INGENSA

UOC
Universitat Oberta de Catalunya

Sistema de Gestió de la Seguretat de la Informació seguint la norma ISO 27001 – ISO 27002 per a la empresa INGENSA, S.L.

Autor: Jordi Sánchez Celma
Consultor: Arsenio Tortajada Gallego
MISTIC
Juny 2016 - UOC

INGENSA, S.L.

Empresa d'enginyeria, consultoria i tecnologies de la informació amb més de 1000 treballadors i seus a nivell nacional i internacional. Amb oficines centrals a Madrid així com el CPD principal.

Serveis principals dels sistemes d'informació:

- Directori Actiu replicat.
- Correu electrònic.
- Intranet.
- CRM.
- ERP.
- Connectivitat VPN.

Organigrama de INGENSA, S.L.

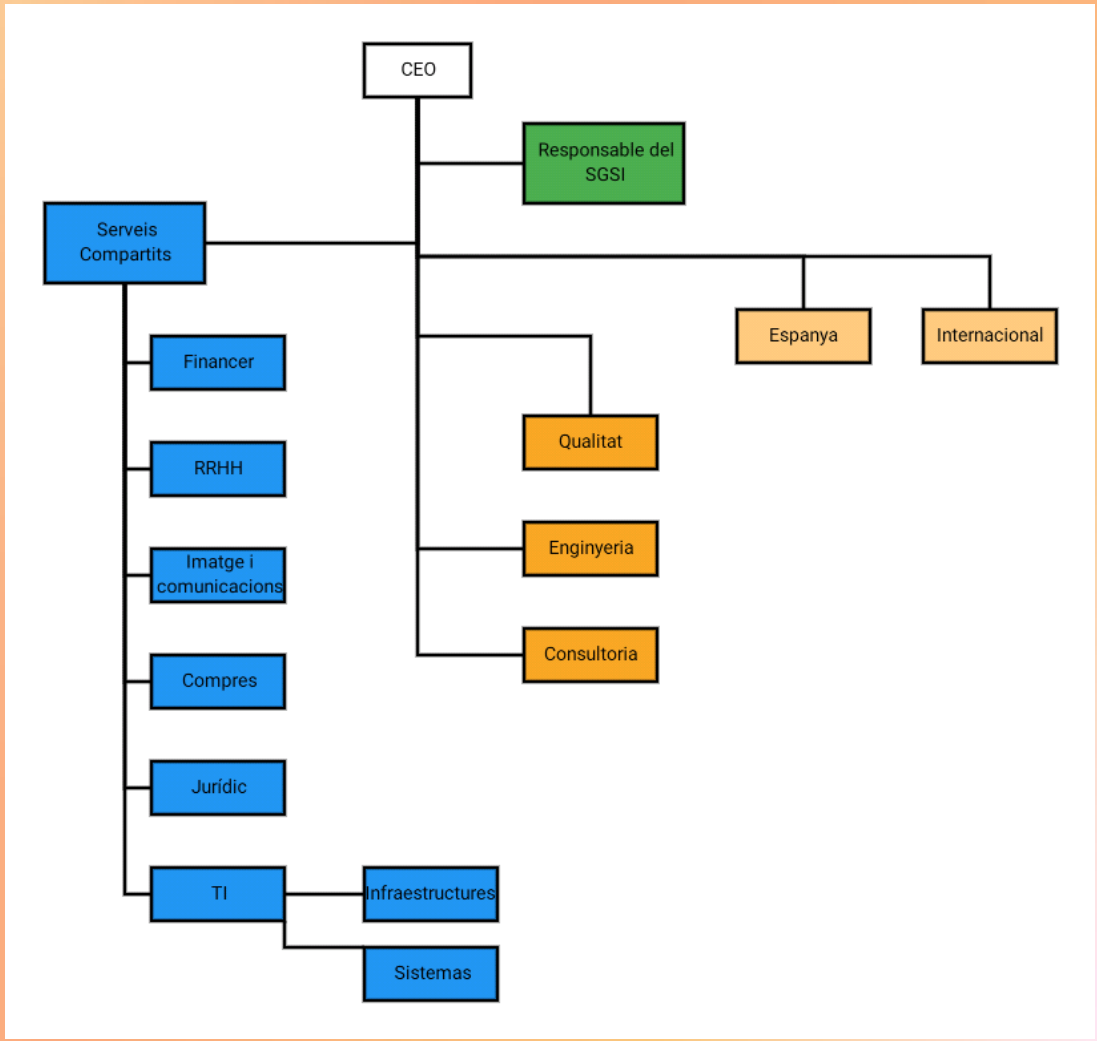
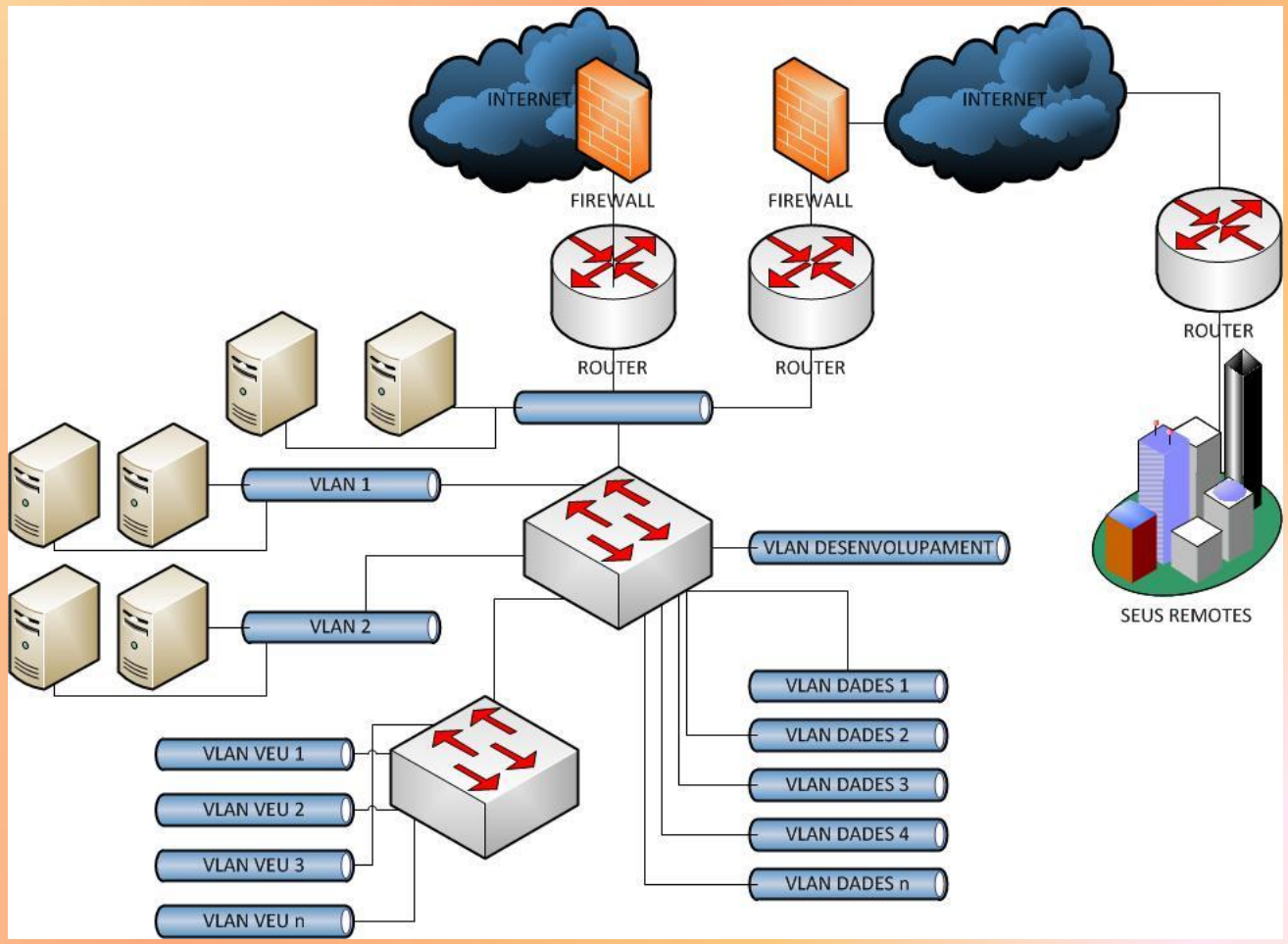


