PLA DIRECTOR DE SEGURETAT

AJUNTAMENT DE FITA ALTA

Juny de 2016

Alumne : Andreu Retamero Pallarès
Consultor : Arsenio Tortajada Gallego
Director : Carles Garrigues Olivella

ÍNDEX

- Motivació
- Enfoc del projecte
- Descripció de les tasques realitzades
- Conclusions

ÍNDEX

Motivació

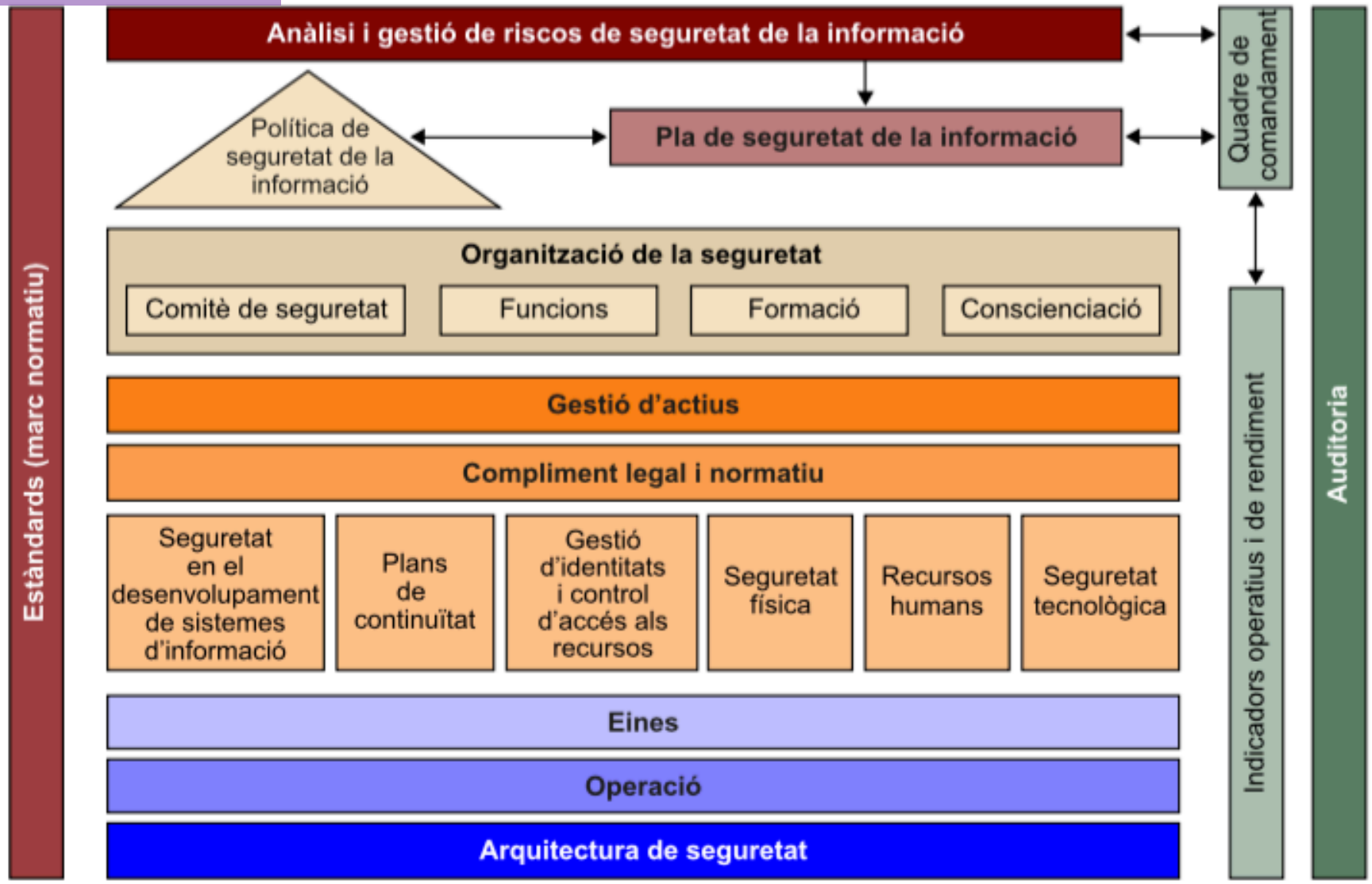
- Les AAPP utilitzen serveis TIC
- Els serveis TIC s'han de protegir
- Normativa d'obligat compliment per a les AAPP
  - LOPD
  - Esquema Nacional de Seguretat
- Administració electrònica
  - Lleis 39/2015 i 40/2015
- Tractament integral de la seguretat
  - Normes ISO/IEC 27000 (27001 i 27002)

Motivació - Els pilars de la Seguretat de la Informació

- Confidencialitat
- Integritat
- Disponibilitat
- Autenticitat
- Traçabilitat

Els pilars de la seguretat de la informació

Motivació - Procés de Gestió de la Seguretat



Motivació - Procés de Gestió de la Seguretat

ISO/IEC 27001:2013
ISO/IEC 27002:2013

PLA DIRECTOR

ENS
LOPD

Estàndards (marc normatiu)

Anàlisi i gestió de riscos de seguretat de la informació

Política de seguretat de la informació

Pla de seguretat de la informació

Quadre de comandament

Organització de la seguretat

Comitè de seguretat | Funcions | Formació | Conscienciació

Gestió d'actius

Compliment legal i normatiu

Seguretat en el desenvolupament de sistemes d'informació | Plans de continuïtat | Gestió d'identitats i control d'accés als recursos | Seguretat física | Recursos humans | Seguretat tecnològica

Eines

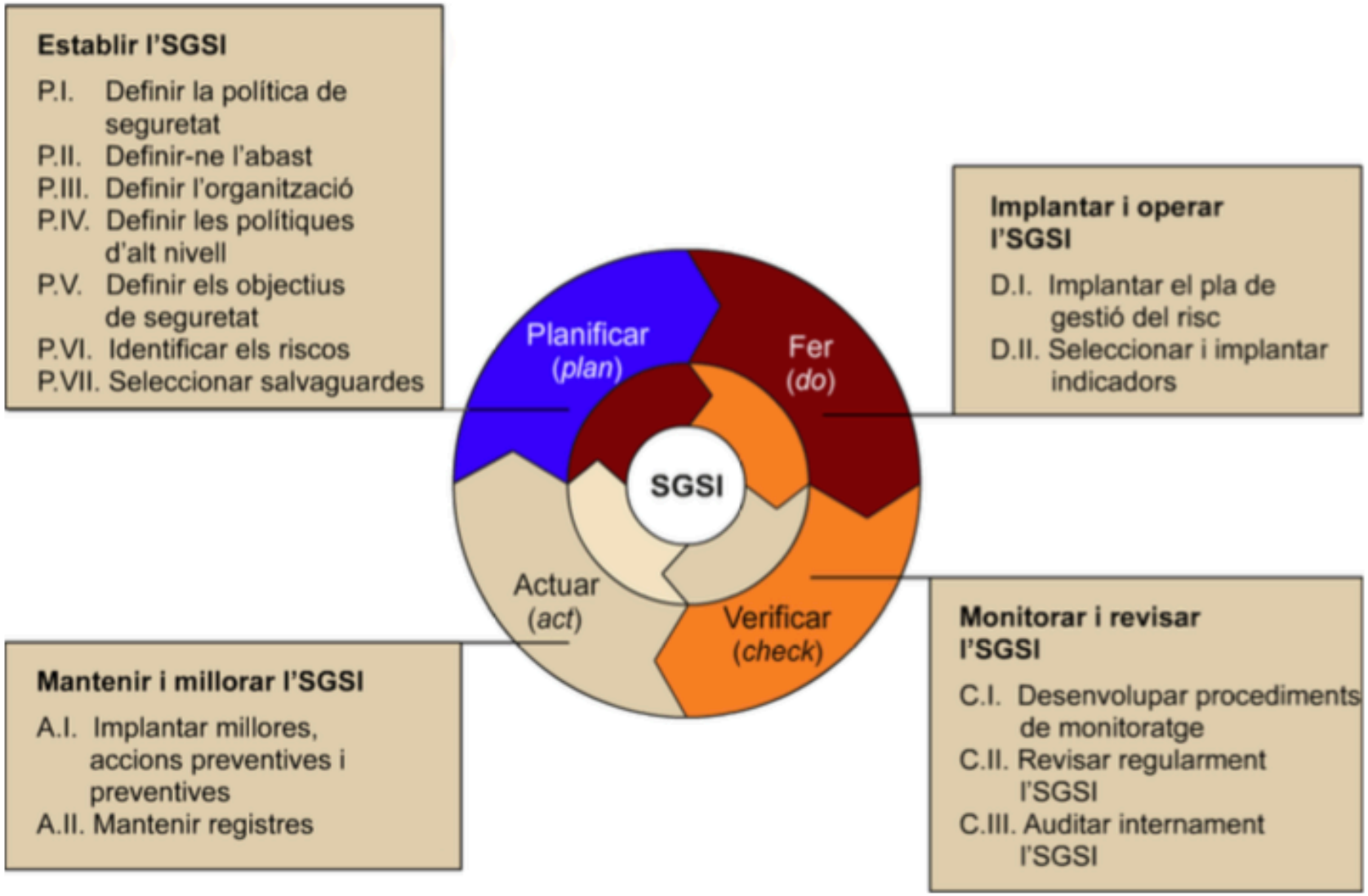
Operació

Arquitectura de seguretat

Indicadors operatius i de rendiment

Auditoria

Motivació - ISO/IEC 27001:2013



ÍNDEX

Enfoc del projecte

Aproximació per fases

1. Situació actual: objectius i anàlisi diferencial
2. Sistema de gestió documental
3. Anàlisi de riscos
4. Proposta de projectes
5. Auditoria de compliment
6. Presentació de resultats

Enfoc del projecte - Situació actual

- Selecció de l'organització d'estudi
- Definició de l'abast del Pla Director
- Anàlisi de compliment inicial

