Esquema Nacional de Seguretat
- Resum executiu -

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

Motivació del projecte

- L’Ajuntament té la voluntat de prestar el millor servei possible a la ciutadania.

- Per fer-ho, farà ús de les TIC com a element facilitador.

- L’Ajuntament és conscient dels perills i amenaces associats i vol gestionar la seguretat en la seva prestació.

- L’Ajuntament és conscient de l’obligatorietat en l’aplicació de l’Esquema Nacional de Seguretat.

Missió, Visió i Valors Ajuntament

- MISSIÓ: 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: 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.

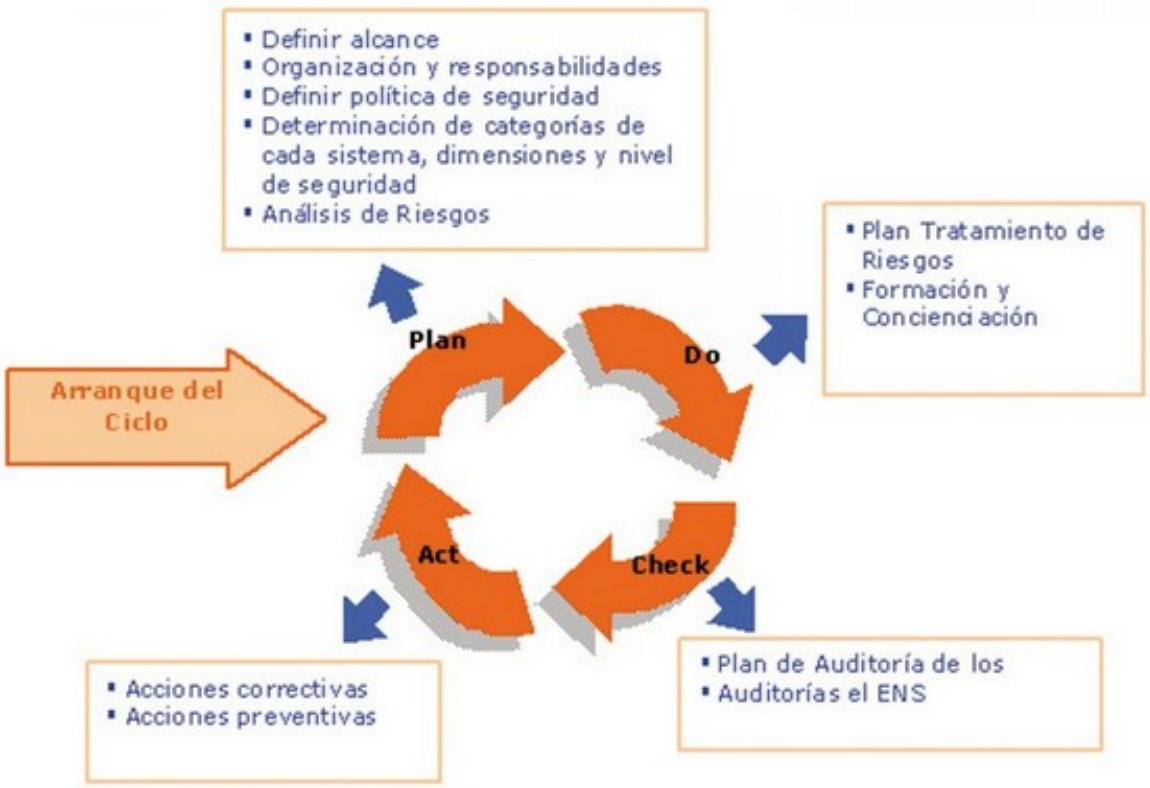
- Governança basada en les persones i destinades a les persones. Cohesió, civisme i convivència

.

Esquema Nacional de Seguretat (ENS)

- Reial Decret 3/2010 regula Esquema Nacional de Seguretat. Obligatori 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)

PLA DE PROJECTE: ADEQUACIÓ ENS

- El projecte es divideix en les següents FASES:

- 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

- Mesura el grau de compliment d'un control de l'annex II

- ENS requereix L3 (90% de compliment).