Diagrama de xarxa de la seu central



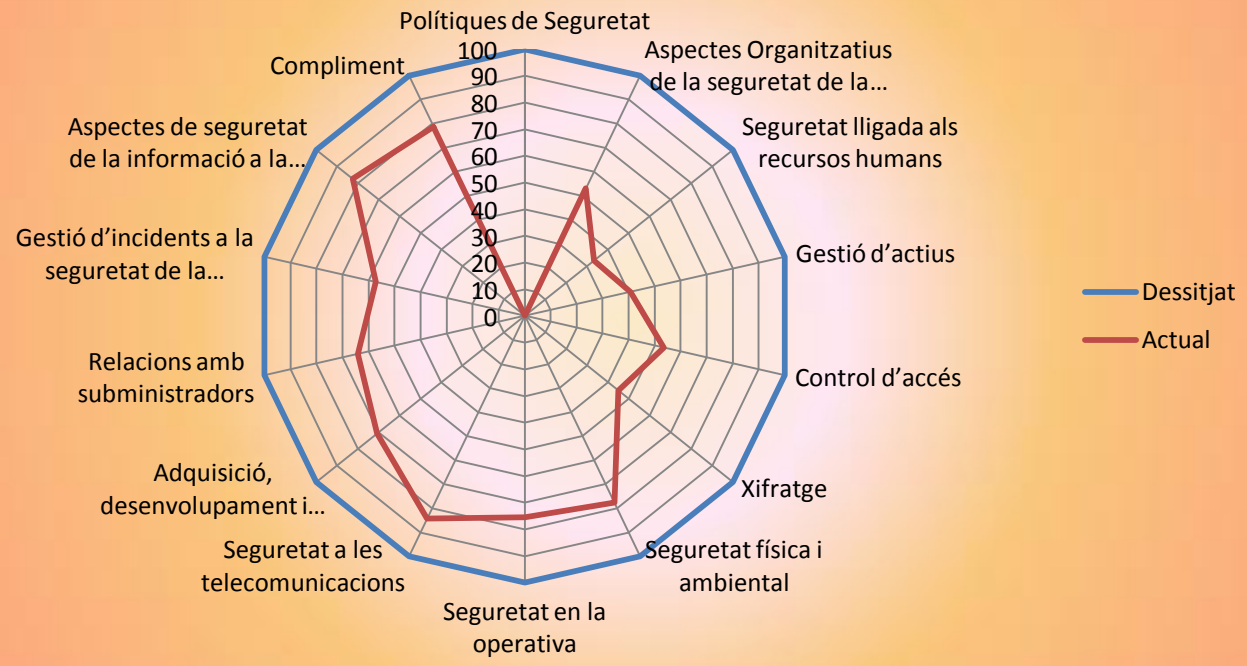
Objectius

L'objectiu principal és l'establiment d'un SGSI per l'empresa INGENSA, S.L. basat en la normativa ISO/IEC 27001 i ISO/IEC 27002.

Principals objectius:

- Creació de política i comitè de seguretat.
- Involucrar l'alta direcció amb l'SGSI.
- Garantir el compliment de la legislació vigent.
- Identificació d'actius, processos crítics i minimització de riscos.
- Garantir la funcionalitat dels serveis d'informació.
- Assegurament de les dades mòbils.
- Anàlisis per minimització de costos.
- Conscienciació dels empleats en seguretat de la informació.

Avaluació de l'estat inicial en seguretat de la informació



Valoració dels 14 dominis de la ISO/IEC 27002:2013 segons el Model de Maduresa de la Capacitat (CMM).

Sistema de Gestió Documental del SGSI

Recull la següent informació:

Documentació:

- Abast.
- Polítiques de seguretat de la informació.
- Declaració d'aplicabilitat.
- Inventari i ús d'actius.
- Metodologia, pla de tractament i informe d'avaluació de riscos.
- Procediments de gestió d'incidents i continuïtat de negoci.
- Requisits legals.

Registres:

- Registres de capacitació, habilitats, esdeveniments de seguretat i activitats, etc...
- Resultats de supervisió, medició, auditories internes, revisió de la direcció i accions correctores.
- Programa d'auditoria interna.

Anàlisis de riscos I

Consta de cinc fases segons la metodologia MAGERIT v.3:

- Fase 1: **Inventari d'actius.**
  Es diferencien els àmbits:
  - Actius d'informació.
  - Aplicacions.
  - Hardware.
  - Xarxa.
  - Equipaments auxiliars.
  - Instal·lacions.
  - Serveis.
  - Personal.

  Classificats de forma qualitativa segons Autenticitat, Confidencialitat, Integritat, Disponibilitat i Auditabilitat (ACIDA).

