MÀSTER INTERUNIVERSITARI DE SEGURETAT DE LES TECNOLOGIES DE LA INFORMACIÓ I DE LA COMUNICACIÓ

# PLA DE SEGURETAT AJUNTAMENT DE RIBEROLA

PRESENTACIÓ A DIRECCIÓ (JUNY 2013)


**DIRECTOR:** Carles Garrigues
**CONSULTOR:** Arsenio Tortajada
**ALUMNE:** Ricard Salvat


UOC Universitat Oberta de Catalunya www.uoc.edu

UAB Universitat Autònoma de Barcelona

Universitat Rovira i Virgili

UIB Universitat de les Illes Balears

# ÍNDEX



# 1. INTRODUCCIÓ

## LA INFORMACIÓ EN LES AA.PP.

- Responsabilitats Legals (Llei 15/1999, ENS, …)
- Funcions operatives i de gestió
- Sosteniment de l'estat de dret
- Responsabilitats de custòdia de la informació
- Oferiment de serveis al ciutadà

# 1. INTRODUCCIÓ

## LA INFORMACIÓ EN LES AA.PP.

És de vital importància protegir-ne:

- La **DISPONIBILITAT** (Accés a la informació)
- La **INTEGRITAT** (Contingut correcte i exacte)
- La **CONFIDENCIALITAT** (Privacitat de les dades)
- L'**AUTENTICITAT** (Per assegurar autoria)
- La **TRAÇABILITAT** (Realització de seguiments)

# 1. INTRODUCCIÓ

## LA INFORMACIÓ EN LES AA.PP.

Possibles amenaces i problemes:

- Hi ha una inundació en un Centre de Procés de Dades
- Robatori d'informació confidencial
- Manca d'implicació en la Direcció de l'organització!!!
- Error de maquinari en servei crític
- Pèrdua del padró d'habitants per error d'aplicació
- Ús malintencionat d'algun element de les TIC
- ...

# 1. INTRODUCCIÓ

## LA INFORMACIÓ EN LES AA.PP.

Problemes en la Seguretat de la Informació:

- Complexitat o mida de les organitzacions
- Heterogeneïtat de sistemes, aplicacions o serveis
- Falta de planificació i visió global
- Manca de formació del personal
- Viabilitat econòmica
- ...

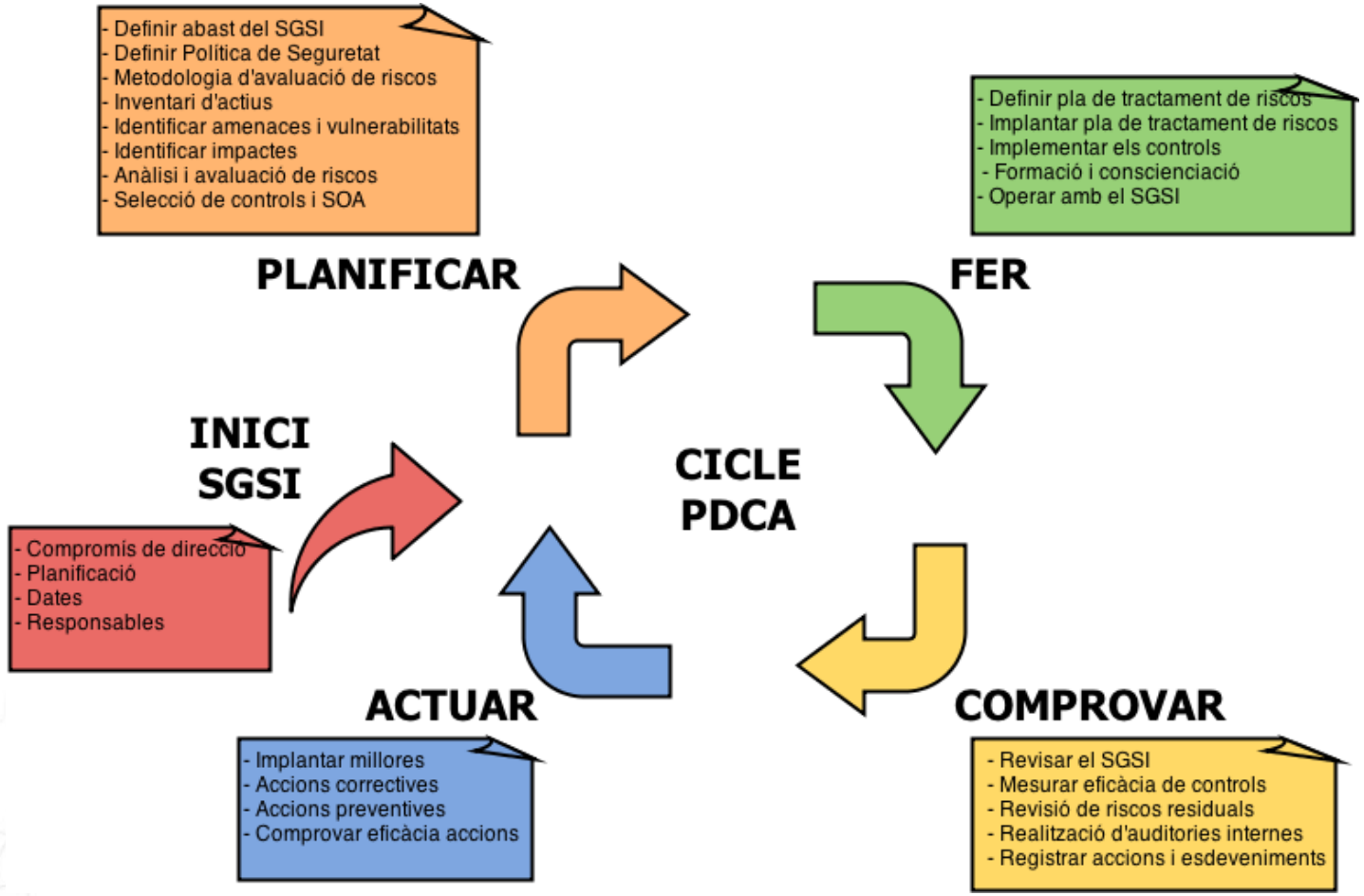
# 1. INTRODUCCIÓ

## PLA DE SEGURETAT, QUÈ APORTA?

- Anàlisi de la situació actual
- Organització de rols i responsabilitats
- Adaptació a normatives de Seguretat de la Informació
  (ISO 27001:2005 – Establiment d'un SGSI)
- Detecció de possibles problemes i/o amenaces
- Definició d'objectius i millores a curt i llarg termini
- Seguiment i control de l'evolució de la Seguretat
  (Cicle PDCA)

# 1. INTRODUCCIÓ

## PLA DE SEGURETAT – SGSI i CICLE PDCA



# 2. PLA DE SEGURETAT

## ÀMBIT:

- Infraestructures i xarxes:

  Sales, cablejats, centres de procés de dades (CPD).

- Aplicacions i serveis

  Gestió de padró, comptabilitat, registre, expedients, etc.

- Dades

  Padró, comptabilitats anuals, convenis i contractes, documents, ...

- Recursos humans relacionats amb les TIC

  Qualsevol treballador afectat per elements TIC de l'Ajuntament

# 2. PLA DE SEGURETAT

## OBJECTIUS:

- Millora de la Seguretat de la Informació
- Facilitar compliment de les lleis actuals (LOPD, ENS, ...)
- Coneixement de l'estat actual de l'organització
- Proposta de millores per evolucionar en la seguretat
- Control periòdic de les mesures aplicades
- Estalvi de diners i/o temps en cas d'incident de seguretat

