran envergadura o estratègics puguin ver-se afectats i, per tant, un projecte com el que ens ocupa ha de tenir la plena implicació de tota la corporació.

Tal i com es desprèn de l'organigrama, l'Ajuntament s'organitza en regidories que poden englobar més de un departament.

3.2 Abast del SGSI

L'abast del projecte que es desenvolupa en aquest TFM consistirà ens els sistemes d'informació que proporcionen la tramitació d'expedients dins de l'Ajuntament, tant des d'un punt de vista intern com la possibilitat de la tramitació telemàtica per part de la ciutadania.

D'una manera més específica l'abast contindrà:

- La seu electrònica.
- El gestor d'expedients
- ERP municipal (específicament els mòduls de padró d'habitants i registre telemàtic).

Tot i que seria desitjable, queda fora de l'abast inicialment la resta de programari municipal, així com la gestió de la LOPD-GDD/RGDP (tot i que es farà alguna referència). Cal indicar que podria ser oportú un anàlisi conjunt, però l'avaluació dels diferents tractaments, així com les possibles AIPD (avaluació d'impacte de dades personals) faria un projecte massa costós per englobar-lo dins d'aquest TFM.

3.3 Objectius del pla director

L'objectiu d'aquest pla director és poder proporcionar les garanties suficient a la ciutadania, empreses, personal i sector públic en general a una protecció de dades de caràcter personal, i en particular a la seguretat i confidencialitat de les dades que figurin en els fitxers, sistemes i aplicacions que gestiona l'ajuntament MISTIC. Específicament, els objectius es poden detallar de la manera següent:

- Obtenir una visió general de l'estat actual de la seva seguretat en els diferents elements que formen les TIC.

- Proporcionar mesures per millorar els punts que puguin ser crítics per a l'ajuntament i establir unes bases per al Sistema de Gestió de Seguretat de l' Informació per tal que el Pla Director de la Seguretat tingui sentit, evolucioni i realitzi les millores esperades.

- Fomentar la relació electrònica entre els ciutadans, empreses i altres administracions amb l'Ajuntament de MISTIC.

- Reducció de la càrrega administrativa de les oficines d'atenció ciutadana. Si podem assegurar la tramitació telemàtica podrem promocionar aquest nou canal de relació amb l'Ajuntament per part de la ciutadania i alliberar part de la càrrega de treball que es feia presencialment (ara ja telemàtica).

- Permetre el control i seguiment dels expedients i documents presentats per al ciutadà de manera confiable i segura, tant dins de l'ajuntament com a través de la seu electrònica, creant una veritable oficina d'atenció ciutadana 24 hores, 365 dies a l'any.

- Millora de la seguretat en general de la informació de l'Ajuntament.

- Compliment de l'Esquema Nacional de Seguretat.

Cal mencionar que en aquest Pla director es detectarà la situació inicial de seguretat i no es centrarà en l'eliminació de vulnerabilitats existents, sinó en la implantació d'una metodologia i un full de ruta amb un conjunt d'accions a realitzar. L'objectiu és introduir el procés de la seguretat de la informació dins de l'Ajuntament, i implementar un procés de millora contínua PDCA, de manera que aquest pla director es revisi, s'actualitzi i tingui un abast cada vegada més ampli dins de l'organització.

Es tracta, doncs, de la primera presa de contacte de l'Ajuntament amb un SGSI i, per tant, haurem d'actuar en conseqüència.

Finalment, a més dels objectius anteriors, amb aquest pla hauríem d'aconseguir:

- Implantar un control periòdic de les mesures aplicades.
- Coneixement de l'estat actual i previsió de futur en matèria de seguretat.
- Conscienciar el personal treballador de la importància de l'seguiment de controls de la seguretat informàtica per disminuir l'impacte davant de qualsevol incidència.

3.4 Anàlisi diferencial.

L'anàlisi diferencial (o gap analysis) és un anàlisi que es fa servir per poder trobar les deficiències existents entre dues situacions. Típicament es fa servir per comparar una situació (normalment l'actual) i una situació que volem aconseguir (la desitjada), de manera que trobarem les diferencies per a cada element que descriuen les situacions i podrem traçar un conjunt d'accions (o pla director) encaminat a millorar la situació actual per tal de que s'assembli a la situació desitjada (és a dir, a anant reduint les diferències o el *gap* que les separa).

Davant d'això, i atès l'objectiu que ens hem fixat sobre l'adequació de l'Ajuntament MISTIC a l'Esquema Nacional de Seguretat, s'haurà de definir quina és la situació objectiu a la que volem arribar. Com ja s'ha comentat, la situació objectiu de l'adequació d'una administració pública a l'ENS depèn del tipus de categoria a la que pertanyi així que podríem no tenir clara aquesta situació en aquest punt si no s'ha realitzat l'inventari d'actius ni la seva categorització.

En aquest punt, i per tal de poder fer servir la metodologia proposada, s'ha adoptat l'aproximació de considerar l'ajuntament com un sistema de categoria MITJANA. Aquesta aproximació es basa fonamentalment en el fet dels diferents tipus de tractament de dades de caràcter personal que es realitzen dins de la seu electrònica. Hem de recordar que els ajuntament tenen atribucions i competències sobre l'àmbit dels serveis socials i que, per tant, és fàcil trobar dades relacionades amb orientació ètnica, de salut, etc, totes elles especialment protegides.

Observació: *Un altre possible aproximació que podríem realitzar és la consideració de que el sistema serà de categoria BAIXA. Si fem aquesta aproximació, estem estalviant d'entrada el fet de realitzar la valoració de la categoria real del sistema i poder començar abans el projecte. A vegades pot ser interessant aquesta aproximació per tal de «ficar» a l'organització d'estudi dins de la roda del canvi, del projecte, i del SGSI. Poder començar ja a definir polítiques, normatives i procediments que puguin ser aplicables ens servirà per fer girar la roda del projecte. Després, i ja dins del cicle de millora contínua PDCA, es podria reconsiderar la categoria del sistema avaluant les conseqüències/impacte que tindríen la materialització de les amenaçes contra el nostre Ajuntament*.

Per tant, un cop ja sabem amb quin conjunt de mesures de l'Annex II de l'ENS hem de realitzar el nostre anàlisi diferencial, passarem a establir els criteris que s'han seguit en la seva realització.

CMM (Capacity Maturity Model)

El model CMM [12] (o Model de Maduresa de la Capacitat) és un model que permet avaluar la maduresa dels processos implementats dins d'una organització.

Si tenim en compte que l'aproximació a la seguretat l'estem contemplant com a un nou procés dins de l'organització, té sentit fer servir els diferents mecanismes que s'apliquen als processos també en aquest que ara ens proposem definir.

Per tal d'aplicar CMM definirem la maduresa d'un control en funció de la capacitat de gestió amb el que es realitza, seguint la taula següent.

EFECTIVITAT	CMM	SIGNIFICAT	DESCRIPCIÓ
0%	L0	Inexistent	Carència completa de qualsevol procés que reconeguem. No s'ha reconegut que existeixi cap problema a resoldre
10%	L1	Inicial / Ad-hoc	Estat inicial on l'èxit de les activitats dels processos es basa la major part dels cops en un esforç personal. Els procediments son inexistents o localitzats en àrees concretes No existeixen plantilles definides a nivell corporatiu
50%	L2	Reproduïble, però intuïtiu	Els processos similars es porten a terme de manera similar per diferents persones amb la mateixa tasca. Es normalitzen les "bones practiques" en base a l'experiència i al mètode. No hi ha comunicació o entrenament formal, les responsabilitats queden a càrrec de cada individu. Es depèn del grau de coneixement de cada individu

90%	L3	Procés definit.	La organització sencera participa al procés. Els processos estan implantats, documentats i comunicats mitjançant entrenament.
95%	L4	Gestionat i mesurable.	Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos.
100%	L5	Optimitzat	Els processos estan sota constant millora. En base criteris quantitatius es determinen les desviacions més comunes i s'optimitzen els processos

Taula 8: Model CMM

Per tant, anirem assignant els diferents valors de maduresa per als controls que l'annex II de l'ENS ens indica. A la següent taula podrem veure un resum del conjunt de controls que especifica l'annex II de l'ENS, així si tenen aplicació o no en funció de la categoria del sistema [17].

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
				org	Marco organizativo
categoría	aplica	=	=	[org.1]	Política de seguridad
categoría	aplica	=	=	[org.2]	Normativa de seguridad
categoría	aplica	=	=	[org.3]	Procedimientos de seguridad
categoría	aplica	=	=	[org.4]	Proceso de autorización

Taula 9: ENS - Mesures organitzatives

				op	Marco operacional
				[op.pl]	Planificación
categoría	aplica	+	++	[op.pl.1]	Análisis de riesgos
categoría	aplica	+	++	[op.pl.2]	Arquitectura de seguridad
categoría	aplica	=	=	[op.pl.3]	Adquisición de nuevos componentes
D	n.a.	aplica	=	[op.pl.4]	Dimensionamiento / Gestión de capacidades
categoría	n.a.	n.a.	aplica	[op.pl.5]	Componentes certificados

Taula 10: ENS - Marc operacional - planificació

				[op.acc]	Control de acceso
A T	aplica	=	=	[op.acc.1]	Identificación
I C A T	aplica	=	=	[op.acc.2]	Requisitos de acceso
I C A T	n.a.	aplica	=	[op.acc.3]	Segregación de funciones y tareas
I C A T	aplica	=	=	[op.acc.4]	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	[op.acc.5]	Mecanismo de autenticación
I C A T	aplica	+	++	[op.acc.6]	Acceso local (local logon)
I C A T	aplica	+	=	[op.acc.7]	Acceso remoto (remote login)

Taula 11: ENS - Marc operacional – control d'accés

				[op.exp]	Explotación
categoría	aplica	=	=	[op.exp.1]	Inventario de activos
categoría	aplica	=	=	[op.exp.2]	Configuración de seguridad
categoría	n.a.	aplica	=	[op.exp.3]	Gestión de la configuración
categoría	aplica	=	=	[op.exp.4]	Mantenimiento
categoría	n.a.	aplica	=	[op.exp.5]	Gestión de cambios
categoría	aplica	=	=	[op.exp.6]	Protección frente a código dañino
categoría	n.a.	aplica	=	[op.exp.7]	Gestión de incidentes
T	aplica	+	++	[op.exp.8]	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	[op.exp.9]	Registro de la gestión de incidentes
T	n.a.	n.a.	aplica	[op.exp.10]	Protección de los registros de actividad
categoría	aplica	+	=	[op.exp.11]	Protección de claves criptográficas

Taula 12: ENS - Marc operacional – explotació

				[op.ext]	Servicios externos
categoría	n.a.	aplica	=	[op.ext.1]	Contratación y acuerdos de nivel de servicio
categoría	n.a.	aplica	=	[op.ext.2]	Gestión diaria
D	n.a.	n.a.	aplica	[op.ext.9]	Medios alternativos

Taula 13: ENS - Marc operacional – serveis externs

				[op.cont]	Continuidad del servicio
D	n.a.	aplica	=	[op.cont.1]	Análisis de impacto
D	n.a.	n.a.	aplica	[op.cont.2]	Plan de continuidad
D	n.a.	n.a.	aplica	[op.cont.3]	Pruebas periódicas

Taula 14: ENS - Marc operacional - continuïtat del servei

				[op.mon]	Monitorización del sistema
categoría	n.a.	aplica	=	[op.mon.1]	Detección de intrusión
categoría	aplica	+	++	[op.mon.2]	Sistema de métricas

Taula 15: ENS - Marc operacional – Monitoratge del sistema.

				mp	Medidas de protección
				[mp.if]	Protección de las instalaciones e infraestructuras
categoría	aplica	=	=	[mp.if.1]	?reas separadas y con control de acceso
categoría	aplica	=	=	[mp.if.2]	Identificación de las personas
categoría	aplica	=	=	[mp.if.3]	Acondicionamiento de los locales
D	aplica	+	=	[mp.if.4]	Energía eléctrica
D	aplica	=	=	[mp.if.5]	Protección frente a incendios
D	n.a.	aplica	=	[mp.if.6]	Protección frente a inundaciones
categoría	aplica	=	=	[mp.if.7]	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	[mp.if.9]	Instalaciones alternativas

Taula 16: ENS - Mesures de protecció d'instal·lacions i infraestructures

				[mp.per]	Gestión del personal
categoría	n.a.	aplica	=	[mp.per.1]	Caracterización del puesto de trabajo
categoría	aplica	=	=	[mp.per.2]	Deberes y obligaciones
categoría	aplica	=	=	[mp.per.3]	Concienciación
categoría	aplica	=	=	[mp.per.4]	Formación
D	n.a.	n.a.	aplica	[mp.per.9]	Personal alternativo

Taula 17: ENS - Mesures de protecció- Gestió de personal

				[mp.eq]	Protección de los equipos
categoría	aplica	+	=	[mp.eq.1]	Puesto de trabajo despejado
A	n.a.	aplica	+	[mp.eq.2]	Bloqueo de puesto de trabajo
categoría	aplica	=	+	[mp.eq.3]	Protección de equipos portátiles
D	n.a.	aplica	=	[mp.eq.9]	Medios alternativos

Taula 18: ENS - Mesures de protecció- Protecció d'equips

				[mp.com]	Protección de las comunicaciones
categoría	aplica	=	+	[mp.com.1]	Perímetro seguro
C	n.a.	aplica	+	[mp.com.2]	Protección de la confidencialidad
I A	aplica	+	++	[mp.com.3]	Protección de la autenticidad y de la integridad
categoría	n.a.	n.a.	aplica	[mp.com.4]	Segregación de redes
D	n.a.	n.a.	aplica	[mp.com.9]	Medios alternativos

Taula 19: ENS - Mesures de protecció- protecció de comunicacions

				[mp.si]	Protección de los soportes de información
C	aplica	=	=	[mp.si.1]	Etiquetado
I C	n.a.	aplica	+	[mp.si.2]	Criptografía
categoría	aplica	=	=	[mp.si.3]	Custodia
categoría	aplica	=	=	[mp.si.4]	Transporte
C	aplica	+	=	[mp.si.5]	Borrado y destrucción

Taula 20: ENS - Mesures de protecció- protecció de suports d'informació

				[mp.sw]	Protección de las aplicaciones informáticas
categoría	n.a.	aplica	=	[mp.sw.1]	Desarrollo
categoría	aplica	+	++	[mp.sw.2]	Aceptación y puesta en servicio

Taula 21: ENS - Mesures de protecció- protecció d'aplicacions informàtiques

				[mp.info]	Protección de la información
categoría	aplica	=	=	[mp.info.1]	Datos de carácter personal
C	aplica	+	=	[mp.info.2]	Calificación de la información
C	n.a.	n.a.	aplica	[mp.info.3]	Cifrado
I A	aplica	+	++	[mp.info.4]	Firma electrónica
T	n.a.	n.a.	aplica	[mp.info.5]	Sellos de tiempo
C	aplica	=	=	[mp.info.6]	Limpieza de documentos
D	aplica	=	=	[mp.info.9]	Copias de seguridad *(backup)*

Taula 22: ENS - Mesures de protecció- protecció de la informació

				[mp.s]	Protección de los servicios
categoría	aplica	=	=	[mp.s.1]	Protección del correo electrónico
categoría	aplica	=	+	[mp.s.2]	Protección de servicios y aplicaciones web
D	n.a.	aplica	+	[mp.s.8]	Protección frente a la denegación de servicio
D	n.a.	n.a.	aplica	[mp.s.9]	Medios alternativos

Taula 23: ENS - Mesures de protecció- protecció dels serveis

A les taules es fan servir les següents convencions:

a) Per a indicar que una determinada mesura de seguretat s'ha d'aplicar a una o diverses dimensions de seguretat en algun nivell determinat s'utilitza la veu 'aplica'.

b) 'n.a.' vol dir 'no aplica'.

c) Per a indicar que les exigències d'un nivell són iguals als de l'nivell inferior s'utilitza el signe "= ?.

d) Per a indicar l'increment d'exigències graduat en funció de de el nivell de la dimensió de seguretat, s'utilitzen els signes "+" i "++".

e) Per a indicar que una mesura protegeix específicament una certa dimensió de seguretat, aquesta s'explicita mitjançant la seva inicial.

f) En les taules de aquest annex s'han emprat colors verd, groc i vermell de la següent manera: el color verd per indicar que una certa mesura s'aplica en sistemes de categoria BÀSICA o superior; el groc per indicar les mesures que comencen a aplicar-se en categoria MITJANA o superior; el vermell per indicar les mesures que només són d'aplicació

Un cop revisats el conjunt de controls que especifica l'ENS, haurem de comprovar el grau de maduresa que tenen les mesures que proposa l'annex II pel nostre sistema de categoria mitjana (si és que les tenim aplicades). Per tant, ens haurem de fixar en els controls de la taula anterior que siguin de color verd o groc, seguin la convenció que hem marcat anteriorment.

org	Marc organitzatiu	Aplica	CMM	Eficàcia
org.1	Política de seguretat	Sí	L0	0%
org.2	Normativa de seguretat	Sí	L0	0%
org.3	Procediments de seguretat.	Sí	L0	0%
org.4	Procés d'autorització.	Sí	L0	0%
	TOTAL			0%

Taula 24: CMM – ENS - Marc organitzatiu

op	Marco operacional	Aplica	CMM	Eficàcia
op.pl	Planificació			
op.pl.1	Anàlisi de riscos.	Sí	L0	0%
op.pl.2	Arquitectura de seguretat.	Sí	L0	0%
op.pl.3	Adquisició de nous components.	Sí	L0	0%
op.pl.4	Dimensionament / Gestió de capacitats	Sí	L0	0%
op.pl.5	Components certificats	No	n.a	n.a
	TOTAL			0%
op.acc	Control de accés			
op.acc.1	Identificació	Sí	L2	50%
op.acc.2	Requisits d'accés	Sí	L2	50%

op.acc.3	Segregació de funcions i tasques	Sí	L0	0
op.acc.4	Procés de gestió de drets d'accés	Sí	L2	50%
op.acc.5	Mecanisme d'autenticació	Sí	L2	50%
op.acc.6	Accés local (*local logon*)	Sí	L2	50%
op.acc.7	Accés remot (*remote login*)	Sí	L1	10%
	TOTAL			37%
op.exp	Explotació			
op.exp.1	Inventari d'actius	Sí	L0	0%
op.exp.2	Configuració de seguretat	Sí	L1	10%
op.exp.3	Gestió de la configuració	Sí	L1	10%
op.exp.4	Manteniment	Sí	L1	10%
op.exp.5	Gestió de canvis	Sí	L0	0%
op.exp.6	Protecció davant codi maligne	Sí	L3	90%
op.exp.7	Gestió d'incidències	Sí	L2	50%
op.exp.8	Registre de l'activitat dels usuaris	Sí	L1	10%
op.exp.9	Registre de la gestió d'incidències	Sí	L2	50%
op.exp.10	Protecció dels registres d'activitat	No	n.a	n.a
op.exp.11	Protecció de les claus criptogràfiques	Sí	L2	50%
	TOTAL			18%
op.ext	Serveis externs			
op.ext.1	Contractació i acords de nivell de servei	Sí	L1	10%
op.ext.2	Gestió diària	Sí	L0	0%
op.ext.9	Mitjans alternatius	No	n.a	n.a
	TOTAL			10%
op.cont	Continuïtat del servei			
op.cont.1	Anàlisis d'impacte	Sí	L0	0%
op.cont.2	Plans de continuïtat	No	n.a	n.a
op.cont.3	Proves periòdiques	No	n.a	n.a
	TOTAL			0%
op.mon	Monitoratge del sistema			
op.mon.1	Detecció d'intrusions	Sí	L0	0
op.mon.2	Sistema de mètriques	Sí	L1	10
	TOTAL			10%

Taula 25: CMM – ENS - Marc operacional

mp	Mesures de protecció	Aplica		
mp.if	Protecció de les instal·lacions i infraestructures			
mp.if.1	Àrees separades i amb control d'accés	Sí	L3	90%
mp.if.2	Identificació de les persones	Sí	L1	10%
mp.if.3	Acondicionament dels locals	Sí	L2	50%
mp.if.4	Energia elèctrica	Sí	L1	10
mp.if.5	Protecció davant incendis	Sí	L3	90%
mp.if.6	Protecció davant inundacions	Sí	L0	0%
mp.if.7	Registre d'entrada i sortida d'equipament	Sí	L0	0%
mp.if.9	Instal·lacions alternatives	No	n.a	n.a
	TOTAL			35%
mp.per	Gestió del personal			
mp.per.1	Caracterització del lloc de treball	Sí	L0	0%
mp.per.2	Deures i obligacions	Sí	L0	0%
mp.per.3	Conscienciació	Sí	L0	0%
mp.per.4	Formació	Sí	L0	0%
mp.per.9	Personal alternatiu	No	n.a	n.a
	TOTAL			0%
mp.eq	Protecció de l'equipament			
mp.eq.1	Lloc de treball net	Sí	L0	0
mp.eq.2	Bloqueig del lloc de treball	Sí	L3	90
mp.eq.3	Protecció dels portàtils	Sí	L0	0
mp.eq.9	Mitjans alternatius	Sí	L0	0
	TOTAL			23%
mp.com	Protecció de las comunicacions			
mp.com.1	Perímetre segur	Sí	L3	80%
mp.com.2	Protecció de la confidencialitat	Sí	L3	80%
mp.com.3	Protecció de la autenticitat i de la integritat	Sí	L3	90%
mp.com.4	Segregació de xarxes	No	n.a	n.a
mp.com.9	Mitjans alternatius	No	n.a	n.a

	TOTAL			93,3%
mp.si	Protecció de dels mitjans d'informació			
mp.si.1	Etiquetatge	Sí	L0	0%
mp.si.2	Criptografia	Sí	L0	0%
mp.si.3	Custodia	Sí	L0	0%
mp.si.4	Transporte	Sí	L0	0%
mp.si.5	Eliminació i destrucció	Sí	L1	10
	TOTAL			10%
mp.sw	Protecció de las aplicacions informàtiques			
mp.sw.1	Desenvolupament	Sí	L0	0%
mp.sw.2	Acceptació i posada en servei	Sí	L0	0%
	TOTAL			0%
mp.info	Protecció de la informació			
mp.info.1	Dades de caràcter personal	Sí	L3	90%
mp.info.2	Qualificació de la informació	Sí	L0	10%
mp.info.3	Xifratge de la informació	No	n.a	n.a
mp.info.4	Signatura electrònica	Sí	L2	50%
mp.info.5	Segells de temps	No	n.a	n.a
mp.info.6	Neteja de documents	Sí	L0	0%
mp.info.9	Còpies de seguretat (backup)	Sí	L3	90%
	TOTAL			48%
mp.s	Protecció dels serveis			
mp.s.1	Protecció del correu electrònic	Sí	L3	90
mp.s.2	Protecció de serveis i aplicacions web	Sí	L1	10
mp.s.8	Protecció davant la denegació de servei	Sí	L0	0
mp.s.9	Mitjans alternatius	No	n.a	n.a
	TOTAL			33%

Taula 26: CMM - ENS – Marc mesures de protecció

D’una manera més resumida, l’anàlisi diferencial ens mostra els següents resultats

Apartats	Òptim	Acceptable	Actual
Organització	100 %	80 %	0 %
Protecció de les comunicacions	100 %	80 %	93 %
Protecció dels suports de la informació	100 %	80 %	2 %
Protecció de las aplicacions informàtiques	100 %	80 %	0 %
Planificació	100 %	80 %	0 %
Control d'accés	100 %	80 %	37 %
Explotació	100 %	80 %	18 %
Serveis externs	100 %	80 %	10 %
Continuïtat del servei	100 %	80 %	0 %
Monitoratge del sistema	100 %	80 %	10 %
Protecció d'instal·lacions i infraestructures	100 %	80 %	35 %
Gestió del personal	100 %	80 %	0 %
Protecció dels equips	100 %	80 %	23 %
Protecció de la informació	100 %	80 %	48 %
Protecció dels serveis	100 %	80 %	33 %

Taula 27: Resum anàlisi diferencial inicial ENS

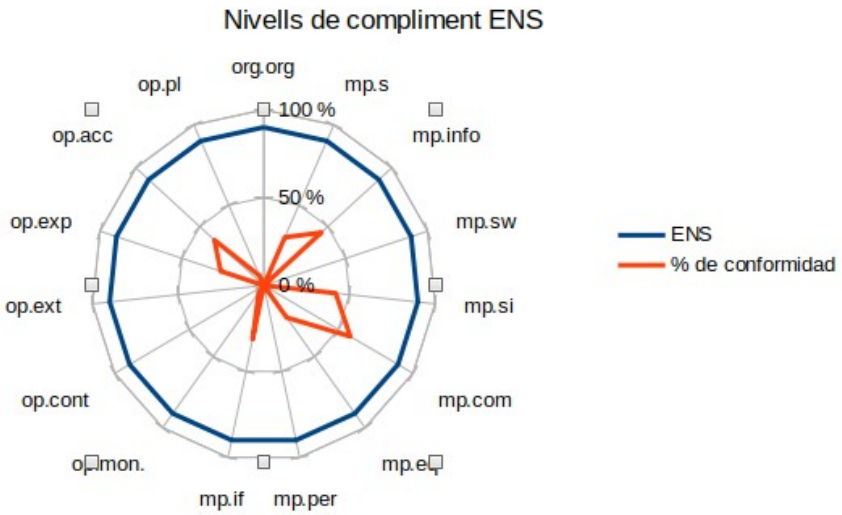


Figura 5: Anàlisi diferencial ENS – esquema radar

Gràficament, podem veure com la situació actual es troba molt allunyada de la situació objectiu.

