Pla adequació Ajuntament Esquema Nacional Seguretat

Alumne: Juan Antonio Vera Nieto

Àrea: Sistemes de Gestió de la Seguretat de la Informació (MISTIC - UOC)
Consultor: Arsenio Tortajada Gallego
Data Lliurament: 28/12/2020

Justificació

- INFORMACIÓ

- És el valor més important d'una organització

- SERVEIS

- Al voltant de la informació es presten serveis
- Els serveis aporten valor a les organitzacions

- Per tant, PROTEGIR LA INFORMACIÓ I SERVEIS ÉS PROTEGIR ELS OBJECTIUS DE L'ORGANITZACIÓ

- Les AAPP gestionen informació i presten serveis.

- Al igual que la resta d'organitzacions, les AAPP estan sotmeses a amenaces i riscos.

Protecció de la Informació: Dimensions de seguretat

- Confidencialitat:

Propietat o característica consistent en el fet que la informació ni es posa a disposició, ni es revela a individus, entitats o processos no autoritzats.

- Disponibilitat:

Propietat o característica dels actius consistent en què les entitats o processos autoritzats tenen accés als mateixos quan ho requereixen.

- Integritat:

propietat o característica consistent en el fet que l'actiu d'informació no ha estat alterat de manera no autoritzada.

- Autenticitat

Propietat o característica consistent en el fet que una entitat és qui diu ser o bé que garanteix la font de la qual procedeixen les dades.

- Traçabilitat

Propietat o característica consistent en el fet que les actuacions d'una entitat poden ser imputades exclusivament a aquesta entitat.

SGSI

- Disseny, implantació, manteniment d'un conjunt de processos per gestionar eficientment l'accessibilitat de la informació, buscant assegurar la confidencialitat, integritat i disponibilitat dels actius d'informació minimitzant alhora els riscos de seguretat de la informació.

- Ha de seguir sent eficient durant un llarg temps adaptant-se als canvis interns de l'organització així com els externs de l'entorn.

ISO 27001

- Estàndard per la implantació de SGSI
- Segueix l'enfoc de millora contínua

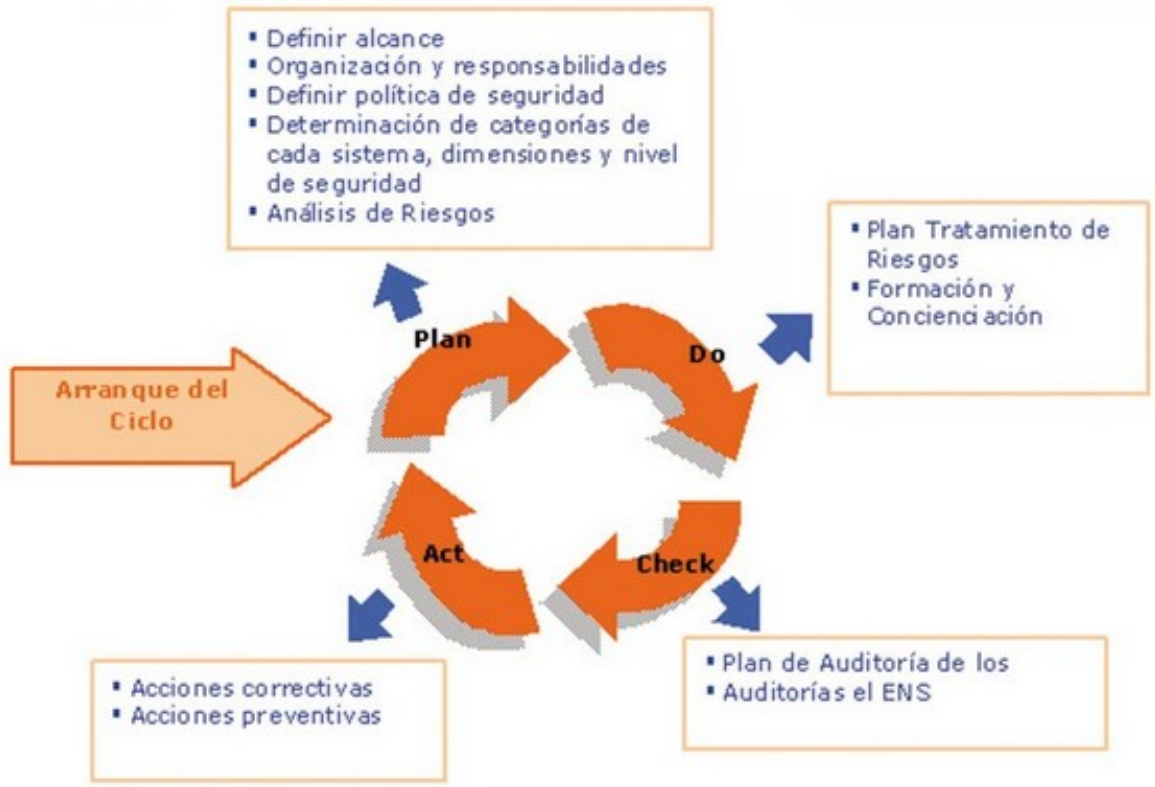
Pla-Do-Check-Act (PDCA) que significa "Planificar-Fer-Controlar-Actuar"