**FUTUR:**

CERTIFICACIÓ RESPECTE NORMA ISO 27001:2005

ISO 27001:2005 – ESQUEMA NACIONAL SEGURETAT

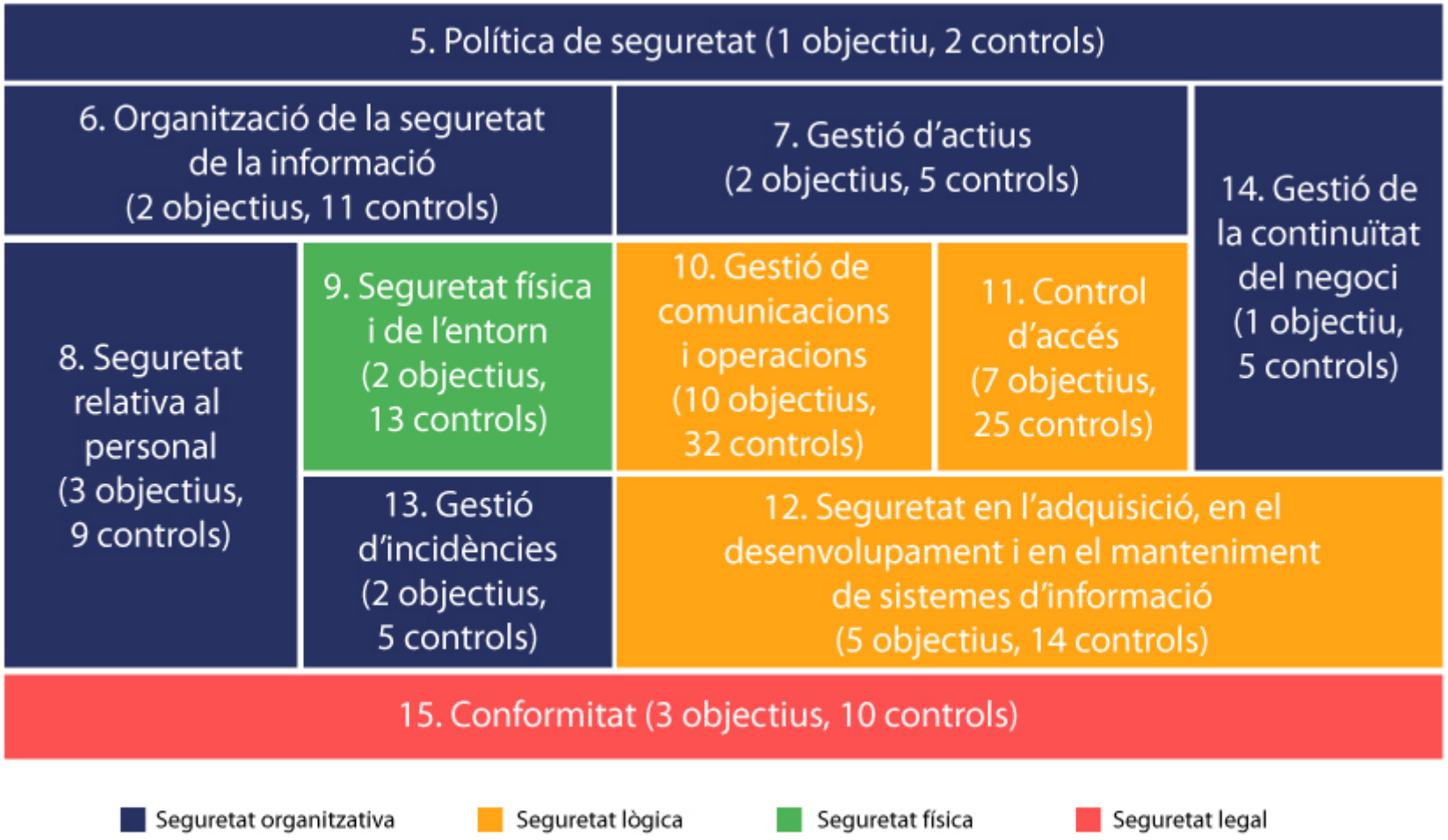
# 2. PLA DE SEGURETAT

## FASES:

- **FASE 1:** Situació actual (context, objectius i anàlisi diferencial ISO)
- **FASE 2:** Sistema de Gestió Documental
- **FASE 3:** Anàlisi de riscos (metodologia MAGERIT)
- **FASE 4:** Propostes de projectes i millores
- **FASE 5:** Auditoria del compliment (respecte ISO 27001:2005)
- **FASE 6:** Presentació de resultats i conclusions