També realitzarem l'anàlisi diferencial respecte als controls definits per la 50ISO27002:2013

ISO / IEC 27002: 2013. 14 DOMINIS, 35 OBJECTIUS DE CONTROL I 114 CONTROLS				
5	**POLÍTIQUES DE SEGURETAT**		**CMM**	**%**
	5.1	**Directrius de la Direcció en seguretat de la informació.**		
	5.1.1	Conjunt de polítiques per a la seguretat de la informació.	L0	0
	5.1.2	Revisió de les polítiques per a la seguretat de la informació.	L0	0

6	**ASPECTES ORGANITZATIUS DE LA SEGURETAT DE LA INFORMACIÓ.**		**CMM**	**%**
	6.1	**Organització interna.**		
	6.1.1	Assignació de responsabilitats per a la segur. de la informació.	L0	0
	6.1.2	Segregació de tasques.	L0	0
	6.1.3	Contacte amb les autoritats.	L1	10
	6.1.4	Contacte amb grups d'interès especial.	L2	50
	6.1.5	Seguretat de la informació en la gestió de projectes.	L0	0
	6.2	**Dispositius per a mobilitat i teletreball.**		
	6.2.1	Política d'ús de dispositius per a mobilitat.	L0	0
	6.2.2	Teletreball.	L0	0

7	**SEGURETAT LLIGADA ALS RECURSOS HUMANS.**		**CMM**	**%**
	7.1	**Abans de la contractació.**		
	7.1.1	Investigació d'antecedents.	L0	0
	7.1.2	Termes i condicions de contractació.	L0	0
	7.2	**Durant la contractació.**		

	7.2.1	Responsabilitats de gestió.	L0	0
	7.2.2	Conscienciació, educació i capacitació en segur. de la informac.	L0	0
	7.2.3	Procés disciplinari.	L0	0
	7.3	**Cessament o canvi de lloc de treball.**		
	7.3.1	Cessament o canvi de lloc de treball.	L0	0

8	**GESTIÓ D'ACTIUS.**		**CMM**	**%**
	8.1	**Responsabilitat sobre els actius.**		
	8.1.1	Inventari d'actius.	L0	0
	8.1.2	Propietat dels actius.	L0	0
	8.1.3	Ús acceptable dels actius.	L0	0
	8.1.4	Devolució d'actius.	L0	0
	8.2	**Classificació de la informació.**		
	8.2.1	Directrius de classificació.	L0	0
	8.2.2	Etiquetatge i manipulat de la informació.	L0	0
	8.2.3	Manipulació d'actius.	L0	0
	8.3	**Maneig dels suports d'emmagatzematge**		
	8.3.1	Gestió de suports extraïbles.	L0	0
	8.3.2	Eliminació de suports.	L1	10
	8.3.3	Suports físics en trànsit.	L0	0

9	**CONTROL D'ACCESSOS.**		**CMM**	**%**
	9.1	**Requisits de negoci per al control d'accessos.**		
	9.1.1	Política de control d'accessos.	L2	50
	9.1.2	Control d'accés a les xarxes i serveis associats.	L2	50
	9.2	**Gestió d'accés d'usuari.**		
	9.2.1	Gestió d'altes / baixes en el registre d'usuaris.	L2	50
	9.2.2	Gestió dels drets d'accés assignats a usuaris.	L2	50
	9.2.3	Gestió dels drets d'accés amb privilegis especials.	L2	50
	9.2.4	Gestió d'informació confidencial d'autenticació d'usuaris.	L2	50
	9.2.5	Revisió dels drets d'accés dels usuaris.	L2	50
	9.2.6	Retirada o adaptació dels drets d'accés	L2	50
	9.3	**Responsabilitats de l'usuari.**		

	9.3.1	Us d'informació confidencial per a l'autenticació.	L2	50
	9.4	**Control d'accés a sistemes i aplicacions.**		
	9.4.1	Restricció de l'accés a la informació.	L2	50
	9.4.2	Procediments segurs d'inici de sessió.	L2	50
	9.4.3	Gestió de contrasenyes d'usuari.	L2	50
	9.4.4	Ús d'eines d'administració de sistemes.	L2	50
	9.4.5	Control d'accés a el codi font dels programes	L1	10

10	**10. XIFRAT**		**CMM**	**%**
	10.1	Controls criptogràfics.		
	10.1.1	Política d'ús dels controls criptogràfics	L0	0
	10.1.2	Gestió de claus.	L0	0

11	**SEGURETAT FÍSICA I AMBIENTAL**		**CMM**	**%**
	11.1	**Àrees segures.**		
	11.1.1	Perímetre de seguretat física.	L3	90
	11.1.2	Controls físics d'entrada.	L3	90
	11.1.3	Seguretat d'oficines, despatxos i recursos.	L3	90
	11.1.4	Protecció contra les amenaces externes i ambientals.	L2	50
	11.1.5	El treball en àrees segures.	L2	50
	11.1.6	Àrees d'accés públic, càrrega i descàrrega.	L2	50
	11.2	**Seguretat dels equips.**		
	11.2.1	Emplaçament i protecció d'equips.	L3	90
	11.2.2	Instal·lacions de subministrament.	L1	10
	11.2.3	Seguretat de l'cablejat.	L2	50
	11.2.4	Manteniment dels equips.	L2	50
	11.2.5	Sortida d'actius fora de les dependències de l'empresa.	L0	0
	11.2.6	Seguretat dels equips i actius fora de les instal·lacions.	L0	0
	11.2.7	Reutilització o retirada segura de dispositius d'emmagatzematge.	L1	10
	11.2.8	Equip informàtic d'usuari desatès.	L3	90
	11.2.9	Política de lloc de treball buidat i bloqueig de pantalla.	L3	90

12	SEGURETAT A L'OPERATIVA.		CMM	%
	12.1	**Responsabilitats i procediments d'operació.**		
	12.1.1	Documentació de procediments d'operació.	L0	0
	12.1.2	Gestió de canvis.	L0	0
	12.1.3	Gestió de capacitats.	L0	0
	12.1.4	Separació d'entorns de desenvolupament, prova i producció.	L0	0
	12.2	**Protecció contra codi maliciós.**		
	12.2.1	Controls contra el codi maliciós.	L3	90
	12.3	Còpies de seguretat.		
	12.3.1	Còpies de seguretat de la informació.	L3	90
	12.4	Registre d'activitat i supervisió		
	12.4.1	Registre i gestió d'esdeveniments d'activitat.	L0	0
	12.4.2	Protecció dels registres d'informació.	L1	10
	12.4.3	Registres d'activitat de l'administrador i operador de sistema.	L1	10
	12.4.4	Sincronització de rellotges.	L1	10
	12.5	**Control de programari en explotació.**		
	12.5.1	Instal·lació del programari en sistemes en producció.	L1	10
	12.6	**Gestió de la vulnerabilitat tècnica.**		
	12.6.1	Gestió de les vulnerabilitats tècniques.	L1	10
	12.6.2	Restriccions en la instal·lació de programari.	L2	50
	12.7	**Consideracions de les auditories dels sistemes d'informació.**		
	12.7.1	Controls d'auditoria dels sistemes d'informació.	L0	0

13	SEGURETAT A LES TELECOMUNICACIONS.		CMM	%
	13.1	**Gestió de la seguretat en les xarxes.**		
	13.1.1	Controls de xarxa.	L3	90
	13.1.2	Mecanismes de seguretat associats a serveis en xarxa.	L3	90
	13.1.3	Segregació de xarxes.	L2	50
	13.2	**Intercanvi d'informació amb parts externes.**		
	13.2.1	Polítiques i procediments d'intercanvi d'informació.	L2	50
	13.2.2	Acords d'intercanvi.	L1	10
	13.2.3	Missatgeria electrònica.	L0	0

	13.2.4	Acords de confidencialitat i secret.	L0	0

14	**ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DELS SISTEMES D'INFORMACIÓ.**		**CMM**	**%**
	14.1	**Requisits de seguretat dels sistemes d'informació.**		
	14.1.1	Anàlisi i especificació dels requisits de seguretat.	L1	10
	14.1.2	Seguretat de les comunicacions en serveis accessibles per xarxes públiques.	L2	50
	14.1.3	Protecció de les transaccions per xarxes telemàtiques.	L1	10
	14.2	**Seguretat en els processos de desenvolupament i suport**		
	14.2.1	Política de desenvolupament segur de programari.	L0	0
	14.2.2	Procediments de control de canvis en els sistemes.	L0	0
	14.2.3	revisió tècnica de les aplicacions després d'efectuar canvis en el sistema operatiu.	L0	0
	14.2.4	Restriccions als canvis en els paquets de programari.	L0	0
	14.2.5	Ús de principis d'enginyeria en protecció de sistemes.	L0	0
	14.2.6	Seguretat en entorns de desenvolupament.	L0	0
	14.2.7	Externalització de el desenvolupament de programari.	L1	10
	14.2.8	Proves de funcionalitat durant el desenvolupament dels sistemes.	L0	0
	14.2.9	Proves d'acceptació.	L0	0
	14.3	**Dades de prova.**		
	14.3.1	Protecció de les dades utilitzades en proves.	L0	0

15	**RELACIONS AMB SUMINISTRADORES.**		**CMM**	**%**
	15.1	**Seguretat de la informació en les relacions amb subministradors.**		
	15.1.1	Política de seguretat de la informació per subministradors.	L0	0
	15.1.2	Tractament de el risc dins d'acords de subministradors.	L1	10
	15.1.3	Cadena de subministrament en tecnologies de la informació i comunicacions	L1	10
	15.2	**Gestió de la prestació de servei per subministradors.**		

	15.2.1	Supervisió i revisió dels serveis prestats per tercers.	L0	0
	15.2.2	Gestió de canvis en els serveis prestats per tercers.	L0	0

16	**GESTIÓ D'INCIDENTS A LA SEGURETAT DE LA INFORMACIÓ.**		**CMM**	**%**
	16.1	**Gestió d'incidents de seguretat de la informació i millores.**		
	16.1.1	Responsabilitats i procediments.	L0	0
	16.1.2	Notificació dels esdeveniments de seguretat de la informació.	L1	10
	16.1.3	Notificació de punts febles de la seguretat.	L1	10
	16.1.4	Valoració d'esdeveniments de seguretat de la informació i presa de decisions.	L1	10
	16.1.5	Resposta als incidents de seguretat.	L1	10
	16.1.6	Aprenentatge dels incidents de seguretat de la informació.	L1	10
	16.1.7	Recull d'evidències.	L1	10

17	**ASPECTES DE SEGURETAT DE LA INFORMACIÓ A LA GESTIÓ DE LA CONTINUÏTAT DEL NEGOCI.**		**CMM**	**%**
	17.1	**Continuïtat de la seguretat de la informació.**		
	17.1.1	Planificació de la continuïtat de la seguretat de la informació.	L0	0
	17.1.2	Implantació de la continuïtat de la seguretat de la informació.	L0	0
	17.1.3	Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació.	L0	0
	17.2	**Redundàncies.**		
	17.2.1	Disponibilitat d'instal·lacions per al processament de la informació.	L0	0

18	**COMPLIMENT**		**CMM**	**%**
	18.1	**Compliment dels requisits legals i contractuals.**		
	18.1.1	Identificació de la legislació aplicable.	L3	90
	18.1.2	Drets de propietat intel·lectual (DPI).	n.a	n.a
	18.1.3	Protecció dels registres de l'organització.	L1	10
	18.1.4	Protecció de dades i privacitat de la informació	L3	90

		personal.		
	18.1.5	Regulació dels controls criptogràfics.	L0	0
	18.2	**Revisions de la seguretat de la informació.**		
	18.2.1	Revisió independent de la seguretat de la informació.	L1	10
	18.2.2	Compliment de les polítiques i normes de seguretat.	L1	10
	18.2.3	Comprovació de l'acompliment	L0	0

Taula 28: Anàlisi diferencial ISO27001 - situació inicial

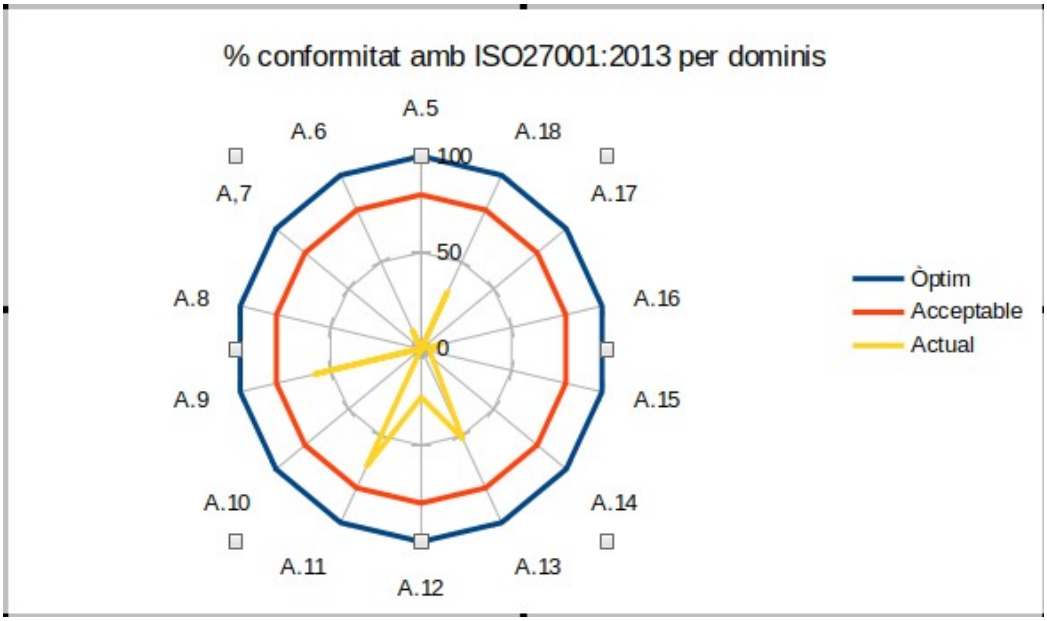


Figura 6: Anàlisi diferencial ISO27002:2013 – esquema radar

Com es pot comprovar, tant l'esquema de radar corresponent a l'ENS com el de la norma ISO27001 son similars, atès que les dues normes mesuren aspectes molt semblant, i el grau d'implementació d'aquests aspectes son el mateix pel nostre sistema d'estudi.

4. FASE 2: Sistema de Gestió Documental

4.1. Necessitat de la gestió documental

Qualsevol sistema de gestió requereix construir una documentació que el pugui sustentar i que podem fer servir com a referència. Aquesta documentació ha de permetre a qualsevol persona entendre el procés de gestió que s'està realitzant, així com el conjunt de mesures que s'estan aplicant per tal de assegurar tant la informació com els sistemes d'informació.

Per tant, s'haurà de disposar d'una normativa comuna de seguretat que reculli les línies metres sobre la manera de treballar de tota l'organització en matèria de seguretat de la informació. Per tant, aquest marc normatiu haurà de validar qualsevol acció que es prengui en matèria de seguretat de la informació, i haurà d'estar aprovat per la direcció.

Els objectius que es persegueixen en documentar i mantenir un sistema de gestió documental son:

1. **Garantir la repetició en el temps d'un procés**. La base per a garantir l'aplicació sistemàtica d'un procés és la seva documentació

2. **Establir un procés de millora**. La documentació d'un procés permet l'accés a una informació valuosa en relació a com es va dissenyar, quins passos o etapes el componen, quins indicadors de gestió es van definir, etc ... Amb aquesta informació recopilada podem avaluar l'eficàcia del nostre sistema de gestió i ens permet prendre decisions per modificar el procés en base a una informació existent. És a dir, la documentació es bàsica en el procés de presa de decisions per millorar el nostre sistema. Aquest és un dels principals motius d'un sistema de gestió: la **MILLORA CONTÍNUA** dels nostres processos

La Millora contínua no es pot aconseguir si no documentem de manera adequada el mateix Sistema de Gestió.

3. **Com evidència el compliment amb els requisits de la norma.** Mantenir informació documentada és el mitjà per justificar el compliment amb els requisits de la norma. NO n'hi ha prou afirmar que realitzem una tasca d'una determinada forma. Cal que hi hagi registres que deixin constància del que fem.

4.2. **Jerarquia documental i terminologia**

Per tal de poder gestionar tota la documentació caldrà definir de bon començament una terminologia clara que ens ajudi a distingir la importància i l'ús de cada document que es generi. D'aquesta manera, aconseguirem anomenar de manera consistent al mateix tipus de document, i podrem avaluar la importància relativa de cadascun dins del nostre sistema documental.

Normalment s'estableixen uns graus d'importància o jerarquia dins de la documentació que s'ha de generar que s'anomena ***piràmide documental [15].***

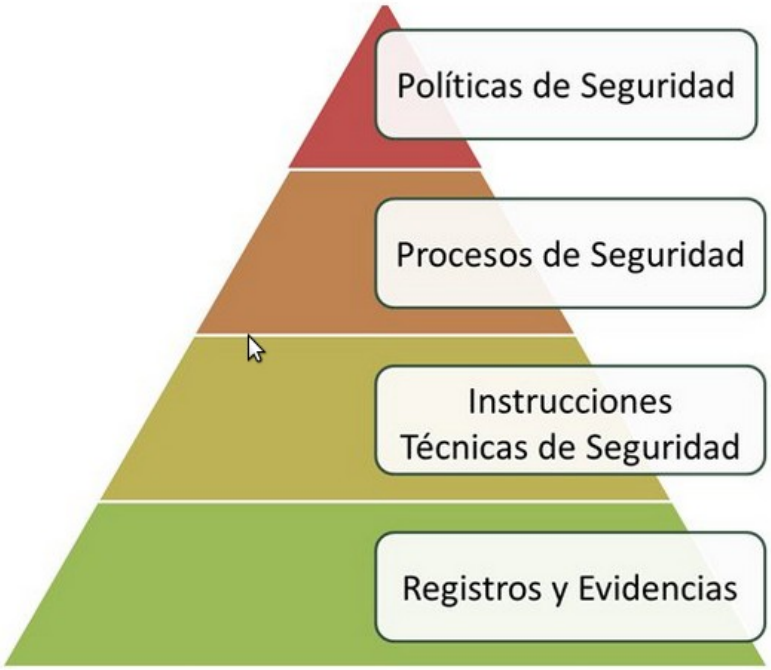


Figura1:Niveles de documentación ISO 27001

Figura 7: Nivells de documentació ISO 27001

Com podrem comprovar, i a tall d'exemple, els diferents nivells de documentació que requereix la certificació ISO27001 es poden classificar en diferents tipus de documents:

- **Polítiques de seguretat i normatives de seguretat:** Recullen directrius estratègiques, d'alt nivell, sota les quals s'empara qualsevol acció en matèria de seguretat de la informació. La resta de documents desenvoluparan les directrius de les polítiques aprovades. Del conjunt de possibles polítiques, trobarem la de política de seguretat de la informació. Alguns exemples de polítiques son:

    - Ús acceptable d'internet dins de l'empresa
    - Ús de dispositius mòbils corporatius
    - Política d'ús de dispositius mòbils no corporatius (BYOD)

- **Processos de seguretat:** Presenten un conjunt d'accions que cal dur a terme per a aconseguir un determinat objectiu i hi poden intervenir actors de diferents àrees o departaments. **Els procediments donen suport a la implantació d'una norma o guia**, per la qual cosa les normes o guies acostumen a referenciar procediments en el seu redactat. En són possibles exemples:

    - procediment de recepció de visites
    - procediment de sol·licitud de serveis
    - procediment de gestió d'incidències o d'escalat de peticions.

- **Manuals/Instruccions**: Són llistes de tasques o instruccions detallades per a fer determinades accions o utilitzar eines concretes. Acostumen a dependre de l'entorn tecnològic, de manera que s'han d'adaptar quan es produeixen canvis de producte o versió. Per exemple :

    - manuals d'ús d'eines o instruccions de configuració de programari
    - d'actualització de pegats, etc

- **Registres/Evidències**: Es tracta de documents que ens proporcionen les evidències objectives de l'observança dels requisits del SGSI. Formen part imprescindible del sistema de seguretat que s'implantarà, atès que demostrarà el funcionament i el compliment de les mesures de seguretat que s'estan implantant d'una manera fefaent.

4.3. **Llistat de documents demanats**

Tant l'ENS com la mateixa ISO / IEC 27001 defineixen quins són els documents necessaris per poder certificar el sistema, que dependrà del

document d'aplicabilitat de controls i mesures que s'han de desenvolupar. Tot i això, per al desenvolupament d'aquest TFM es demanen uns documents específics. A banda de la documentació que es demana, es proporciona un document addicional com a guia per la elaboració de la documentació del sistema gestor de documents.

Obs: La llista de documents són un subconjunt de tots els que es necessitaran si es vol assolir l'objectiu de certificar el nostre SGSI

GESTOR DOCUMENTAL

TÍTOL	**GUIA_GESTOR_DOCUMENTAL**
CODI	SGSI-RD-PR01-1.0
UBICACIÓ	/home/javera/TFM2021/ENTREGA/DEFINITIVO/ GESTOR_DOCUMENTAL/ GUIA_GESTOR_DOCUMENTAL.odt
DESCRIPCIÓ	Indicar de forma detallada l'estructura metodològica per a l'elaboració i codificació dels documents de el Sistema de Gestió de la documentació del SGSI de l'Ajuntament MISTIC
OBSERVACIONS	Aquest document **no és demanava,** però s'ha cregut important per poder tenir normes comunes a la redacció i presentació de tota la documentació del SGSI.

POLÍTICA DE SEGURETAT

TÍTOL	**POLÍTICA DE SEGURETAT**
CODI	SGSI-SI-PO01-1.0
UBICACIÓ	/home/javera/TFM2021/ENTREGA/DEFINITIVO/ POLITICA_SEGURETAT/POLITICA_SEGURETAT_AJSAB.odt
DESCRIPCIÓ	Normativa interna que ha de conèixer i complir tot el personal afectat per l'abast de el Sistema de Gestió de Seguretat de la Informació. El contingut de la Política ha de cobrir aspectes relatius a l'accés de la informació, ús de recursos de l'Organització, comportament en cas d'incidents de seguretat, etc.
OBSERVACIONS	En la política es fa referència expressa al Reial Decret que regula ENS per denotar l'obligatorietat del seu compliment.

GESTIÓ D'INDICADORS

TÍTOL	GUIA GESTIÓ INDICADORS
CODI	SGSI-GI-GU01-1.0
UBICACIÓ	/home/javera/TFM2021/ENTREGA/DEFINITIVO/ GESTIO_INDICADORS/GUIA_GESTIO_INDICADORS.odt
DESCRIPCIÓ	Guia a on s'explica com extreure les dades i el procés de generació d'indicadors pel nostre SGSI
OBSERVACIONS	Es basa en la definició de mètriques i indicadors de MAGERIT

TÍTOL	RELACIÓ INDICADORS
CODI	SGSI-GI-RE01-1.0
UBICACIÓ	/home/javera/TFM2021/ENTREGA/DEFINITIVO/ GESTIO_INDICADORS/RELACIO_INDICADORS.odt
DESCRIPCIÓ	Relació d'indicadors del nostre SGSI (només s'indiquen alguns a tall d'exemple). S'hauran de completar per obtenir un quadre de comandament real del nostre SGSI
OBSERVACIONS	CAP

PROCEDIMENT DE REVISIÓ PER DIRECCIÓ

TÍTOL	PROCEDIMENT REVISIÓ PER LA DIRECCIÓ
CODI	SGSI-RD-PR01-1.0
UBICACIÓ	/home/javera/TFM2021/ENTREGA/DEFINITIVO/ PROCEDIMENT_REVISIO_DIRECCIO/ PROCEDIMENT_REVISIO_DIRECCIO.odt
DESCRIPCIÓ	Procediment que es segueix per revisar l'estat del SGSI per part de la direcció.
OBSERVACIONS	CAP

GESTIÓ DE ROLS I RESPONSABLES

TÍTOL	GESTIÓ DE ROLS I RESPONSABILITATS
CODI	SGSI-GRLS-PR01-1.0

UBICACIÓ	/home/javera/TFM2021/ENTREGA/DEFINITIVO/ GESTIO_ROLS_I_RESPONSABILITATS/ GUIA_ROLS_I_RESPONSABILITATS.odt
DESCRIPCIÓ	- Procediment d'assignació de rols i responsabilitats en matèria de seguretat dins del nostre SGSI
OBSERVACIONS	- L'ENS especifica la definició de rols, responsabilitats i assignació dins de la política. - ISO27001 requereix un document específic.