- Pla (planificar): és una fase de disseny del SGSI, realitzant l'avaluació de riscos de seguretat de la informació i la selecció de controls adequats .
- Do (fer): Implantació dels controls (ISO27002)
- Check (controlar): Revisar i avaluar (eficàcia i eficiència) del SGSI.
- Act (actuar): Realització de modificacions per corregir/millorar el SGSI

Esquema Nacional de Seguretat (ENS)

- Reial Decret 3/2010 regula Esquema Nacional de Seguretat. Obligació per totes les AAPP

- Principis bàsics:
  - Seguretat integral
  - Gestió de riscos
  - Categorització de sistemes
  - Catàleg de controls
  - Avaluació periòdica (PDCA)



ENS – Mesures de controls (annex II)

ENS vs ISO27001

Concepte	ISO/IEC 27000	ENS
Tipus norma	Voluntari	Obligatori (AAPP)
Abast	Lliure	Obligat sistemes prestació serveis ciutadans
Categorització	NO	SÍ (BAIX, MITJÀ i ALTA)
Controls	144 controls	75 controls (en funció de la categoria)
Orientada a riscos ?	Sí	Sí
Auditories ?	Sí - periòdiques	Sí - biannual

- CCN-STIC 825 - ESQUEMA NACIONAL DE SEGURETAT CERTIFICACIONS 27001
- CCN-STIC-852 - Aplicació del ENS en organismes pagadors

Metodologia adaptació ENS

- FASE 1: Context, abast i anàlisi diferencial
- FASE 2: Sistema de gestió documental
- FASE 3: Anàlisi de riscos
- FASE 4: Proposta de projectes
- FASE 5: Auditoria de compliment
- Conclusions

ENS – FASE 1: Context i abast

Context:

- Ajuntament 40.000 hab (recursos propis).
- 1 CPD: 4 servidors (20 VM), 200 PCS (Windows,Office 2019) 2 cabines de disc
- Programari JAVA (Tomcat/JBOSS)

Abast:

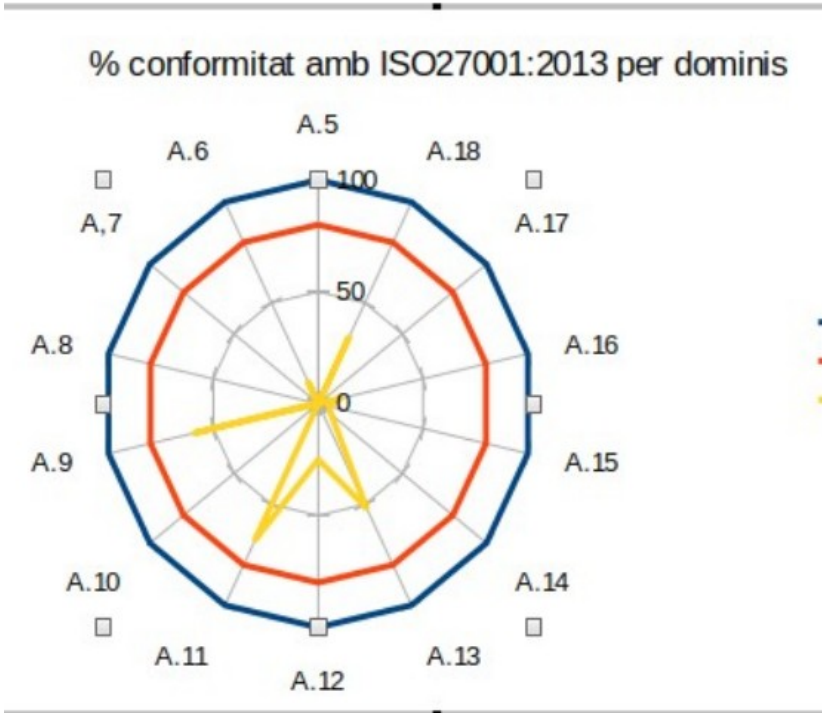
- Seu electrònica, gestor d'expedients, atenció presencial
- ERP municipal