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

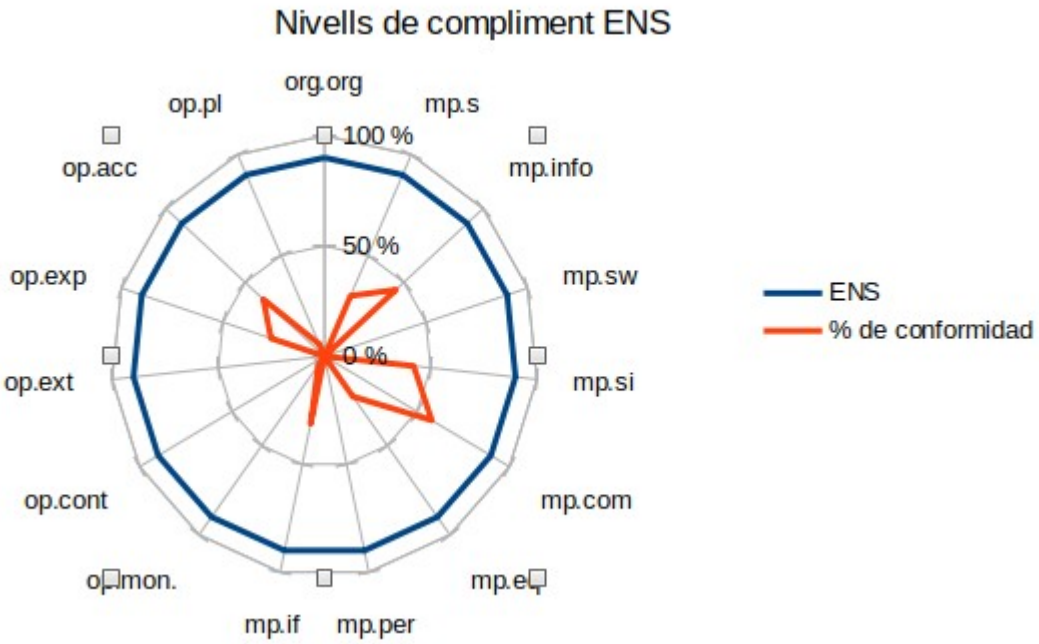
SITUACIÓ INICIAL:

- FORTALESES:

- Suport de la direcció
- Existència controls tècnics

- FEBLESES:

- Manca de normativa
- Manca d'alguns controls tècnics
- Manca formació i conscienciació.



FASE 2: Gestió documental

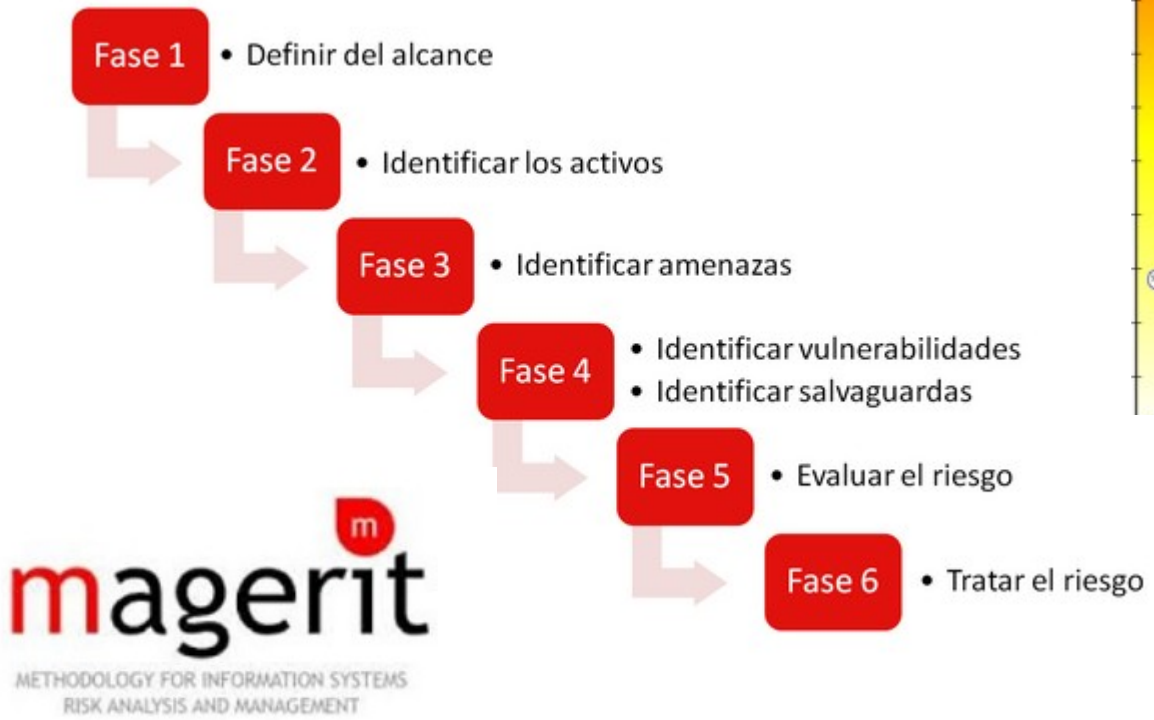
- **OBJ: Establir la gestió documental del SGSI**
- **Documents**
  - Guia Gestor Documental
  - Declaració d'aplicabilitat ENS
  - Política de seguretat
  - Indicadors: Gestió indicadors i relació d'indicadors.
  - Procediment revisió direcció
  - Gestió rols responsabilitat
  - Metodologia gestió de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