METODOLOGIA GESTIÓ DE RISCOS

TÍTOL	**PROCEDIMENT D'ANÀLISI DE RISCOS**
CODI	SGSI-GU-AR-G01-1.0
UBICACIÓ	/home/javera/TFM2021/ENTREGA/DEFINITIVO/ GUIA_ANALISIS_DE_RISCOS/ PROCEDIMENT_ANALISIS_DE_RISCOS.odt
DESCRIPCIÓ	- Procediment a on es detallen les diferents fases i accions a realitzar en l'anàlisi i gestió de riscos.
OBSERVACIONS	- Es basa íntegrament en MAGERIT. S'ha intentat simplificar i resumin el mètode de MAGERIT per tal de tenir el procediment dins del nostre sistema documental propi, sense haver de referir-se a documents externs.

AUDITORIES INTERNES

- Programa d'auditories anual

TÍTOL	**GUIA PLA ANUAL AUDITORIA INTERNA**
CODI	SGSI-PA-G01-1.0
UBICACIÓ	/home/javera/TFM2021/ENTREGA/DEFINITIVO/ AUDITORIES_INTERNES/PLA_AUDITORIES/ GUIA_PLA_AUDITORIA.odt
DESCRIPCIÓ	Descriu el pla d'auditories anual interna que ha de seguir l'organització. Descriu la temporalització, responsables i auditories a realitzar durant l'any per fer la revisió del SGSI.
OBSERVACIONS	- Necessitarà SGSI-PPAI-RE01-1.0

TÍTOL	PLANTILLA PLANIFICACIÓ PROGRAMA AUDITORIES
CODI	SGSI-PPAI-RE01-1.0
UBICACIÓ	/home/javera/TFM2021/ENTREGA/DEFINITIVO/ AUDITORIES_INTERNES/PLA_AUDITORIES/ PLANTILLA_PLANIFICACIO_PROGRAMA_AUDITORIES.odt
DESCRIPCIÓ	Plantilla a on es registra la planificació anual del programa d'auditories.
OBSERVACIONS	CAP

- Auditories Internes

TÍTOL	PROCEDIMENT AUDITORIA INTERNA
CODI	SGSI-AI-PR01-1.0
UBICACIÓ	/home/javera/TFM2021/ENTREGA/DEFINITIVO/ PROCEDIMENT_AUDITORIA_INTERNA/ PROCEDIMENT_AUDITORIA_INTERNA.odt
DESCRIPCIÓ	Document que ha d'incloure una planificació de les tasques a realitzar, requisits que s'establiran als auditors interns.
OBSERVACIONS	- Necessitarà SGSI-PIAI-RE01-1.0 - Necessitarà SGSI-PPAI-RE02-1.0

TÍTOL	PLANTILLA INFORME AUDITORIA INTERNA
CODI	SGSI-PIAI-RE01-1.0
UBICACIÓ	/home/javera/TFM2021/ENTREGA/DEFINITIVO/ PROCEDIMENT_AUDITORIA_INTERNA/ PLANTILLA_INFORME_AUDITORIA.odt
DESCRIPCIÓ	Plantilla que s'omplirà amb els resultats de l'auditoria interna.
OBSERVACIONS	CAP

TÍTOL	PLANTILLA PLANIFICACIÓ AUDITORIA INTERNA
CODI	SGSI-PPAI-RE02-1.0
UBICACIÓ	/home/javera/TFM2021/ENTREGA/DEFINITIVO/ PROCEDIMENT_AUDITORIA_INTERNA/ PLANTILLA_PLANIFICACIO_AUDITORIA_INTERNA.odt
DESCRIPCIÓ	Plantilla que s'omplirà amb els resultats de la planificació de les

	auditories internes anuals.
OBSERVACIONS	CAP

DECLARACIÓ APLICABILITAT

TÍTOL	**DOCUMENT D'APLICABILITAT ESQUEMA NACIONAL DE SEGURETAT**
CODI	CODI: SGSI-GU-DO_APL_ENS-1.0
UBICACIÓ	DECLARACION_DE_APLICABILIDAD/ DOCUMENT_APLICABILITAT_ENS.pdf
DESCRIPCIÓ	Document que inclou tots els controls de seguretat establerts en l'Organització, amb el detall de la seva aplicabilitat, estat i documentació relacionada.
OBSERVACIONS	CAP

5. FASE 3: Estat del risc: Identificació i valoració de riscos – anàlisi de riscos.

5.1. Introducció

Quan es decideix protegir el nostre sistema d'informació hem de poder respondre a aquest seguit de preguntes:

- Què constitueix el nostre sistema d'informació ?. Amb això ens referim a allò que sustenta tots els processos de negoci que vam definir a l'abast del nostre SGSI. Ens referirem a aquests elements com els ***actius del nostre sistema d'informació.***

- A quines amenaces estan sotmesos els nostres actius ?. Considerarem amenaça com tot allò que pot degradar el valor/utilitat del nostre actiu. És important tenir present que el valor no es refereix tant al cost d'adquisició de l'actiu si no al fet de què ens aporta aquest actiu per aconseguir els objectius del nostre negoci.

- Quin impacte tindria la materialització d'una amenaça ?. Amb això ens referim en quin impacte tindria per la missió i objectiu de la nostra organització que es materialitzés l'amenaça que estem considerant.

- Amb quina probabilitat es pot materialitzar l'amenaça ?

Com es pot comprovar, el resultat de respondre a totes aquestes preguntes ens proporcionarà la situació de risc a la que està sotmès el nostre sistema d'informació. [7]

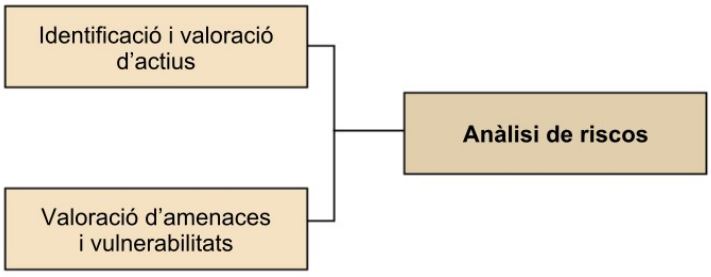


Figura 8: Anàlisi de riscos

És feina i tasca de l'anàlisi de riscos poder trobar les respostes a totes aquestes preguntes per, i en una fase posterior, gestionar aquests riscos

per sota d'un llindar de risc acceptable, llindar de risc que l'organització ha de prendre i decidir per a cada risc identificat.

L'anàlisi de riscos és l'eina a través de la qual es pot obtenir una visió clara i prioritzada dels riscos als quals s'enfronta una organització: té com a propòsit identificar els principals riscos als quals una organització està exposada, ja siguin desastres naturals , fallades en infraestructura o riscos introduïts pel propi personal (intencionats o no) [4].

METODOLOGIA MAGERIT [4]

Com es pot comprovar, la tasca de fer l'anàlisi i gestió de riscos és una tasca de considerable envergadura que només es pot realitzar si fem servir procés de gestió de riscos d'una manera metòdica. Existeixen diverses metodologies de gestió de riscos (EBIOS: https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/, per exemple) però nosaltres farem servir la metodologia MAGERIT per tal de poder-los gestionar.

MAGERIT és la metodologia d'anàlisi i gestió de riscos desenvolupada per un equip de el Comitè Tècnic de Seguretat dels Sistemes d'Informació i Tractament Automatitzat de Dades Personals de l'consell Superior d'Administració Electrònica. El nom de MAGERIT ve de Metodologia d'Anàlisi i GEstió de Riscos dels Sistemes d'Informació de les administracions públiques. Tot i el seu origen i orientació cap a les AAPP, també proporciona un marc vàlid per al desenvolupament d'anàlisi de riscos en entitats privades.

En el nostre cas es basarà en l'execució de l'anàlisi de riscos seguint la metodologia proposada a MAGERIT.

A més de fer servir la metodologia MAGERIT farem anar l'eina de gestió de riscos PILAR desenvolupada també pel Ministeri i que segueix la filosofia de MAGERIT, com no podia ser d'altra manera.

Tot això exposat prèviament ens permetrà conèixer una aproximació dels riscos seguint les següents pautes:

- Determinar els actius rellevants per a l'ajuntament, la seva interrelació i el seu valor en el cas de degradació i perjudicis associats.
- Determinar quins salvaguardes estan disponibles i la seva eficàcia.
- Estimar l'impacte, definit com el perjudici sobre l'actiu derivat de la materialització de l'amenaça.
- Estimar el risc, definit com l'impacte ponderat amb la taxa de freqüència (o expectativa de materialització) de l'amenaça.

5.2. Identificació d'actius

En aquesta fase del procés de gestió de riscos, identificarem els actius que sustenten els processos de negoci que es troben dins de l'abast del nostre sistema. Per poder realitzar una divisió dels actius, MAGERIT [4] proposa classificar-los en les següents categories:

- [S] - Serveis: Funció que satisfà una necessitat als usuaris. Poden ser anònims, al públic en general, a usuaris externs o a usuaris interns.

- [K] - Claus Criptogràfiques: S'utilitza per protegir el secret o autentificar les diferents parts d'una d'una comunicació. Són essencials per a garantir el funcionament dels mecanismes criptogràfics. Per exemple, claus privades de testimonis.

- [D] - Dades: Contenen la informació que permet a una organització prestar els seus serveis. És un actiu abstracte, com ara bases de dades, còpies de seguretat, etc.

- [SW] - Aplicacions informàtiques: Es gestionen, analitzen i transformen les dades permetent la explotació d'aquesta informació per a la prestació de serveis. Exemples: Antivirus, servidor de correu, sistemes operatius, etc.

- [COM] - Xarxes de comunicació: Mitjans de transport que transfereixen dades d'un lloc a un altre. Exemple: Xarxes, encaminadors, Internet, etc.

- [HW] - Maquinari: Mitjans materials físics destinats a suportar, directament o indirectament els serveis que presta l'organització. Exemple: PDA, servidor, etc.

- [Media] - Suports d'informació: Dispositius físics que permeten emmagatzemar informació de manera permanent o durant períodes llargs de temps. No obstant això, no són capaços de tractar la informació, únicament de emmagatzemar-la. Exemples: memòries USB, DVD, discs durs, etc.

- [AUX] - Equipament auxiliar: Elements de suport als sistemes de la informació sense estar relacionats directament amb el tractat de dades. Exemple: Sistemes d'alimentació, cablejat, etc.

- [L] - Instal·lacions: Llocs on s'allotgen els sistemes de la informació. Exemple: Centre de Processament de Dades.

- [P] - Personal: Persones vinculades als sistemes de la informació.

Per a cada actiu haurem de valorar l'impacte que tindria un incident de seguretat en cadascuna de les dimensions de seguretat: confidencialitat, integritat i disponibilitat (CID). També hauríem de valorar l'impacte sobre les dues altres dimensions: traçabilitat i autenticitat, o podem fer aquesta valoració fent servir la següent aproximació:

$$A = màx\ (C.I)$$
$$T = màx(C,i)$$

Per tal de facilitar la valoració dels actius, tant la metodologia MAGERIT com l'eina de suport PILAR ens permet **distingir entre actius essencials i no essencials.** Els actius essencials son aquells actius com la informació i els serveis prestats com organització, i que existeixen encara que la forma de prestar-se es modifiqui. Podem dir que **és allò que dona sentit a la missió de la nostre organització.**

Per un altre banda, tenim la resta d'actius que permeten implementar i que donen suport als actius essencials, de manera que els actius vénen a formar **arbres o grafs de dependències** on la seguretat dels actius que es troben més a dalt depenen dels que es troben més a baix o 'inferiors'. Aquestes estructures de dalt abaix reflecteixen aquestes dependències. En canvi, si les mirem de baix cap a dalt estaríem considerant la propagació del impacte que pugui passar en la materialització d'una amenaça (un actiu superior es veu afectat per l'incident de seguretat d'un actiu inferior).

El més habitual és definir les dependències entre actius seguint el següent diagrama:

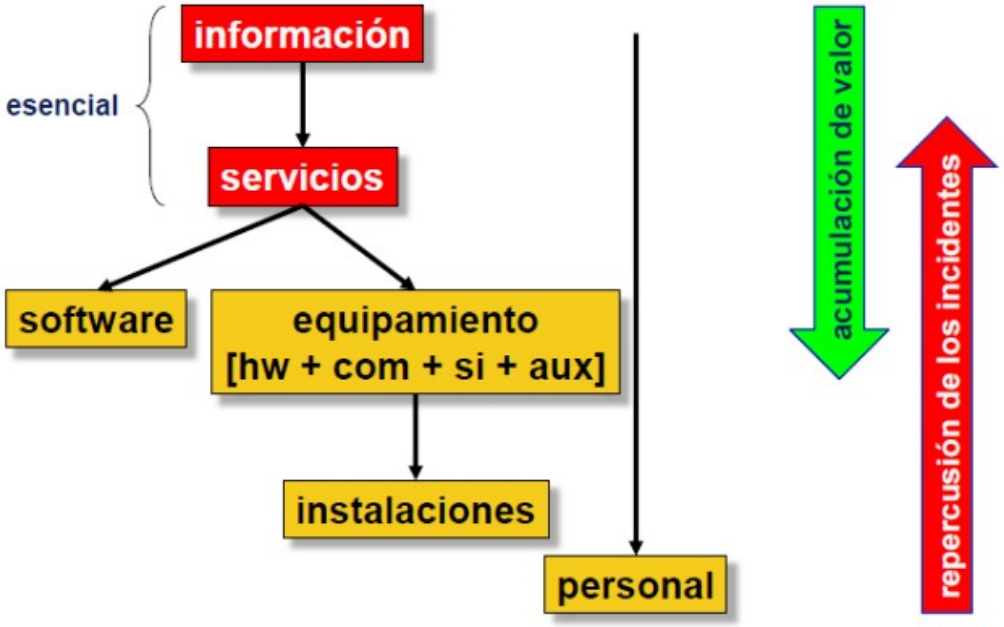


Figura 9: Dependències d'actius

Tot l'anàlisi de riscos s'ha realitzat amb l'eina PILAR i el detall de tot el projecte es pot consultar a l'arxiu de projecte que genera l'eina. Tot i això, comentarem alguns exemples del que podem trobar dins del projecte.

ACTIUS IDENTIFICATS

Hem fet servir els epígrafs que suggereix PILAR per separar els nostres actius. En el nostre cas, podem identificar els següents actius:

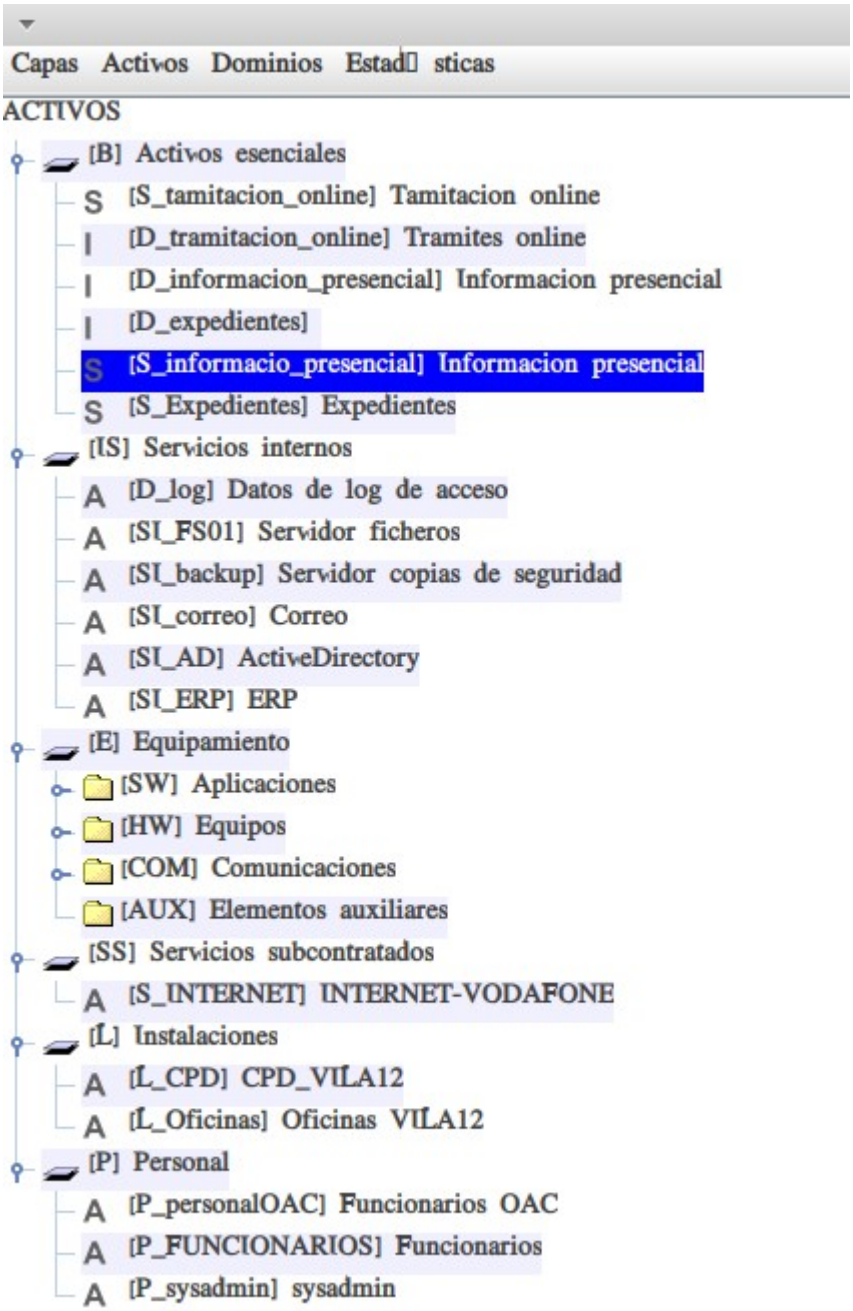


Figura 10: PILAR - Actius identificats (1/2)

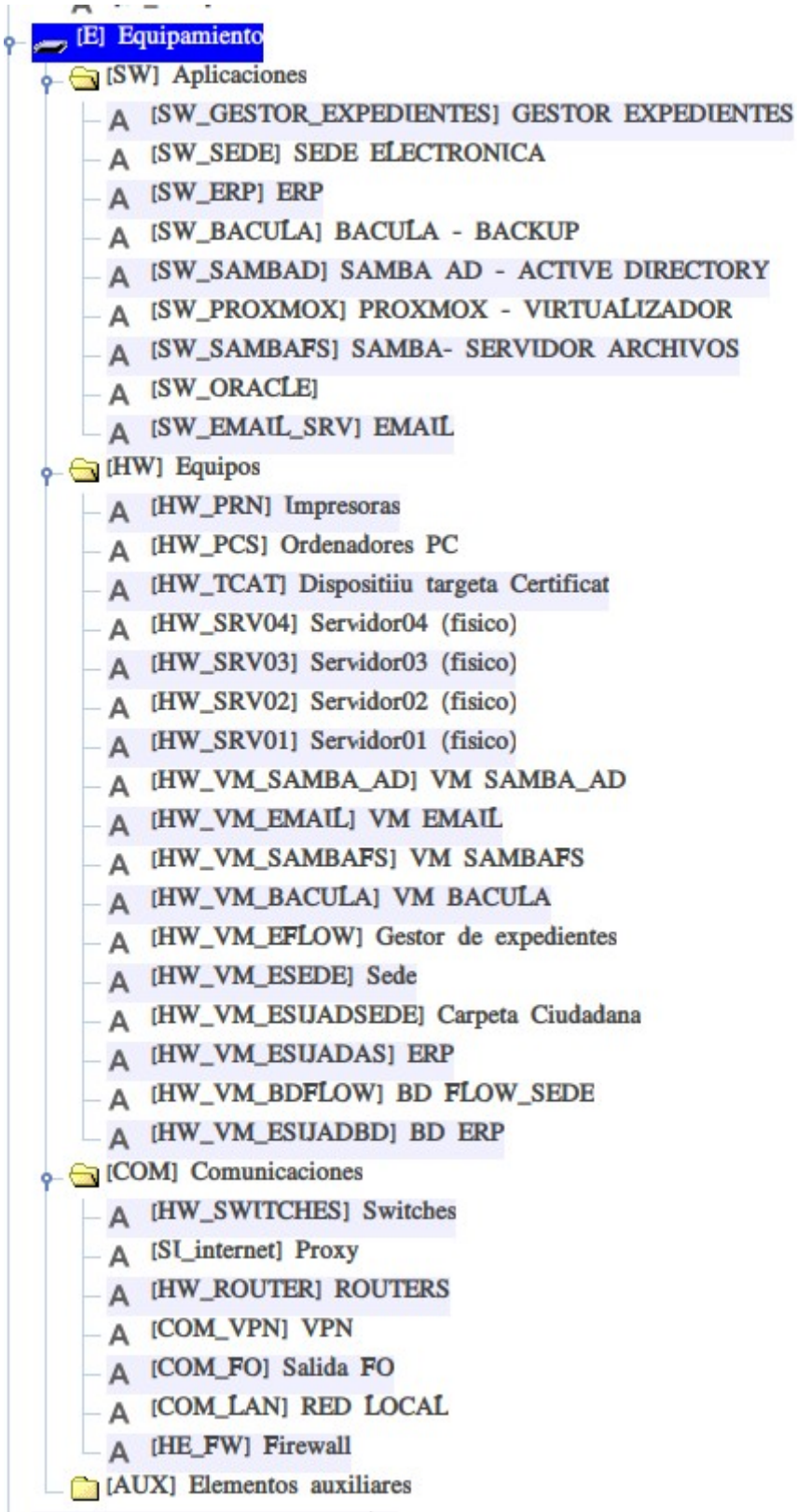


Figura 11: PILAR - actius identificats (2/2)

Com podem comprovar, s'han estructurat seguin les recomanacions que MAGERIT ens indica, diferenciant entre actius essencials i de suport.

CARACTERITZACIÓ DELS ACTIUS

Per tal de poder fer servir el catàleg d'amenaces de MAGERIT haurem de caracteritzar i/o classificar els diferents actius segons la seva tipologia (software, hardware, xarxa, etc ..).

Posarem com a exemple la caracterització de la màquina virtual que s'encarrega de gestionar la base de dades d'expedients

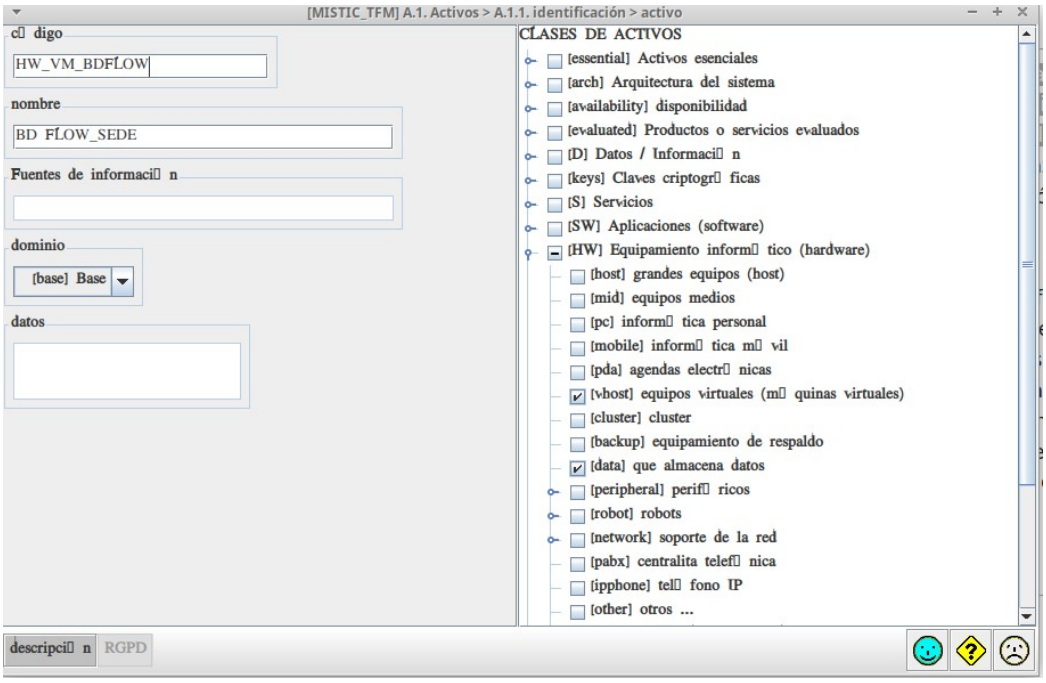


Figura 12: PILAR - Caracterització dels actius

Com es pot veure a la imatge, a la part de la dreta hem indicat que es tracta d'un vhost (equip virtual) i que emmagatzema dades. D'aquesta manera, PILAR seleccionarà el conjunt d'amenaces que poden afectar a l'actiu.

Tota la resta d'actius s'han caracteritzat de la mateixa manera, i es troba al projecte de MAGERIT que s'annexa a la memòria del TFM.

DEPENDÈNCIES D'ACTIUS

Com ja hem comentat, podem realitzar l'anàlisi de riscos construint les dependències entre actius per tal de poder valorar els impactes de que tenen la materialització d'una amenaça en un actiu i com afecta als altres actius que hi depenen.