Enfoc del projecte - Sistema de gestió documental

Documents elaborats

- Política de Seguretat
- Procediment d'auditories internes
- Gestió d'indicadors
- Procediment de revisió per la direcció
- Gestió de rols i responsabilitats
- Metodologia d'anàlisi de riscos
- Declaració d'aplicabilitat

Enfoc del projecte - Anàlisi de riscos

Metodologia MAGERIT

- Identificació i valoració dels actius
- Definició de les amenaces
- Avaluació del risc i l'impacte potencial

Eines d'anàlisi de risc EAR-PILAR / CCN-CERT

- PILAR
- Micro Pilar

Enfoc del projecte - Proposta de projectes

Planificació dels projectes

- Definició de 12 projectes
  - Projectes de primer semestre
  - Projectes de segon semestre

Definició dels objectius dels projectes

Enfoc del projecte - Auditoria de compliment

- Auditoria dels controls de la ISO/IEC 27002:2013
- Informe d'auditoria
- Recomanacions de millora

Enfoc del projecte - Presentació de resultats

- Memòria del projecte
- Resum executiu
- Presentació de defensa del treball
- Vídeo de defensa del treball

ÍNDEX

Tasques realitzades

Aproximació per fases

1. Situació actual: objectius i anàlisi diferencial
2. Sistema de gestió documental
3. Anàlisi de riscos
4. Proposta de projectes
5. Auditoria de compliment
6. Presentació de resultats

Tasques realitzades- Situació actual: contextualització

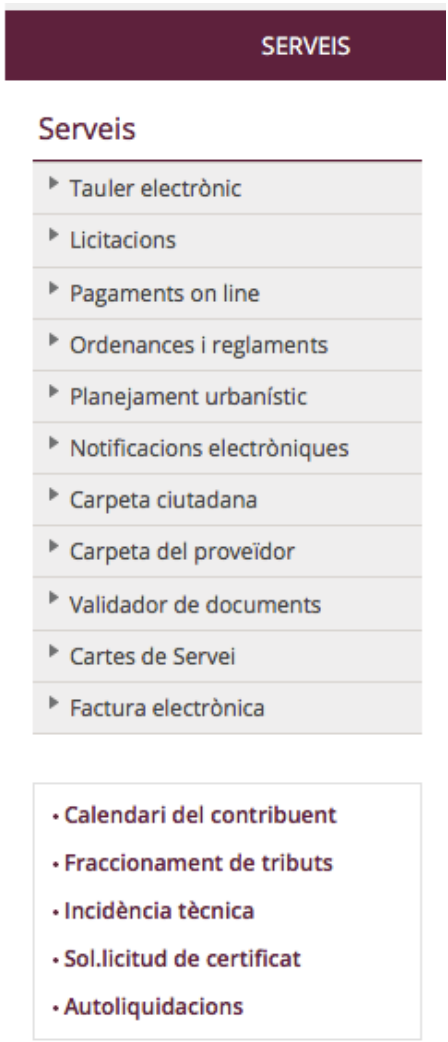
- Ajuntament de Fita Alta
- Municipi de 100.000 habitants
- 800 treballadors i 700 ordinadors
- 80 servidors
- 2 CPD
- Tecnologia basada en la virtualització
- 40 edificis municipals connectats amb FO
- Xarxa de telecomunicacions pròpia
- Gestió de telefonia IP
- Personal propi de TI i personal extern

Tasques realitzades - Situació actual: Abast del Pla (I)

Sistemes d'informació de la Seu Electrònica

"Serveis essencials" de la Seu Electrònica

- El Tauler electrònic d'Edictes
- Licitacions de l'Ajuntament i dels organismes autònoms
- Pagament de tributs
- Consulta d'ordenances i reglaments
- Consulta del planejament urbanístic
- Consulta de les notificacions electròniques
- Carpeta ciutadana
- Carpeta del proveïdor
- Validador de documents electrònics
- Presentació de factures electròniques
- Consulta de les cartes de servei a la ciutadania

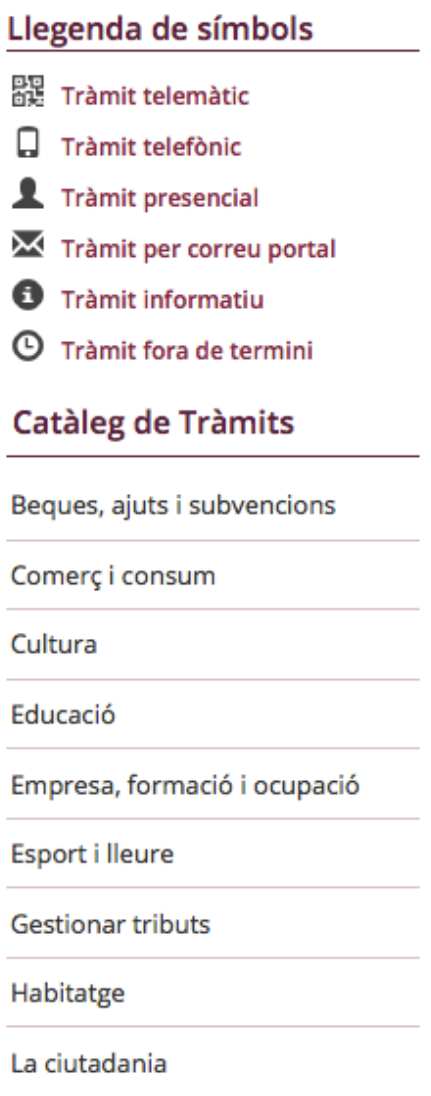


Tasques realitzades - Situació actual: Abast del Pla (II)

Sistemes d'informació de la Seu Electrònica

Punt d'accés únic per a l'administració electrònica

- Catàleg de tràmits – Oficina virtual



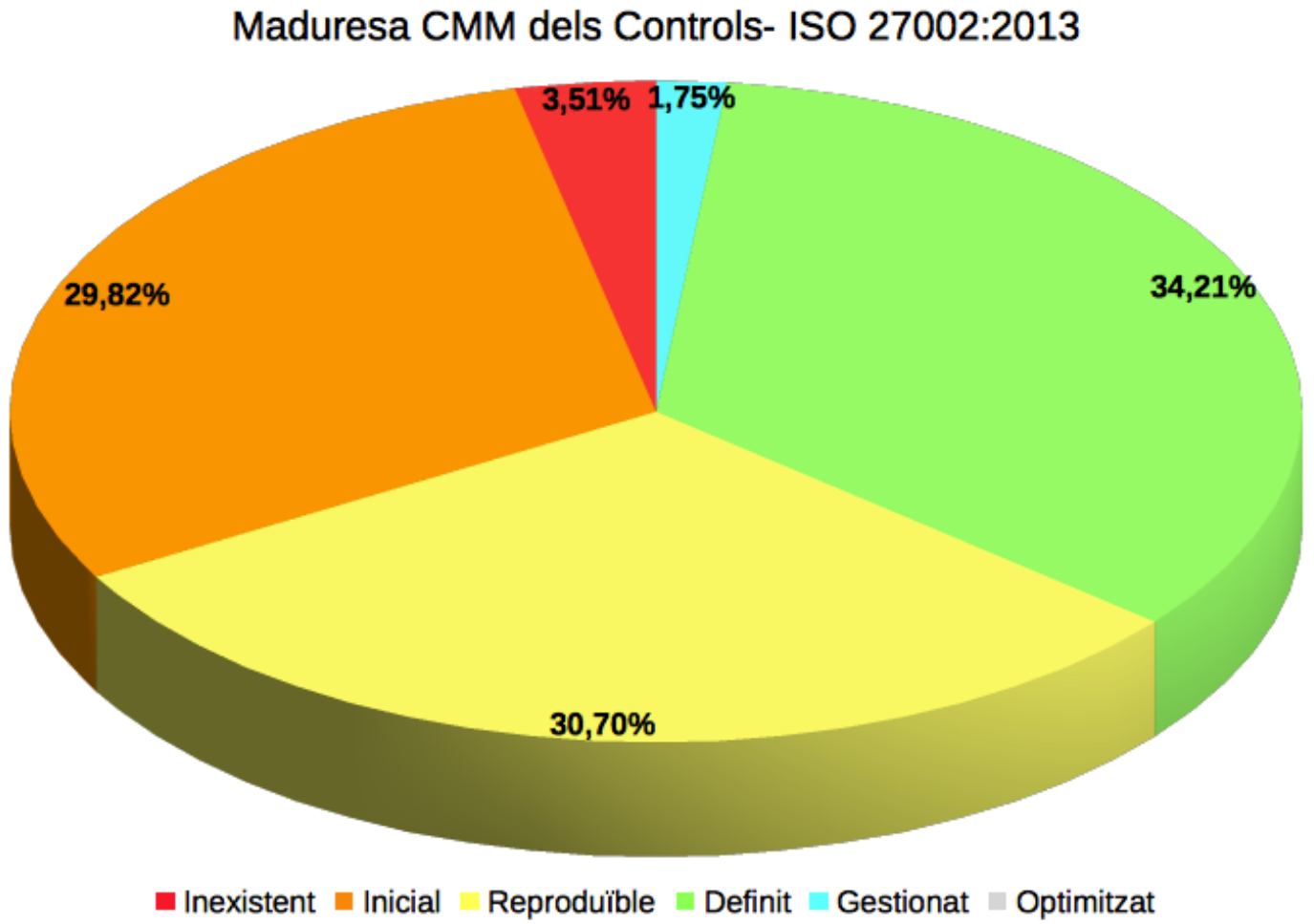
Tasques realitzades - Situació actual: Objectius

- Compliment de la normativa legal en matèria de seguretat: ENS, LOPD
- Implantació de les bones pràctiques en Seguretat dels SGSI definides a les normes ISO/IEC 27000
  - 27001:2013 com a norma certificable
  - 27002:2013 com a recull de bones pràctiques
- Millorar la seguretat dels sistemes de gestió de la informació de l'Ajuntament
- Oferir serveis segurs a la ciutadania
- Millorar la confiança que tenen els ciutadans en l'administració