# 2. PLA DE SEGURETAT

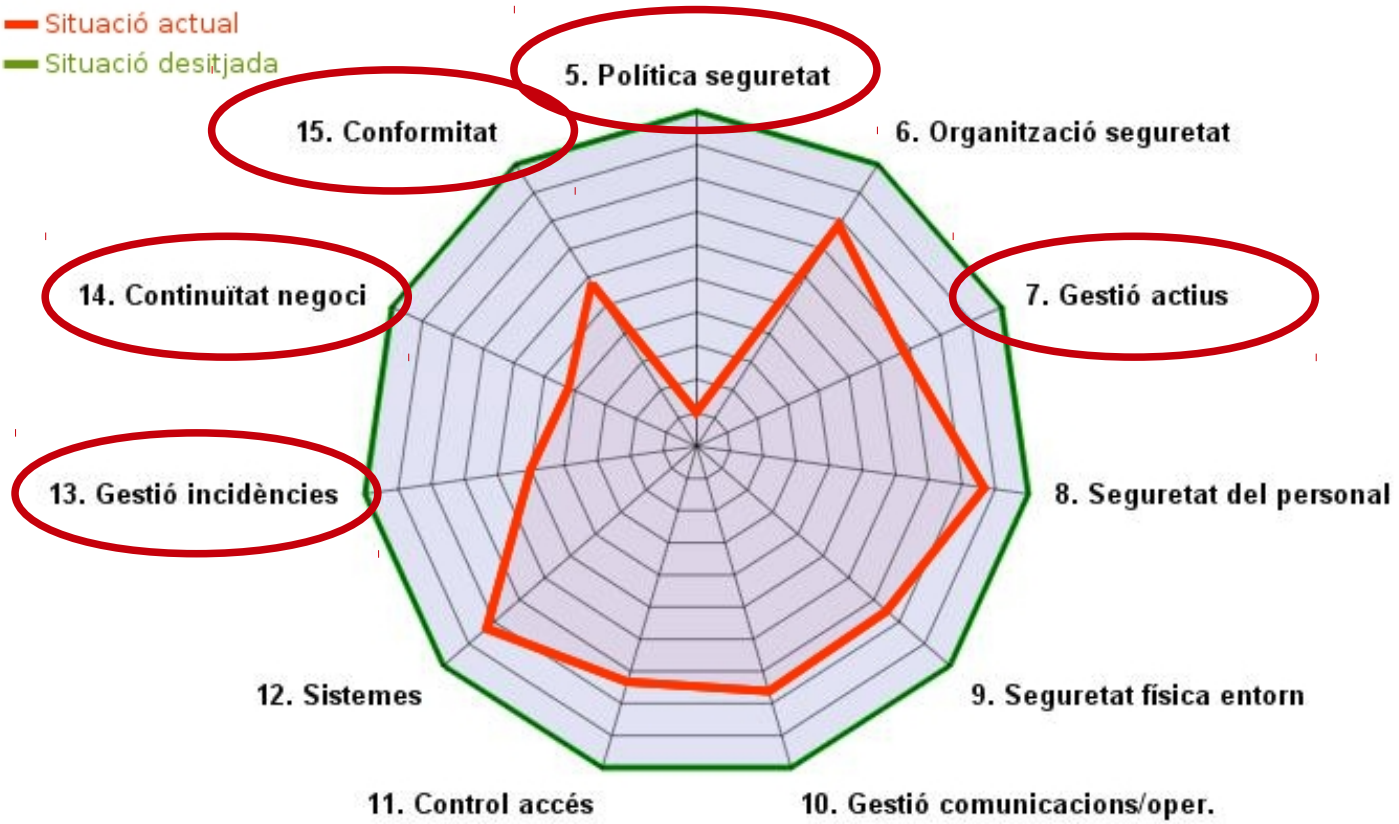
## ISO 27002:2005




11 DOMINIS, 39 OBJECTIUS DE CONTROL I 133 CONTROLS

# 3. ANÀLISI DE RESULTATS

## SITUACIÓ ACTUAL – ANÀLISI DIFERENCIAL ISO

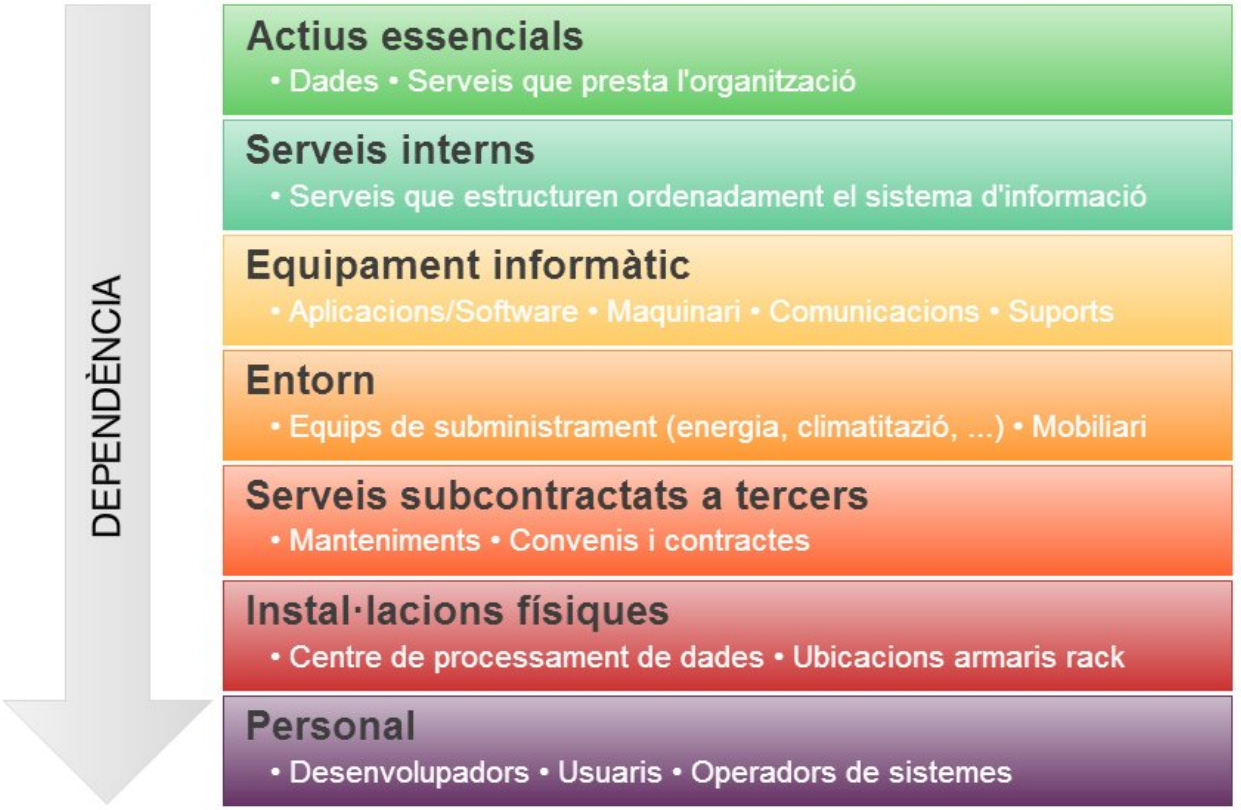


# 3. ANÀLISI DE RESULTATS

## ANÀLISI DE RISCOS

**METODOLOGIA: MAGERIT**

- VALORACIÓ ACTIUS
- CLASSIFICACIÓ
- ANÀLISI AMENACES
- IMPACTE POTENCIAL
- CÀLCUL DEL RISC

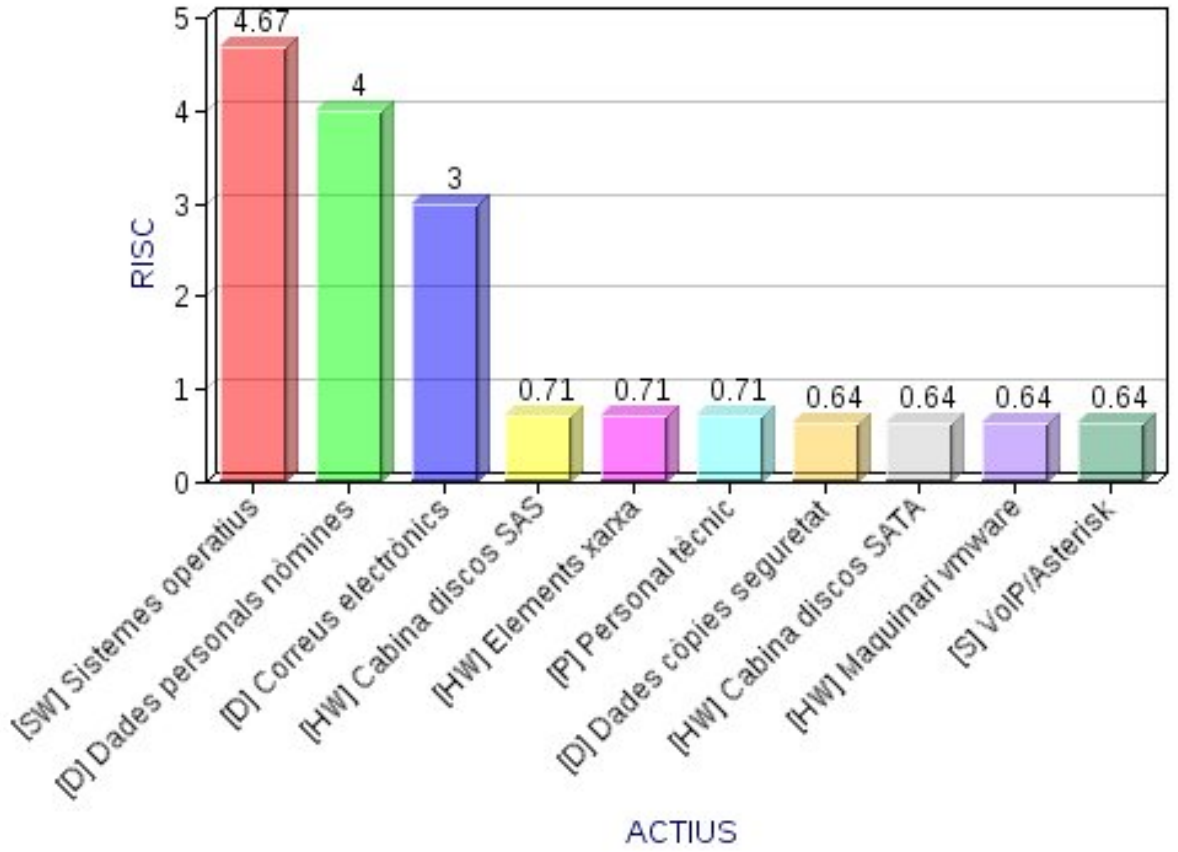


# 3. ANÀLISI DE RESULTATS

## ANÀLISI DE RISCOS - SITUACIÓ ACTUAL

10 ACTIUS AMB
RISC MÉS ELEVAT

Alta freqüència d'amenaça o fort impacte per l'organització



# 3. ANÀLISI DE RESULTATS

## ANÀLISI DE RISCOS – SITUACIÓ ACTUAL

### 10 AMENACES MÉS FREQÜENTS I ACTIUS AMENAÇATS:

| | |
|---|---|
| [E.8] DIFUSIÓ DE MALWARE | Programari |
| [E.1] ERRORS D'USUARI | Programari, Serveis i Claus Criptogràfiques |
| [E.18] DESTRUCCIÓ DE LA INFORMACIÓ | Programari i Serveis |
| [E.2] ERRORS DE L'ADMINISTRADOR | Programari i Dades |
| [A.6] ABÚS DE PRIVILEGIS D'ACCÈS | Programari |
| [A.7] ÚS NO PREVIST | Programari |
| [E.10] ERRORS DE SEQÜÈNCIA | Serveis |
| [E.15] ALTERACIÓ ACCIDENTAL DE LA INFORMACIÓ | Serveis |
| [E.28] INDISPONIBILITAT DEL PERSONAL | Personal |
| [I.5] AVERIA D'ORIGEN FÍSICA O LÒGICA | Maquinari |
| [I.7] CONDICIONS INADEQUADES TEMPERATURA | Maquinari |
| [E.3] ERRORS DE MONITORITZACIÓ | Dades |
| [I.1] FALLADA SERVEI COMUNICACIONS | Comunicacions |
| [E.23] ERRORS DE MANTENIMENT/ACTUALITZACIÓ | Programari i Equipaments auxiliars |
| [A.11] ACCÈS NO AUTORITZAT | Programari, Claus Criptogràfiques i Dependències |