Anàlisis de riscos II

- Fase 2: **Avaluació d'amenaces.**
  Classificades com:
  - Desastres naturals [N].
  - D'origen industrial [I].
  - Errors o fallides no intencionades [E].
  - Atacs intencionats [A].

  Avaluació de l'impacte potencial: és el percentatge d'actiu que es perd en cas d'amenaça abans d'aplicar salvaguardes.

  *Impacte Potencial = Valor_Actiu * Impacte*

Anàlisis de riscos III

- Fase 3: **Salvaguardes.**
  Procediments per reduir el risc d'impacte, hi ha dos tipus:
  - Redueix la probabilitat d'amenaça.
  - Redueix l'impacte causat.

- Fase 4: **Impacte residual.**
  Càlcul de l'impacte sobre els actius en aplicar les salvaguardes.

Anàlisis de riscos IV

- Fase 5: **Nivells de risc.**
  - Risc acceptable: es pot assumir sense prendre mesures per reduir-lo, a INGENSA, S.L. tindran les següents característiques:
    - Valor d'actiu mig (5).
    - Impacte del 40%.
    - Freqüència mensual (8).

    Els valors superiors a 16 es troben per sobre del risc acceptable.

  - Risc residual: risc que romandrà en aplicar salvaguardes.

Propostes de projectes I

L'anàlisi de riscos d'INGENSA, S.L. identifica:

- Els actius més crítics.
- Actius d'impacte més greu.
- Vulnerabilitats més freqüents

Amb l'avaluació de dominis de la norma ISO/IEC 27002:2013 es coneix els que es troben al nivell inicial L0 segons classificació CMM.

Aplicació de projectes per reduir el nivell de risc en seguretat de la informació i assolir els principals objectius de l'implementació del SGSI.

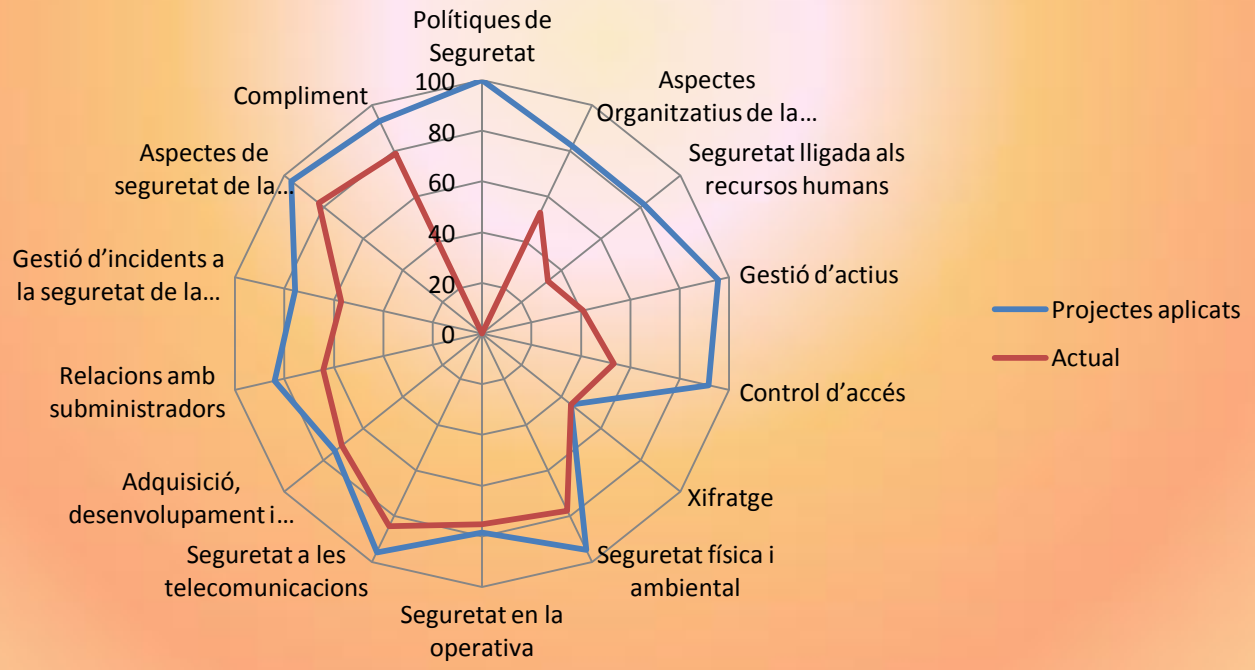
Propostes de projectes II

Llistat de projectes:

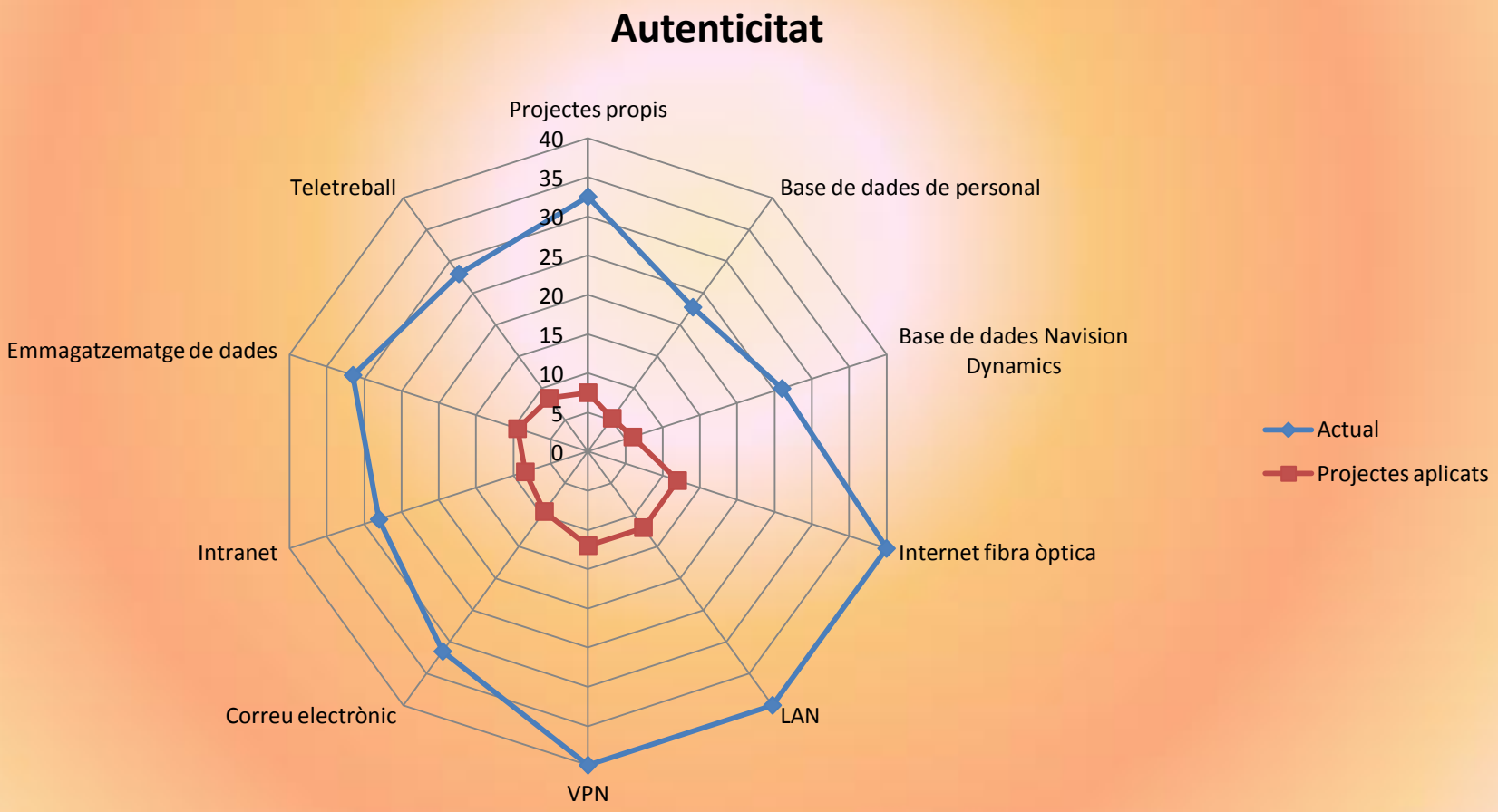
- PRO-001: Establiment de la política de seguretat.
- PRO-002: Document de seguretat per a les noves contractacions.
- PRO-003: Document per establir el protocol de classificació de la informació.
- PRO-004: Implantació d'un MDM.
- PRO-005: Procediment per a la documentació de TI.
- PRO-006: Política de seguretat per a la instal·lació de Software.
- PRO-007: Seguretat del Hardware i serveis crítics.
- PRO-008: Document de control de còpies de seguretat.
- PRO-009: Continuïtat de les comunicacions externes a la companyia.
- PRO-010: Pla de formació als usuaris en seguretat de la informació.