Tasques realitzades- Situació actual: Anàlisi diferencial

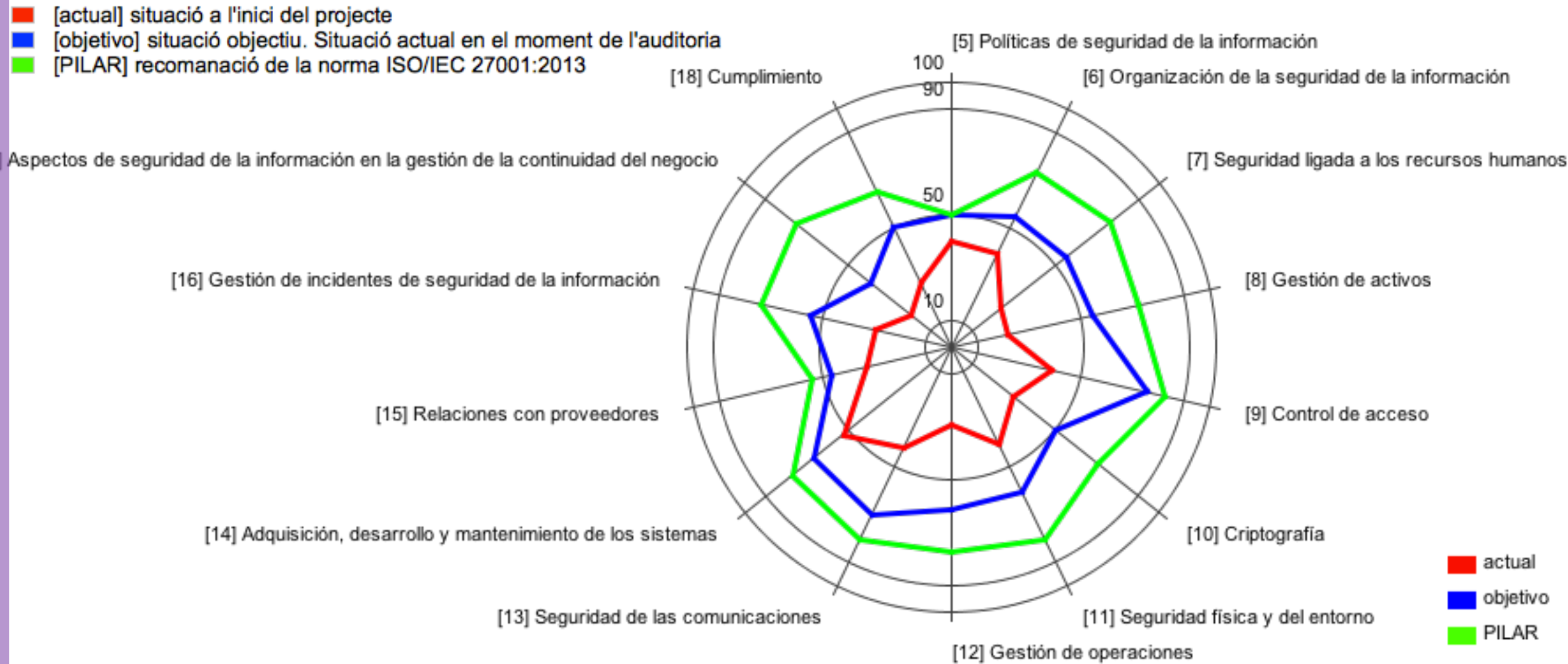
Avaluació dels nivells de maduresa

Efectivitat	CMM	Significat
0%	L0	Inexistent
10%	L1	Inicial / Ad-hoc
50%	L2	Repetible, però intuïtiu
90%	L3	Definit
95%	L4	Gestionat i mesurable
100%	L5	Optimitzat



Tasques realitzades- Situació actual: Anàlisi diferencial

Diagrama de radar – nivell de compliment (inicial)



Tasques realitzades

Aproximació per fases

1. Situació actual: objectius i anàlisi diferencial
2. Sistema de gestió documental
3. Anàlisi de riscos
4. Proposta de projectes
5. Auditoria de compliment
6. Presentació de resultats

Tasques realitzades - Sistema de Gestió documental

Documents elaborats

- Política de Seguretat
- Procediment d'auditories internes
- Gestió d'indicadors
- Procediment de revisió per la direcció
- Gestió de rols i responsabilitats
- Metodologia d'anàlisi de riscos
- Declaració d'aplicabilitat

Tasques realitzades - Sistema de Gestió documental

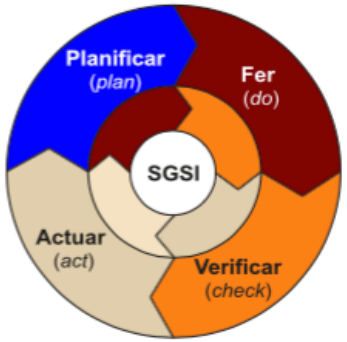
Política de Seguretat

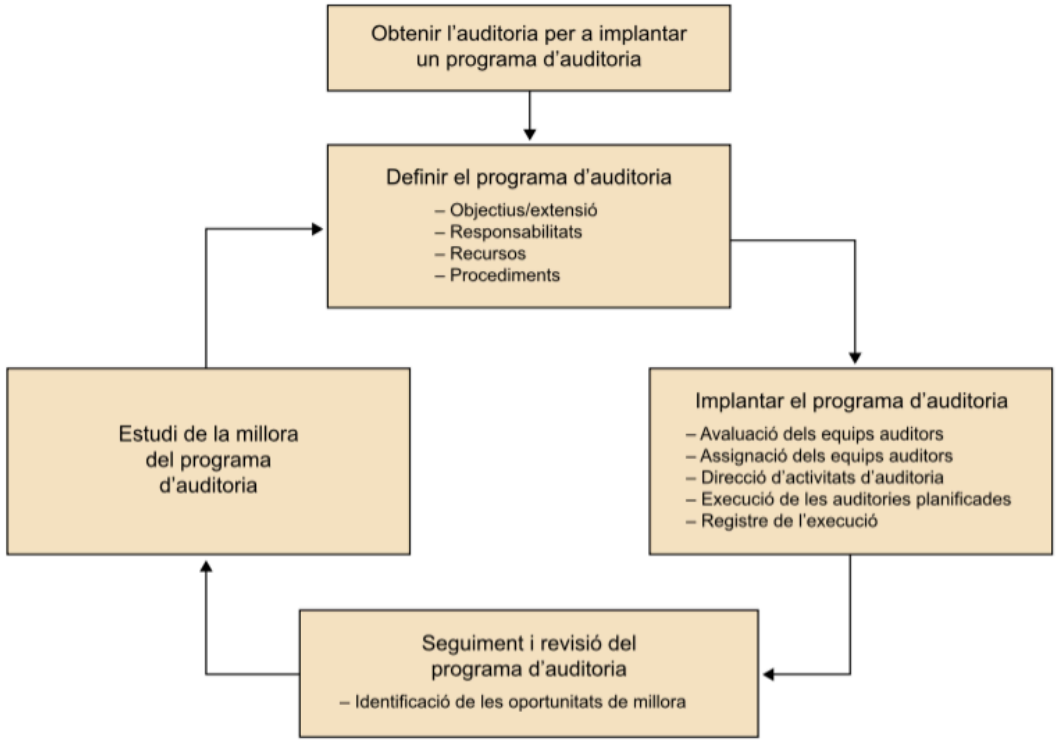
- Abast
- Missió
- Marc Normatiu
- Dades de caràcter personal
- Obligacions del personal
- Terceres parts

Tasques realitzades - Sistema de Gestió documental

Procediment d'auditories internes

- Programa d'auditoria
- Assignació de rols
- Compromís de la direcció
- Planificació
- Model d'informe d'auditoria





Tasques realitzades - Sistema de Gestió documental

Gestió de rols i responsabilitats

- Estructura de supervisió
  - Alcalde
  - Comitè de Seguretat Corporativa
- Estructura d'operació - Rols
  - Responsable de Seguretat Corporativa
  - Responsables de la informació
  - Responsable del Sistema
  - Operadors de seguretat
  - Usuaris

Tasques realitzades - Sistema de Gestió documental

Metodologia d'anàlisi de riscos

- Metodologia MAGERIT
  - Definició d'actius
  - Identificació de les amenaces
  - Especificació de les salvaguardes
  - Determinació de l'Impacte potencial i residual
  - Determinació del risc potencial i residual
- Eina EAR-PILAR del CCN-CERT
  - PILAR
  - PILAR-Basic
  - Micro-Pilar

Tasques realitzades - Sistema de Gestió documental

Declaració d'aplicabilitat

A.5 POLÍTIQUES DE SEGURETAT DE LA INFORMACIÓ				
A.5.1 Directrius de la Direcció en Seguretat de la informació				
	A.5.1.1	Conjunt de polítiques per a la seguretat de la informació	Sí	Tota organització ha de tenir una normativa comuna de seguretat que reguli les línies mestres sobre la forma de treballar de tota l'organització en matèria de seguretat.
	A.5.1.2	Revisió de les polítiques de seguretat de la informació	Sí	Les polítiques s'han de revisar de forma periòdica per a garantir la seva vigència.