# 4. PROPOSTA DE PROJECTES

## **DOS** PRINCIPALS OBJECTIUS:

- **REDUIR** EL **RISC** DE DETERMINATS ACTIUS
- **MILLORAR** EL NIVELL DE COMPLIMENT **ISO 27001**

### OBJECTIUS ADDICIONALS:

- MAJOR OPTIMITZACIÓ DELS RECURSOS
- MILLORES EN LA GESTIÓ DE PROCESSOS
- MILLORES EN LES TECNOLOGIES EMPRADES

### DURADA PREVISTA DE L'EXECUCIÓ: 3 ANYS

# 4. PROPOSTA DE PROJECTES

## 1. PROJECTES A CURT TERMINI – 1r ANY

**PROJ-001:** Adquisició de programari antivirus corporatiu
Durada: 2 mesos // Cost econòmic: 2.500 €

**PROJ-002:** Procediments d'actualitzacions de sistemes operatius
Durada: 1 mes // Cost econòmic: 0 €

**PROJ-003:** Documentació / Implantació de Polítiques de Seguretat
Durada: 10 mesos // Cost econòmic: 5.500 €

**PROJ-004:** Realització de l'inventari d'actius
Durada: 2 mesos // Cost econòmic: 500 €

**PROJ-005:** Millora de climatització en els CPDades
Durada: 4 mesos // Cost econòmic: 12.000 €

**PROJ-006:** Revisió de procediments en Recursos Humans
Durada: 2 mesos // Cost econòmic: 500 €

**INVERSIÓ TOTAL ANUAL:** 21.000 €

# 4. PROPOSTA DE PROJECTES

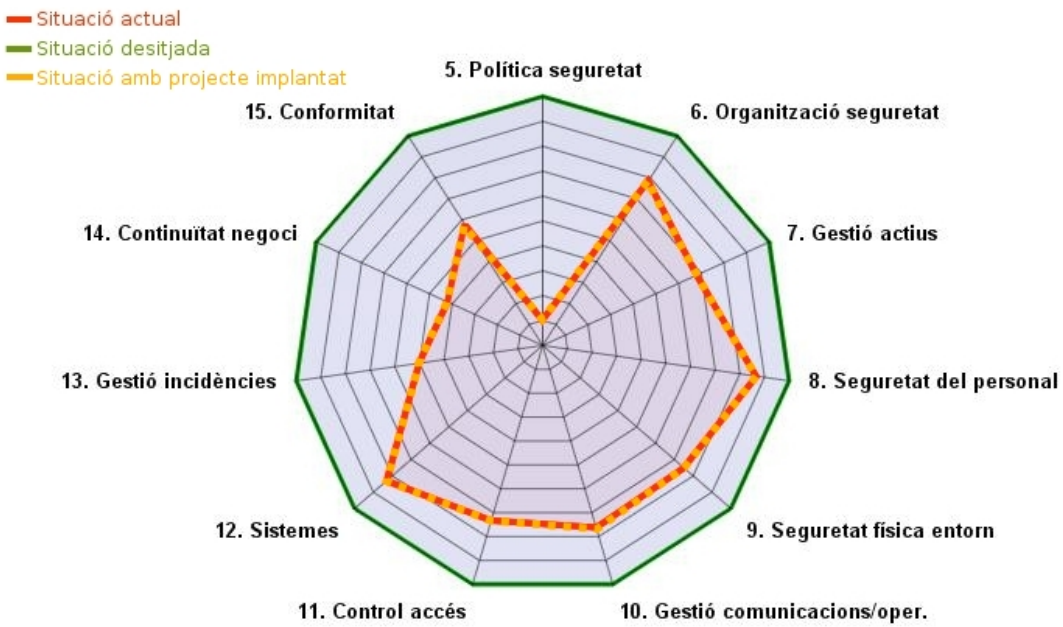
## 1. PROJECTES A CURT TERMINI – 1r ANY

**PROJ-001:** Adquisició de programari antivirus corporatiu

Durada: 2 mesos // Cost econòmic: 2.500 €

Objectiu: Definir, planificar, gestionar i executar auditories internes o externes de manera periòdica.

Afectació: Alta en el risc dels SS.OO., baixa en domini 10 ISO



# 4. PROPOSTA DE PROJECTES

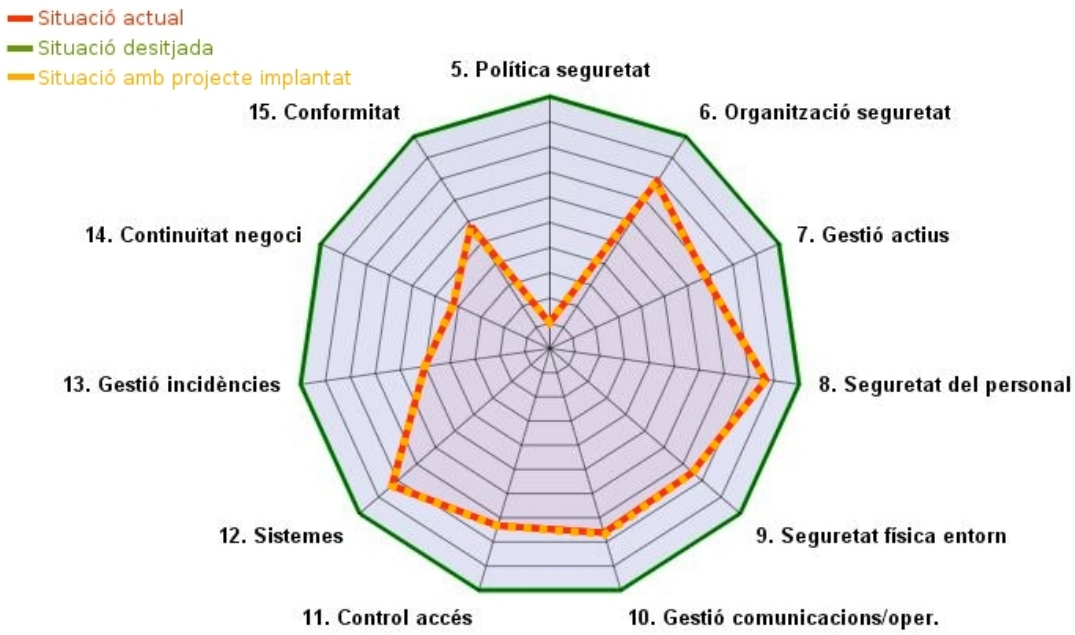
## 1. PROJECTES A CURT TERMINI – 1r ANY

**PROJ-002:** Procediments d'actualitzacions en sistemes operatius

Durada: 1 mes // Cost econòmic: 0 €

Objectiu: Definir, planificar, gestionar actualitzacions dels SS.OO. de manera periòdica.

Afectació: Alta en el risc dels SS.OO., baixa en dominis ISO



# 4. PROPOSTA DE PROJECTES

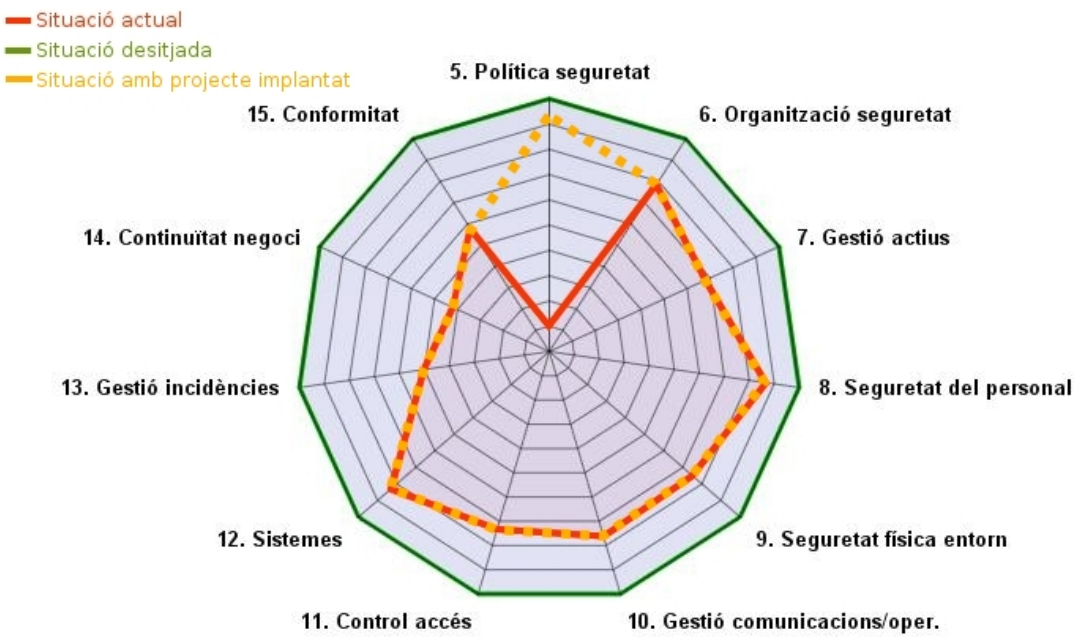
## 1. PROJECTES A CURT TERMINI – 1r ANY

**PROJ-003:** Documentació/Implantació de polítiques de Seguretat

Durada: 10 mesos // Cost econòmic: 5.500 €

Objectiu: Definició, aprovació i aplicació de les Polítiques de Seguretat necessàries.

Afectació: Cap en el risc dels actius, molt alta en domini 5 ISO.