Comparativa dels controls ISO/IEC 27002:2013 en l'actualitat i en aplicar els projectes

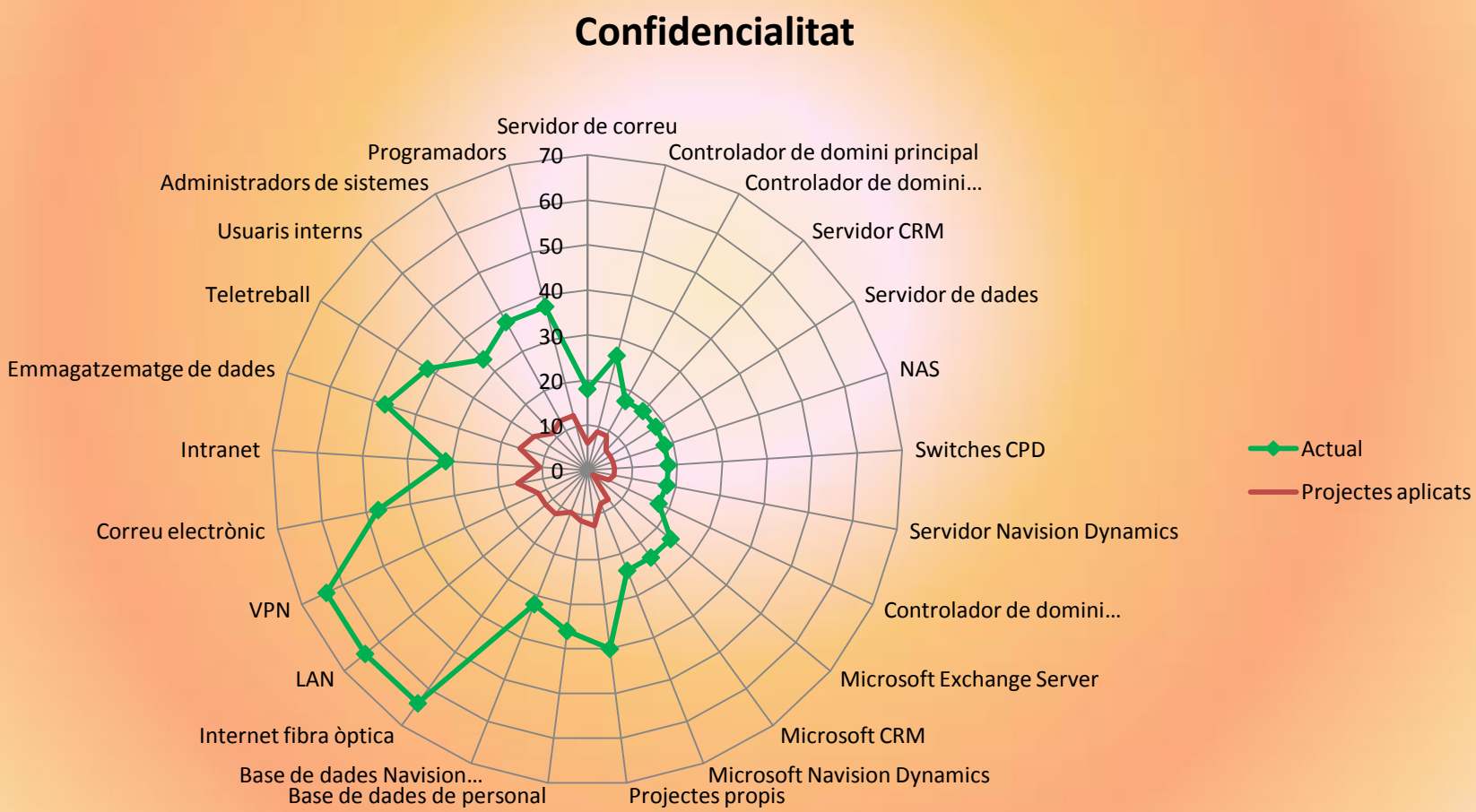
Millora del nivell de risc dels actius i la maduració CMM dels controls ISO/IEC 27002:2013 en aplicar els projectes proposats.