3 ISO/IEC 27002:2013

3.1 [5] Políticas de seguridad de la información

[base] Base

control	aplicable
[5] Políticas de seguridad de la información	sí
[5.1] Dirección de la gestión de la seguridad de la información	sí
[5.1.1] Políticas de seguridad de la información	sí
[5.1.2] Revisión de las políticas de seguridad de la información	sí

Tasques realitzades

Aproximació per fases

1. Situació actual: objectius i anàlisi diferencial
2. Sistema de gestió documental
3. Anàlisi de riscos
4. Proposta de projectes
5. Auditoria de compliment
6. Presentació de resultats

Tasques realitzades - Anàlisi de riscos

Anàlisi dels actius

- Inventari d'actius
- Valoració dels actius

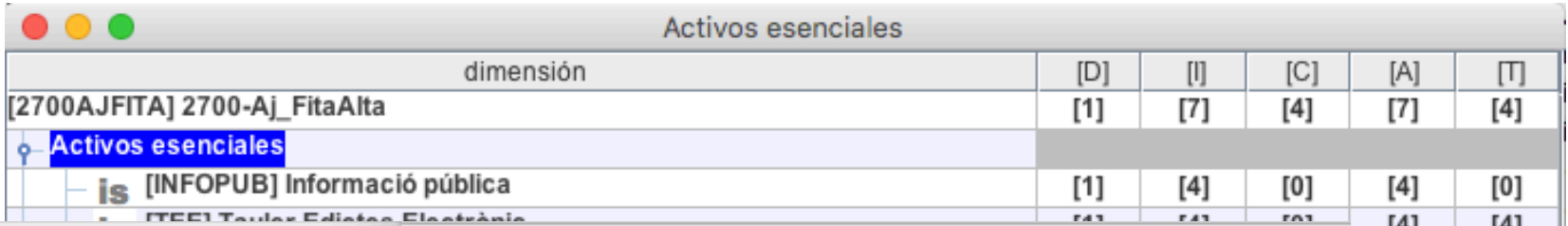
Activos esenciales

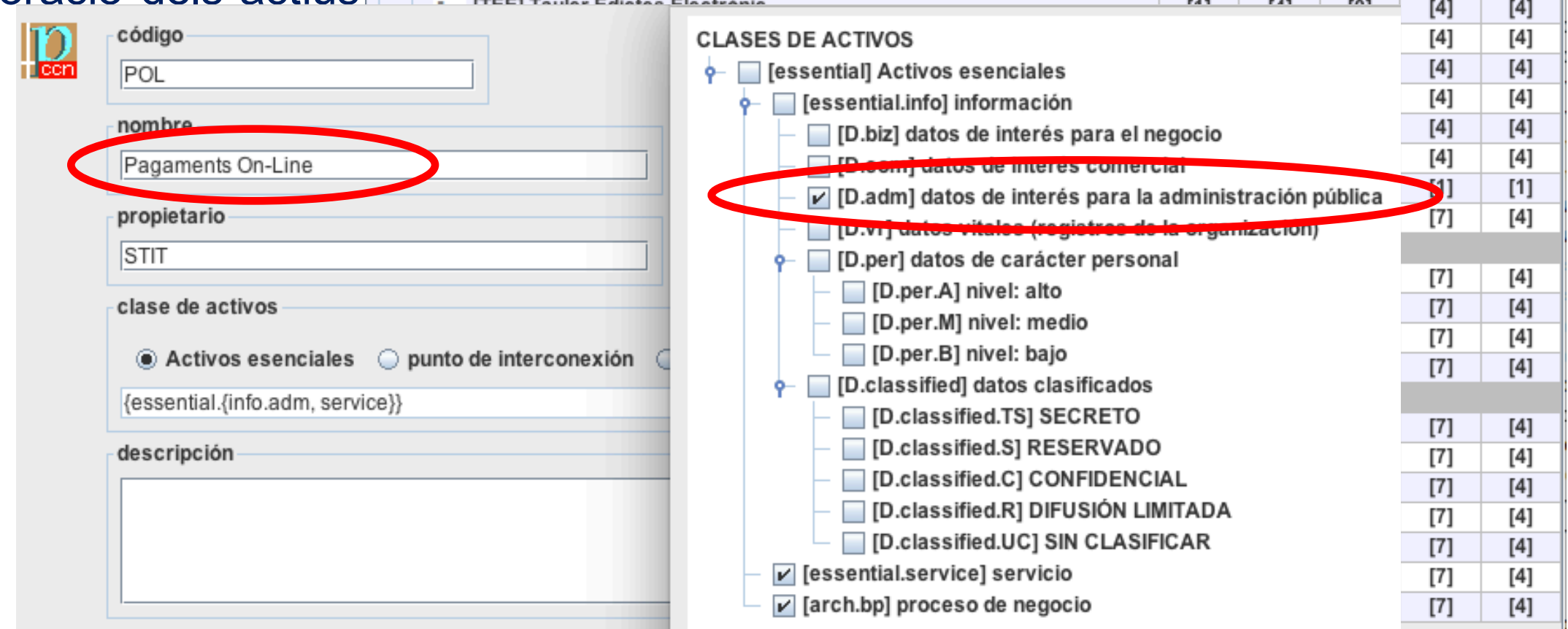
dimensión	[D]	[I]	[C]	[A]	[T]
[2700AJFITA] 2700-Aj_FitaAlta	[1]	[7]	[4]	[7]	[4]
Activos esenciales					
is [INFOPUB] Informació pública	[1]	[4]	[0]	[4]	[0]
is [TEE] Tauler Edictes Electrònic	[1]	[4]	[0]	[4]	[4]
is [IniTram] Inici de tràmits	[1]	[1]	[4]	[4]	[4]
is [CARCIUTADANA] Carpeta ciutadana	[1]	[4]	[4]	[4]	[4]
is [CARPROVEIDOR] Carpeta del proveïdor	[1]	[4]	[4]	[4]	[4]
is [VALDOCS] Validador de documents	[1]	[4]	[4]	[4]	[4]
is [NOT-ELEC] Notificacions telemàtiques	[1]	[4]	[4]	[4]	[4]
is [LICIT] Licitacions	[1]	[4]	[0]	[1]	[1]
is [POL] Pagaments On-Line	[1]	[7]	[4]	[7]	[4]
punto de interconexión					
[VLAN-DMZ] VLAN DMZ	[1]	[7]	[4]	[7]	[4]
[Internet] Internet	[1]	[7]	[4]	[7]	[4]
[LINK-REDUNDANT-CPDs] Connexió redundant entre CPDs	[1]	[7]	[4]	[7]	[4]
[VLAN-Servers] VLAN servidors	[1]	[7]	[4]	[7]	[4]
contratado a una tercera parte					
[INET-CORP] Contracte amb Telefònica per accés a internet dels servidors	[1]	[7]	[4]	[7]	[4]
[PSIS] Plataforma de Signatura Electrònica	[1]	[7]	[4]	[7]	[4]
[eTauler] Tauler electrònic AOC	[1]	[7]	[4]	[7]	[4]
[eNotum] Notificacions elctròniques AOC	[1]	[7]	[4]	[7]	[4]
[viaoberta] Serveis d'interoperabilitat AOC	[1]	[7]	[4]	[7]	[4]
[TPV-Virtual] Passarel·la de pagament online	[1]	[7]	[4]	[7]	[4]
[SUB.ELECTRIC] Contracte de subministrament elèctric	[1]	[7]	[4]	[7]	[4]