# 4. PROPOSTA DE PROJECTES

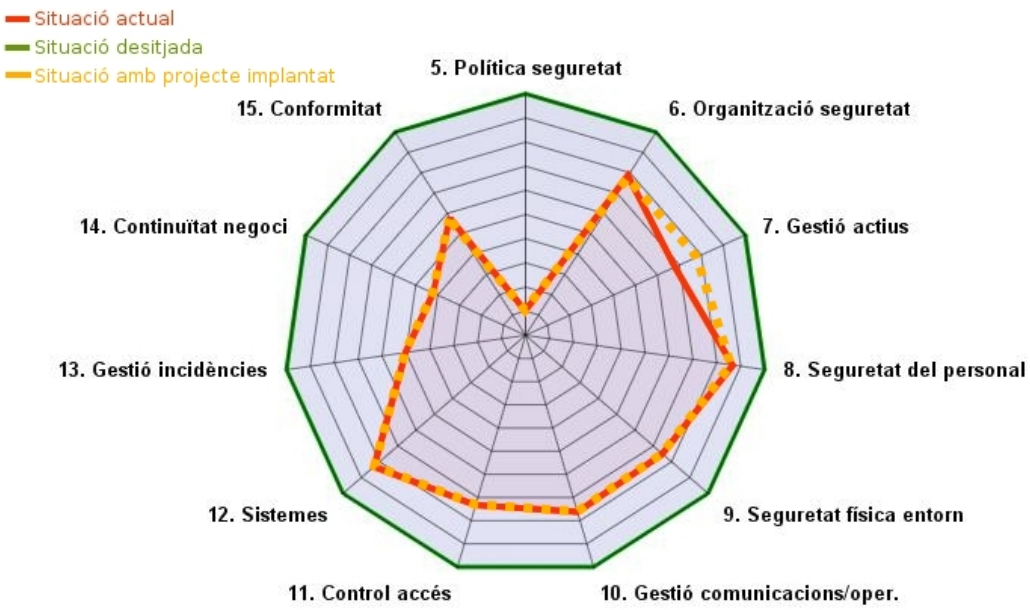
## 1. PROJECTES A CURT TERMINI – 1r ANY

**PROJ-004:** Realització de l'inventari d'actius

Durada: 2 mesos // Cost econòmic: 500 €

Objectiu: Realització minuciosa i detallada de tot l'inventari d'actius de l'Ajuntament.

Afectació: Cap en el risc dels actius, mitjana en domini 7 de la ISO.



# 4. PROPOSTA DE PROJECTES

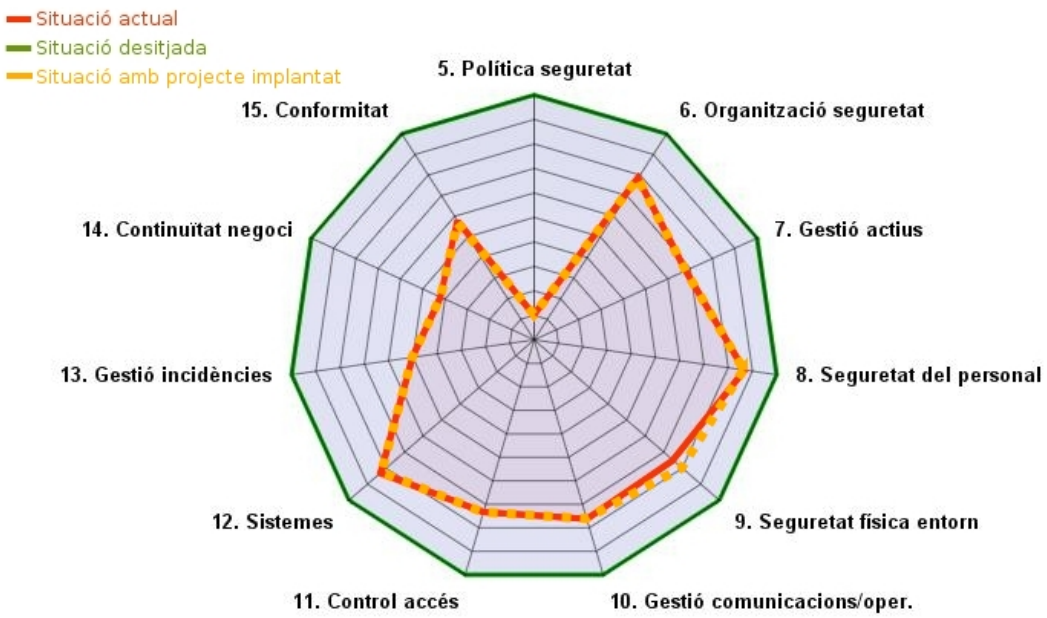
## 1. PROJECTES A CURT TERMINI – 1r ANY

**PROJ-005:** Millora de la climatització dels C.P.D.

Durada: 4 mesos // Cost econòmic: 12.000 €

Objectiu: Millora de la climatització dels diferents Centres de Processament de Dades.

Afectació: Molt alta en riscos del HW, baixa en el domini 9 de la ISO.



# 4. PROPOSTA DE PROJECTES

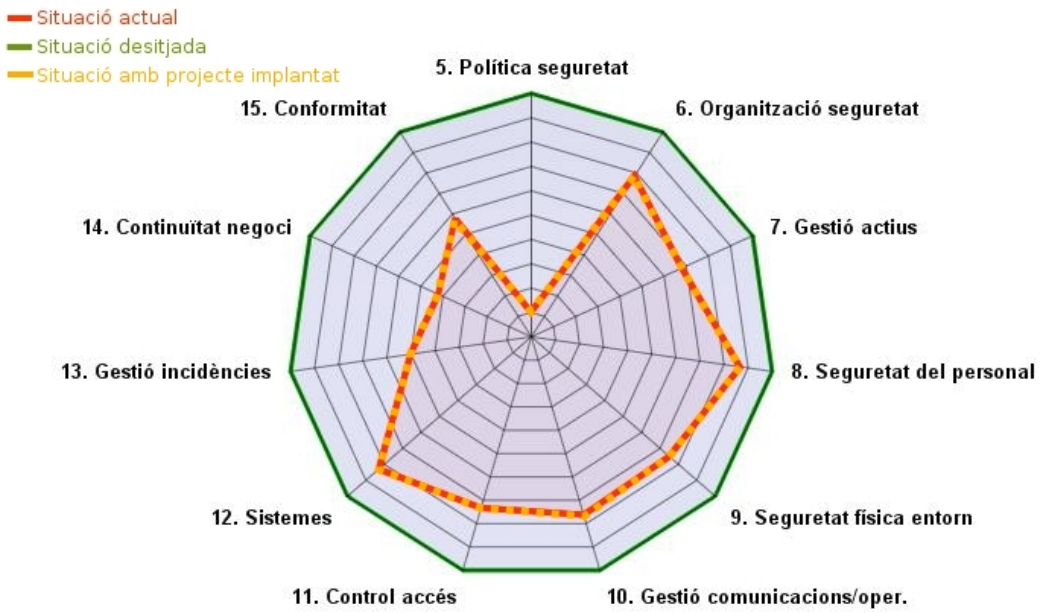
## 1. PROJECTES A CURT TERMINI – 1r ANY

**PROJ-006:** Revisió de procediments de Recursos Humans

Durada: 2 mesos // Cost econòmic: 500 €

Objectiu: Millora de seguretat dels procediments de RR.HH.

Afectació: Molt alta en errades amb dades de personal, molt baixa en el domini 10 de la ISO.



# 4. PROPOSTA DE PROJECTES

## 2. PROJECTES A MITJÀ TERMINI – 2n ANY

**PROJ-007:** Formació del personal en Seguretat de les TIC
Durada: 4 mesos // Cost econòmic: 5.000 €

**PROJ-008:** Gestió d'incidències, programari i procediments
Durada: 8 mesos // Cost econòmic: 12.700 €

**PROJ-009:** Definició de plans de continuïtat
Durada: 10 mesos // Cost econòmic: 10.000 €

**PROJ-010:** Definició de procediments de còpies de seguretat
Durada: 2 mesos // Cost econòmic: 1.500 €

**INVERSIÓ TOTAL ANUAL: 20.200 €**

# 4. PROPOSTA DE PROJECTES

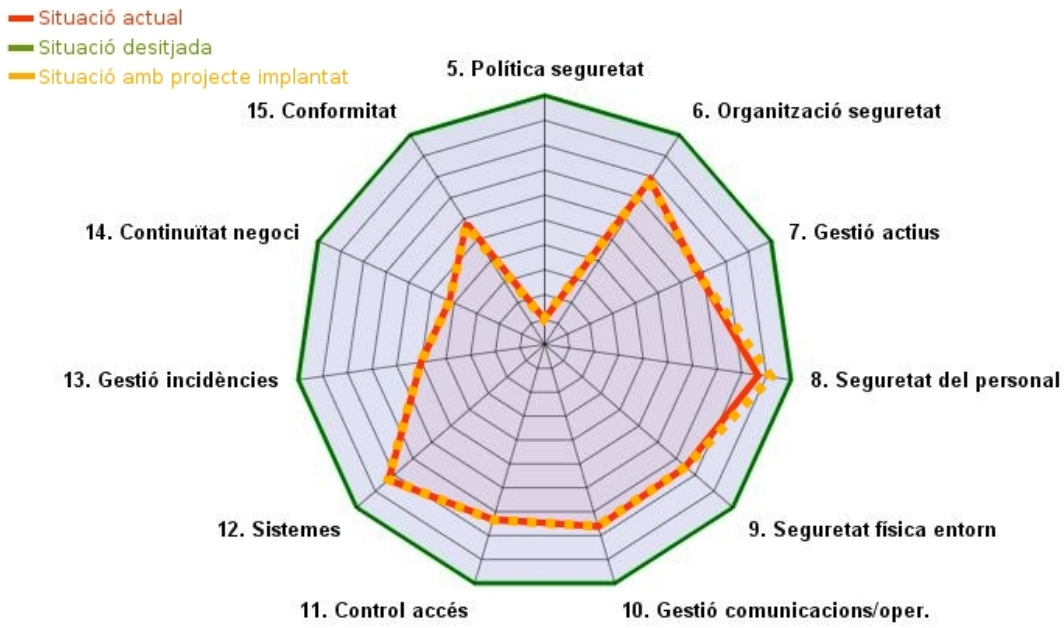
## 2. PROJECTES A MITJÀ TERMINI – 2n ANY

**PROJ-007:** Formació del personal en Seguretat de les TIC

Durada: 4 mesos // Cost econòmic: 5.000 €

Objectiu: Reduir els errors d'usuari, molt freqüents. Millorar conscienciació en seguretat.