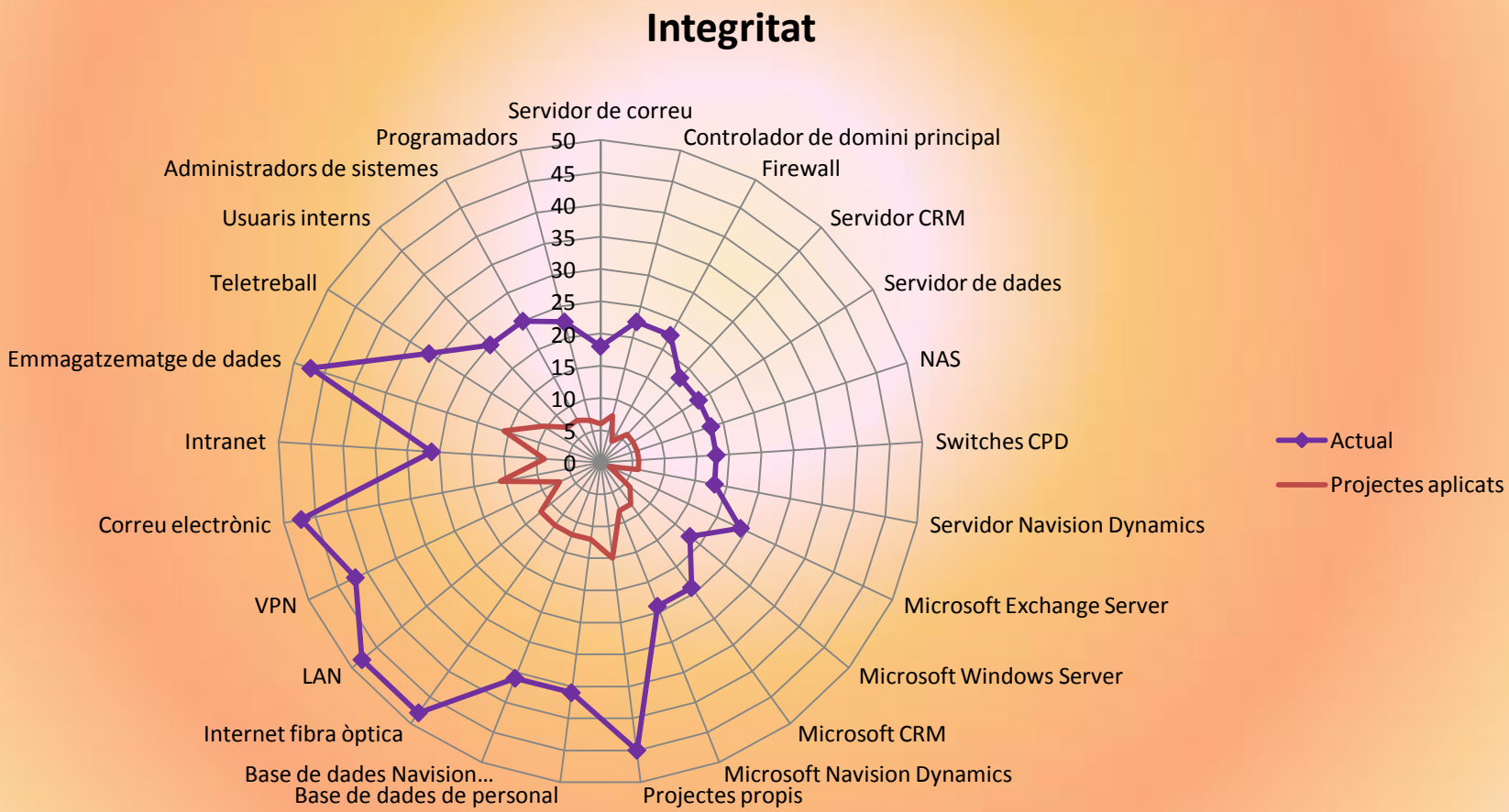
Comparativa nivells de risc abans i després d'aplicar els projectes en les dimensions ACIDA I