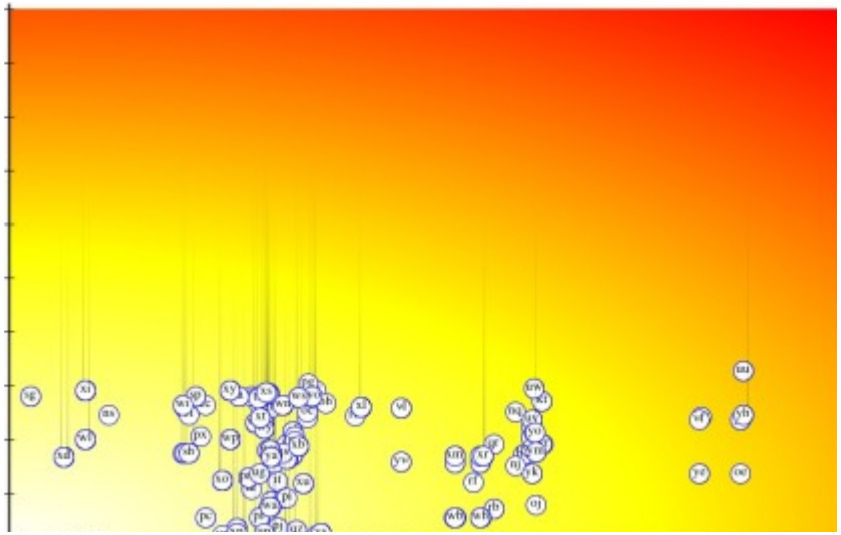
FASE 3: Anàlisi de riscos

OBJ: Determinar els riscos de l'Ajuntament

- Metodologia anàlisi de riscos: MAGERIT

Resultat: Mapa de riscos





MAPA DE RISCOS

FASE 4: Proposta de projectes

- 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 INTERNA

VIII. CONCLUSIONS AUDITORIA INTERNA

CONCLUSIÓ 1:

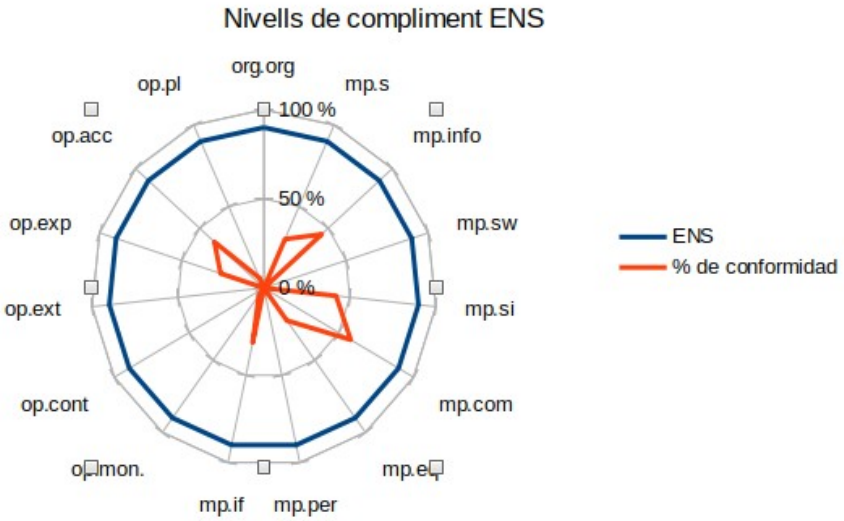
- S'ha detectat que encara falta molta normativa per redactar. És necessari poder plasmar en un document les diferents polítiques i normatives que es segueixen en els diferents aspectes valorats.
- Tot i faltar la documentació, es verifiquen que s'estan aplicant mesures tècniques i que existeixen evidències de la seva aplicació.
- Per això es classifiquen com a menors

CONCLUSIÓ 2:

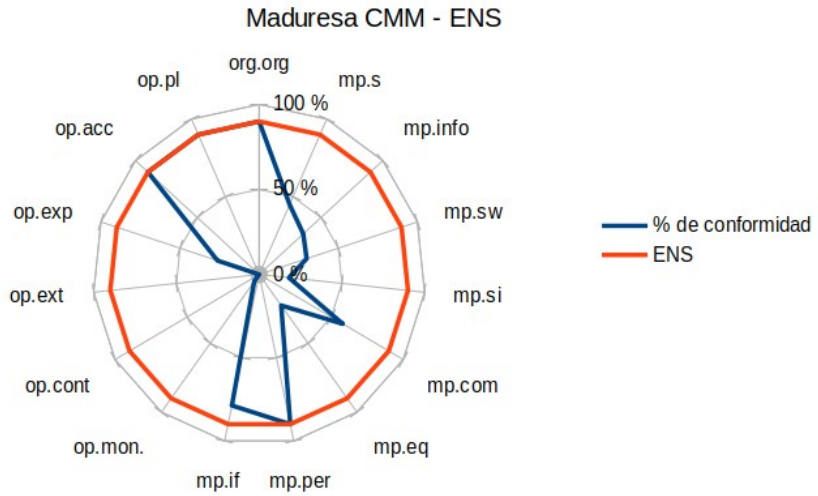
- Es classifiquen com a una NO CONFORMITAT MAJOR en detectar que no s'estan aplicant cap salvaguarda en l'aspecte que s'estigui considerant. En aquest sentit,

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

EVOLUCIÓ COMPLIMENT



Situació inicial



Situació final

RECOMENACIONS

- Seguiment del SGSI.

- Projectes a abordar:

- Definició SLA amb proveïdors externs
- Monitoratge del sistema
- Gestió de la continuïtat del servei.
- Protecció mitjans d'informació

GRÀCIES