Afectació: Normal en risc d'errades amb dades i processos, normal en el domini 8 de la ISO.



# 4. PROPOSTA DE PROJECTES

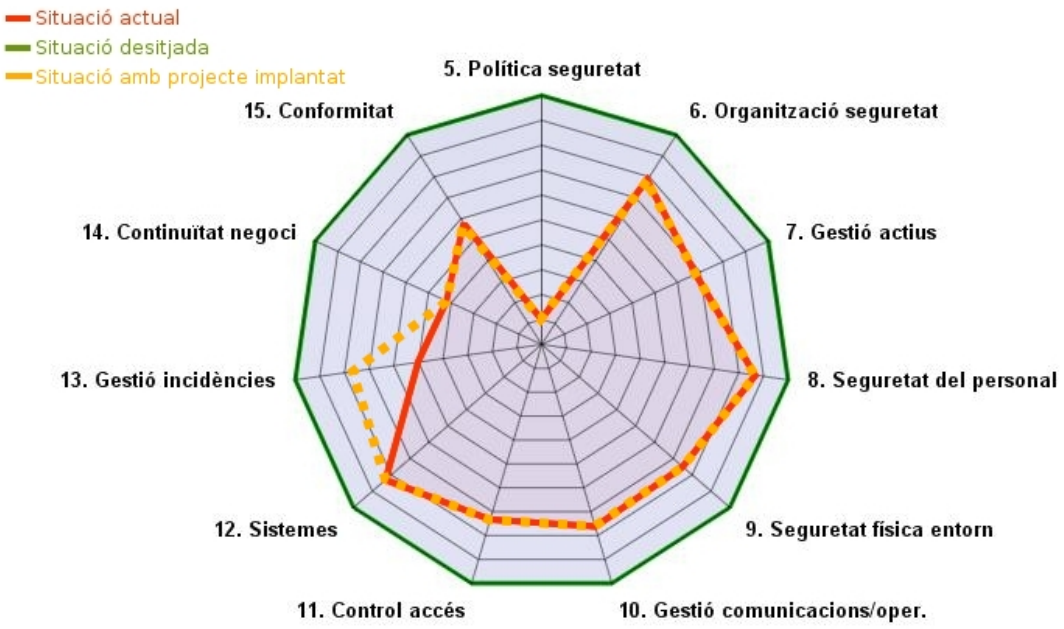
## 2. PROJECTES A MITJÀ TERMINI – 2n ANY

**PROJ-008:** Gestió d'incidències, programari i procediments

Durada: 8 mesos // Cost econòmic: 12.700 €

Objectiu: Control i millora de la gestió d'incidències en les TIC.

Afectació: Cap de directa en l'AA.RR, però alta en el domini 13 de la ISO.



# 4. PROPOSTA DE PROJECTES

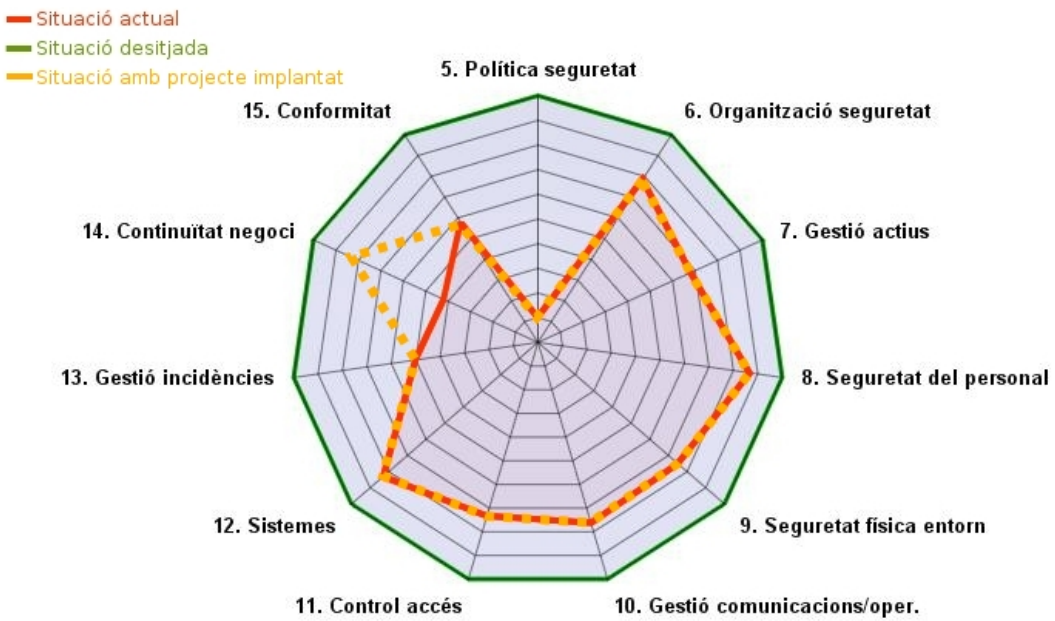
## 2. PROJECTES A MITJÀ TERMINI – 2n ANY

**PROJ-009:** Definició de plans de continuïtat

Durada: 10 mesos // Cost econòmic: 10.000 €

Objectiu: Documentar i planificar els diferents plans de continuïtat.

Afectació: Reducció de risc per disponibilitat en certs actius, alta en el domini 14 de la ISO.



# 4. PROPOSTA DE PROJECTES

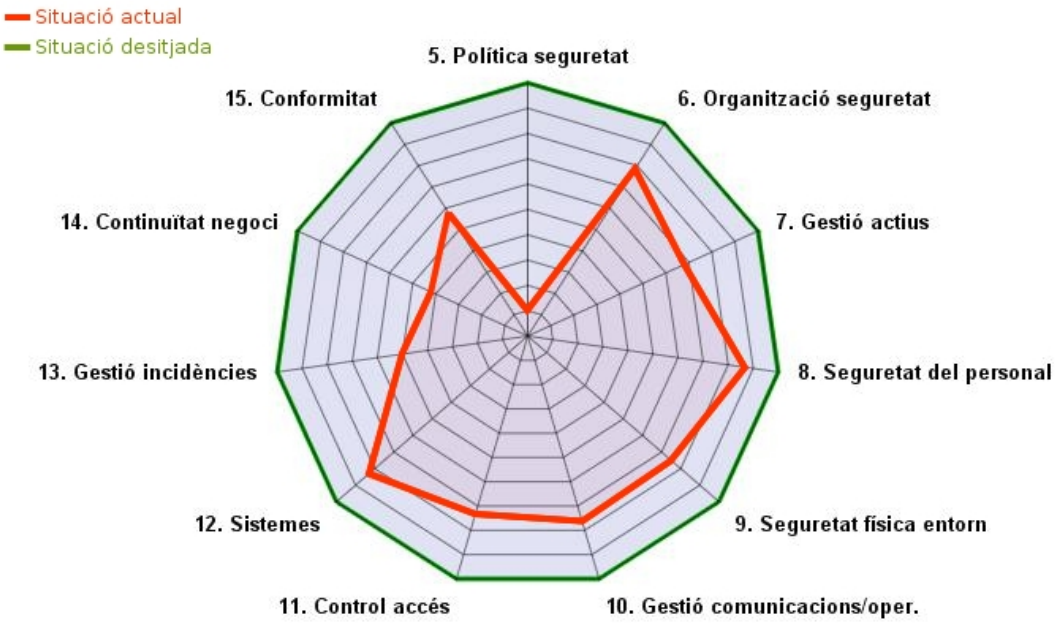
## 2. PROJECTES A MITJÀ TERMINI – 2n ANY

**PROJ-010:** Definició de procediments de còpies de seguretat

Durada: 2 mesos // Cost econòmic: 1.500 €

Objectiu: Planificar i documentar els diferents plans de còpies de seguretat.