Tasques realitzades - Anàlisi de riscos

Anàlisi dels actius

- Inventari d'actius
- Valoració dels actius





Tasques realitzades - Anàlisi de riscos

Classes d'actius

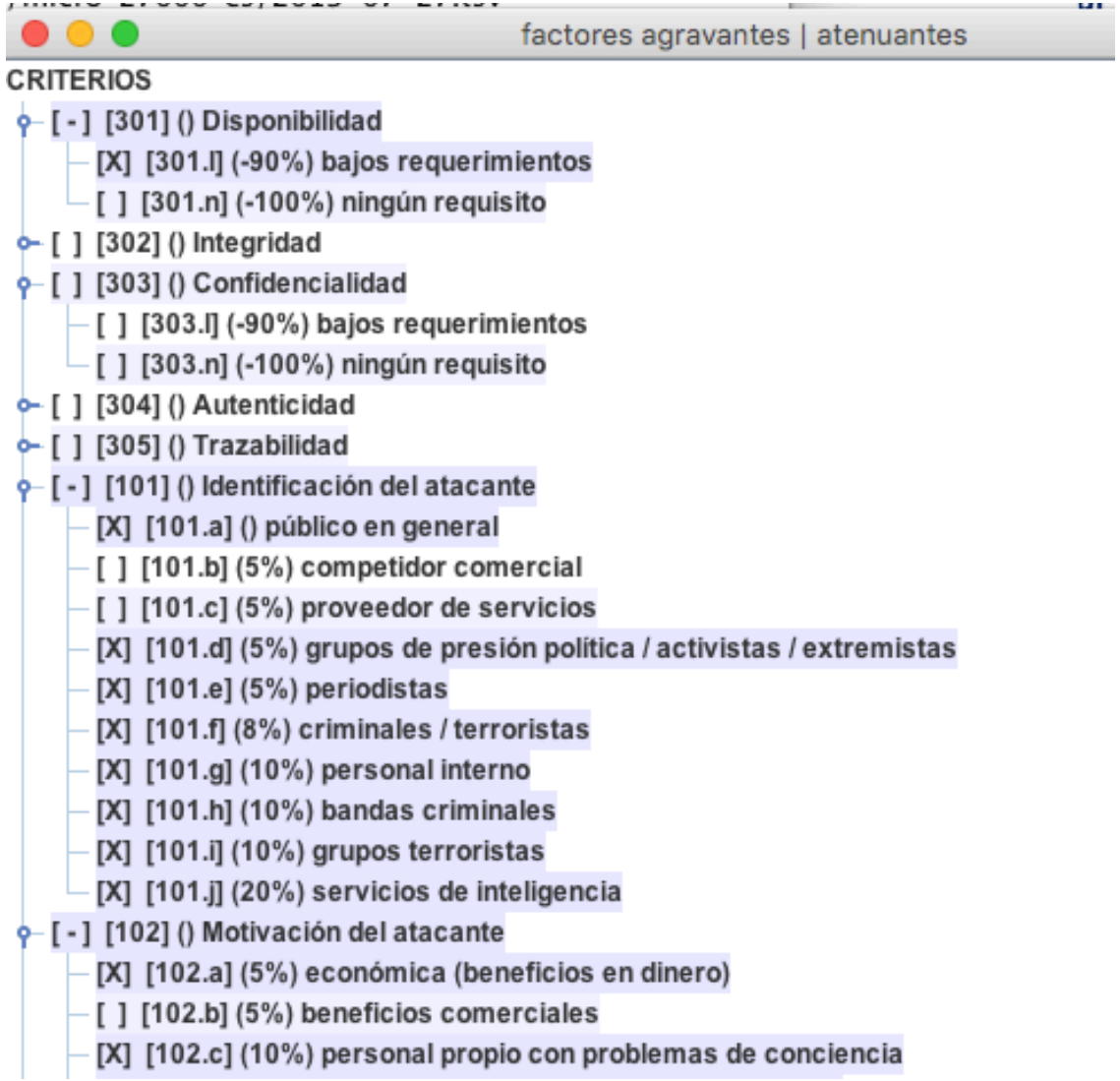
Micro-Pilar no permet

- definir Actius No essencials
- Dependències entre actius

CLASES DE ACTIVOS
- [-] [D] Datos / Información
  - [X] [files] ficheros de datos
  - [X] [backup] copias de respaldo
  - [X] [conf] datos de configuración
  - [X] [int] datos de gestión interna
  - [X] [password] credenciales (ej. contraseñas)
  - [ ] [auth] datos de validación de credenciales
  - [ ] [acl] datos de control de acceso
  - [X] [log] registro de actividad (log)
  - [ ] [voice] voz
  - [ ] [multimedia] multimedia
  - [X] [source] código fuente
  - [X] [exe] código ejecutable
  - [X] [test] datos de prueba
  - [ ] [other] otros ...
- [-] [keys] Claves criptográficas
- [-] [S] Servicios
- [-] [SW] Aplicaciones (software)
  - [X] [prp] desarrollo propio (in house)
  - [X] [sub] desarrollo a medida (subcontratado)
  - [-] [std] estándar (off the shelf)
    - [X] [browser] navegador web
    - [X] [www] servidor de presentación
    - [X] [app] servidor de aplicaciones
    - [X] [email_client] cliente de correo electrónico
    - [X] [email_server] servidor de correo electrónico
    - [X] [directory] servidor de directorio
    - [X] [file] servidor de ficheros
    - [X] [dbms] sistema de gestión de bases de datos
    - [ ] [tm] monitor transaccional
    - [X] [office] ofimática
    - [X] [av] anti virus

Tasques realitzades - Anàlisi de riscos

Factors agreujants/atenuants



Tasques realitzades - Anàlisi de riscos

Anàlisi d'amenaces

- Avaluació de perfils
  - ✓ LOPD
  - ✓ 27002:2005
  - ✓ 27002:2013
- Salvaguardes

Peso relativo

	máximo peso	crítica
	peso alto	muy importante
	peso normal	importante
	peso bajo	interesante
✓	aseguramiento: componentes certificados	

[actual] situació a l'inici del projecte
[objetivo] situació objectiu.
Situació actual en el moment de l'auditoria
[PILAR] recomanació de la norma ISO/IEC 27001:2013

[27002:2013] Código de buenas prácticas para la Gestión de la Seguridad de la Información

Expandir operación madurez

porcentaje
madurez
PILAR

rec...	control	actual	objetivo	PILAR
	[27002:2013] Código de buenas prácticas para la Gestión de la Seguridad de la Información	L0-L3	L0-L4	L2-L5
2	[5] Seguridad de la información	L1-L2	L2	L2
5	[6] Organización de la seguridad de la información	L0-L3	L1-L3	L2-L3
5	[6.1] Organización interna	L0-L3	L2-L3	L2-L3
3	[6.1.1] Roles y responsabilidades relativas a la seguridad de la información	L1-L3	L2-L3	L2-L3
5	[6.1.2] Separación de tareas	L0-L3	L2-L3	L2-L3
5	[H.ST] Segregación de tareas	L0-L3	L2-L3	L2-L3
5	[H.ST.1] Todos los procesos críticos requieren al menos 2 personas	L1	L2	L3
4	[H.ST.2] Se definen roles con autorización exclusiva para realizar tareas	L0-L3	L2-L3	L2-L3
3	[H.ST.2.1] Usuario del sistema	L3	L3	L3
3	[H.ST.2.2] Entrada de datos	L3	L3	L3
4	[H.ST.2.3] Autorización de datos	L1	L3	L3
3	[H.ST.2.4] Administrador del sistema	L2	L3	L3
4	[H.ST.2.5] Administrador de comunicaciones (redes)	L2	L3	L3
3	[H.ST.2.6] Administrador de Seguridad	L2	L3	L3
3	[H.ST.2.7] Desarrollo y mantenimiento de sistemas	L2	L3	L3
3	[H.ST.2.8] Administración de cambios	L1	L2	L3
3	[H.ST.2.9] Auditoría de seguridad	L0	L2	L3
2	[H.ST.2.a] Se proporciona formación en las funciones de cada rol del sistema	L1	L2	L2
4	[H.ST.3] Se controla la efectividad de la estructura de segregación	L0-L3	L2-L3	L3
3	[6.1.3] Contacto con las autoridades	L2	L3	L3
4	[6.1.4] Contacto con grupos de especial interés	L2-L3	L3	L3

Tasques realitzades - Anàlisi de riscos

Avaluació del risc

riesgos

potencial | actual | objetivo | PILAR

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{1,1}	{6,6}	{5,7}	{6,9}	{5,0}
[INFOPUB] Informació pública	{1,1}	{4,8}	{3,3}	{5,1}	{2,6}
[TEE] Tauler Edictes Electrònic	{1,1}	{4,8}	{3,3}	{5,1}	{5,0}
[IniTram] Inici de tràmits	{1,1}	{3,0}	{5,7}	{5,1}	{5,0}
[CARCIUTADANA] Carpeta ciutadana	{1,1}	{4,8}	{5,7}	{5,1}	{5,0}
[CARPROVEIDOR] Carpeta del proveïdor	{1,1}	{4,8}	{5,7}	{5,1}	{5,0}
[VALDOCS] Validador de documents	{1,1}	{4,8}	{5,7}	{5,1}	{5,0}
[NOT-ELEC] Notificacions telemàtiques	{1,1}	{4,8}	{5,7}	{5,1}	{5,0}
[LICIT] Licitacions	{1,1}	{4,8}	{3,3}	{3,4}	{3,2}
[POL] Pagaments On-Line	{1,1}	{6,6}	{5,7}	{6,9}	{5,0}

potencial | actual | objetivo | PILAR

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{0,62}	{5,1}	{3,7}	{5,4}	{3,4}
[INFOPUB] Informació pública	{0,62}	{3,4}	{1,3}	{3,6}	{1,1}
[TEE] Tauler Edictes Electrònic	{0,62}	{3,4}	{1,3}	{3,6}	{3,4}
[IniTram] Inici de tràmits	{0,62}	{1,6}	{3,7}	{3,6}	{3,4}
[CARCIUTADANA] Carpeta ciutadana	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
[CARPROVEIDOR] Carpeta del proveïdor	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
[VALDOCS] Validador de documents	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
[NOT-ELEC] Notificacions telemàtiques	{0,62}	{3,4}	{3,7}	{3,6}	{3,4}
[LICIT] Licitacions	{0,62}	{3,4}	{1,3}	{1,8}	{1,7}
[POL] Pagaments On-Line	{0,62}	{5,1}	{3,7}	{5,4}	{3,4}

- 9 - NIVEL 9
- 8 - NIVEL 8
- 7 - extremadamente crítico
- 6 - muy crítico
- 5 - crítico
- 4 - muy alto
- 3 - alto
- 2 - medio
- 1 - bajo
- 0 - despreciable

Tasques realitzades - Anàlisi de riscos

Avaluació del risc

riesgos

potencial | actual | objetivo | PILAR

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{0,40}	{3,7}	{2,6}	{3,8}	{2,1}
[INFOPUB] Informació pública	{0,40}	{1,9}	{0,84}	{2,0}	{0,74}
[TEE] Tauler Edictes Electrònic	{0,40}	{1,9}	{0,84}	{2,0}	{2,1}
[IniTram] Inici de tràmits	{0,40}	{0,82}	{2,6}	{2,0}	{2,1}
[CARCIUTADANA] Carpeta ciutadana	{0,40}	{1,9}	{2,6}	{2,0}	{2,1}
[CARPROVEIDOR] Carpeta del proveïdor	{0,40}	{1,9}	{2,6}	{2,0}	{2,1}
[VALDOCS] Validador de documents	{0,40}	{1,9}	{2,6}	{2,0}	{2,1}
[NOT-ELEC] Notificacions telemàtiques	{0,40}	{1,9}	{2,6}	{2,0}	{2,1}
[LICIT] Licitacions	{0,40}	{1,9}	{0,84}	{0,85}	{0,85}
[POL] Pagaments On-Line	{0,40}	{3,7}	{2,6}	{3,8}	{2,1}

potencial | actual | objetivo | PILAR

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{0,09}	{2,1}	{0,92}	{2,0}	{0,85}
[INFOPUB] Informació pública	{0,09}	{0,86}	{0,45}	{0,84}	{0,38}
[TEE] Tauler Edictes Electrònic	{0,09}	{0,86}	{0,45}	{0,84}	{0,85}
[IniTram] Inici de tràmits	{0,09}	{0,51}	{0,92}	{0,84}	{0,85}
[CARCIUTADANA] Carpeta ciutadana	{0,09}	{0,86}	{0,92}	{0,84}	{0,85}
[CARPROVEIDOR] Carpeta del proveïdor	{0,09}	{0,86}	{0,92}	{0,84}	{0,85}
[VALDOCS] Validador de documents	{0,09}	{0,86}	{0,92}	{0,84}	{0,85}
[NOT-ELEC] Notificacions telemàtiques	{0,09}	{0,86}	{0,92}	{0,84}	{0,85}
[LICIT] Licitacions	{0,09}	{0,86}	{0,45}	{0,48}	{0,49}
[POL] Pagaments On-Line	{0,09}	{2,1}	{0,92}	{2,0}	{0,85}