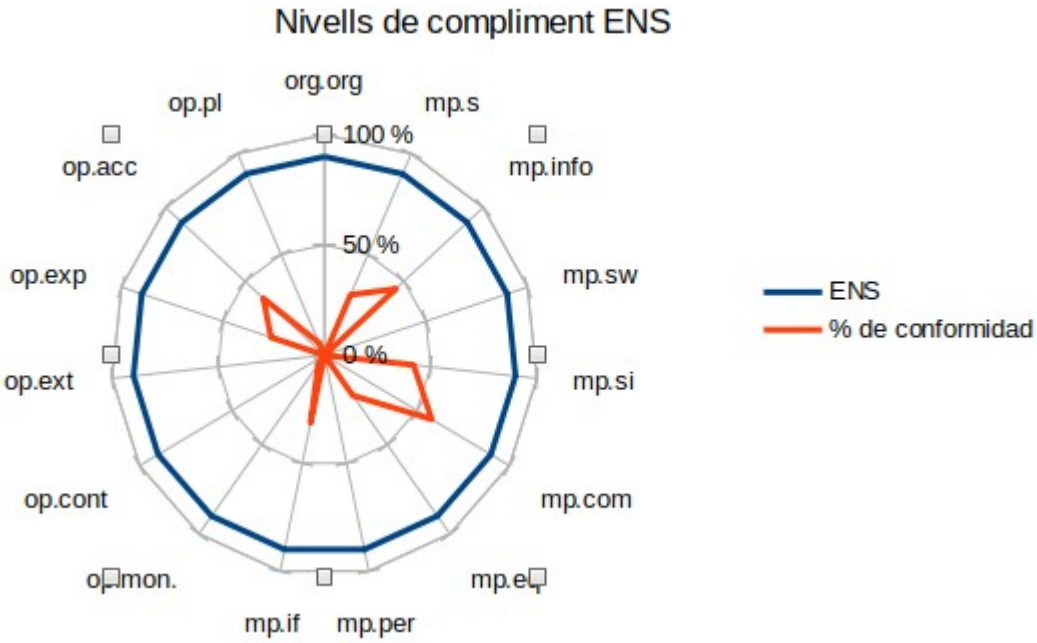
FASE 1: Anàlisi diferencial – Models de Maduresa

- Defineix la maduresa de la implantació de processos

Valor	Efectivitat	Significat	Descripió
L0	0 %	Inexistent	No existeix
L1	10 %	Inicial /Ad-hoc	L'èxit es fruit dels esforços personal
L2	50 %	Reproduïble, però intuitiu	Basat en l'experiència, però sense comunicació formal
L3	90 %	Procéss definit	Procés implantat i documentat
L4	95 %	Gestionat i mesurable	Existeixen indicadors
L5	100 %	Optimitzat	Avaluació dels indicadors i millora contínua
L6	N/A	No aplica	No aplica

FASE 1 – Anàlisi diferencial – Situació inicial



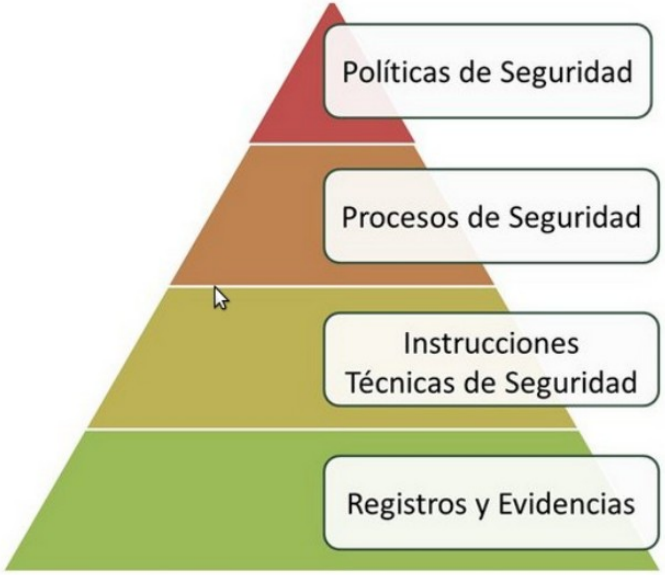


FASE 2: Gestió documental

- Formalitzar polítiques, normes, instruccions, procediments i registres => deixar evidència