Afectació: Alta reducció de risc per certs actius de dades, mínima en el domini 10 de la ISO, no varia el diagrama radar.



# 4. PROPOSTA DE PROJECTES

## 3. PROJECTES A LLARG TERMINI – 3r ANY

**PROJ-011:** Procediment i gestió d'auditories internes/externes
Durada: 5 mesos // Cost econòmic: 25.000 €

**PROJ-012:** Revisió i millora de les polítiques d'*Active Directory*
Durada: 4 mesos // Cost econòmic: 2.000 €

**PROJ-013:** Reestructuració del departament TIC
Durada: 6 mesos // Cost econòmic: 34.000 € (anuals)

**INVERSIÓ TOTAL ANUAL: 61.000 €**

# 4. PROPOSTA DE PROJECTES

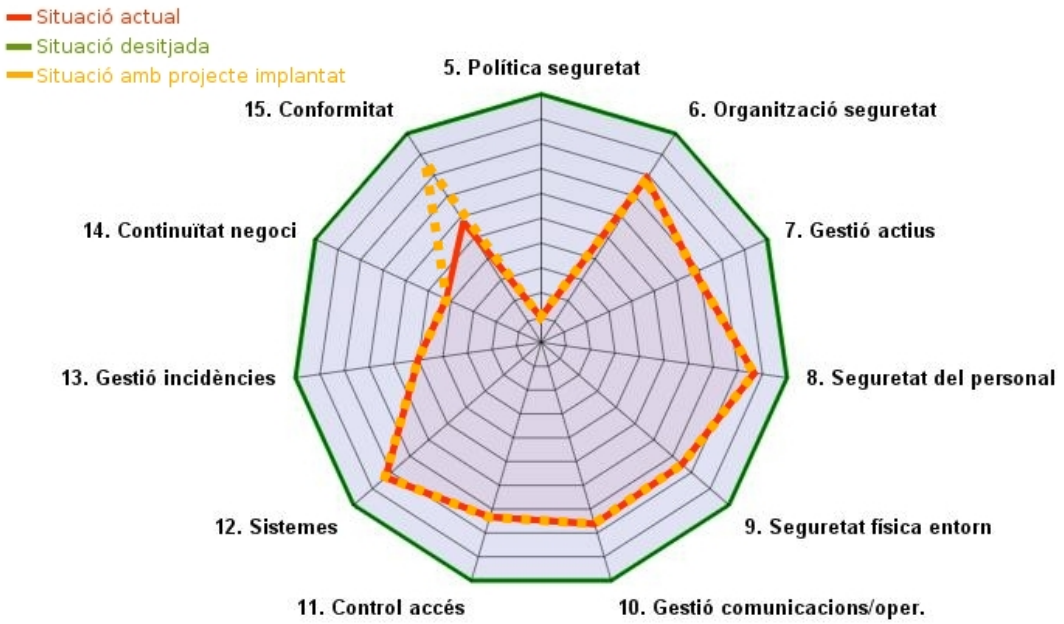
## 3. PROJECTES A LLARG TERMINI – 3r ANY

**PROJ-011:** Procediment i gestió d'auditories internes/externes

Durada: 5 mesos // Cost econòmic: 25.000 €

Objectiu: Planificació d'auditories periòdiques internes i externes.

Afectació: Cap reducció de risc directa, però molt alta en en el domini 15 de la ISO.



# 4. PROPOSTA DE PROJECTES

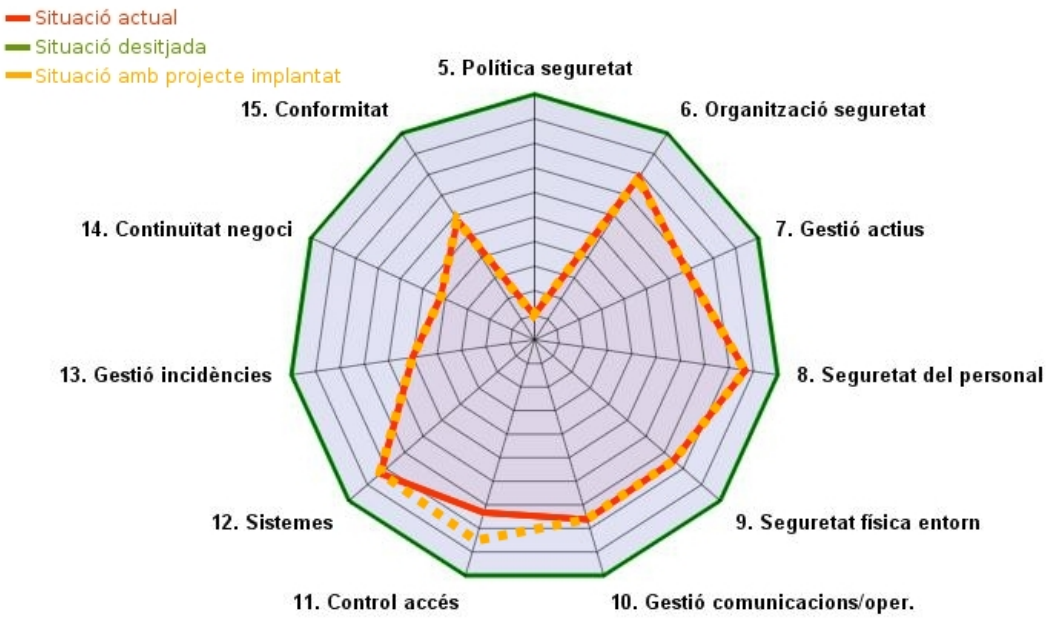
## 3. PROJECTES A LLARG TERMINI – 3r ANY

**PROJ-012:** Revisió i millora de les polítiques d'*Active Directory*

Durada: 4 mesos // Cost econòmic: 2.000 €

Objectiu: Millora i revisió de polítiques d'Active Directory.

Afectació: Reducció de risc en SS.OO. estacions de treball, i mitjana en el domini 11 de la ISO.



# 4. PROPOSTA DE PROJECTES

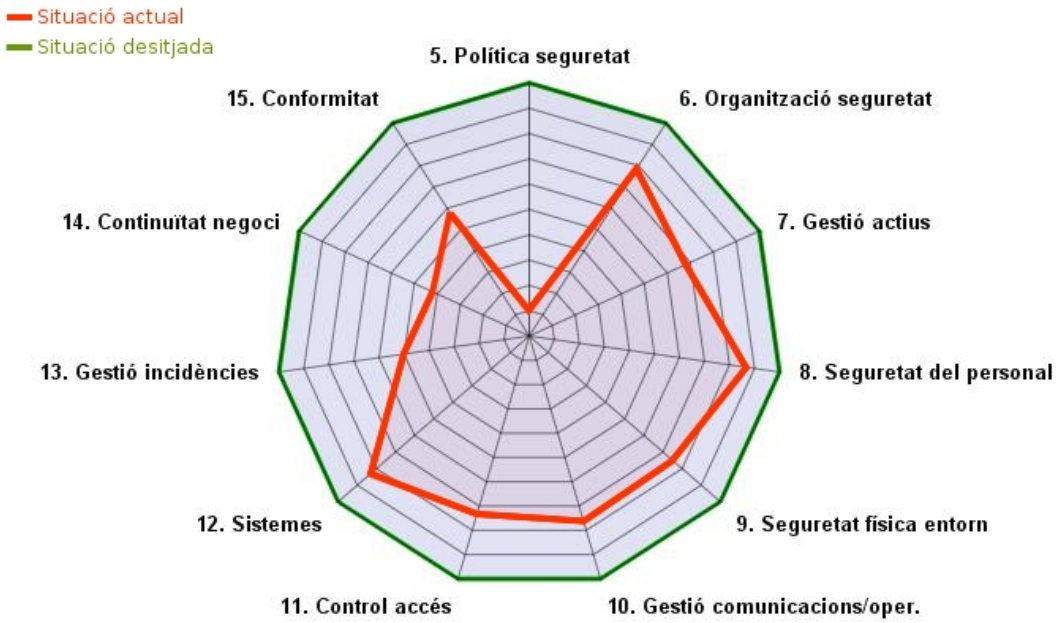
## 3. PROJECTES A LLARG TERMINI – 3r ANY

**PROJ-013:** Reestructuració del departament TIC

Durada: 6 mesos // Cost econòmic: 34.000 € (anual)