9 - NIVEL 9
8 - NIVEL 8
7 - extremadamente crítico
6 - muy crítico
5 - crítico
4 - muy alto
3 - alto
2 - medio
1 - bajo
0 - despreciable

Tasques realitzades

Aproximació per fases

1. Situació actual: objectius i anàlisi diferencial
2. Sistema de gestió documental
3. Anàlisi de riscos
4. Proposta de projectes
5. Auditoria de compliment
6. Presentació de resultats

Tasques realitzades - Proposta de projectes

Planificació dels projectes

- Definició de 12 projectes
- Projectes de primer semestre (6 projectes -140 accions)
- Projectes de segon semestre (6 projectes - 80 accions)

[actual] situació a l'inici del projecte
[objetivo] situació objectiu. Situació actual en el moment de l'auditoria
[PILAR] recomanació de la norma ISO/IEC 27001:2013

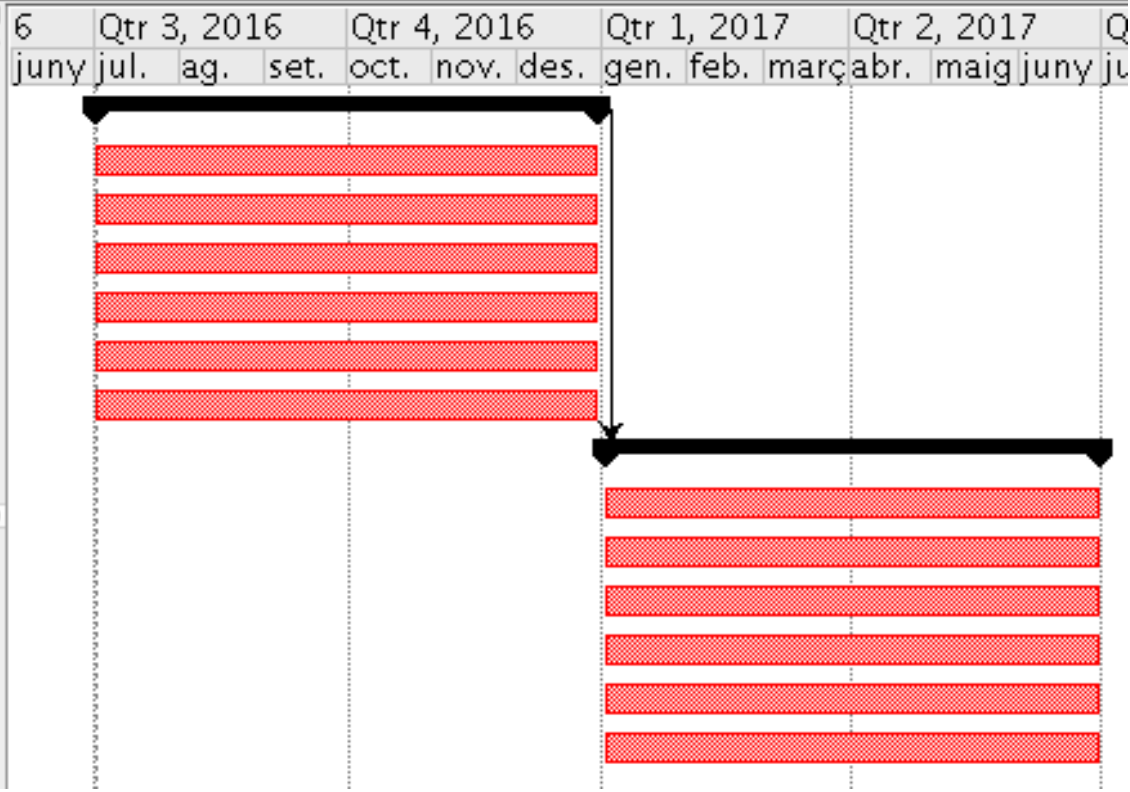
Objectius dels projectes

- Reduir els principals riscos detectats
- Implantació de la norma ISO/IEC 27001:2013

Tasques realitzades - Proposta de projectes

Temporalització

	Name
1	**Accions de primer semestre**
2	Desenvolupament del marc normatiu i procedimental de seguretat
3	Control d'accés lògic
4	Gestió de suports d'emmagatzemament
5	Pla de continuïtat del negoci
6	Ús de criptografia
7	Enfortiment de les configuracions en els equips i les aplicacions
8	**Accions de segon semestre**
9	Monitorització operativa de la seguretat
10	Gestió de la seguretat de la informació
11	Formació i conscienciació en seguretat
12	Processos d'operació tècnica de la seguretat
13	Aspectes jurídics relacionats amb la seguretat
14	Protecció física de les infraestructures



Tasques realitzades - Proposta de projectes

Projectes a realitzar el primer semestre

* Reduir els riscos que afecten al servei de pagament On-Line

PROJECTES A REALITZAR EL PRIMER SEMESTRE	ACCIONS
Desenvolupament del marc normatiu i procedimental de seguretat	75
Control d'accés lògic *	5
Gestió de suports d'emmagatzemament *	9
Pla de continuïtat del negoci *	24
Ús de criptografia *	10
Enfortiment de les configuracions en els equips i les aplicacions	17
Total accions	**140**

Tasques realitzades - Proposta de projectes

Projectes a realitzar el segon semestre

PROJECTES A REALITZAR EL SEGON SEMESTRE	ACCIONS
Monitorització operativa de la seguretat	18
Gestió de la seguretat de la informació	10
Formació i conscienciació en seguretat	11
Processos d'operació tècnica de la seguretat	25
Aspectes jurídics relacionats amb la seguretat	8
Protecció física de les infraestructures	8
Total accions	**80**

Tasques realitzades

Aproximació per fases

1. Situació actual: objectius i anàlisi diferencial
2. Sistema de gestió documental
3. Anàlisi de riscos
4. Proposta de projectes
5. Auditoria de compliment
6. Presentació de resultats

Tasques realitzades - Auditoria de compliment

Informe d'auditoria

- Objectiu de l'auditoria
- Abast
- Metodologia utilitzada
- Procés d'auditoria
- Recomanacions
- Llista detallada de les constatacions

Tasques realitzades - Auditoria de compliment

Objectiu de l'auditoria

- Avaluar la maduresa del SGSI
- Bones pràctiques - Norma ISO/IEC 27002:2013
  - 14 dominis
  - 35 objectius
  - 114 controls

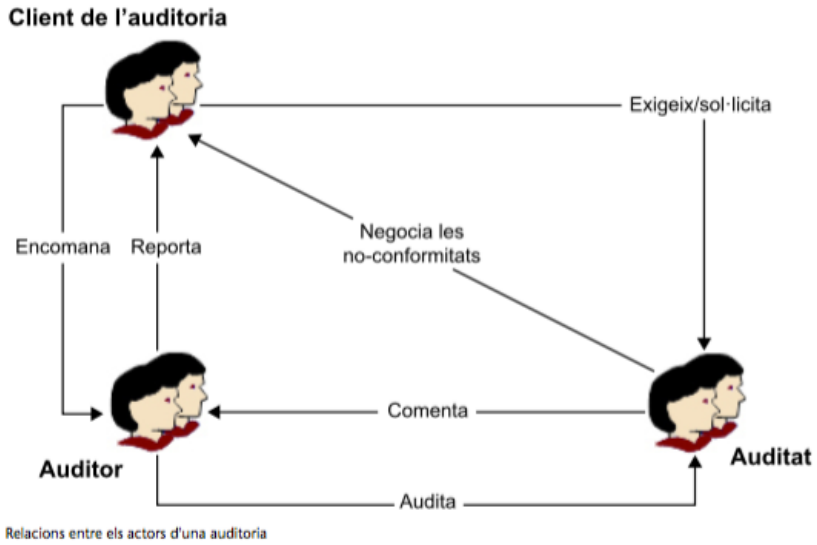
Abast

- SGSI de l'Ajuntament
- Domini de seguretat "Seu electrònica"

Tasques realitzades - Auditoria de compliment

Metodologia utilitzada

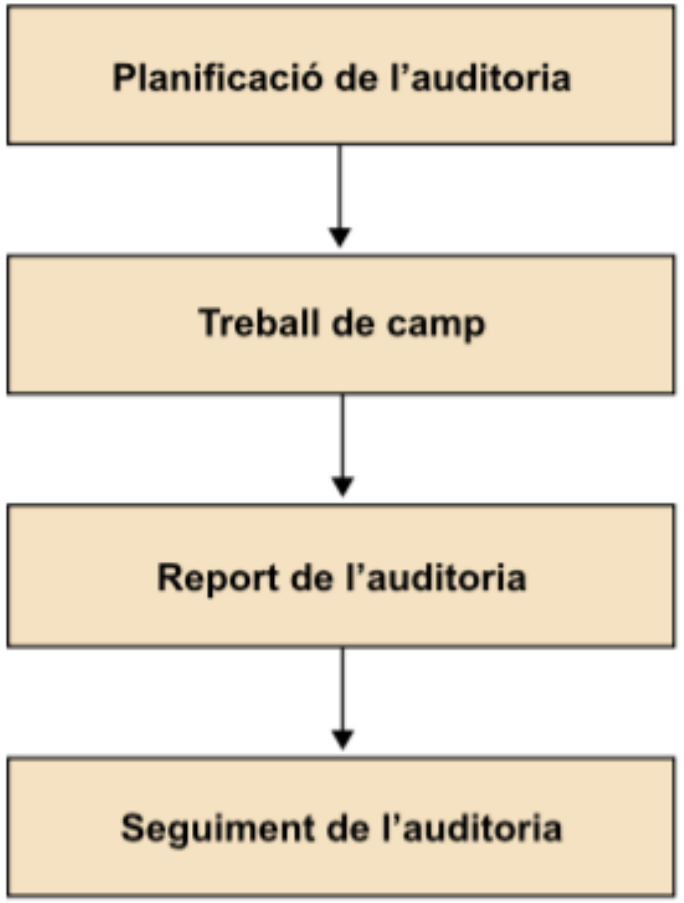
- Auditoria Interna o de "Primera part"
- Equip auditor propi
- Auditor en cap - Responsable de seguretat