A la següent figura podem veure un exemple d'aquesta dependència (en aquest cas, s'ha desplegat l'actiu essencial per observar el conjunt de dependències per capes que hi tenen).

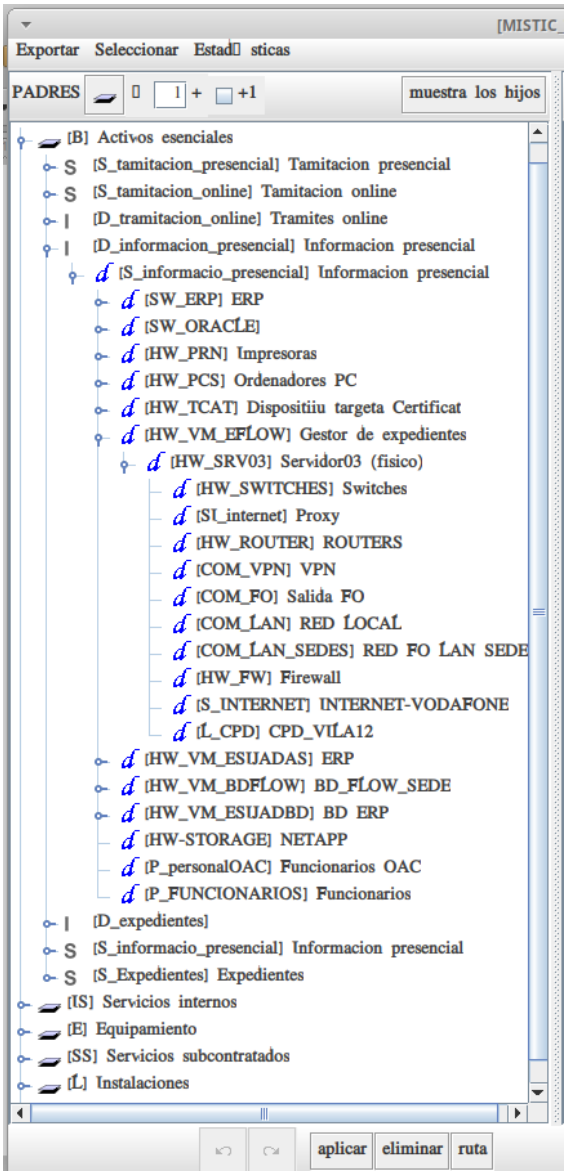


Figura 13: PILAR - dependències entre actius

També podem extreure diferents representacions visuals d'aquestes dependències. Podem veure el cas del servei de tramitació online en una representació de les dependències en bloc.

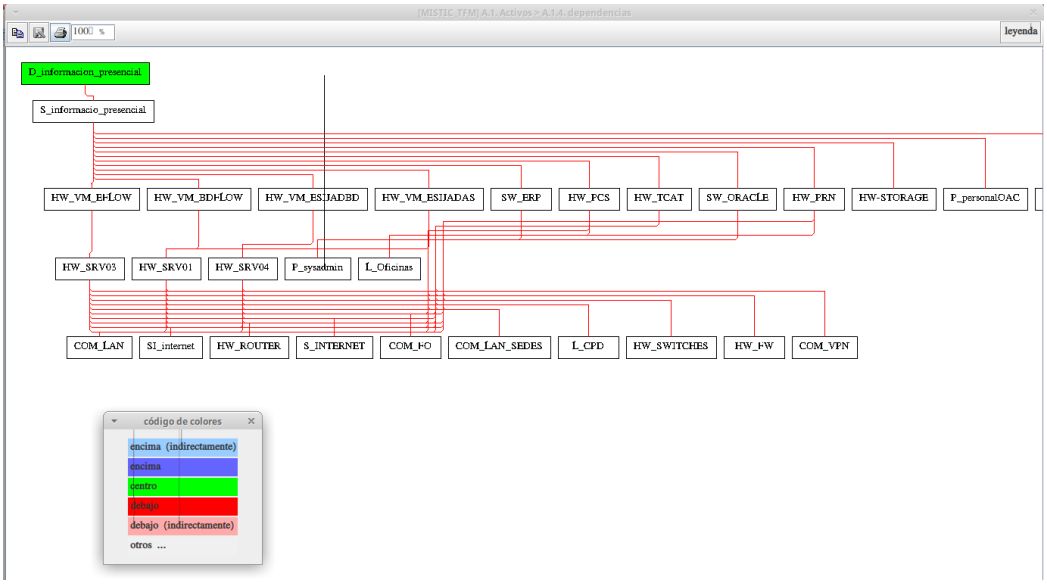


Figura 14: PILAR - dependències actius (diagrama bloc)

VALORACIÓ DELS ACTIUS

Com ja hem comentat anteriorment, es poden distingir les següents dimensions/dominis de seguretat: [4]

[D] - Disponibilitat: Propietat o característica dels actius. Consisteix en que les entitats o processos autoritzats tenen accés als actius quan es requereixen.

[I] - Integritat de les dades: Característica que indicaria que l'activitat d'informació no ha estat alterat de manera no autoritzada.

[C] - Confidencialitat: Propietat consistent en que la informació no es posa a disposició ni es revela a entitats o processos no autoritzats.

[A] - Autenticitat: Propietat que consisteix en que la entitat, individual o procés és qui dóna ser, o garanteix la font de dades.

[T] - Traçabilitat: Característica que consisteix en les actuacions d'una entitat que poden ser imputades en aquesta entitat o subjecte.

En aquest punt haurem de valorar per a cada actiu com és afectat la materialització d'una amenaça per a cadascuna de les dimensions anteriors.

OBS: La versió que s'ha instal·lat de PILAR està caracteritzada per a l'ENS, i els criteris seran de tipus B,M i A. D'aquesta manera el sistema queda ja categoritzat sota els criteris que requereix l'ENS.

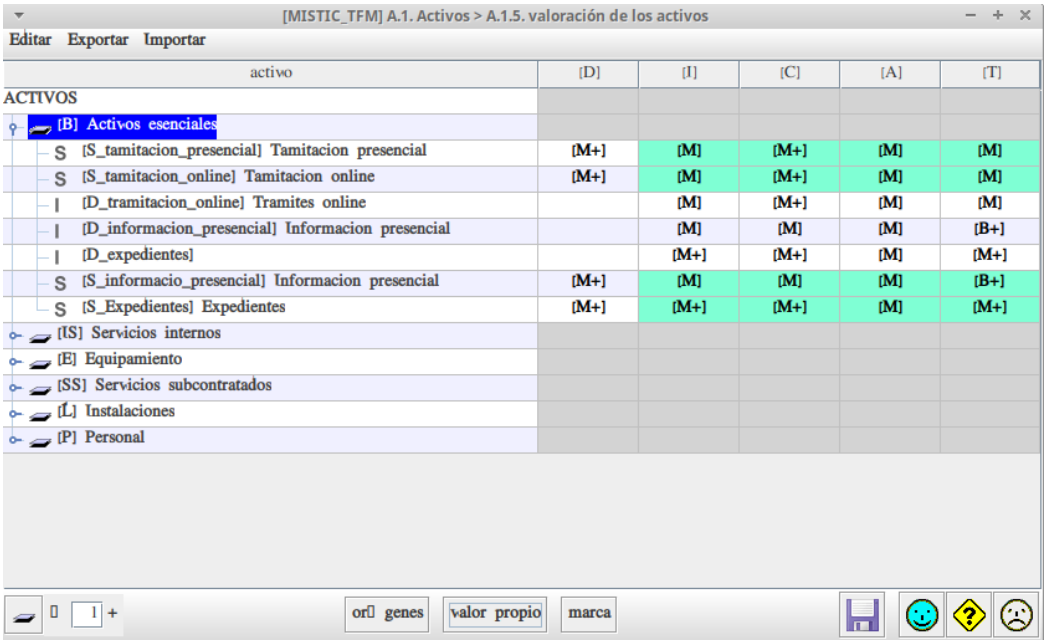


Figura 15: PILAR - Valoració dels actius essencials

Podem veure com les dependències van propagant les valoracions de manera acumulada als actius de sota.

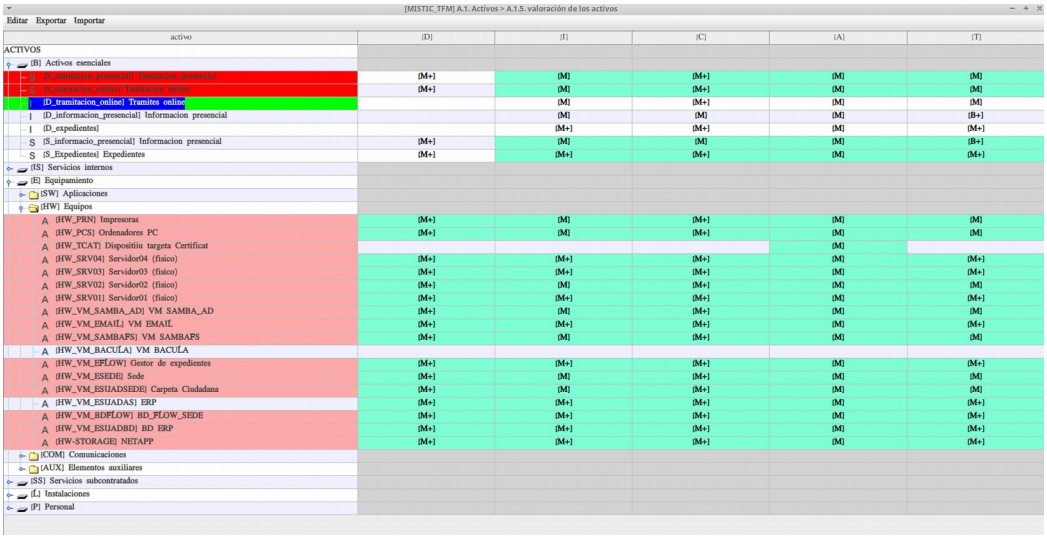


Figura 16: PILAR - Propagació de la valoració entre actius

5.3. Estudi de les amenaces

Com ja hem comentat, MAGERIT incorpora un conjunt d'amenaces que podem fer servir de manera inicial per poder avaluar els riscos del nostre sistema. Fent servir l'eina PILAR podem aplicar de manera automàtica el conjunt d'amenaces als nostres actius.

De fet, PILAR classifica les amenaces en 4 grups:

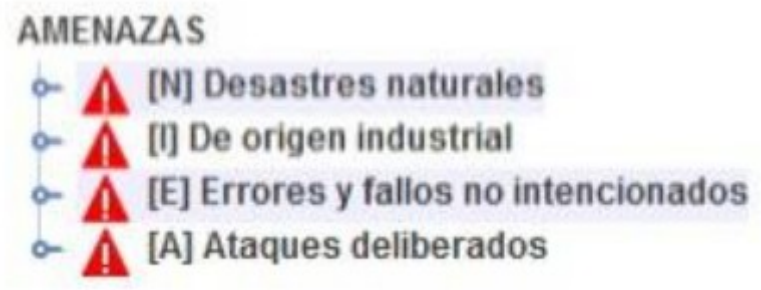


Figura 17: PILAR - Grups d'amenaces

A més, PILAR ens permet incorporar alguns factors que agreugen o alleugen les amenaces disponibles al catàleg. En el nostre cas, hem seleccionat un conjunt de factors que modelen i s'ajusten la nostra organització d'estudi.

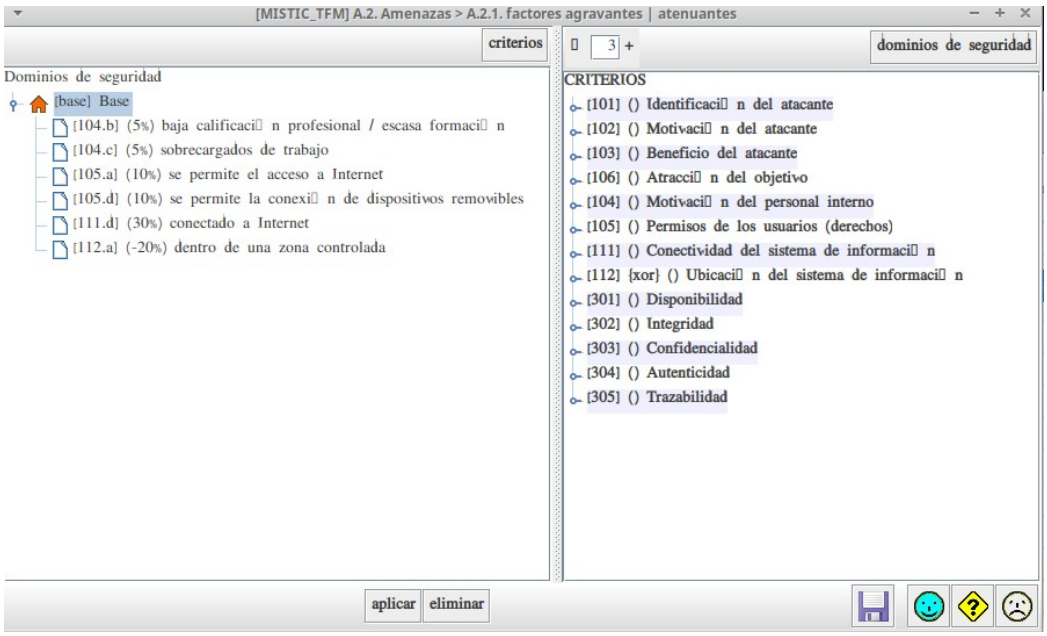
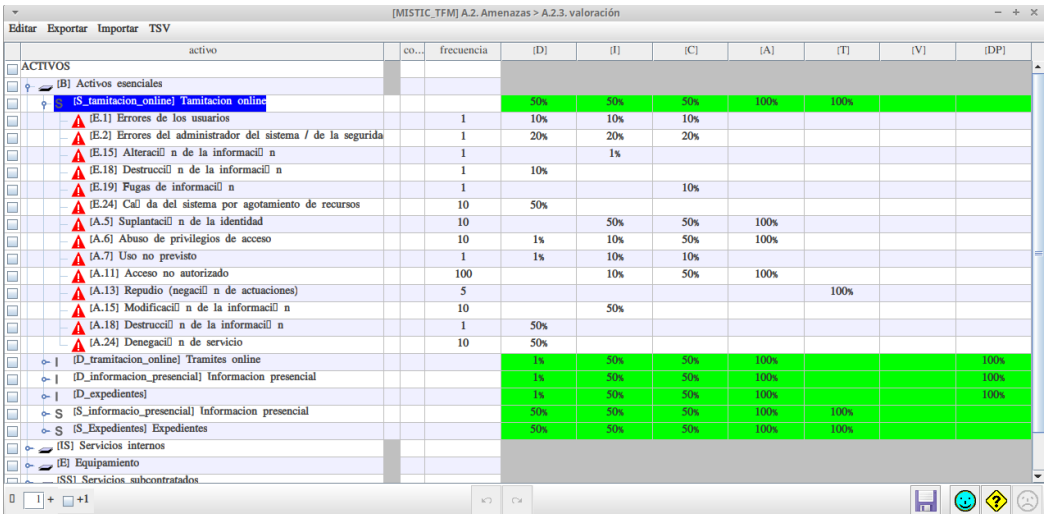


Figura 18: PILAR - Factors agravants de la nostra organització

A continuació mostrem un exemple de les amenaces que ens modela PILAR pel nostre sistema.



activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS									
[B] Activos esenciales									
[S_tamitacion_online] Tamitacion online			50%	50%	50%	100%	100%		
[E.1] Errores de los usuarios		1	10%	10%	10%				
[E.2] Errores del administrador del sistema / de la segurida		1	20%	20%	20%				
[E.15] Alteraci n de la informaci n		1		1%					
[E.18] Destrucci n de la informaci n		1	10%						
[E.19] Fugas de informaci n		1			10%				
[E.24] Ca da del sistema por agotamiento de recursos		10	50%						
[A.5] Suplantaci n de la identidad		10		50%	50%	100%			
[A.6] Abuso de privilegios de acceso		10	1%	10%	50%	100%			
[A.7] Uso no previsto		1	1%	10%	10%				
[A.11] Acceso no autorizado		100		10%	50%	100%			
[A.13] Repudio (negaci n de actuaciones)		5					100%		
[A.15] Modificaci n de la informaci n		10		50%					
[A.18] Destrucci n de la informaci n		1	50%						
[A.24] Denegaci n de servicio		10	50%						
[D_tramitacion_online] Tramites online			1%	50%	50%	100%			100%
[D_informacion_presencial] Informacion presencial			1%	50%	50%	100%			100%
[D_expedientes]			1%	50%	50%	100%			100%
[S_informacio_presencial] Informacion presencial			50%	50%	50%	100%	100%		
[S_Expedientes] Expedientes			50%	50%	50%	100%	100%		
[IS] Servicios internos									
[E] Equipamiento									
[SS] Servicios subcontratados									

Figura 19: PILAR - Amenaces al servei de tramitació online

Com podem comprovar amb la següent figura, les amenaces son diferents depenent del tipus d'actiu

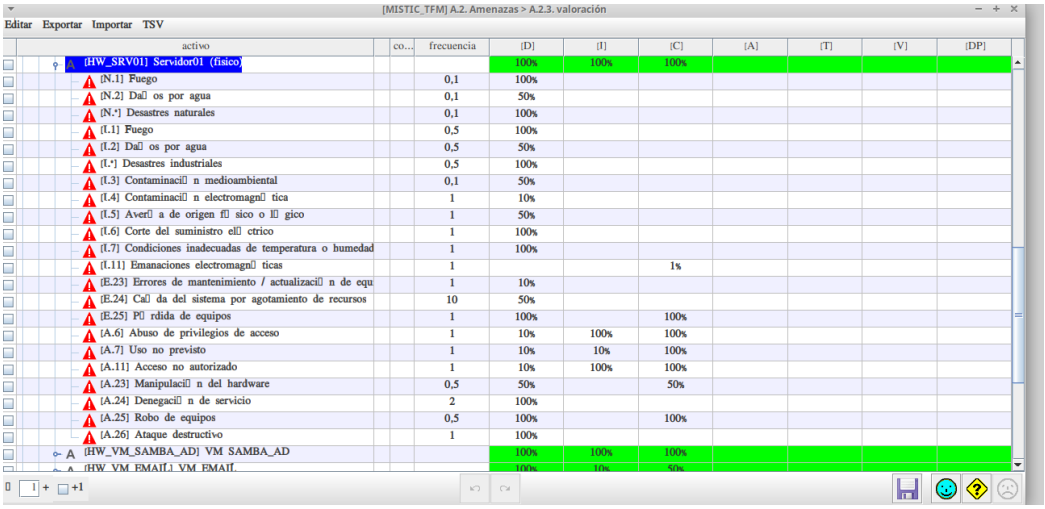


Figura 20: PILAR - Amenaces a un servidor

Cal mencionar que PILAR ens proposa, a més de una llista d'amenaces, tant la probabilitat d'ocurrència d'una possible amenaça, així com la degradació en el valor de l'actiu respecte a cadascuna de les dimensions de seguretat, facilitant la primera versió d'anàlisi de riscos notablement.

A tall d'exemple, podem presentar una taula per un actiu essencial amb les amenaces detectades:

[S_tamitacion_online] Tamitacion online

amenaza	frecuencia	[D]	[I]	[C]	[A]	[T]
[E.1] Errores de los usuarios	1	10%	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	-	-
[E.15] Alteración de la información	1	-	1%	-	-	-
[E.18] Destrucción de la información	1	10%	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[A.5] Suplantación de la identidad	10	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	10	1%	10%	50%	100%	-
[A.7] Uso no previsto	1	1%	10%	10%	-	-

[A.11] Acceso no autorizado	100	-	10%	50%	100%	-
[A.13] Repudio (negación de actuaciones)	5	-	-	-	-	100%
[A.15] Modificación de la información	10	-	50%	-	-	-
[A.18] Destrucción de la información	1	50%	-	-	-	-
[A.24] Denegación de servicio	10	50%	-	-	-	-

Taula 29: PILAR - Amenaces del servei essencial tràmits online

Amb la identificació dels actius, i la caracterització dels mateixos que hem realitzat podem fer servir (com ja hem vist) el catàleg d'amenaces que incorpora l'eina PILAR, juntament amb la freqüència de cada tipus d'amenaça i l'impacte sobre cada dimensió de seguretat de que disposa l'actium poden calcular els riscos del nostre sistema.

RISC = PROBABILITAT x IMPACTE

Com podem comprovar, el risc està associat a la probabilitat de la materialització d'una amenaça així com l'impacte en la degradació del nostre actiu, entenent degradació com la pèrdua de valor de l'actiu en la consecució dels objectius del negoci.

L'aplicació de salvaguardes dins del nostre sistema poden fer minvar la probabilitat d'ocurrència de l'amenaça i/o l'impacte sobre l'organització.

Si fem el càlcul dels riscos **sense tenir en compte cap salvaguarda, obtindrem el RISC INTRÍNSEC**. Podem veure un exemple del mapa de riscos intrínsecs dels nostres actius essencials a la següent figura:

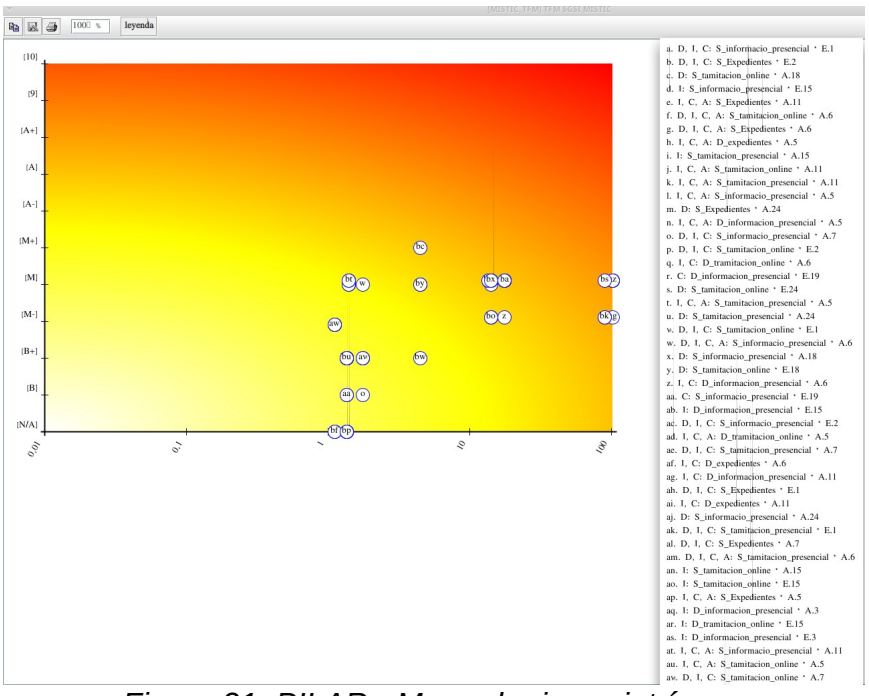


Figura 21: PILAR - Mapa de riscos intrínsec

També podem explorar els riscos intrínsecs de manera tabular:

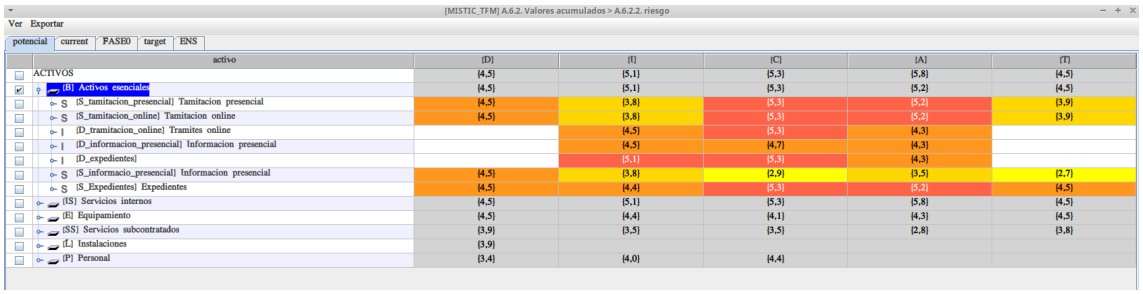


Figura 22: PILAR - Llistat de riscos intrínsec

Podem fer servir la següent escala de criticitat per tal d'entendre visualment la importància de cada risc identificat.

Figura 23: PILAR - Nivells de criticitat dels risc

5.4. Valoració salvaguardes implementades

La nostra organització no parteix d'una situació de zero sense cap aplicació de cap mesura de seguretat. Això és, ja té implementat un conjunt de mesures de seguretat que poden reduir inicialment el risc intrínsec que tenen les possibles amenaces contra els actius identificats.

Per tal que es tinguin en compte, poden aplicar-les en dos punts diferents: o com a salvaguarda o dins de l'apartat de perfils de seguretat que proporciona PILAR.

Aplicació en el cas de salvaguardes

Ho podem aplicar fent servir l'apartat A.3.