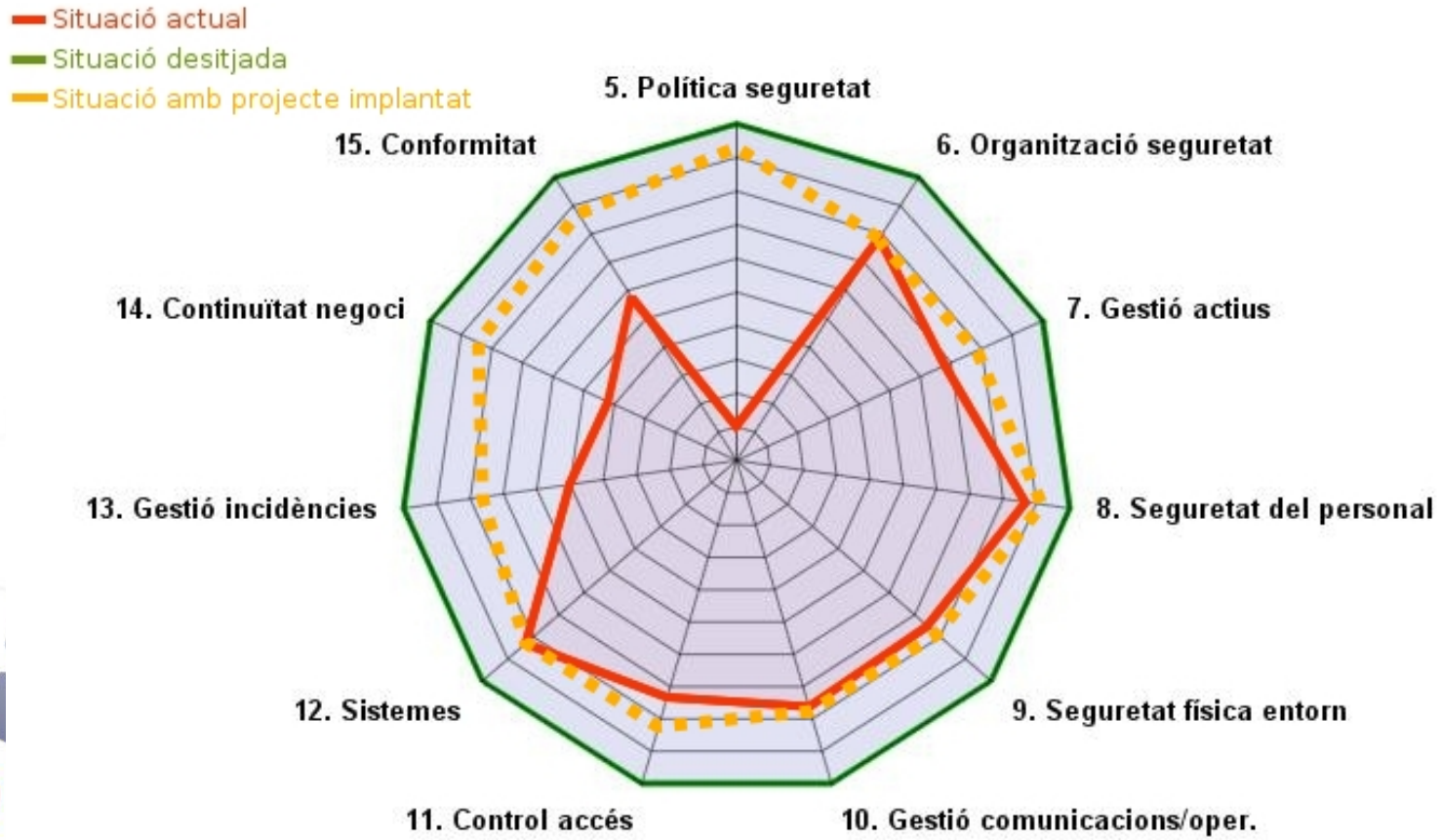
Objectiu: Contractació de tècnic de sistemes per departament TIC.

Afectació: Reducció de risc en indisponibilitat de personal, sense afectació directa a dominis ISO.



# 4. PROPOSTA DE PROJECTES

## IMPACTE DE TOTS ELS PROJECTES (3 ANYS)



# 5. AUDITORIA DE COMPLIMENT ISO

## OBJECTIUS

- Avaluació de la maduresa de la seguretat

  *(Model de maduresa de la capacitat - CMM)*
- Revisió detallada dels 133 controls de la ISO 27002
- Detecció de no conformitats majors i menors
- Anotació de les diferents observacions

# 5. AUDITORIA DE COMPLIMENT ISO

## RESULTATS

S'han detectat 30 no conformitats, de les quals:

- 9 són **no conformitats majors**
- 21 són **no conformitats menors**

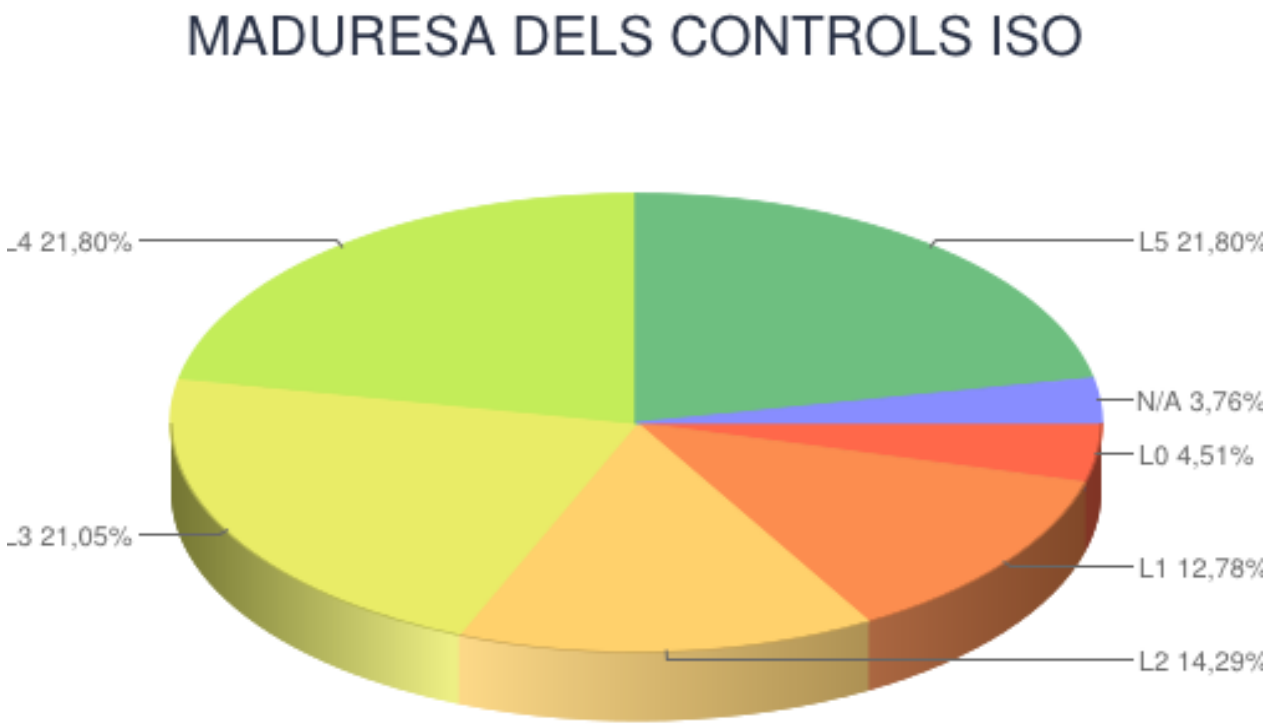
S'han anotat **8 observacions**.

**NOTA:** Algunes de les no conformitats pertanyen a controls que són necessaris per poder obtenir una certificació respecte la norma ISO/IEC 27001:2005.

# 5. AUDITORIA DE COMPLIMENT ISO

## RESULTATS

Una tercera part dels controls precisa d'una acció correctora per poder obtenir un nivell de compliment del 90% o superior.



# 6. CONCLUSIONS

## PLA DE SEGURETAT – AJUNTAMENT DE RIBEROLA

- S'HAN DEFINIT L'ABAST I ELS OBJECTIUS DEL PLA DE SEGURETAT
- S'HA AVALUAT LA SITUACIÓ ACTUAL DE LA SEGURETAT
- S'HA REALITZAT L'ANÀLISI DE RISCOS (MAGERIT)
- S'HAN PROPOSAT PROJECTES DE MILLORA
- S'HA REALITZAT UNA AUDITORIA DE COMPLIMENT ISO 27002:2005

MITJANÇANT L'EXECUCIÓ DELS PROJECTES PROPOSATS EL NIVELL DE COMPLIMENT DE LA ISO 27001 AUGMENTARIA CONSIDERABLEMENT. L'ANÀLISI DE RISCOS MOSTRARIA EL RISC MÉS CONTROLAT PELS ACTIUS TRACTATS.

# 7. PRECS I PREGUNTES

## PLA DE SEGURETAT – AJUNTAMENT DE RIBEROLA

PRECS I PREGUNTES...