Relacions entre els actors d'una auditoria

Procés d'auditoria

- Dividit en 4 fases



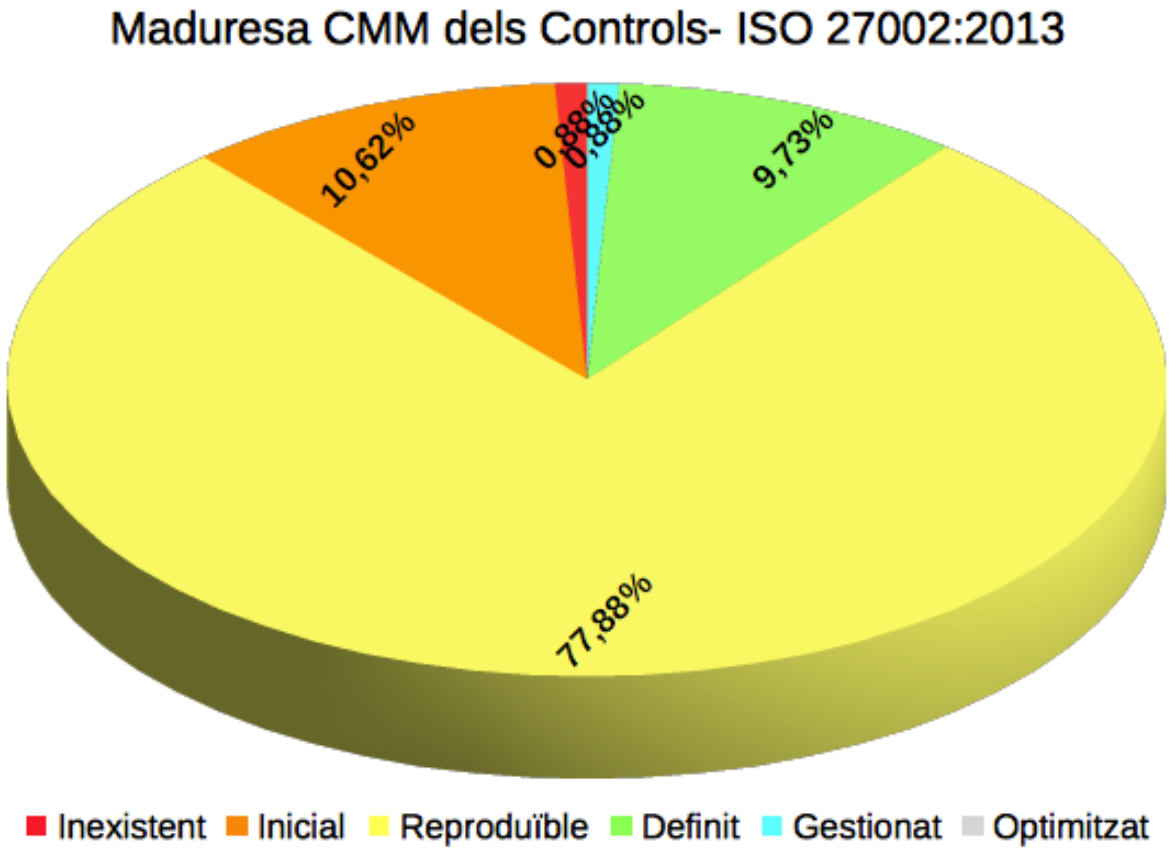
Tasques realitzades - Auditoria de compliment

Informe d'auditoria

- 1 No-Conformitat major
- Múltiples No-Conformitats menors

Avaluació Nivells de Maduresa

Efectivitat	CMM	Significat
0%	L0	Inexistent
10%	L1	Inicial / Ad-hoc
50%	L2	Repetible, però intuïtiu
90%	L3	Definit
95%	L4	Gestionat i mesurable
100%	L5	Optimitzat



Tasques realitzades - Auditoria de compliment

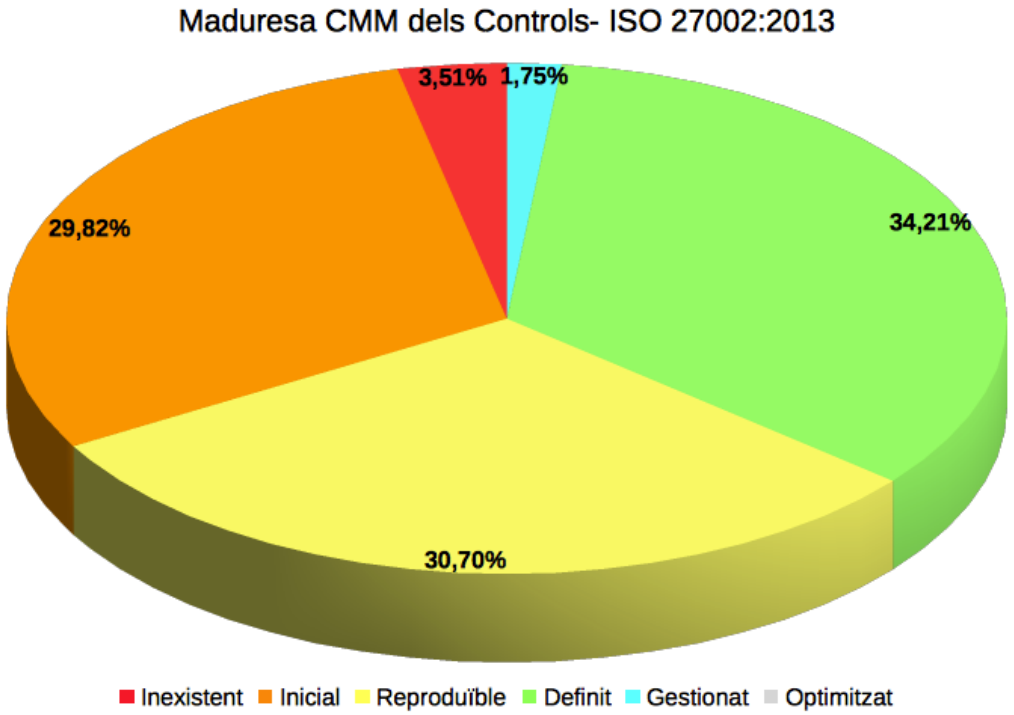
Nivell de Maduresa Inicial

Avaluació subjectiva

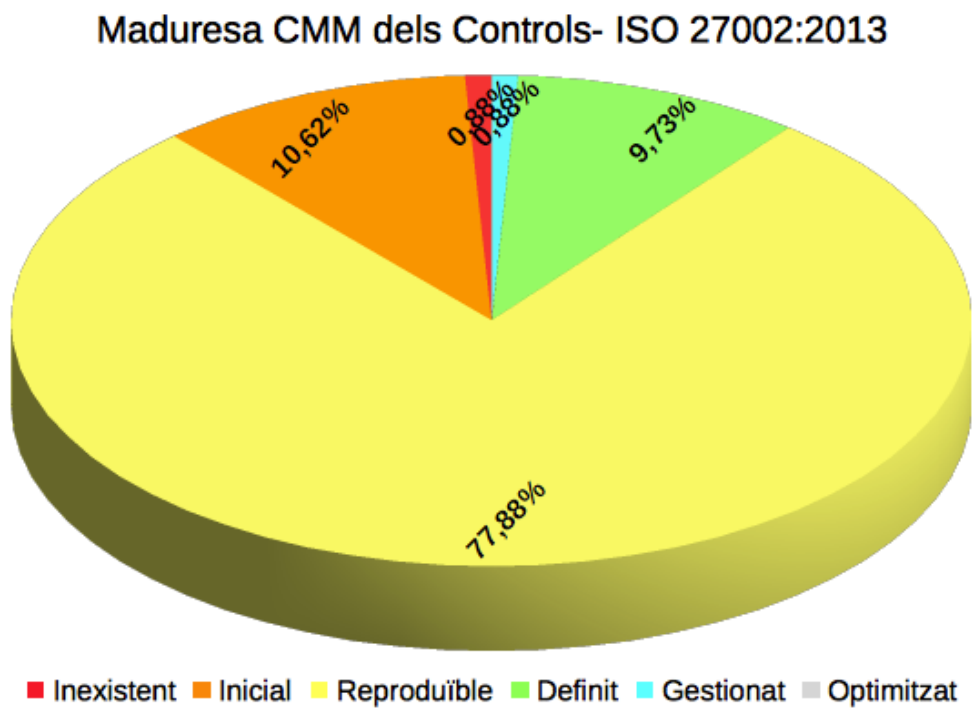
Nivell de Maduresa Auditoria

Avaluació i quantificació objectiva

- més de 1.700 salvaguardes
- Abast :114 controls de la norma



Efectivitat	CMM	Significat
0%	L0	Inexistent
10%	L1	Inicial / Ad-hoc
50%	L2	Repetible, però intuïtiu
90%	L3	Definit
95%	L4	Gestionat i mesurable
100%	L5	Optimitzat