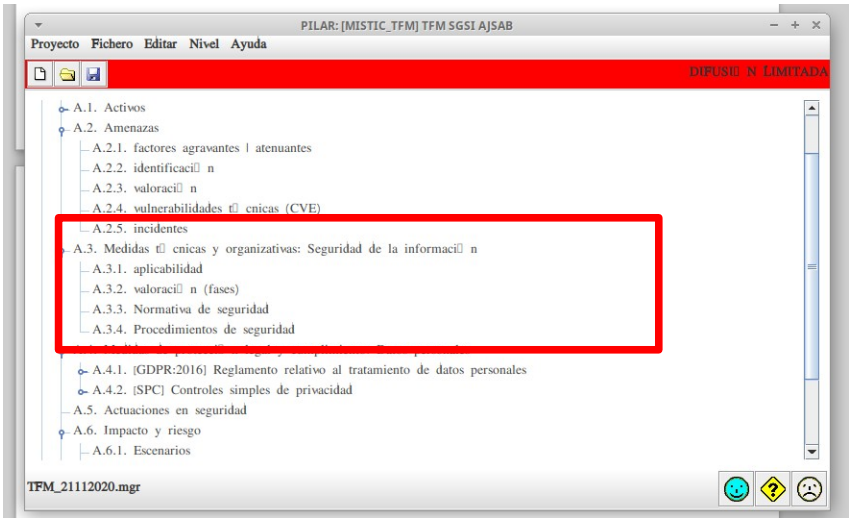


Figura 24: PILAR - Aplicació de salvaguardes

Aquí ens apareixen un conjunt de mesures tant tècniques com organitzatives que haurem d'especificar el seu nivell de maduresa CMM.

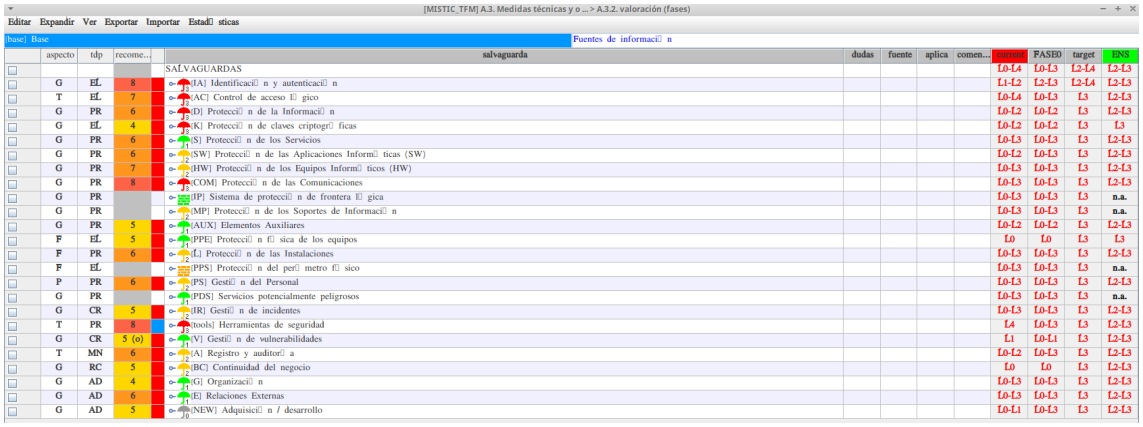


Figura 25: PILAR - Salvaguardes aplicades

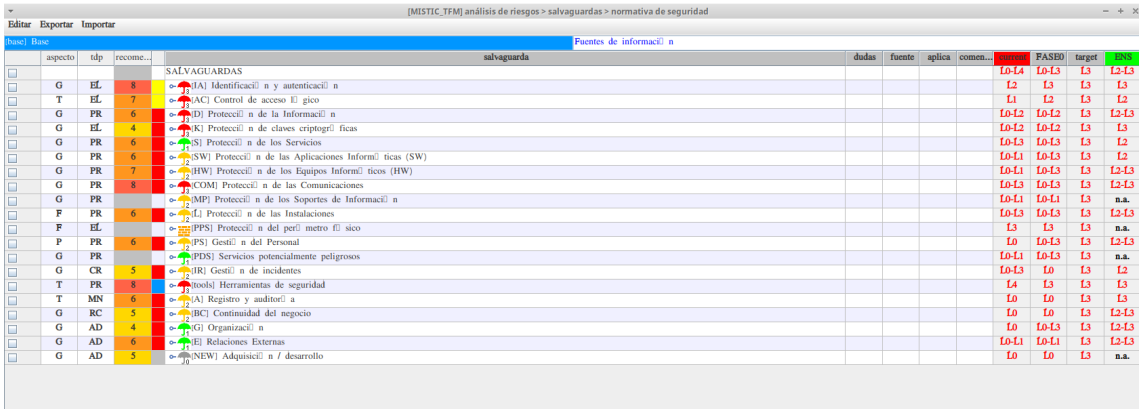


Figura 26: PILAR - Normativa de seguretat

Figura 27: PILAR - Procediments de seguretat

Aplicació en el cas de perfils de seguretat

Com ja hem comentat, també podem especificar quines salvaguardes tenim actualment en aplicació en funció d'uns controls predefinits dins d'uns perfils de

seguretat. En el nostre cas, farem servir els perfils de seguretat de l'ENS i de la ISO27002 a on es recullen els controls que contemplen cadascuna de les normes, indicant par a cadascun dels controls el seu grau de maduresa en la seva implantació.

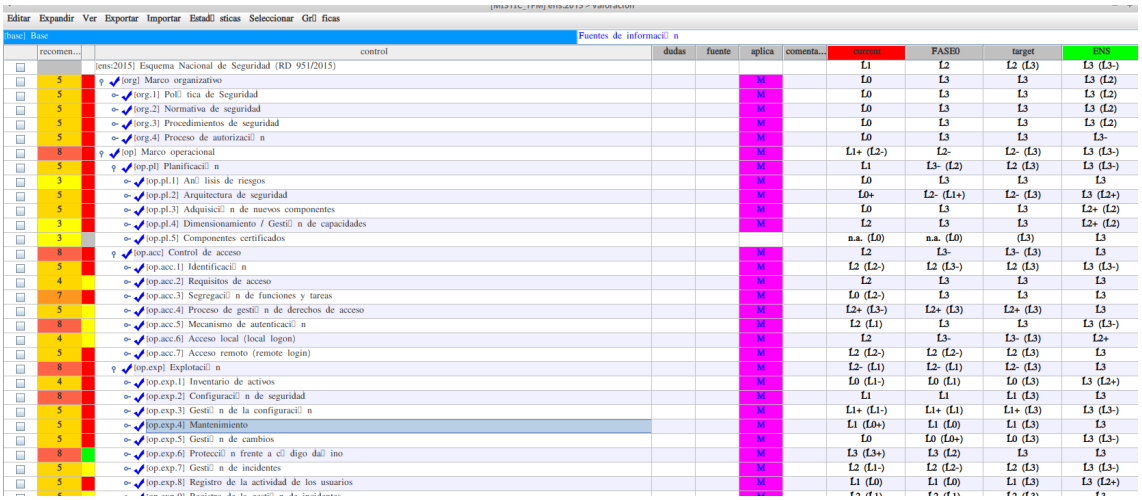


Figura 28: PILAR - Aplicació del perfil de seguretat ENS

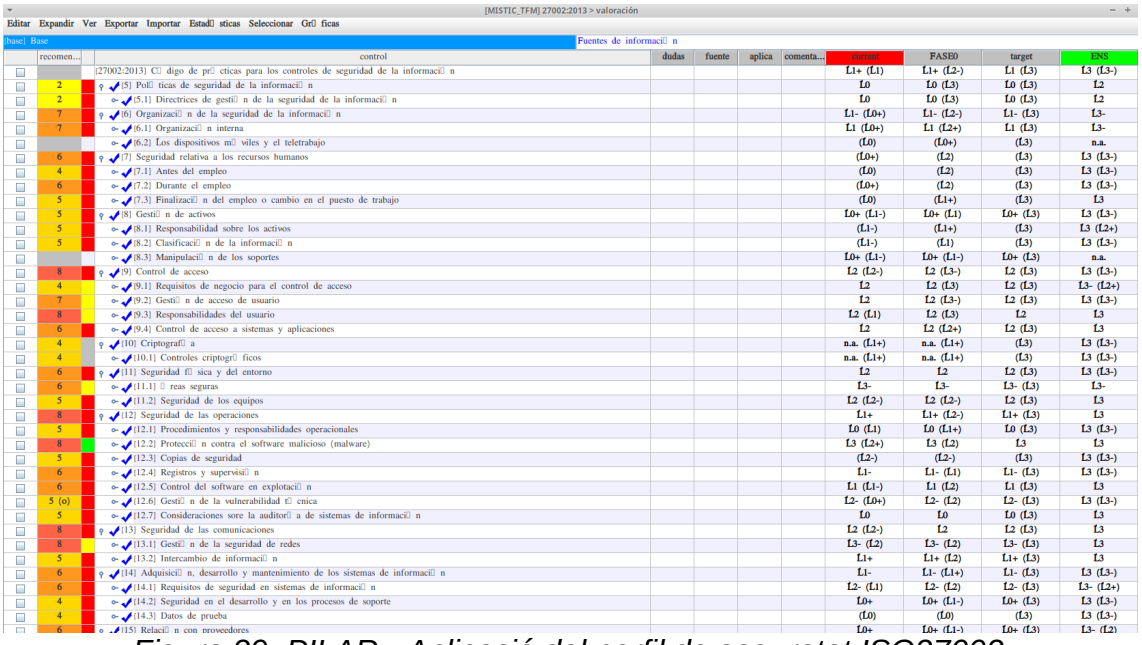


Figura 29: PILAR - Aplicació del perfil de seguretat ISO27002

5.5. VALORACIÓ IMPACTE/ NIVELL DE RISC RESIDUAL

Abans de poder veure el valor del nivell de risc residual que tenim un cop aplicades les salvaguardes, hem d'explicar l'aproximació que realitza l'eina PILAR en la gestió de les fases del projectes

PILAR: FASES DE PROJECTE i RISC DE CADA FASE

Amb PILAR podem definir diferents fases per tal de poder descriure quina és la situació del nostre sistema en un determinant moment. Hi han algunes fases predeterminades com:

- potential: És la fase potencial i descriu la situació del sistema sense aplicació de cap salvaguarda. És la que hem fet servir prèviament per tal de definit el nivell de risc intrínsec. No es pot escollir aquesta fase per especificar quines salvaguardes tenim aplicades, atès que perdria el seu sentit (recordem que és el risc intrínsec).

- **current:** És la fase actual i modela la situació del sistema realment (és a dir, a dia d'avui). Aquesta fase es podrà escollir per determinar quines salvaguardes tenim aplicades.

- target: És una situació o fase a la que volem arribar. La podem escollir en l'aplicació de perfils i salvaguardes per tal de definir-nos un objectiu, i poder determinar com de lluny o a prop estem del seu compliment.

- ENS: Només tindrem aquesta fase si tenim aplicat el perfil de ENS dins de PILAR. Especifica els nivells de compliment (o de maduresa) dels diferents controls que l'ENS necessita. Podríem pensar que és com una fase tipus target però adaptada al compliment de l'ENS.

Una vegada hem explicat el funcionament de les fases, i hem caracteritzat els actius i associat les amenaces a cadascú d'ells, haurem de valorar la situació dels risc que ens queda amb les salvaguardes que tenim desplegades seleccionant la fase *current*.

Explorarem el risc residual tant amb la vessant del risc acumulat com la del risc repercutit. Per tal de fer-ho, extraurem una representació dels mateixos de manera tabular i en un mapa de riscos. Aquestes representacions assignaran un color per a cada risc en funció del perill que te associat seguint el següent esquema de colors:

Figura 30: PILAR - Escala de criticitat

[MISTIC_TFM] A.6.2. Valores acumulados > A.6.2.2. riesgo

Ver Exportar

potencial | current | PASE0 | target | ENS

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[2,4]	[3,6]	[3,7]	[4,2]	[2,4]
[B] Activos esenciales	[2,2]	[3,5]	[3,7]	[3,6]	[2,4]
[S_tamitacion_presencial] Tamitacion presencial	[2,2]	[2,2]	[3,7]	[3,6]	[1,8]
[S_tamitacion_online] Tamitacion online	[2,2]	[2,2]	[3,7]	[3,6]	[1,8]
[D_tramitacion_online] Tramites online		[2,9]	[3,7]	[2,4]	
[D_informacion_presencial] Informacion presencial		[2,9]	[3,1]	[2,4]	
[D_expedientes]		[3,5]	[3,7]	[2,4]	
[S_informacio_presencial] Informacion presencial	[2,1]	[2,2]	[1,3]	[1,9]	[0,86]
[S_Expedientes] Expedientes	[2,2]	[2,8]	[3,7]	[3,6]	[2,4]
[IS] Servicios internos	[2,2]	[3,6]	[3,7]	[4,2]	[2,4]
[D_privilegios] Datos con los privilegios de acceso	[2,2]	[2,8]	[3,7]	[4,2]	[2,4]
[D_log] Datos de log de acceso	[2,2]	[3,6]	[3,7]	[4,2]	[2,4]
[SI_FS01] Servidor ficheros	[1,5]				
[SI_backup] Servidor copias de seguridad	[1,5]				
[SI_correo] Correo	[1,5]	[0,89]			
[SI_AD] ActiveDirectory	[1,5]				
[SI_ERP] ERP	[1,5]				
[E] Equipamiento	[2,4]	[2,8]	[2,2]	[2,7]	[2,1]
[SW] Aplicaciones	[1,6]	[1,7]	[1,7]		
[HW] Equipos	[2,2]	[2,1]	[2,2]	[2,7]	
[HW_PRN] Impresoras	[0,88]	[0,73]	[1,5]		
[HW_PCS] Ordenadores PC	[0,93]	[1,6]	[2,2]		
[HW_TCAT] Dispositiiu targeta Certificat				[2,7]	
[HW_SRV04] Servidor04 (fisico)	[2,2]	[2,1]	[2,1]		
[HW_SRV03] Servidor03 (fisico)	[2,2]	[2,1]	[2,1]		
[HW_SRV02] Servidor02 (fisico)	[2,2]	[1,5]	[2,1]		
[HW_SRV01] Servidor01 (fisico)	[2,2]	[2,1]	[2,1]		
[HW_VM_SAMBA_AD] VM SAMBA_AD	[2,2]	[1,5]	[2,1]		
[HW_VM_EMAIL] VM EMAIL	[2,2]	[0,85]	[1,5]		
[HW_VM_SAMBAFS] VM SAMBAFS	[2,2]	[0,73]	[1,5]		
[HW_VM_EFLOW] Gestor de expedientes	[2,2]	[0,85]	[1,5]		
[HW_VM_ESEDE] Sede	[2,2]	[0,73]	[1,5]		
[HW_VM_ESUADSEDE] Carpeta Ciudadana	[2,2]	[0,73]	[1,5]		
[HW_VM_ESUADAS] ERP	[2,2]	[0,85]	[1,5]		
[HW_VM_BDFLOW] BD_FLOW_SEDE	[2,2]	[2,1]	[2,1]		
[HW_VM_ESUADBD] BD ERP	[2,2]	[2,1]	[2,1]		
[HW-STORAGE] NETAPP	[2,2]	[2,1]	[2,1]		
[COM] Comunicaciones	[2,4]	[2,8]	[1,9]	[1,9]	[2,1]
[SS] Servicios subcontratados	[1,9]	[1,3]	[1,3]	[0,89]	[1,4]
[L] Instalaciones	[2,0]				
[P] Personal	[1,3]	[1,8]	[2,4]		

Taula 30: PILAR - Risc actual acumulat

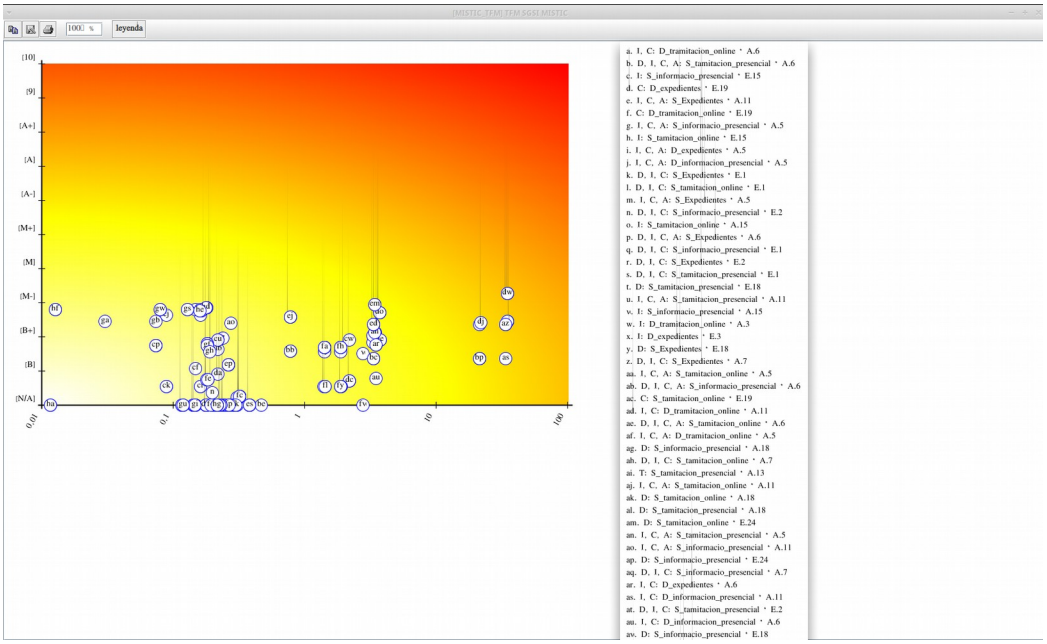
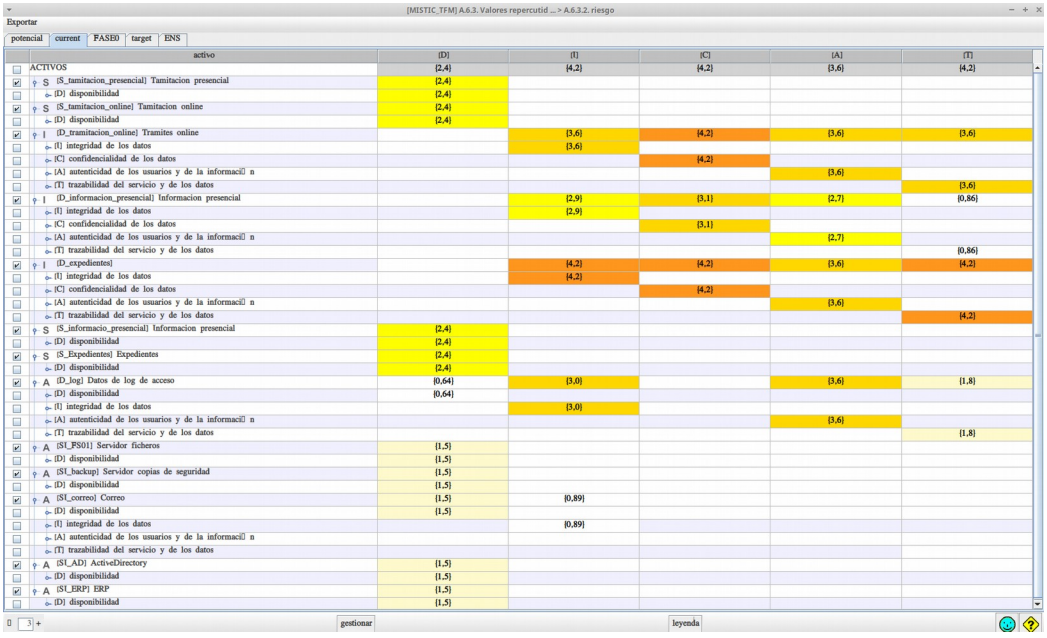
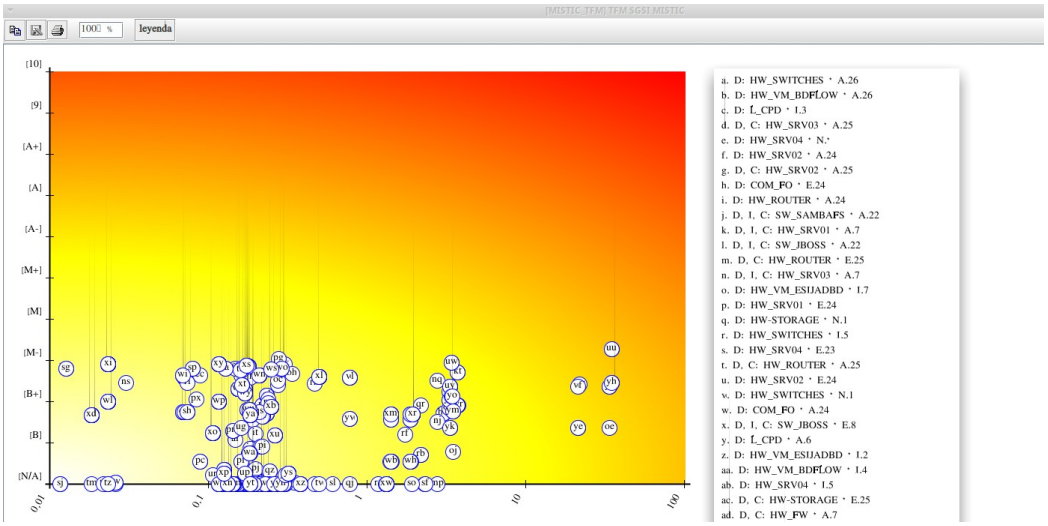


Figura 31: PILAR - Figura mapa risc actual acumulat



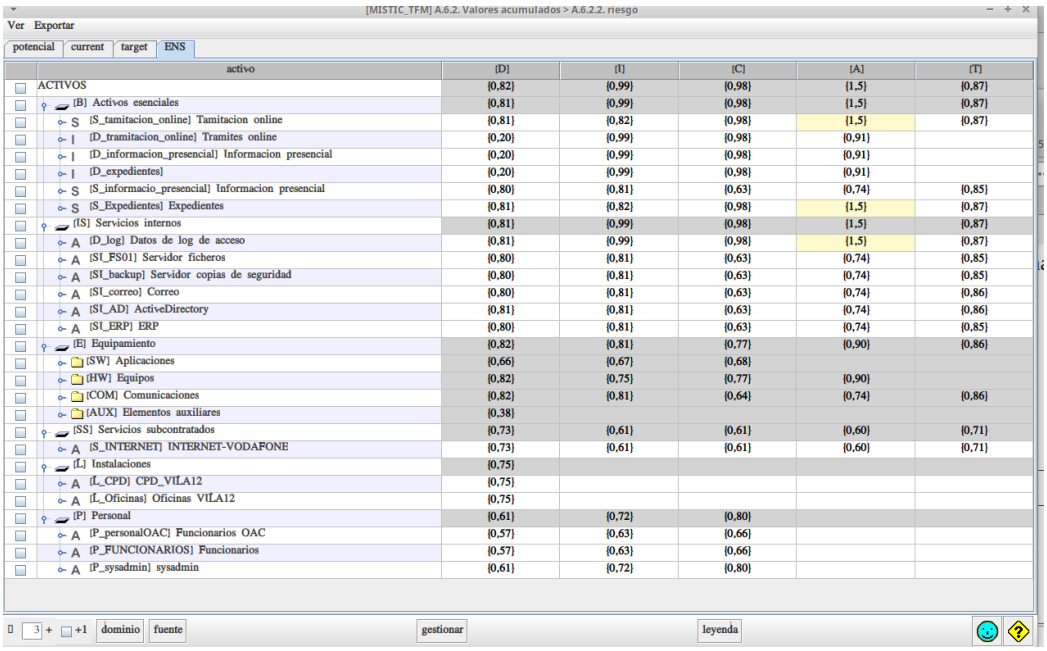
activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[2,4]	[4,2]	[4,2]	[3,6]	[4,2]
S [S_tamitacion_presencial] Tamitacion presencial	[2,4]				
[D] disponibilidad	[2,4]				
S [S_tamitacion_online] Tamitacion online	[2,4]				
[D] disponibilidad	[2,4]				
I [D_tramitacion_online] Tramites online		[3,6]	[4,2]	[3,6]	[3,6]
[I] integridad de los datos		[3,6]			
[C] confidencialidad de los datos			[4,2]		
[A] autenticidad de los usuarios y de la informaci□ n				[3,6]	
[T] trazabilidad del servicio y de los datos					[3,6]
I [D_informacion_presencial] Informacion presencial		[2,9]	[3,1]	[2,7]	[0,86]
[I] integridad de los datos		[2,9]			
[C] confidencialidad de los datos			[3,1]		
[A] autenticidad de los usuarios y de la informaci□ n				[2,7]	
[T] trazabilidad del servicio y de los datos					[0,86]
I [D_expedientes]		[4,2]	[4,2]	[3,6]	[4,2]
[I] integridad de los datos		[4,2]			
[C] confidencialidad de los datos			[4,2]		
[A] autenticidad de los usuarios y de la informaci□ n				[3,6]	
[T] trazabilidad del servicio y de los datos					[4,2]
S [S_informacio_presencial] Informacion presencial	[2,4]				
[D] disponibilidad	[2,4]				
S [S_Expedientes] Expedientes	[2,4]				
[D] disponibilidad	[2,4]				
A [D_log] Datos de log de acceso	[0,64]	[3,0]		[3,6]	[1,8]
[D] disponibilidad	[0,64]				
[I] integridad de los datos		[3,0]			
[A] autenticidad de los usuarios y de la informaci□ n				[3,6]	
[T] trazabilidad del servicio y de los datos					[1,8]
A [SI_FS01] Servidor ficheros	[1,5]				
[D] disponibilidad	[1,5]				
A [SI_backup] Servidor copias de seguridad	[1,5]				
[D] disponibilidad	[1,5]				
A [SI_correo] Correo	[1,5]	[0,89]			
[D] disponibilidad	[1,5]				
[I] integridad de los datos		[0,89]			
[A] autenticidad de los usuarios y de la informaci□ n					
[T] trazabilidad del servicio y de los datos					
A [SI_AD] ActiveDirectory	[1,5]				
[D] disponibilidad	[1,5]				
A [SI_ERP] ERP	[1,5]				
[D] disponibilidad	[1,5]				

Taula 31: PILAR - risc actual repercutit



Taula 32: PILAR - Mapa risc actual repercutit

Amb les anteriors figures hem pogut veure els riscos actuals. Com podem observar, tenim riscos en ***«zones calentes»*** **que l'organització considera que no son acceptables i que haurem de gestionar** aquests riscos per arribar a la següent situació de riscos objectiu (al nostre cas, ENS).