- Documents

- Guia Gestor Documental
- Declaració d'aplicabilitat ENS
- Política de seguretat
- Indicadors: Gestió indicadors i relació d'indicadors.
- Procediment revisió direcció
- Gestió rols responsabilitat
- Metodologia gestió de riscos
- Auditories internes: Programa annual i procediment auditoria interna



FASE 3: Anàlisi de riscos (1/2)

- **MAGERIT**
  - Determinació actius
  - Anàlisi amenaces
  - Salvaguardes existents
  - Estimació de l'impacte
  - Estimació ocurrència
  - Estimació dels risc

FASE 3: Anàlisi de riscos: PILAR

- **EAR (Entorno de Análisis de Riesgos)**
- **Segueix metodologia MAGERIT.**
- **Perfils de seguretat: ENS, ISO27001**
- **Funcionament:**
  - Identificació i categorització d'actius
  - Valoració dels actius
  - Dependències
  - Caracterització de les amenaces
  - Aplicació salvaguardes i perfils de seguretat
  - Càlcul risc
  - Accions de tractament

FASE 3: PILAR -> Fases i riscos

[MISTIC_TFM] ens:2015 > valoración

Editar Expandir Ver Exportar Importar Estad□ sticas Seleccionar Gr□ ficas

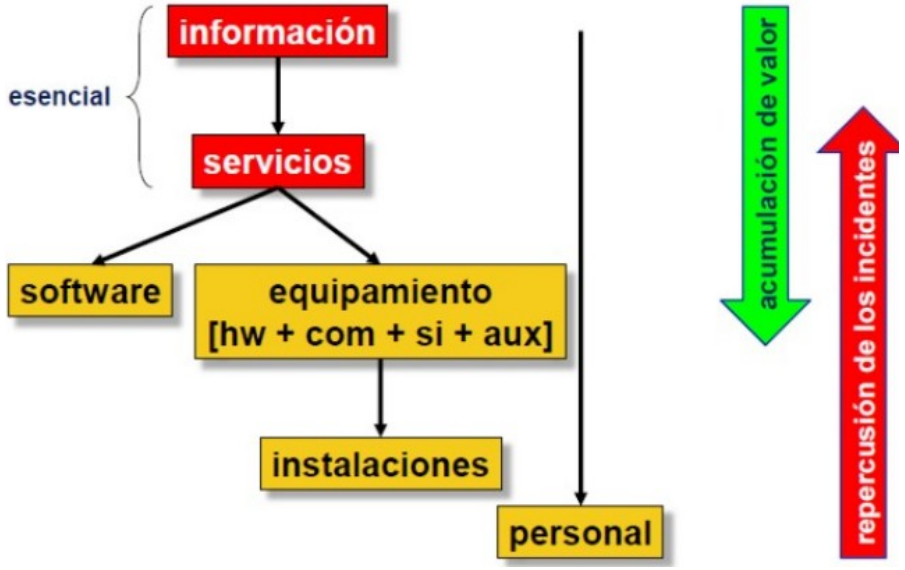
base] Base | Fuentes de informaci□ n

	reco...		control	dudas	fuente	aplica	come...	current	FASE0	target	ENS
☐			[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)					L0-L3 (L0-L4)	L0-L3	_-L3 (L2-L4)	L2-L3
☑	5		[org] Marco organizativo			M		L0	L3	L3	L2-L3
☑	5		[org.1] Pol□ tica de Seguridad			M		L0	L3	L3	L2-L3
☑	5		[org.2] Normativa de seguridad			M		L0	L3	L3	L2-L3 (L2)
☑	5		[org.3] Procedimientos de seguridad			M		L0	L3	L3	L2-L3 (L2)
☑	5		[org.4] Proceso de autorizaci□ n			M		L0	L3	L3	L2-L3
☑	8		[op] Marco operacional			M		L0-L3 (L0-L4)	L0-L3	_-L3 (L2-L4)	L2-L3
☑	5		[op.pl] Planificaci□ n			M		L0-L2 (L0-L3)	L0-L3	_-L3 (L3)	L2-L3