Tasques realitzades - Auditoria de compliment

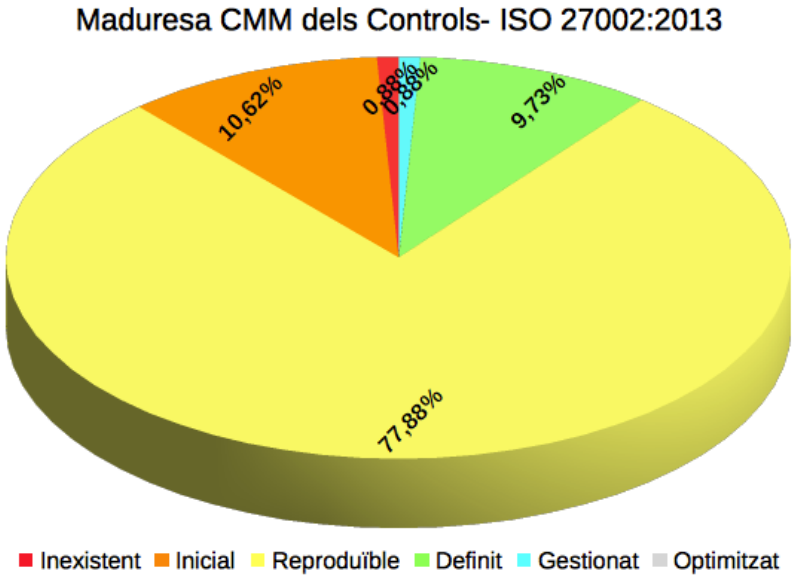
Nivell de Maduresa Auditoria

	[Inicial]	[Auditat]	[Norma]
[5] Políticas de seguridad de la información	**L1-L2 40%**	**L2 50%**	**L2 50%**
[5.1] Dirección de la gestión de la seguridad de la información	L1-L2 40%	L2 50%	L2 50%

	[Inicial]	[Auditat]	[Norma]
[6] Organización de la seguridad de la información	**L0-L3 39%**	**L1-L3 L2-54%**	**L2-L3 73%**
[6.1] Organización interna	L0-L3 53%	L2-L3 L2-79%	L2-L3 76%
[6.2] Dispositivos móviles y teletrabajo	L0-L2 25%	L1-L2 L2-30%	L2-L3 70%

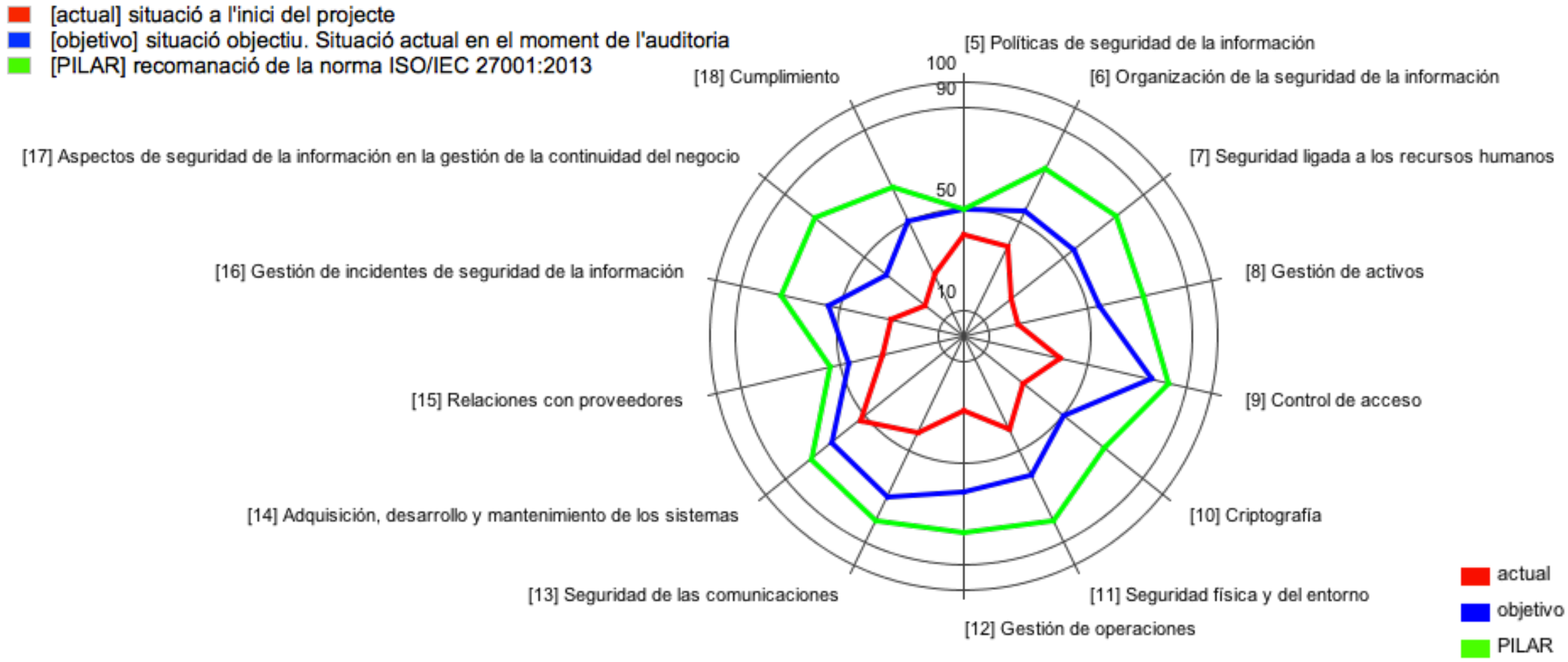
	[Inicial]	[Auditat]	[Norma]
[7] Seguridad ligada a los recursos humanos	**L0-L3 23%**	**L1-L3 L3-55%**	**L2-L4 76%**
[7.1] Antes del empleo	L0-L3 21%	L1-L3 L2-45%	L2-L3 80%
[7.2] Durante el empleo	L0-L3 31%	L2-L3 L3-60%	L2-L4 68%
[7.3] Cese del empleo o cambio de puesto de trabajo	L0-L2 17%	L1-L3 L2-60%	L2-L3 80%

Avaluació i quantificació objectiva
- més de 1.700 salvaguardes
- Abast :114 controls de la norma



Tasques realitzades - Auditoria de compliment

Diagrama de radar – nivell de compliment auditoria (Fase Objectiu)



Tasques realitzades - Auditoria de compliment

Recomanacions

- Corregir les No-Conformitats
- Realitzar un nou Pla de Projectes (12 mesos)
- Planificar una nova auditoria (12 mesos)
- Fer una auditoria de certificació de la norma ISO/IEC 27001:2013 (en 18 mesos)

Tasques realitzades - Auditoria de compliment

Llista detallada de constatacions

- 1 No-Conformitat major

Id. No-Conformitat	**NC01**
Tipus de no conformitat	**Major** / ~~Menor~~
Descripció	Inexistència del Pla de Continuïtat de l'organització, la qual cosa fa que la seva verificació, revisió i avaluació no siguin possibles.
Paràgrafs de la norma afectats	17.1.3 Verificar, revisar i avaluar la continuïtat de la seguretat de la informació.
Acció correctora	Elaboració del Pla de Continuïtat de Negoci de l'organització.

Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[17.1] Continuidad de la seguridad de la información	L0-L3	L0-L3	L2-L3
[17.1.3] Verificar, revisar y evaluar la continuidad de la seguridad de la información	L0	L0-L1	L3

[17.1] Continuidad de la seguridad de la información	3%	25%	76%
[17.1.3] Verificar, revisar y evaluar la continuidad de la seguridad de la información	0%	3%	90%

Tasques realitzades - Auditoria de compliment

Llista detallada de constatacions

- Múltiples No-conformitats menors

Id. No-Conformitat	**NC02**
Tipus de no conformitat	~~Major~~ / **Menor**
Descripció	Es realitza una insuficient comprovació, prèvia a la contractació, dels antecedents dels treballadors que es dediquen a la gestió de la seguretat del sistema d'informació.
Paràgrafs de la norma afectats	7.1.1 Investigació d'antecedents
Acció correctora	Informar-se dels antecedents dels treballadors abans de formalitzar la contractació.

Maduresa	**[actual]**	**[objetivo]**	**[PILAR]**
[7.1] Antes del empleo	L0-L3	L1-L3	L2-L3
[7.1.1] Investigación de antecedentes	L0-L1	L1-L2	L3

[7.1] Antes del empleo	21%	45%	80%
[7.1.1] Investigación de antecedentes	5%	30%	90%

Tasques realitzades

Aproximació per fases

1. Situació actual: objectius i anàlisi diferencial
2. Sistema de gestió documental
3. Anàlisi de riscos
4. Proposta de projectes
5. Auditoria de compliment
6. Presentació de resultats

ÍNDEX

Conclusions - 1a conclusió - Objectius

- Compliment de la normativa legal en matèria de seguretat: ENS, LOPD

- Implantació de les bones pràctiques en Seguretat dels SGSI definides a les normes ISO/IEC 27000
  - 27001:2013 com a norma certificable
  - 27002:2013 com a recull de bones pràctiques

- Millorar la seguretat dels sistemes de gestió de la informació de l'Ajuntament

- Oferir serveis segurs a la ciutadania

- Millorar la confiança que tenen els ciutadans en l'administració

Conclusions - 2a conclusió - Pla Director

- Fulla de ruta per a la millora del SGSI
- Eina per a adquirir la capacitació per a la gestió del SGSI

Conclusions - 3a conclusió - Auditoria

- Evidències de millora després de 12 mesos
- Previsió d'assolir els nivells de compliment de la norma ISO/IEC 27001:2013 en els propers 12 mesos

Conclusions - 4a conclusió - Eines PILAR

- Valoració positiva de les eines EAR-PILAR
- Especialment indicades per al manteniment del sistema al llarg del temps
- Recomanació de l'eina PILAR

Conclusions - 5a conclusió - Gestió de la seguretat

- La gestió de la seguretat és un procés
- Necessita monitorització i avaluació permanent
- Serveix per a detectar i corregir els problemes
- S'ha d'adequar a la realitat de les organitzacions
- És un procés que no acaba mai

Màster Interuniversitari en Seguretat de les Tecnologies de la informació i de les Comunicacions

UOC Universitat Oberta de Catalunya www.uoc.edu

UAB Universitat Autònoma de Barcelona

Universitat Rovira i Virgili

Universitat de les Illes Balears

SISTEMES DE GESTIÓ DE LA SEGURETAT DE LA INFORMACIÓ

PLA DIRECTOR DE SEGURETAT

AJUNTAMENT DE FITA ALTA

Juny de 2016

MOLTES GRÀCIES !!!!!!

Alumne : Andreu Retamero Pallarès
Consultor : Arsenio Tortajada Gallego
Director : Carles Garrigues Olivella