Taula 33: PILAR - Risc acumulat ENS

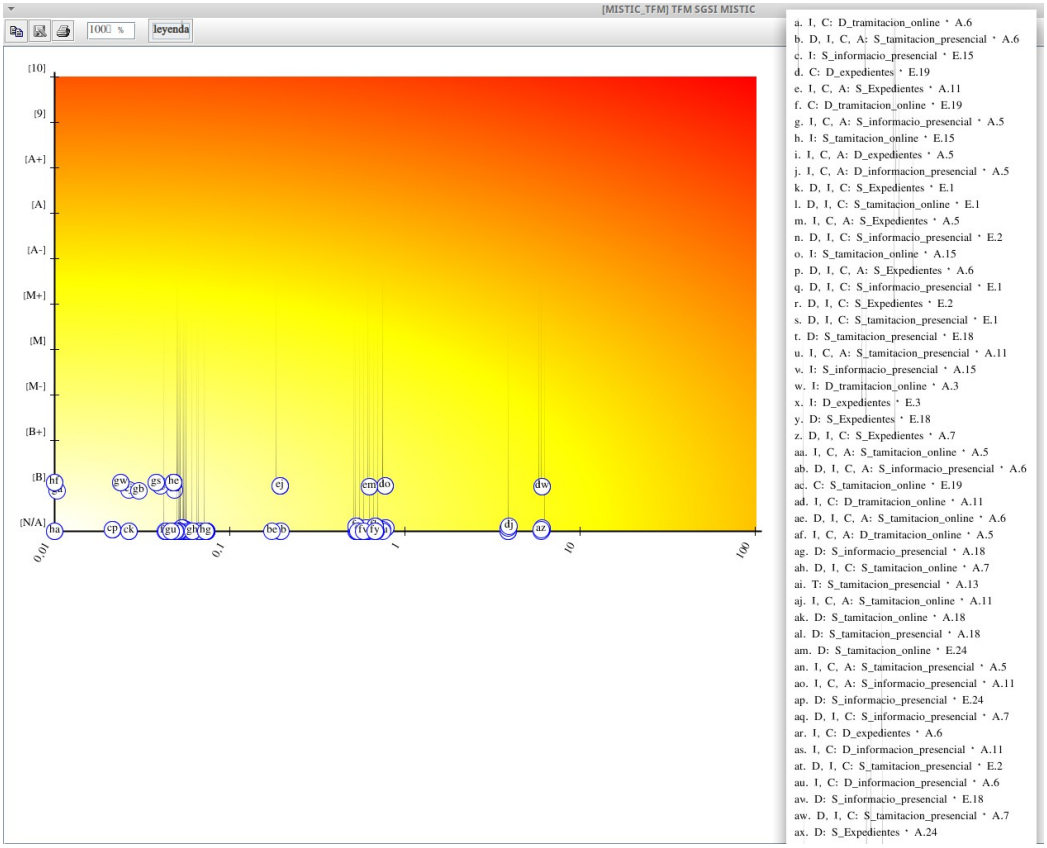


Figura 32: PILAR - Mapa risc ENS acumulat

Tenim en compte la representació en colors tant de la situació actual com de la situació de riscos associades a una situació 'ENS', podem dir que l'organització es troba encara lluny dels objectius fixats i que, per tant, haurà d'implementar un full de ruta amb una priorització de projectes que vagin acostant i reduint els riscos establint prioritats, atenent primers als riscos més importants.

6. FASE 4: Proposta de projectes

6.1. Introducció

Després de l'anàlisi de riscos hem pogut constatar que el nostre sistema té carències tant en l'aspecte de compliment de normatives com riscos clars que s'han pogut visualitzar a través de diferents formes de representació dels mateixos. En aquest capítol proposarem uns quants projectes per tal de començar a controlar aquests riscos. Es tracta d'una petita mostra de projectes que s'hauran de portar a terme, atès que no podem abordar tot el que es necessita de cop (de fet, la proposta és realitzar diferents fases de grups de projectes per tal de poder avaluar posteriorment el seu efecte sobre la seguretat del nostre sistema).

6.2. Detecció de projectes

Com ja hem vist anteriorment, tot i que tenim salvaguardes implementades, hem contrastat que encara tenim cert risc residual que haurem de gestionar. A més, si ens fixem més encara en els controls que indica l'ENS i la ISO27002, podem veure que PILAR ens indica de color vermell que hi han molts controls que no han assolit en nivell L3 que requereix les dues normatives.

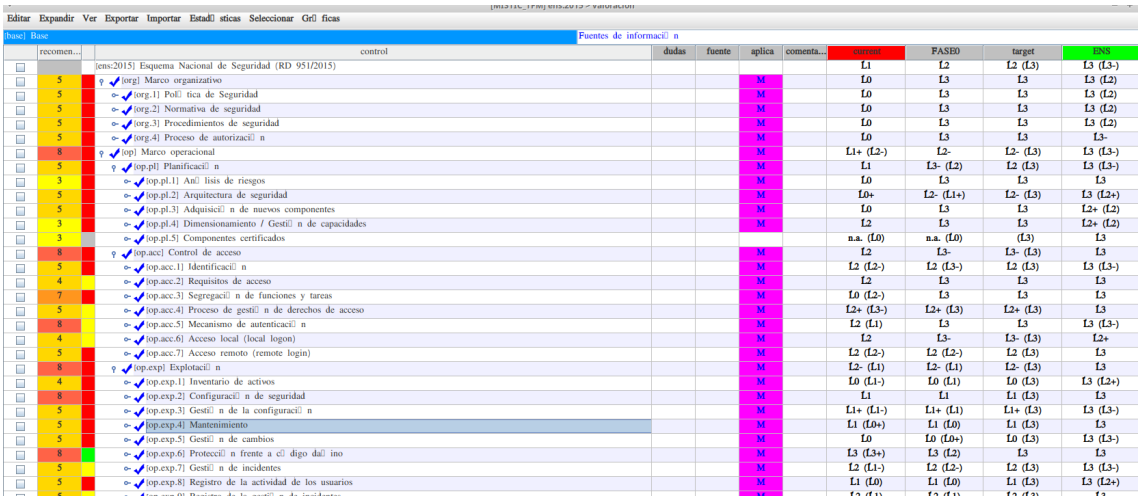


Figura 33: PILAR - Aplicació de salvaguardes ENS actualment

També s'han avaluat les salvaguardes o controls que la norma ISO27002:2013 ens indica, obtenint com a resultat els següents nivells de CMM

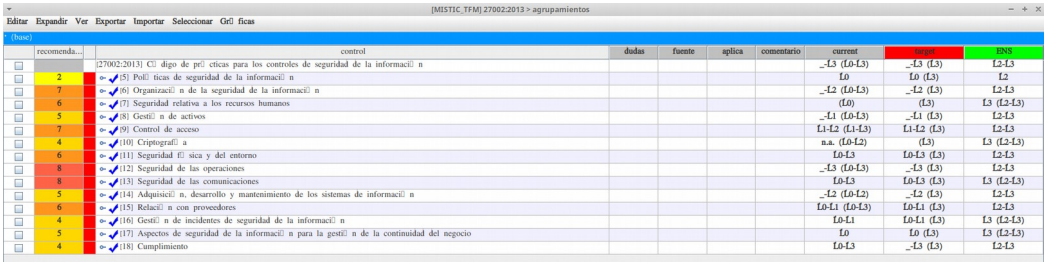


Figura 34: PILAR - Aplicació de controls ISO27002 actualment

Com podem veure a les figures anteriors, estem treballant sempre sobre la fase actual per tal de veure el nivell de compliment actual dels controls i salvaguardes de les dues normes. Aquest compliment PILAR el notifica en una escala de colors a la tercera columna, i amb un nivell de recomanació del control a aplicar. Per exemple:

Figura 35: PILAR - Nivell maduresa CMM ISO27002

El color vermell indica no compliment, el groc compliment parcial i el verd indica compliment satisfactori.

Anem a posar un exemple de mitigació d'un risc fent servir PILAR. Anem a la representació tabular dels nostres riscos.

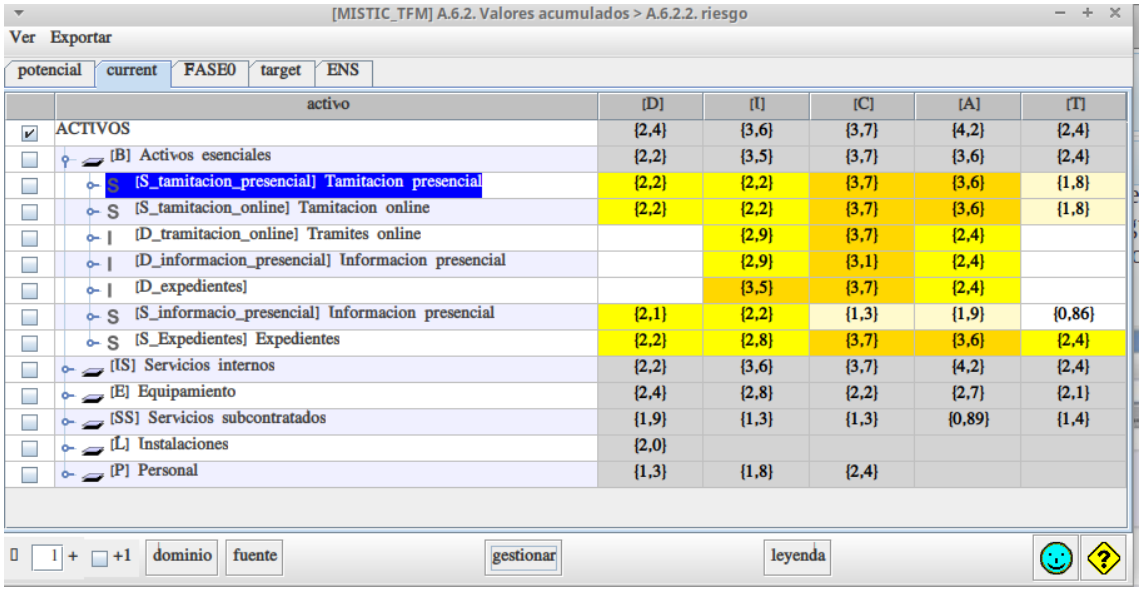


Figura 36: Riscos residuals a tractar

En aquesta representació, podem clicar a sobre del botó «gestionar», que ens portarà a una pantalla amb un conjunt de salvaguardes que podem aplicar per gestionar els riscos que PILAR ha detectat

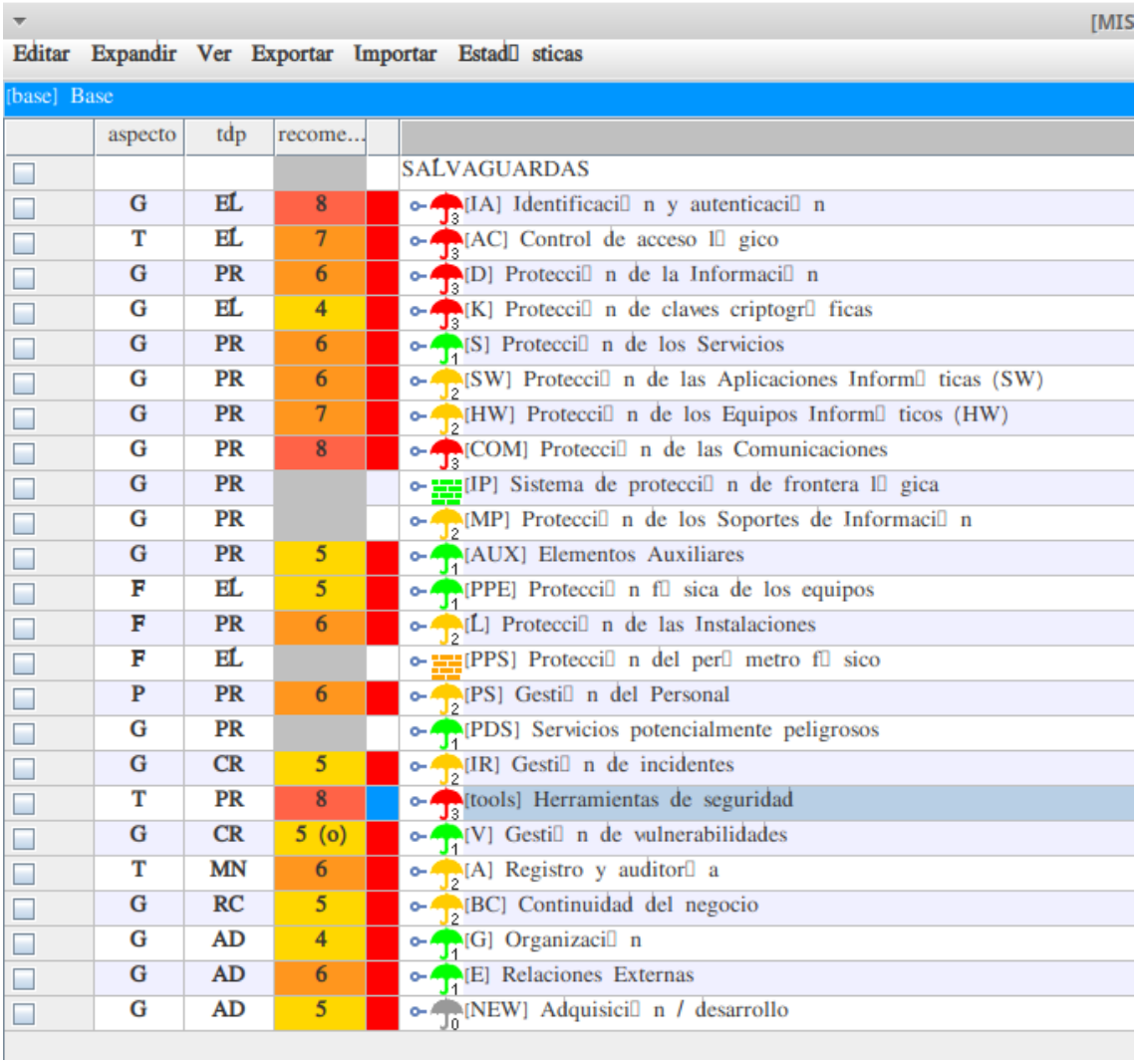


Figura 37: Salvaguardes per gestionar el risc

Com ja hem indicat en capítols anteriors, els colors de la quarta columna indica si la salvaguarda està ben aplicada i no hi ha risc provocat per una manca d'ella. Haurem de fitxar-nos en les files de color vermell, i en el número que PILAR recomana de prioritat en la gestió d'aquest risc.

La gestió dels riscos la podem fer «manualment» (és a dir, decidint nosaltres què farem i amb quin ordre de gestió) o demanar a PILAR que ens suggereixi alguna acció (fent clic a sobre del botó «sugerir»).

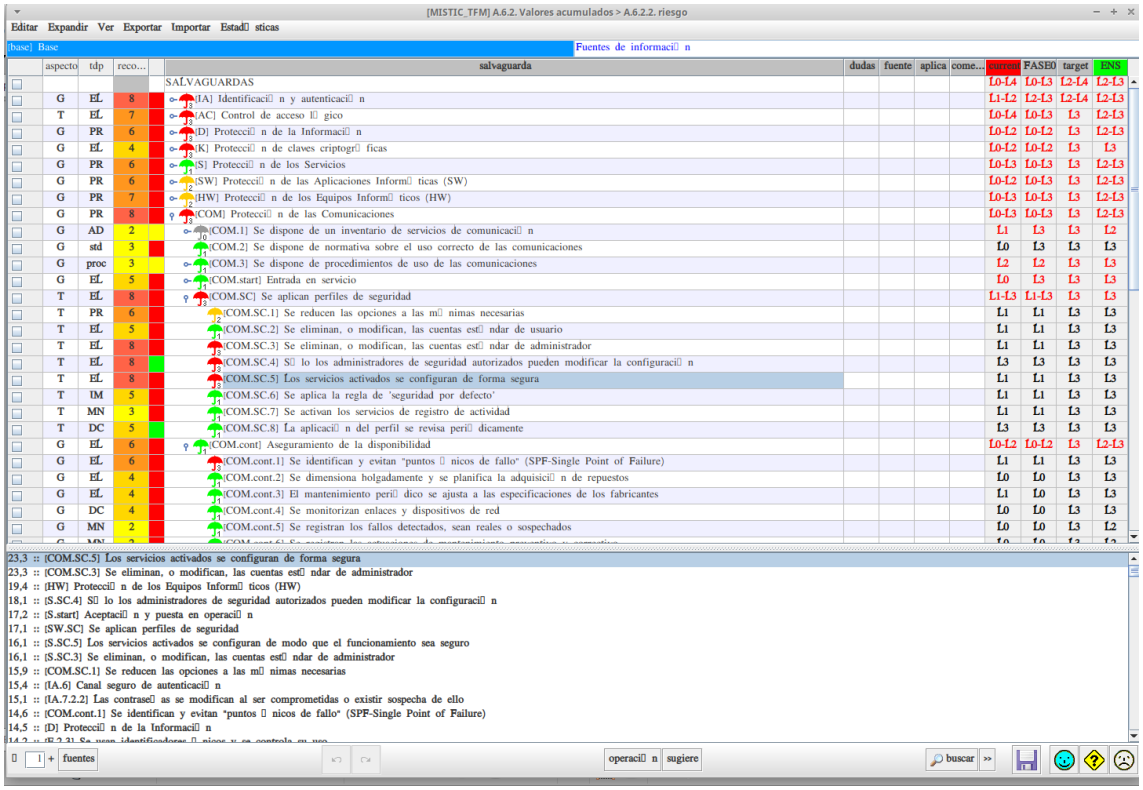


Figura 38: Salvaguardes prioritzades

En aquest cas, ens suggereix que comencem a tractar els riscos per la vessant de «protecció de comunicacions», atès que actualment no tenim prou maduresa (L1) i és més prioritari (segons PILAR) tenir assegurat aquest aspecte.

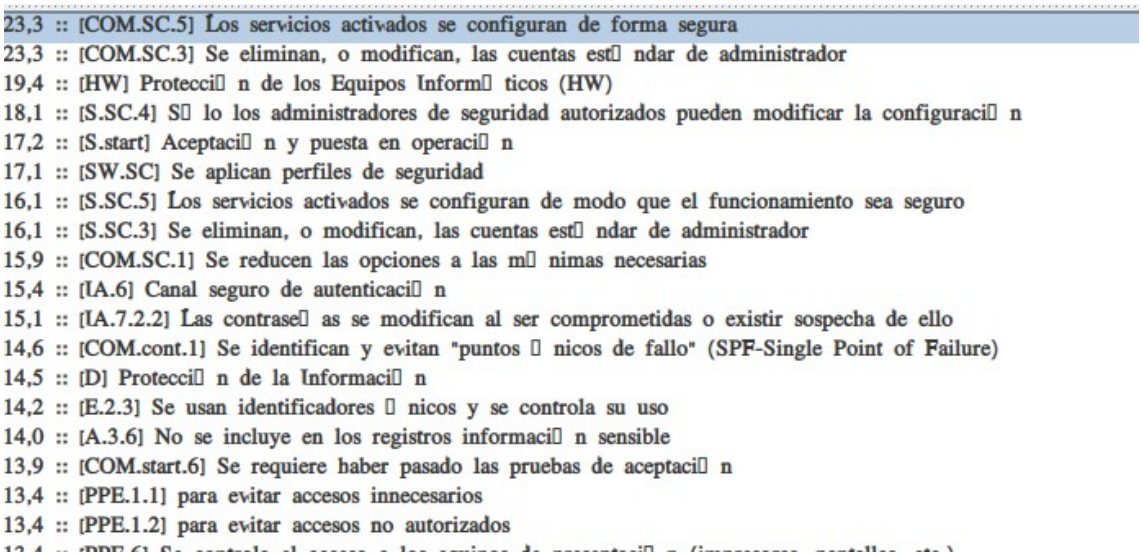


Figura 39: Salvaguardes recomanades

Per tant, podríem definir un projecte o una acció que contemplés incrementar el grau de maduresa de les salvaguardes COM.SC.5, COM.SC.3 i COM.SC.1 per tal d'agrupar-les en un projecte comú.

6.3. Projectes de la FASE 1

Tal i com hem vist en l'apartat anterior l'organització encara es troba lluny de complir els seus objectius en relació als riscos acceptables que ha definit. Per tant, haurem d'abordar un seguit de projectes que ens acostin als nostres objectius i, per tant, permetin passar una futura auditoria de compliment. **A banda dels projectes que pugui detectar PILAR com a mancança clara de controls, s'ha determinat sobretot la manca de documentació escrita, sigui polítiques, normatives i procediments, i es farà un especial ressò en aquests aspectes**. **A més, la implantació de normativa sensibilitzarà molt més al nivell directiu que l'establiment de determinades eines informàtiques que potser no tenen visibilitat a aquest nivell, reforçant la implicació de la direcció** amb el projecte.

Tot i això, i com a exemple de projecte detectat per PILAR (controls COM.SC.5, COM.SC.3 i COM.SC.1) es proposa el **PROJECTE 7: PROTECCIÓ DE LES COMUNICACIONS,** per tal de poder posar sota el control alguns dels aspectes que PILAR ha detectat.

També s'ha constatat que ja existeixen mesures tècniques instaurades (protecció davant codi maliciós, tallafocs, etc ..) així que, tot i que no ens trobem en un estat òptim, es considera que la primera fase es treballa molt en la vessant normativa.

L'ajuntament **proposa la realització de projectes en fases,** de manera que a cada fase s'implementin uns projectes determinats. Aquesta aproximació per fases permetrà avaluar la situació a cada final de fase fent de nou un anàlisi de riscos per determinar si s'ha complert els objectius o no de cada fase, i auditories internes per tal de verificar compliment dels indicadors

És objectiu de l'ajuntament que a la finalització del conjunt de fases estigui implementat tot el conjunt de projectes necessari per millorar la seva seguretat.