☐	3		[op.pl.1] An□ lisis de riesgos			M		L0	L3	L3	L3
☐	5		[op.pl.2] Arquitectura de seguridad			M		L0-L1 (L0-L3)	L0-L3	L0-L3 (L3)	L2-L3
☐	5		[op.pl.3] Adquisici□ n de nuevos componentes			M		L0	L3	L3	L2-L3 (L2)
☐	3		[op.pl.4] Dimensionamiento / Gesti□ n de capacidades			M		L0-L2 (L2)	L3	L3	L2-L3
☐	3		[op.pl.5] Componentes certificados					n.a. (L0)	n.a. (L0)	(L3)	L3
☑	8		[op.acc] Control de acceso			M		L0-L3 (L0-L4)	L1-L3 (L0-L3)	L1-L3 (L2-L4)	L2-L3
☐	5		[op.acc.1] Identificaci□ n			M		L1-L2	L2 (L2-L3)	L2 (L3)	L2-L3
☐	4		[op.acc.2] Requisitos de acceso			M		L2 (L2-L3)	L3	L3	L3 (L2-L3)
☐	7		[op.acc.3] Segregaci□ n de funciones y tareas			M		L0 (L0-L4)	L3	L3	L3 (L2-L3)
☐	5		[op.acc.4] Proceso de gesti□ n de derechos de acceso			M		L2-L3	L2-L3 (L3)	L2-L3 (L3)	L3 (L2-L3)
☐	8		[op.acc.5] Mecanismo de autenticaci□ n			M		L2 (L1-L2)	L3	L3 (L2-L4)	L3 (L2-L3)
☐	4		[op.acc.6] Acceso local (local logon)			M		L2	L2-L3	L2-L3 (L3)	L2-L3
☐	5		[op.acc.7] Acceso remoto (remote login)			M		L1-L3 (L0-L3)	L1-L3 (L0-L3)	L1-L3 (L3)	L2-L3
☑	8		[op.exp] Explotaci□ n			M		L0-L3 (L0-L4)	L0-L3	L0-L3 (L3)	L2-L3
☐	4		[op.exp.1] Inventario de activos			M		L0 (L0-L2)	L0 (L0-L3)	L0 (L3)	L3 (L2-L3)
☐	8		[op.exp.2] Configuraci□ n de seguridad			M		L1	L1	L1 (L3)	L3 (L2-L3)
☐	5		[op.exp.3] Gesti□ n de la configuraci□ n			M		L1-L2 (L0-L3)	L1-L2 (L0-L3)	L1-L2 (L3)	L2-L3
☐	5		[op.exp.4] Mantenimiento			M		L1 (L0-L1)	L1 (L0)	L1 (L3)	L3 (L2-L3)
☐	5		[op.exp.5] Gesti□ n de cambios			M		L0	L0 (L0-L1)	L0 (L3)	L3 (L2-L3)
☐	8		[op.exp.6] Protecci□ n frente a c□ digo da□ ino			M		L3 (L3-L4)	L3 (L0-L3)	L3	L3 (L2-L3)
☐	5		[op.exp.7] Gesti□ n de incidentes			M		L2 (L0-L3)	L2 (L0-L3)	L2 (L3)	L3 (L2-L3)
☐	5		[op.exp.8] Registro de la actividad de los usuarios			M		L1 (L0-L2)	L1 (L0-L3)	L1 (L3)	L2-L3

FASE 3: Anàlisi de riscos → Identificació i valoració d'actius

Identificació d'actius

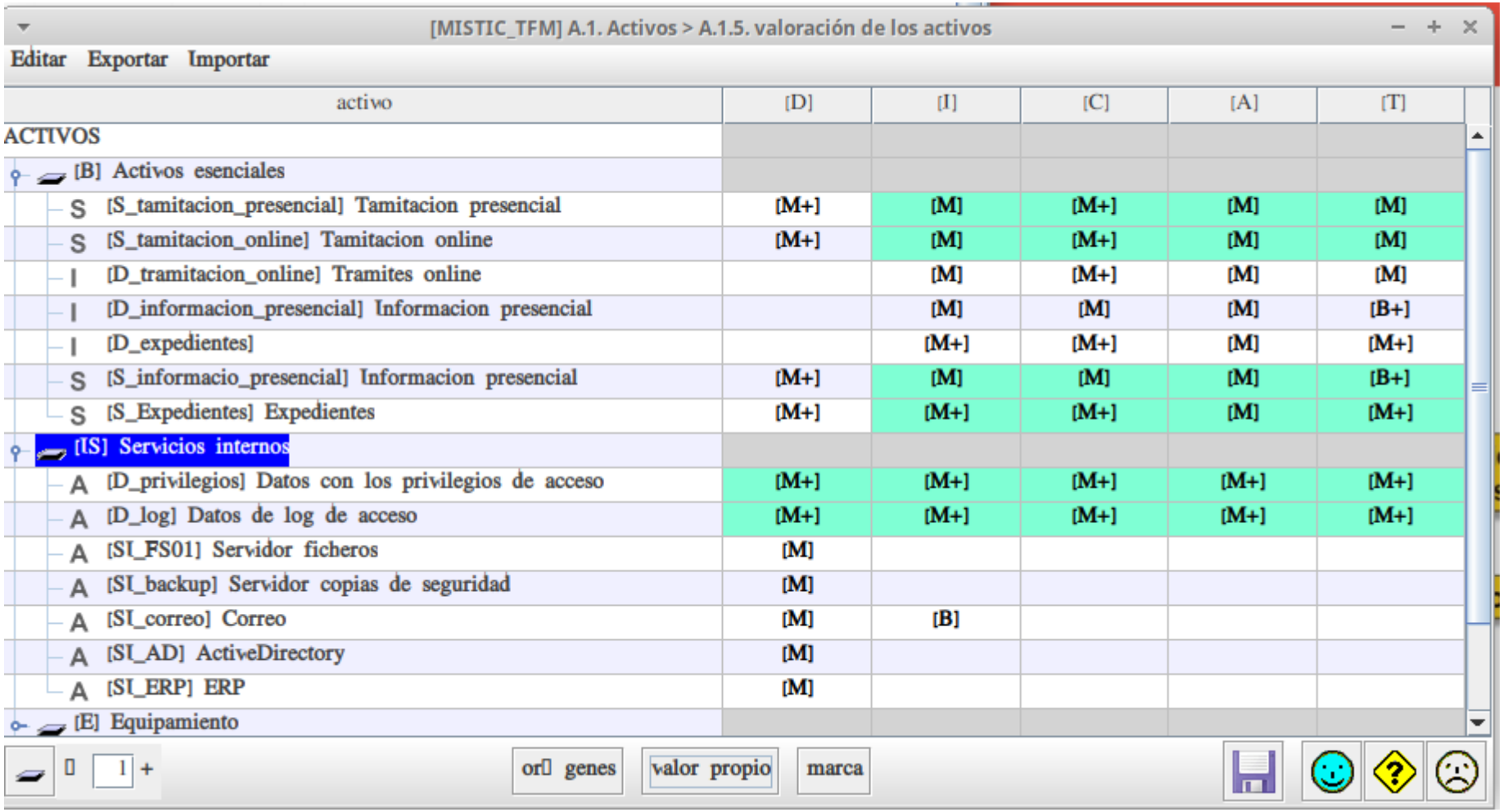
- Identificació d'actius essencials i de suport
- Categorització (tipus d'amenaces)