A continuació es presenten un seguit de projectes a implementar en la FASE 1

PROJECTE 1: MARC ORGANITZATIU	
EQUIP	- Responsable de seguretat - Responsable de sistemes - Responsable jurídic
OBJECTIU	- Redacció dels documents: 0. Política gestió documental 1. Política de seguretat 2. Normativa de seguretat 3. Procediments de seguretat 4. Procés d'autorització
BENEFICI	- Es formalitzarà la voluntat de l'organització i es crearà la documentació de referència - Es designaran els rols, òrgans i responsables de la seguretat dins de l'organització. - Es conscienciarà als treballadors del projecte
TEMPS	3 setmanes
COST	1500 €
OBSERVACIONS	-

PROJECTE 2: FORMACIÓ i CONSCIENCIACIÓ	
EQUIP	- Responsable de RRHH - Responsable de seguretat - Responsable de sistemes
OBJECTIU	- Establir un pla de formació anual per a tot el personal. - Els cursos seran de 10 horas tindran una durada de 10 hores anuals. - S'establiran cada any els objectius de la formació
BENEFICI	- Increment de la seguretat total de l'organització - Reducció d'incidents de seguretat provocat per pràctiques dolentes en seguretat - Involucrar a tot el personal en el SGSI.
TEMPS	2 setmanes
COST	1000 €
OBSERVACIONS	

PROJECTE 3: PLANIFICACIÓ DE LA SEGURETAT	
EQUIP	- Responsable de sistemes - Responsable de seguretat
OBJECTIU	- Redacció de la *"Normativa de Gestión de Ciclo de Vida de las Plataformas Tecnológicas"* - Revisió procediment anàlisi de riscos - Inventariar i documentar els sistemes i la seva arquitectura de seguretat - Redacció de "*Normativa de Gestión de capacidades".*
BENEFICI	- Tenir un procediment d'anàlisi de riscos actualitzat. - Tenir documentat l'aquitectura de seguretat. - Establir el procediment que especifica els requeriments previs a la posada en marxa d'un nou servei diminuirà incidents de seguretat
TEMPS	4 setmanes
COST	2.000 €
OBSERVACIONS	

PROJECTE 4: NORMATIVA ACTUALITZACIÓ DE VERSIONS	
EQUIP	- Responsable de sistemes
OBJECTIU	- Definit una política per tal de saber com i de quina manera s'aplicaran les noves versions de producte - Redactar "*Normativa de Gestión de Ciclo de Vida de las Plataformas Tecnológicas"* - Redactar *"Normativa de Gestión de Cambios"*
BENEFICI	- Disposar els sistemes el més actualitzats possible, garantint que l'actualització no malmet el funcionament normal
TEMPS	2 setmanes
COST	1000 €
OBSERVACIONS	

PROJECTE 5: NORMATIVA DE GESTIÓ DE ACCÉS LÒGIC	
EQUIP	- Responsable de sistemes - Responsable de seguretat
OBJECTIU	- Definir la normativa que asseguri: 1. mínim privilegi d'accés amb autorització expresa responsable 2. ús únic d'identificador 3. segregació de tasques 4. Definició política de contrasenyes
BENEFICI	- Els usuaris només tindran accés a allò que realment necessitin - Gestió del identificador i de les contrasenyes
TEMPS	1 setmanes
COST	500 €
OBSERVACIONS	

PROJECTE 6: NORMATIVA DE SEGURETAT FÍSICA I ENTORN	
EQUIP	- Responsable de sistemes - Responsable de seguretat - Responsable seguretat física
OBJECTIU	- Definir la normativa "*Normativa de Seguridad Física y del Entorno".* - Identificar totes les persones que accedeixen als locals amb equipament que forma part dels sistemes d'informació. - Portar un registre de persones que entren i surten - Realitzar mapa de les instal·lacions - Portar registre d'equipament entrant i surtint.
BENEFICI	- Prevenir l'accés físic no autoritzat i qualsevol incidència derivada de l'entorn.
TEMPS	2 setmanes
COST	1000 €
OBSERVACIONS	

PROJECTE 7: PROTECCIÓ DE LES COMUNICACIONS	
EQUIP	- Responsable de sistemes - Responsable de seguretat
OBJECTIU	- Definir la normativa "*Normativa de ús i securització de les comunicacions»* - Definir què està permès i què no. - Definir procediments de posada en servei sistemes de comunicació - Aplicació de perfils de seguretat (desactivació de serveis no necessaris, configuració mínima, eliminació d'usuaris innecessaris, modificació de contrasenyes per defecte, etc, securització dels serveis proporcionats ..)
BENEFICI	- Protegir la prestació dels serveis que es presten a través de xarxes de comunicacions
TEMPS	2 setmanes
COST	1000 €
OBSERVACIONS	

Per finalitzar, recordar que queden molts més projectes que PILAR ha detectat per millorar la nostre seguretat, però la proposta de fer per fases els projecte i de incentivar el procés d'implantació d'una gestió de la seguretat de la informació han fet aparèixer projectes en relació a la normativa, polítiques de seguretat que, tot i no ser tant prioritàries per l'eina PILAR, es considera que facilita el fet d'implantar la conscienciació i la necessitat de la gestió de la seguretat dins de l'organització.

Com a resultat de l'aplicació dels projectes dissenyats en la primera fase, podrem tornar a avaluar el nostre sistema amb els models de maduresa CMM, i així podem comparar amb el gràfic de radar que vam obtenir a l'inici del projecte.

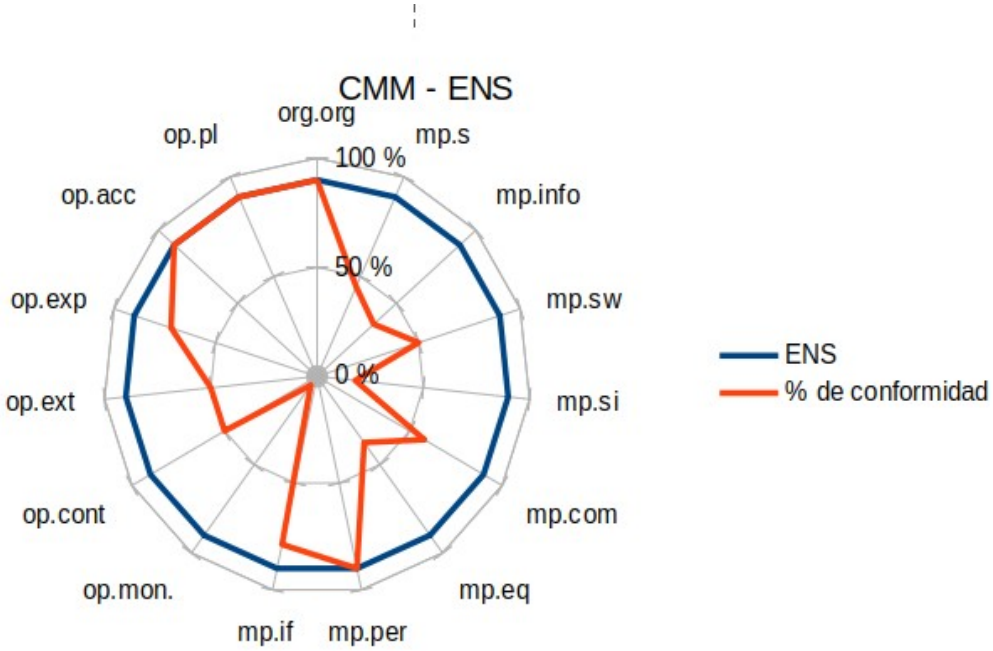


Figura 40: CMM - ENS - Final FASE 1 projectes

Com podem comprovar, s'ha millorat en molts aspectes (de fet, els aspectes que s'havien planificat), però encara queda molts altres que queden fora de l'òrbita de compliment de l'ENS. Com és normal, una possible auditoria haurà de trobar un número important de no conformitats majors i menors, tal i com veurem al següent capítol.

7. FASE 5: Auditoria de compliment

7.1. Introducció

En aquest punt del projecte s'aborda el procés de realització d'una auditoria interna. Tot i que és probable que no s'hagin abordat tots els projectes necessaris per tal disposar d'un SGSI certificable, és interessant que l'organització abordi aquesta fase d'auditories interna per poder acabar el cicle complert del procés de millora contínua que implica un SGSI. Tant important és el disposar d'un SGSI funcionant com transformar l'Ajuntament cap a un organització en busca de la millora contínua, implantant procediments i metodologies de treball que facilitin aquest objectiu.

7.2. Metodologia

Com ja hem comentat, l'Ajuntament de MISTIC necessita complir amb l'ENS i, per tant, es farà una auditoria per exteure quin nivell de compliment es troba després de la realització dels projectes que s'havien detectat i planificat per la FASE 1 (recordem que l'Ajuntament preveu més projectes en diferents fases posteriors).

És intenció de l'Ajuntament la realització d'una auditoria interna a la finalització de cadascuna de les FASES d'implantació de projectes que té planificat.

7.3. Realització de l'auditoria.

A continuació es descriu les troballes i evidències recopilades durant la realització de l'auditoria.

Código	Mesura ENS	ISO 27001:2013 ISO 27002:2013		Salvaguardas necesarias	
org.1	**POLÍTICA DE SEGURIDAD**	**27001:2013** **- 4:Contexto de la organización** **- 5.2: Política** **- 5.3: Roles, responsabilidades y autoridad** **27002:2013** **- 6.1.1:Roles y responsabilidades relativas a la seguridad de la información** **- 18.1.1: Identificación de legislación aplicable y requisitos contractuales**	**SÍ aplica**	**- Política de Seguridad** **- Documento designación roles y constitución comités.**	**- SI: Existeix un document de política de seguretat dins del sistema gestor documental (CODI DOCUMENT : SGSI-SI-PO01-1.0)** **- SI: Existeix document de designació de rols (CODI: SGSI-GRLS-PR01-1.0)**
org.2	**NORMATIVA DE SEGURIDAD**	**27002:2013** **- 5.1.1: Políticas de seguridad de la información** **- 5.1.2: Revisión de las políticas de seguridad de la información** **-6.1.4: Contacto con grupos de especial interés** **-8.1.3: Uso aceptable de los activos** **-13.2.1: Políticas y procedimientos de transferencia de información** **15.1.1: Política de seguridad de la información en las relaciones con proveedores** **- 16.1.1: Responsabilidades y procedimientos** **- 18.2.2: Cumplimiento de las políticas y normas de seguridad**	**SÍ aplica**	**- Normativa de Uso de Recursos y Accesos a Sistemas de Información** **- Registros de conocimiento de la normativa**	**- SI: Com a resultat del projecte 1, existeix normativa d'ús i recursos dels sistemes d'informació** **- NO: no es presenten registres de coneixement per part dels empleats de la normativa**
org.3	**PROCEDIMIENTOS DE SEGURIDAD**	**27002:2013** **o 6.1.3 - Contacto con las autoridades** **o 12.1.1 - Documentación de los procedimientos de operación** **o 13.2.1 - Políticas y procedimientos de transferencia de información** **o 16.1.1 - Responsabilidades y procedimientos**	**SÍ aplica**	**- Procedimiento Operativo del Servicio ENS** **- Inventario de procedimientos**	**- SI: Com a resultat del projecte 1, existeix un inventari de procediments de seguretat**

		o 18.1.2 - Derechos de propiedad intelectual (IPR) o 18.2.3 - Comprobación del cumplimiento técnico			
org.4	PROCESO DE AUTORIZACIÓN	27002:2013 o 6.1.1 - Roles y responsabilidades relativas a la seguridad de la información o 6.2.1 - Política de dispositivos móviles o 8.2.3 - Manejo de activos o 8.3.1 - Gestión de soportes extraíbles o 12.5.1 - Instalación de software en sistemas operacionales o 12.6.2 - Restricciones a la instalación de software o 13.1.1 - Controles de red o 13.1.2 - Seguridad de los servicios de red o 14.2.4 - Restricciones a los cambios en los paquetes de software	SÍ aplica	- Normativa de Gestión de Autorizaciones - Herrramienta de evidencias	- SI: Com a resultat del projecte 1, existeix un procés d'autoritzacions
op.pl.1	ANÁLISIS DE RIESGOS	27001:2013 o 6.1 – Acciones para abordar riesgos y oportunidades o 6.1.1 - General o 6.1.2 – Evaluación de riesgos o 6.1.3 – Tratamiento de los riesgos o 8.2 - Evaluación de riesgos o 8.3 – Tratamiento de los riesgos	SÍ aplica	Procediment/Normativa de Gestión de Riesgos Archivo anàlisi de riesgos (PILAR) Informe Anàlisi de Riegos Acta aceptación análisi de riesgos	- SI: Existeix una normativa/procediment de gestió de riscos dins del SGD-SGSI (CODI: SGSI-GU-AR-G01-1.0) - SI: Existeix arxiu de projecte TFM.mgr de PILAR. - NO: No existeix acta d'acceptació risc residual.
op.pl.2	ARQUITECTURA DE SEGURIDAD	27002:2013 o 8.1.1 - Inventario de activos o 8.1.2 - Propiedad de los activos o 13.1.1 - Controles de red o 14.2.5 - Principios para la ingeniería de sistemas seguros	SÍ aplica	Normativa de Arquitectura de Seguridad Esquemas de red físicos y lógicos	- SI: Existeix inventari d'actius - SI: com a resultat del projecte 3
op.pl.3	ADQUISICIÓN DE NUEVOS COMPONENTES	27002:2013 o 14.1.1 - Análisis y especificación de los requisitos de seguridad	SÍ aplica	Normativa de Gestión de Ciclo de Vida de las Plataformas Tecnológicas	- SI. Com a resultat del projecte 3
op-pl.4	DIMENSIONAMIENTO /	27002:2013 o 12.1.3 - Gestión de capacidades	SÍ aplic	Normativa de Gestión de capacidades	- SI: Com a resultat del projecte 3

	GESTIÓN DE CAPACIDADES		a		
op.pl.5	COMPONENTES CERTIFICADOS	27002:2013 o No se contempla	NO aplica		
op.acc.1	IDENTIFICACIÓN	27002:2013 o 9.2.1 - Altas y bajas de usuarios	SÍ aplica	- Procedimiento de gestión de acceso Herramienta gestión solicitudes y evidencias	- NO: no existeix procedimient - SI: Existeix eina de gestió i evidències
op.acc.2	REQUISITOS DE ACCESO	27002:2013 o 9.1.1 - Política de control de acceso o 9.1.2 - Acceso a redes y servicios en red o 9.4.1 - Restricción del acceso a la información o 9.4.4 - Uso de los recursos del sistema con privilegios especiales o 9.4.5 - Control de acceso al código fuente de los programas	SÍ aplica	- Procedimiento de gestión de acceso - Herramienta gestión solicitudes y evidencias	- NO: No exiseix procediment - SI: Existeix eina de gestió i evidències
op.acc.3	SEGREGACIÓN DE FUNCIONES Y TAREAS	27002:2013 o 6.1.2 - Separación de tareas	SÍ aplica	- Procedimiento de gestión de acceso - Herramienta gestión solicitudes y evidencias	- NO: No exiseix procedimen t - SI: Existeix eina de gestió i evidències
op.acc.4	PROCESO DE GESTIÓN DE DERECHOS DE ACCESO	27002:2013 o 9.2.2 - Gestión de derechos de acceso de los usuarios o 9.2.3 - Gestión de derechos de acceso especiales o 9.2.5 - Revisión de derechos de acceso de usuario o 9.2.6 - Terminación o revisión de los privilegios de acceso	SÍ aplica	- Procedimiento de gestión de acceso - Herramienta gestión solicitudes y evidencias	- NO: No exiseix procediment - SI: Existeix eina de gestió i evidències
op.acc.5	MECANISMO DE AUTENTICACIÓN	27002:2013 o 9.2.4 - Gestión de la información secreta de autenticación de usuarios o 9.3.1 - Uso de la información secreta de autenticación o 9.4.3 - Gestión de las contraseñas de usuario	SÍ aplica	- Procedimiento de gestión de acceso - Herramienta gestión solicitudes y evidencia - Instrucciones técnicas administradores	- NO: No exiseix procediment - SI: existeix eina - SI: existeix documentació tècnica
op.acc.6	ACCESO LOCAL (LOCAL LOGON)	27002:2013 o 9.4.2 - Procedimientos seguros de inicio de sesión	SÍ aplica	- Procedimiento de gestión de acceso - Herramienta gestión solicitudes y evidencia	- NO: No exiseix procediment - SI: Existeix eina
op.acc.	ACCESO	27002:2013	SÍ	- Procedimiento de	- NO: No exiseix

7	REMOTO (REMOTE LOGIN)	o 9.4.2 - Procedimientos seguros de inicio de sesión o 10.1.1 - Política de uso de los controles criptográficos o 13.1.1 - Controles de red o 13.1.2 - Seguridad de los servicios de red o 18.1.5 - Regulación de los controles criptográficos	aplica	gestión de acceso - Herramienta gestión solicitudes y evidencia	procediment - SI: Existeix eina
op.exp.1	INVENTARIO DE ACTIVOS	27002:2013 o 8.1.1 - Inventario de activos o 8.1.2 - Propiedad de los activos	SÍ aplica	Normativa de Gestión de Activos Herramienta inventario activos	- NO: No existeix normativa - SI: Existeix eina (OCS-Inventory)
op.exp.2	CONFIGURACIÓN DE SEGURIDAD	27002:2013 o No se contempla explícitamente	SÍ aplica	- Normativa de Gestión de Bastionados - Instrucciones tècnicas bationado	- NO: No existeix normativa - SI: Existeix documentació tècnica
op.exp.3	GESTIÓN DE LA CONFIGURACIÓN	27002:2013 o No se contempla explícitamente	SÍ aplica	Normativa de gestión de la configuración Herramienta solicitud y evidencias	- NO: No exiseix procedimen**t** - SI: Existeix eina
op.exp.4	MANTENIMIENTO	27002:2013 o 11.2.4 - Mantenimiento de los equipos	SÍ aplica	- Normativa de Gestión de Ciclo de Vida de las Plataformas Tecnológicas - Herramienta de solicitud + evidencias	- SI: Com a resultat del projecte 4 - SI: Existeix eina.
op.exp.5	GESTIÓN DE CAMBIOS	27002:2013 o 12.1.2 - Gestión de cambios o 14.2.2 - Procedimientos de control de cambios en el sistema o 14.2.3 - Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma	SÍ aplica	- Normativa de Gestión de Cambios - Herramienta de solicitud + evidencia	- SI: com a resultat del projecte 4 - SI: Existeix eina
op.exp.6	PROTECCIÓN FRENTE A CÓDIGO DAÑINO	27002:2013 o 12.2.1 - Controles contra el código malicioso	SÍ aplica	- Normativa de Gestión del Código Dañino Evidencias herramienta antivirus	- NO: No existeix normativa - SI: Existeix eina antivirus i evidències
op.exp.7	GESTIÓN DE INCIDENCIAS	27002:2013 o 6.1.3 - Contacto con las autoridades o 6.1.4 - Contacto con grupos de especial interés	SÍ aplica	Normativa de Gestión de incidencias Herramienta gestión incidencias +	- NO: no exiteix normativa - SI: Existeix eina i evidències

		o 16.1.2 - Notificación de eventos de seguridad de la información o 16.1.3 - Notificación de puntos débiles de seguridad o 16.1.4 - Evaluación y decisión respecto de los eventos de seguridad de la información o 16.1.5 - Respuesta a incidentes de seguridad de la información o 16.1.6 - Aprendizaje de los incidentes de seguridad de la información o 16.1.7 - Recopilación de evidencias		evidencias	
op.exp.8	REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS	27002:2013 o 12.4.1 - Registro de eventos o 12.4.3 – Registros de administración y operación	SÍ aplica	Normativa de Gestión Logs de Sistemas y Aplicaciones Herramienta gestión logs	- NO: no existeix normativa - SI: si existeix eina de gestió de logs
op.exp.9	REGISTRO DE LA GESTIÓN DE INCIDENCIAS	27002:2013 o 16.1.5 - Respuesta a incidentes de seguridad de la información o 16.1.7 - Recopilación de evidencias	SÍ aplica	Normativa de Gestión de incidencias Herramienta incidencia + informes	- SI existeix normativa - Si existeix eina
op.exp.10	PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD	27002:2013 o 12.4.2 - Protección de la información de los registros o 12.4.4 – Sincronización del reloj	NO aplica		
op.exp.11	PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS	27002:2013 o 10.1.2 - Gestión de claves	SÍ aplica	- Normativa de Gestión de Claves de Acceso a Sistemas y Cifrado - Evidències de la gestió	- SI: Existeix normativa - SI: existeixen evidències
op.ext.1	CONTRATACIÓN Y ACUERDOS DE NIVEL DE SERVICIO	27002:2013 o 13.2.2 - Acuerdos de transferencia de información o 15.1.1 - Política de seguridad de la información en las relaciones con proveedores o 15.1.2 - Tratamiento de la seguridad en contratos con proveedores o 15.1.3 - Cadena de suministro de tecnologías de la información y comunicaciones	SÍ aplica	Normativa de Contratación y acuerdos de nivel de servicio Evidencias contratos firmados	- NO: No existeix normativa - SI. Existeixen contractes signats
op.ext.2	GESTIÓN DIARIA	27002:2013 o 15.2.1 - Supervisión y revisión de los servicios prestados por terceros	SÍ aplica	Normativa de Contratación y acuerdos de nivel de	- NO: No existeix normativa - NO: no existeixen

		o 15.2.2 - Gestión del cambio en los servicios prestados por terceros		servicio Informes revisión SLA	registres revisió SLAs
op.ext.9	MEDIOS ALTERNATIVOS	27002:2013 o No se contempla: OBS: Aunque en las normas 27002 no se trata explícitamente, probablemente sea parte de los controles de continuidad de negocio.	NO aplica		
op.cont.1	ANÁLISIS DE IMPACTO	27002:2013 o 17.1.1 - Planificar la continuidad de la seguridad de la información	SÍ aplica	Normativa de análisis de impacto y disaster recovery	- NO: No existeix normativa
op.cont.2	PLAN DE CONTINUIDAD	27002:2013 o 17.1.2 - Implementar la continuidad de la seguridad de la información	NO aplica		
op.cont.3	PRUEBAS PERIÓDICAS	27002:2013 o 17.1.3 - Verificar, revisar y evaluar la continuidad de la seguridad de la información	NO aplica		
op.mon.1	DETECCIÓN DE INTRUSIÓN	27002:2013 o No se contempla de forma explícita OBS: La norma 27002:2013 menciona el sistema de detección en varios lugares, pareciendo que se da por supuesto: 12.4.1 – Registro de eventos 12.4.3 – Registros de administración y operación 13.1.2 – Seguridad de los servicios de red	SÍ aplica	Normativa de Métricas Indicadores de Seguridad Herramienta IDS	- NO: No existeix normativa - NO: No existeix eina IDS
op.mon.2	SISTEMA DE MÉTRICAS	27001:2013 o 9 – Evaluación del desempeño o 9.1 – Monitorización, medidas, análisis y evaluación	SÍ aplica	Normativa de Métricas Indicadores de Seguridad Registro métricas + indicadores	- SI: Existeix documents de mètriques - NO: Encara no hi han dades recollides
mp.if.1	ÁREAS SEPARADAS Y CON CONTROL DE ACCESO	27002:2013 o 11.1.1 - Perímetro de seguridad física o 11.1.2 - Controles físicos de entrada o 11.1.3 - Seguridad de oficinas, despachos e instalaciones o 11.1.4 - Protección contra las amenazas externas y de origen ambiental o 11.1.5 - Trabajo en áreas seguras	SÍ aplica	Normativa de Seguridad Física y del Entorno Planos instalaciones	- SI: Com a resultat del projecte 6 - SI: Com a resultat del projecte 6

		o 11.1.6 - Áreas de carga y descarga o 11.2.1 - Emplazamiento y protección de equipos			
mp.if.2	IDENTIFICACIÓN DE LAS PERSONAS	27002:2013 o 11.1.2 - Controles físicos de entrada	SÍ aplica	Normativa de Seguridad Física y del Entorno Registros de acceso	- SI: Com a resultat del projecte 6 - SI:Com a resultat del projecte 6
mp.if.3	ACONDICIONAMIENTO DE LOS LOCALES	27002:2013 o 11.2.2 - Instalaciones de suministro o 11.2.3 - Seguridad del cableado	SÍ aplica	Normativa de Seguridad Física y del Entorno Herramienta de sensores Revisiones y mantenimientos	- SI: Com a resultat del projecte 6 - SI: Existeixen sensors i detectors - SI: Existeixen revisions i manteniments extintors i AACC
mp.if.4	ENERGÍA ELÉCTRICA	27002:2013 o 11.2.2 - Instalaciones de suministro	SÍ aplica	Normativa de Seguridad Física y del Entorno Revisiones del SAI Pruebas realizadas	- SI: Com a resultat del projecte 6 - SI: Es fan revisions i proves del SAI
mp.if.5	PROTECCIÓN FRENTE A INCENDIOS	27002:2013 o 11.1.4 - Protección contra las amenazas externas y de origen ambiental	SÍ aplica	Normativa de Seguridad Física y del Entorno Revisions de mantenimiento.	- SI: Com a resultat del projecte 6 - SI: Es fan revisions de manteniment per llei.
mp.if.6	PROTECCIÓN FRENTE A INUNDACIONES	27002:2013 o 11.1.4 - Protección contra las amenazas externas y de origen ambiental	SÍ aplica	Normativa de Seguridad Física y del Entorno	- SI: Com a resultat del projecte 6
mp.if.7	REGISTRO DE ENTRADA Y SALIDA DE EQUIPAMIENTO	27002:2013 o 11.2.5 - Retirada de materiales propiedad de la empresa o 11.2.6 - Seguridad de los equipos fuera de las instalaciones	SÍ aplica	Normativa de Seguridad Física y del Entorno	- SI: Com a resultat del projecte 6
mp.if.9	INSTALACIONES ALTERNATIVAS	27002:2013 o 17.2.1 - Disponibilidad de los medios de procesamiento de información	NO aplica		
mp.per.1	CARACTERIZACIÓN DEL PUESTO DE TRABAJO	27002:2013 o 7.1.1 - Investigación de antecedentes	SÍ aplica	Normativa de Uso de Recursos y Accesos a Sistemas de Información	- NO: No hi ha normativa