Valoració d'actius

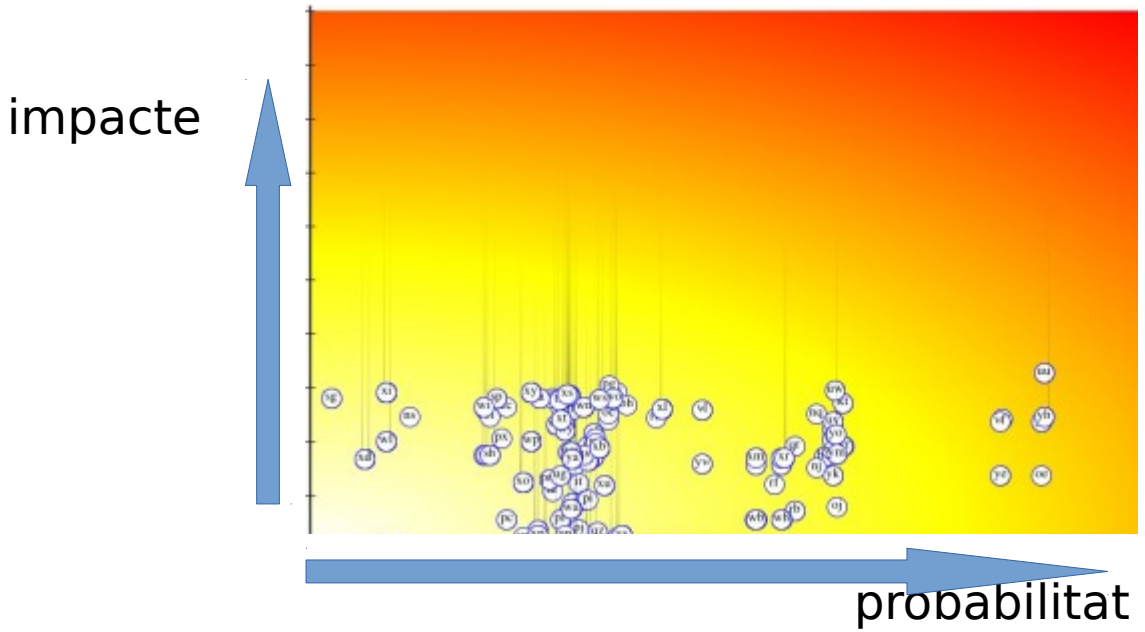
- Valoració dimensions (DICAT) actius: Baix, Mitjà, Alt
- Dependències

FASE 3: Actius → Valoració per dominis



FASE 3: Anàlisi de riscos → Valoració d'amenaces i vulnerabilitats

- **Catàleg d'amenaces extensible de PILAR.**
- **Mapa de risc intrínsec (sense salvaguardes)**
- **Mapa de risc residual (amb salvaguardes)**
- **Zones "calentes" => risc a tractar**



FASE 4: Proposta de projectes

- Projectes dividits en FASES: cicle PDCA.

- Objectius dels projectes: Conscienciació, compliment i reducció de risc

- Projectes:

- PROJECTE 1: MARC ORGANITZATIU: Política documental, política de seguretat, normativa de seguretat, procediments de seguretat, procés d'autorització.

- PROJECTE 2: FORMACIÓ I CONSCIENCIACIÓ: Pla de formació RRHH.

- PROJECTE 3: PLANIFICACIÓ DE LA SEGURETAT: Inventari d'actius, gestió de riscos, arquitectura de seguretat

- PROJECTE 4: NORMATIVA ACTUALITZACIÓ DE VERSIONS: Periode d'actualitzacions, procediments, entorn de test

- PROJECTE 5: NORMATIVA DE GESTIÓ DE ACCÉS LÒGIC: Política de contrasenyes, identificadors d'usuari, mínim privilegi

- PROJECTE 6: NORMATIVA DE SEGURETAT FÍSICA I ENTORN: Mapa d'instal·lacions, identifciació de persones, registre d'entrades/sortides.

- PROJECTE 7: PROTECCIÓ DE LES COMUNICACIONS: Configuració mínima, desactivació de serveis, eliminació usuaris per defecte, etc .

FASE 5: AUDITORIA

- Validació estat actual

- Declaració d'aplicabilitat

- Verificació salvaguardes

- Infome auditoria:

- Número de conformitats menors: Salvaguarda parcialment aplicada.

- Número de conformitats majors: Salvaguarda no aplicada

AUDITORIA INTERNA: CONCLUSIONS

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

CONCLUSIONS TFM (1/2)

- La implantació SGSI és un procés integral, i afecta a tothom.

- Es necessita un lideratge i suport clar de la direcció

- La implantació requereix un pla director

- ENS: La seguretat no és opcional → ÉS UNA OBLIGACIÓ !!

- Fonamental la gestió de riscos

- PILAR: Molt potent, poc amigable.

CONCLUSIONS TFM (2/2)

- ENS + ISO27001

- Objectius similars
- Correspondència entre controls i salvaguardes

- ENS + ISO27001 + LOPD-GDD/RGPD

- Tancar la roda de la seguretat
- Projecte integral

GRÀCIES