mp.per.2	DEBERES Y OBLIGACIONES	27002:2013 o 7.1.2 - Términos y condiciones de contratación o 7.2.1 - Responsabilidades de la Dirección o 7.2.3 - Proceso disciplinario o 7.3.1 - Terminación o cambio de responsabilidades laborales o 8.1.4 - Devolución de activos o 13.2.4 - Acuerdos de confidencialidad o no divulgación	SÍ aplica	Normativa de Uso de Recursos y Accesos a Sistemas de Información	- NO: no hi ha normativa
mp.per.3	CONCIENCIACIÓN	27001:2013 o 7.3 - Concienciación 27002:2013 o 7.2.2 - Concienciación, formación y capacitación en seguridad de la información	SÍ aplica	- Normativa de Gestión de Formación de Concienciación y Sensibilización - Evidències (certificats d'assitència)	- SI: Com a resultat del projecte 2 - NO: No es presenten certificats d'assitència (encara no han començat cap curs)
mp.per.4	FORMACIÓN	27001:2013 o 7.2 - Competencias 27002:2013 o 7.2.2 - Concienciación, formación y capacitación en seguridad de la información	SÍ aplica	Normativa de Gestión de Formación de Concienciación y Sensibilización	- SI: Com a resultat del projecte 2 - NO: No es presenten certificats d'assitència (encara no han començat cap curs)
mp.per.9	PERSONAL ALTERNATIVO	27002:2013 o 17.2.1 - Disponibilidad de los medios de procesamiento de información	NO aplica		
mp.eq.1	PUESTO DE TRABAJO DESPEJADO	27002:2013 o 11.2.9 - Política de puesto de trabajo despejado y pantalla limpia	SÍ aplica	Normativa de Uso de Recursos y Accesos a Sistemas de Información	- NO_ No hi ha normativa
mp.eq.2	BLOQUEO DEL PUESTO DE TRABAJO	27002:2013 o 11.2.8 - Equipo de usuario desatendido	SÍ aplica	- Normativa de Uso de Recursos y Accesos a Sistemas de Informació - Evidències	- NO: no hi ha normativa - SI: Evidència
mp.eq.3	PROTECCIÓN DE EQUIPOS PORTÁTILES	27002:2013 o 6.2.1 - Política de dispositivos móviles	SÍ aplica	Normativa de Gestión del Parque de Puesto de Trabajo de Digital	- NO_ No hi ha normativa
mp.eq.9	MEDIOS ALTERNATIVOS	27002:2013 o 17.2.1 - Disponibilidad de los medios de procesamiento de información	SÍ aplica	Normativa de Disponibilidad de procesamiento de información	- NO: no hi ha normativa

mp.com.1	PERÍMETRO SEGURO	27002:2013 o 13.1.2 - Seguridad de los servicios de red	SÍ aplica	Normativa de Gestión de Redes y Comunicaciones	- NO_ No hi ha normativa
mp.com.2	PROTECCIÓN DE LA CONFIDENCIALIDAD	27002:2013 o 10.1.1 - Política de uso de los controles criptográficos o 13.1.1 - Controles de red o 13.1.2 - Seguridad de los servicios de red o 14.1.2 - Aseguramiento de servicios y aplicaciones en redes públicas o 18.1.5 - Regulación de los controles criptográficos	SÍ aplica	Normativa de Gestión de Redes y Comunicaciones - Eines i evidències	- NO: no hi ha normativa - Si hi han controls de xarxa
mp.com.3	PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD	27002:2013 o 10.1.1 - Política de uso de los controles criptográficos o 13.1.1 - Controles de red o 13.1.2 - Seguridad de los servicios de red o 14.1.2 - Aseguramiento de servicios y aplicaciones en redes públicas	SÍ aplica	- Normativa de Gestión de Redes y Comunicaciones - Eines i evidències	- NO_ No hi ha normativa - Si hi han controls de xarxa
mp.com.4	SEGREGACIÓN DE REDES	27002:2013 o 13.1.3 - Segregación de redes	NO aplica		
mp.com.9	MEDIOS ALTERNATIVOS	27002:2013 o 17.2.1 - Disponibilidad de los medios de procesamiento de información	NO aplica		
mp.si.1	ETIQUETADO	27002:2013 o 8.2.2 - Marcado de la información o 8.3.1 - Gestión de soportes extraíbles	SÍ aplica	Normativa de Gestión y Soportes	- NO_ No hi ha normativa
mp.si.2	CRIPTOGRAFÍA	27002:2013 o 8.3.1 - Gestión de soportes extraíbles o 10.1.1 - Política de uso de los controles criptográfico	SÍ aplica	Normativa de Gestión y Soportes	- NO: no hi ha normativa
mp.si.3	CUSTODIA	27002:2013 o 8.3.1 - Gestión de soportes extraíbles	SÍ aplica	Normativa de Gestión y Soportes	- NO_ No hi ha normativa
mp.si.4	TRANSPORTE	27002:2013 o 8.3.3 - Transferencia de soportes físicos o 11.2.5 - Retirada de materiales propiedad de la empresa	SÍ aplica	Normativa de Gestión y Soportes	- NO_ No hi ha normativa
mp.si.5	BORRADO Y DESTRUCCIÓN	27002:2013 o 8.3.2 - Retirada de soportes o 11.2.7 - Reutilización o retirada segura de equipos	SÍ aplica	Normativa de Gestión y Soportes	- NO_ No hi ha normativa

mp-sw.1	DESARROLLO DE APLICACIONES	27002:2013 o 9.4.5 - Control de acceso al código fuente de los programas o 12.1.4 - Separación de los entornos de desarrollo, prueba y operación o 14.2.1 - Política de desarrollo seguro o 14.2.5 - Principios para la ingeniería de sistemas seguros o 14.2.6 - Entorno de desarrollo seguro o 14.2.7 - Externalización del desarrollo de software o 14.3.1 - Protección de los datos de prueba	SÍ aplica	Normativa de Gestión de Desarrollo Seguro - Instruccions tècniques	- NO: no hi ha normativa SI: Si hi ha evidències separació entorns
mp.sw.2	ACEPTACIÓN Y PUESTA EN SERVICIO	27002:2013 o 12.1.4 - Separación de los entornos de desarrollo, prueba y operación o 12.5.1 - Instalación de software en sistemas operacionales o 12.6.1 - Control de las vulnerabilidades técnicas o 14.2.8 - Pruebas de seguridad del sistema o 14.2.9 - Pruebas de aceptación del sistema o 14.3.1 - Protección de los datos de prueba o 14.2.7 - Externalización del desarrollo de software	SÍ aplica	- Normativa de Gestión de Desarrollo Seguro - Evidències	- No hi ha normativa - SI: Si hi ha evidencies separació entorns
mp.info.1	DATOS DE CARÁCTER PERSONAL	27002:2013 o 18.1.4 - Protección de datos e información de carácter personal	SÍ aplica	Normativa de Gestión del RAT	- SI hi ha normativa
mp.info.2	CALIFICACIÓN DE LA INFORMACIÓN	27002:2013 o 8.1.2 - Propiedad de los activos o 8.2.1 - Clasificación de la información	SÍ aplica	Normativa de Gestión de la clasificación y tratamiento de la Información	- NO_ No hi ha normativa
mp.info.3	CIFRADO DE LA INFORMACIÓN	27002:2013 o 10.1.1 - Política de uso de los controles criptográficos o 8.3.3 - Transferencia de soportes físicos o 13.1.1 - Controles de red o 13.1.2 - Seguridad de los servicios de red o 18.1.5 - Regulación de los controles criptográficos	NO aplica		
mp.info.4	FIRMA ELECTRÓNICA	27002:2013 o 10.1.1 - Política de uso de los controles criptográficos o 14.1.3 - Protección de las transacciones o 18.1.5 - Regulación de los controles criptográficos	SÍ aplica	Política de Firma Electrónica	- NO_ No hi ha normativa

mp.info.5	SELLOS DE TIEMPO	27002:2013 o 14.1.3 - Protección de las transacciones	NO aplica		
mp.info.6	LIMPIEZA DE DOCUMENTOS	27002:2013 o No se contempla OBS: Este aspecto no se contempla en las normas 27001 o 27002. Deberá cubrirse específicamente lo requerido por el ENS.	SÍ aplica	Normativa de Gestión de la clasificación y tratamiento de la Información	- NO_ No hi ha normativa
mp.info.9	COPIAS DE SEGURIDAD (BACKUP)	27002:2013 o 12.3.1 - Copias de seguridad de la información	SÍ aplica	- Normativa de Gestión del Respaldo de la Información - Herramienta + evidencias	- NO_ No hi ha normativa - SI: Eina + evidències
mp.s.1	PROTECCIÓN DEL CORREO ELECTRÓNICO (E-MAIL)	27002:2013 o 13.2.3 - Mensajería electrónica	SÍ aplica	Normativa de Gestión del Aseguramiento de Servicios - Instrucciones tècnicas de configuración	- NO: No hi ha normativa - SI: Existeixen manuals de bastionats de serveis.
mp.s.2	PROTECCIÓN DE SERVICIOS Y APLICACIONES WEB	27002:2013 o No se contempla OBS: Este aspecto no se contempla en las normas 27001 o 27002. Deberá cubrirse específicamente lo requerido por el ENS.	SÍ aplica	Normativa de Gestión del Aseguramiento de Servicios - Instrucciones técnicas de configuración	- NO: No hi ha normativa - SI: Existeixen manuals de bastionats de serveis.
mp.s.8	PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO	27002:2013 o 12.1.3 – Gestión de capacidades OBS: Este aspecto no se contempla en las normas 27001 o 27002. Deberá cubrirse específicamente lo requerido por el ENS.	SÍ aplica	- Normativa de Gestión de capacidades	- SI: Existeix normativa
mp.s.9	MEDIOS ALTERNATIVOS	27002:2013 o 17.2.1 - Disponibilidad de los medios de procesamiento de información	NO aplica		

Taula 34: Checklist auditoria controls ENS

A continuació s'inclourà l'acta de l'auditoria conforme amb la plantilla d'auditoria que es va desenvolupar a la fase de gestió documental del SGSI.

AUDITORIA INTERNA SGSI - FASE 1

AJUNTAMENT DE MISTIC

Quadre de Control

Títol:	Treball Final (Plantilla)		
Tipus de document:	REGISTRE		
Nom del Fitxer:	TFM.odt		
Classificació:	Ús Intern		
Estat:	Aprovat		
Autor:	**Juan Antonio Vera**		
Versió:	1.0	**Data: 28/12/20**	

Revisió i aprovació			
	Nom i cognoms	**Data**	**Signatura**
Revisat per:			
Aprovat per:			

Control de Canvis			
Versió	**Data**	**Autor**	**Descripció del Canvi**
1.0	28/12/20	Juan Antonio Vera	- Creació document

INFORME AUDITORIA INTERNA

Data: dd/mm//aaaa

I. DADES DE L'AUDITORIA INTERNA			
1.1. N.º de auditoria	01	1.2. Norma de referència	ENS
1.3. Data auditoria	11/12/2020		
1.4. Lloc d'auditoria	AJUNTAMENT MISTIC		

II. OBJECTIU DE L'AUDITORIA
- Avaluar el grau de compliment dels controls del document d'aplicabilitat de l'ENS a la finalització dels projectes de la FASE1

III. ABAST DE L'AUDITORIA
- L'abast coincideix amb l'abast de la definicio del SGSI. - Es farà servir com a referència el document d'aplicabilitat.

IV. EQUIP AUDITOR	
4.1. AUDITOR LÍDER	JUAN ANTONIO VERA (JAVERA)
4.2. AUDITORS INTERNS	JUAN ANTONIO VERA (JAVERA)

V. CONVIDATS	
5.1. EXPERTS	
5.2. OBSERVADORS	

VI. FORTALESES I FEBLESES	
FORTALESES	FEBLESES

- -	- -

VII. RESULTATS DE L'AUDITORIA	
N.º No conformitats:	N.º Oportunitats de millora:

No conformitats					
N.º	Menor ?	Procés/ Àrea	Descripció	Responsable	Auditor
1	SI	org.2	- No es presenten registres de coneixement per part dels empleats de la normativa	Responsable seguretat	JAVERA
2	SI	op.pl.1	- No existeix acta d'acceptació risc residual.	Responsable seguretat	JAVERA
3	SI	op.acc.1	- No existeix procedimient	Responsable sistemes	JAVERA
4	SI	op.acc.2	- No existeix normativa	Responsable sistemes	JAVERA
5	SI	op.acc.3	- No existeix normativa	Responsable sistemes	JAVERA
6	SI	op.acc.4	- No existeix normativa	Responsable sistemes	JAVERA
7	SI	op.acc.5	- No existeix normativa	Responsable sistemes	JAVERA
8	SI	op.acc.6	- No existeix normativa	Responsable sistemes	JAVERA
9	SI	op.acc.7	- No existeix normativa	Responsable sistemes	JAVERA
10	SI	op.exp.1	- No existeix normativa	Responsable sistemes	JAVERA
11	SI	op.exp.2	- No existeix normativa	Responsable sistemes	JAVERA
12	SI	op.exp.3	- No existeix procediment	Responsable sistemes	JAVERA
13	SI	op.exp.7	- No existeix normativa	Responsable sistemes	JAVERA

14	**SI**	**op.exp.8**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
15	**SI**	**op.ext.1**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
16	**NO**	**op.ext.2**	**- No existeix normativa - No existeix registres revisió SLAs**	**Responsable sistemes**	**JAVERA**
17	**SI**	**op.cont.1**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
18	**NO**	**op.mon.1**	**- No existeix normativa - No existeix IDS**	**Responsable sistemes**	**JAVERA**
19	**SI**	**op.mon.2**	**- No hi han registres d'indicadors (massa aviat per tenir dades)**	**Responsable sistemes**	**JAVERA**
20	**SI**	**mp.per.3**	**- No es presenten certificats d'assitència (encara no han començat cap curs)**	**Responsable sistemes**	**JAVERA**
21	**SI**	**mp.per.4**	**- No es presenten certificats d'assitència (encara no han començat cap curs)**	**Responsable sistemes**	**JAVERA**
22	**SI**	**mp.eq.1**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
23	**SI**	**mp.eq.2**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
24	**SI**	**mp.eq.3**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
25	**SI**	**mp.eq.9**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
26	**SI**	**mp.com.1**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
27	**SI**	**mp.com.2**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
28	**SI**	**mp.com.3**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
29	**SI**	**mp.si.1**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
30	**SI**	**mp.si.2**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**

31	**SI**	**mp.si.4**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
32	**SI**	**mp.si.5**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
33	**SI**	**mp.sw.1**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
34	**SI**	**mp.sw.1**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
35	**SI**	**mp.inf.2**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
36	**SI**	**mp.inf.4**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
37	**SI**	**mp.inf.6**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
38	**SI**	**mp.inf.9**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
39	**SI**	**mp.s.1**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**
40	**SI**	**mp.s.2**	**- No existeix normativa**	**Responsable sistemes**	**JAVERA**

Oportunitats de millora				
N.º	**Procés/Àrea**	**Descripció**	**Responsable**	**Auditor**

VIII. CONCLUSIONS AUDITORIA INTERNA
CONCLUSIÓ 1: **- S'ha detectat que encara falta molta normativa per redactar. És necessari poder plasmar en un document les diferents polítiques i normatives que es segueixen en els diferents aspectes valorats.** **- Tot i faltar la documentació, es verifiquen que s'estan aplicant mesures tècniques i que existeixen evidències de la seva aplicació.** **- Per això es classifiquen com a menors** **CONCLUSIÓ 2:** **- Es classifiquen com a una NO CONFORMITAT MAJOR en detectar que no s'estan aplicant cap salvaguarda en l'aspecte que s'estigui considerant. En aquest sentit,** **1. op.ext.2: GESTIÓ DIÀRIA => es necessita revisar periòdicament els SLAs dels proveïdors de les aplicacions contractades** **2. op.mon.1: DETECCIÓ DE INTRUSIÓ => es necessita implantar un IDS el més aviat possible per tal d'assegurar la xarxa davant possibles penetracions**

IX. APROVACIÓ INFORME	
ELABORAT PER:	**APROVAT PER:**
JUAN ANTONIO VERA	
Nom, càrrec i signatura **Data: __11__/_12___/_2020___**	**Nom, càrrec i signatura** **Data: ____/____/____**

8. Conclusions

El compliment de l'ENS per part d'un Ajuntament requereix d'una pla d'adequació a on es planifiqui unes etapes amb uns objectius clars i un resultats que puguin ser avaluats per tal de veure l'evolució de l'adequació en tot moment. Tenir clares aquestes fases i poder-les comunicar adequadament son claus per poder tirar endavant un projecte d'aquest tipus.

El fet de que l'Ajuntament hagi de complir amb l'ENS obliga a tota l'organització a treballar amb un procés d'implantació d'un SGSI completament desconegut per una entitat d'aquest tipus. Tot i això, el resultats que s'obtenen d'assegurar la gestió de la informació han de facilitar aquesta adaptació a tots els nivells, i l'esforç necessari en aquesta tasca.

Els esforços potser més importants els podem trobar a la fase d'anàlisi de riscos, atès que l'inventariat i categorització dels nostres actius, així com les salvaguardes implementades marcaren els riscos als que es troben sotmesos. Aquesta feina ha de ser una feina sincera, sense amagar les carències que l'organització pugui tenir atès que l'objectiu final és eliminar-ne totes aquelles que s'identifiquin (en aquest sentit, és clau tenir la confiança del personal tècnic a l'hora de transmetre el nivell d'implantació de les salvaguardes existents), El compromís per part de tothom (personal polític i caps de departaments) és crucial per poder realitzar un anàlisi de riscos sincer i coherent.

En relació als objectius plantejats en aquest TFM d'adequació podem concloure que:

- S'han posat les bases per mantenir un sistema de gestió documental que suporti el conjunt de normatives que es deriven de la implantació del SGSI

- S'han obtingut un conjunt de documentació (política de seguretat, gestió d'indicadors, gestió de rols i responsabilitats, etc) que han de marcar el camí pel desenvolupament de la restant normativa del sistema.

- S'ha obtingut un projecte d'anàlisi de riscos amb la identificació dels actius més importants, s'han caracteritzat les seves amenaces i avaluat els riscos associats.

- S’ha obtingut un coneixement ampli de l’eina PILAR i com fer-la servir durant les diferents fases de vida del SGSI.

- S’han extret una línia de projectes a implementar en una FASE 1 que haurà d’anar acompanyada de l’avaluació dels seus resultats per tal de definir uns nous projectes en fases posteriors.
- S’han comparat els controls ISO27001 vs ENS i s’ha avaluat la possibilitat de fer la doble adequació. S’ha arribat a la conclusió de que molts controls de l’ENS coincideixen amb els de la ISO27001 i que la conformitat amb l’ENS ens aplana molt el camí de la certificació ISO27001 (i a l’inrevés).

- . i que es poden fer servir per una etapa inicial, i que s’haurà de revisar i ampliar a cada iteració de millora contínua del procés SGSI. Entenem que el SGSI està sempre viu i, per tant, sempre s’ha d’anar revisant i ampliant.

Tot i que s’ha tractat la doble adequació a l’ENS i a la ISO27001, quedarà pendent per possibles etapes posteriors la revisió dels controls implementats per veure si satisfan els requeriments de totes dues normatives.

En relació a la metodologia prevista, crec que ha estat encertada atès que permet entregar resultats parcials en tot moment susceptibles a revisions i correccions en entregues successives. Això provoca que al haver de presentar resultats de cada fase del projecte cada poques setmanes permet un contacte continu amb la direcció del projecte i el no-oblit de la necessitat de gestió i seguiment de la implantació del SGSI dins de l’organització

Finalment, com a treballs de futur que no s’ha pogut explorar dins d’aquest TFM podem considerar la inclusió de l’adequació a LOPD-GDD/RGPD dins de l’anàlisi de riscos amb PILAR, i abordar un projecte complert d’adequació a l’ENS, ISO27001 i LOPD-GDD/RGPD. Aquest projecte suposarà una veritable transformació dins de l’organització, al haver-se d’alinear tothom amb el mateix objectiu: assegurament de la informació sota qualsevol format i dels sistemes que la gestionen.

9. Glossari

- Acceptació del risc: Acció o decisió d'acceptar les conseqüències o possibilitats que un risc es materialitzi.

- Autenticitat: Propietat que consisteix en que la entitat, individual o procés és qui dóna ser, o garanteix la font de dades.

- Causa o vulnerabilitat: Buit o fallada de seguretat.

- Confidencialitat: La propietat que aquesta informació estigui divulgada i no sigui divulgada a persones, entitats o processos no autoritzats.

- Declaració d'aplicabilitat: És un document on s'expressa quins controls de la norma s'implementaran i els no seleccionats (s'ha d'indicar perquè no).

- Disponibilitat: Propietat o característica dels actius. Consisteix en que les entitats o processos autoritzats tenen accés als actius quan es requereixen.

- Efecte o conseqüència: Impacte que té un sistema una determinada acció en un sistema (normalment negatiu).

- ENS: Esquema Nacional de Seguretat

- Escenari de risc: És el risc en si, és la combinació d'un conjunt d'amenaces que poden causar un impacte negatiu en els actius, concorde a a el vulnerabilitats explotades.

- Gestió del risc: Procés iteratiu que consta de passos que s'executen per tal gestionar les conseqüències del risc.

- Indicador: Mecanisme de mesurament o comparació de resultat, amb la finalitat d'obtenir el nivell d'efectivitat de compliment d'accions implementades, aquesta s'obté a partir de qualificacions.

- Integritat de les dades: Característica que indicaria que l'activitat d'informació no ha estat alterat de manera no autoritzada.

- LOPD-GDD: Llei Orgànica Protecció de Dades – Garantia Drets Digitals

- Norma: Principi que s'imposa o s'adopta per dirigir la conducta o la correcta realització d'una acció o el correcte desenvolupament d'una activitat.

- Política de seguretat: Document aprovat per l'alta gerència que expressa de manera la voluntat de la mateixa en relació a la seguretat de la informació, expressant què cosa es pot o no realitzar respecte a la seguretat de la informació.

- Probabilitat: Possibilitat que ocorri un esdeveniment, la qual aquesta mesura en percentatge.

- RGPD: Reglament de Protecció de Dades.

- Risc: Esdeveniment no rutinari que en el moment que succeeixi, pot generar impactes negatius en els processo i/o els objectius del negoci.

- Risc acceptable: És aquell risc que, una vegada qualificat, el seu nivell d'impacte pot ser tolerat per la organització, això és, s'accepta i s'assumeix

- Risc intrínsec: Risc associat al tipus d'actius que es gestionen. No es consideren salvaguardes aplicades.

- Risc residual: Risc resultant després d'executar mesures de tractament.

- Traçabilitat: Característica que consisteix en les actuacions d'una entitat que poden ser imputades en aquesta entitat o subjecte.

10. Bibliografia

- [1] Abhishek Chopra, Mukund Chaudhary - Implementing An Information Security Management System_ Security Management Based On ISO 27001 Guidelines-Apress (2020)

- [2] Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
  https://www.boe.es/buscar/act.php?id=BOE-A-2007-12352

- [3] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
  https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330

- [4] MAGERIT v.3 : Metodologia d'Anàlisi i Gestió de Riscos dels Sistemes d'Informació
  https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=ca

- [5] EAR / PILAR https://www.ar-tools.com/magerit/index.html

- [6] Serie 800 (ENS)
  https://www.ccn-cert.cni.es/ca/guies/serie-800-ens.html

- [7] Material assignatura SISTEMES DE SEGURETAT DE LA INFORMACIÓ

- [8] Esquema Nacional de Seguridad – Certificaciones 27001
  https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/543-ccn-stic-825-ens-iso27001/file.htm
  l
  [9] Esquema Nacional de Seguridad e ISO 27001 ¿Cómo puedo implantar ambos en mi empresa?
  https://empresas.blogthinkbig.com/implantar-esquema-nacional-de-seguridad-iso/

- [10] Esquema Nacional de Seguridad ENS 27001
  https://www.isotools.org/2013/09/20/esquema-nacional-de-seguridad/

- [11] CCN-STIC-852 - Aplicación del ENS en organismos pagadores

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/4943-ccn-stic-852-aplicacion-del-ens-en-organismos-pagadores.html

- [12] Capability Maturity Model https://es.wikipedia.org/wiki/Capability_Maturity_Model

- [13] Steve G Watkins - An Introduction to Information Security and ISO 27001-IT Governance Publishing (2008)

- [14] Sigurjon Thor Arnason, Keith D. Willett - How to Achieve 27001 Certification_ An Example of Applied Compliance Management-Auerbach Publications (2007)

- [15] Implementar ISO 27001 Paso a Paso- 5 ¿Que Documentar y por qué? https://normaiso27001.es/fase-5-documentacion-del-sgsi/

- [16] Security Policy Templates https://www.sans.org/information-security-policy/

- [17] ENS – Anexe II https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1071

11. Annexos

Aquí es detallen tots els documents generats dins d'aquest TFM i que, juntament amb aquesta memòria, engloben tot els lliuraments d'aquest TFM.

- DOCUMENT_APLICABILITAT_ENS.pdf
- GUIA_GESTIO_INDICADORS.pdf
- RELACIO_INDICADORS.pdf
- GUIA_ROLS_I_RESPONSABILITATS.pdf
- GUIA_GESTOR_DOCUMENTAL.pdf
- PROCEDIMENT_ANALISIS_DE_RISCOS.pdf
- POLITICA_SEGURETAT.pdf
- PROCEDIMENT_REVISIO_DIRECCIO.pdf
- PLANTILLA_INFORME_AUDITORIA.pdf
- PLANTILLA_PLANIFICACIO_AUDITORIA_INTERNA.pdf
- PROCEDIMENT_AUDITORIA_INTERNA.pdf

A més dels documents anteriors, es facilita el projecte PILAR generat dins d'aquest TFM.