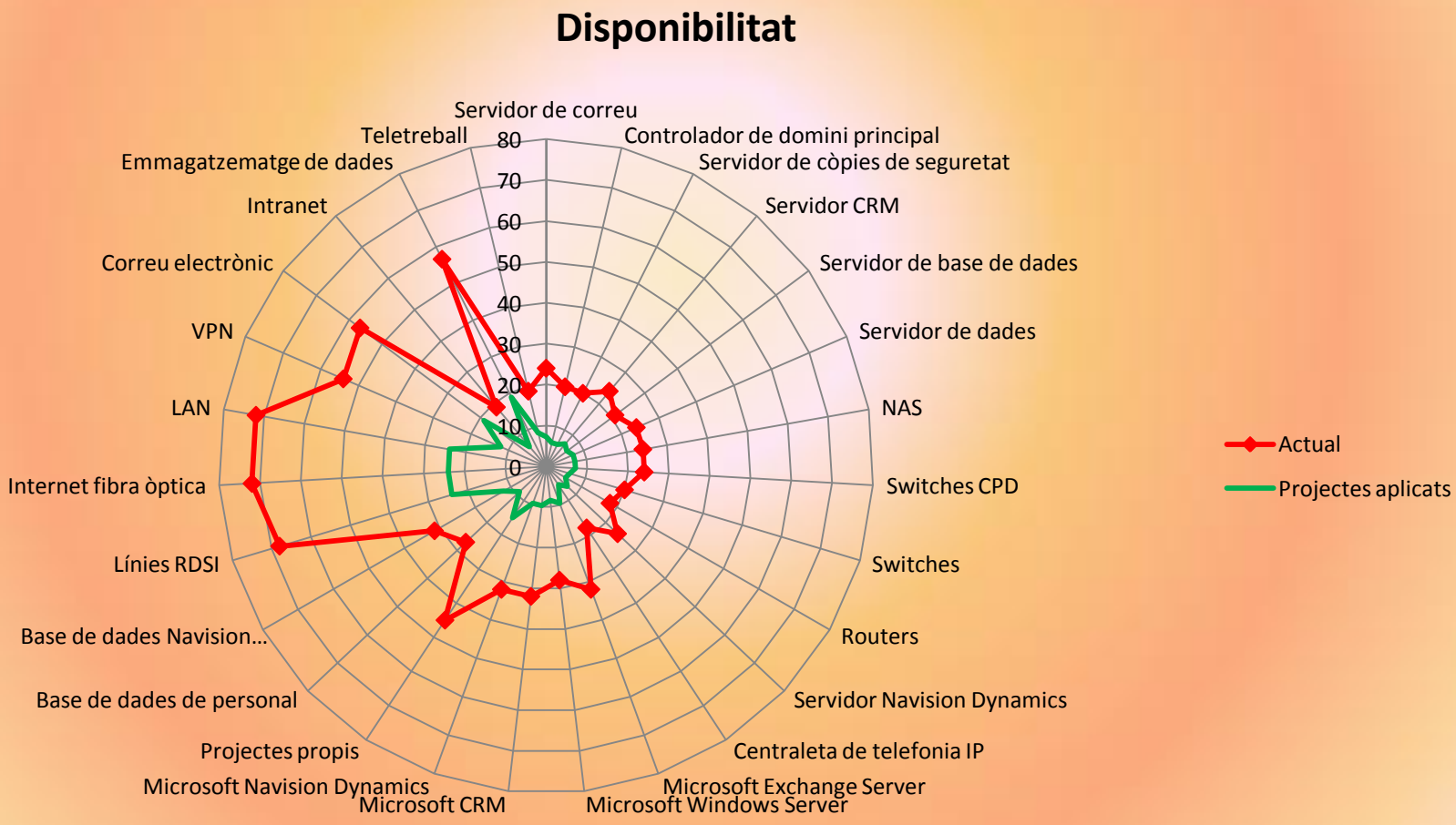
Comparativa nivells de risc abans i després d'aplicar els projectes en les dimensions ACIDA II



Comparativa nivells de risc abans i després d'aplicar els projectes en les dimensions ACIDA III



Comparativa nivells de risc abans i després d'aplicar els projectes en les dimensions ACIDA IV



Auditoria de compliment I

S'estableix un protocol d'auditories internes, per verificar:

- Controls aplicats de la norma ISO/IEC 27002:2013.
- Procediments.
- Objectius.
- Sistema de gestió documental.

Realització d'auditoria de compliment per avaluar l'estat de maduresa d'INGENSA, S.L. front a la norma ISO/IEC 27001 en aplicar els projectes proposats, s'obtenen les evidències de no compliment amb la norma i es redacten les no conformitats.

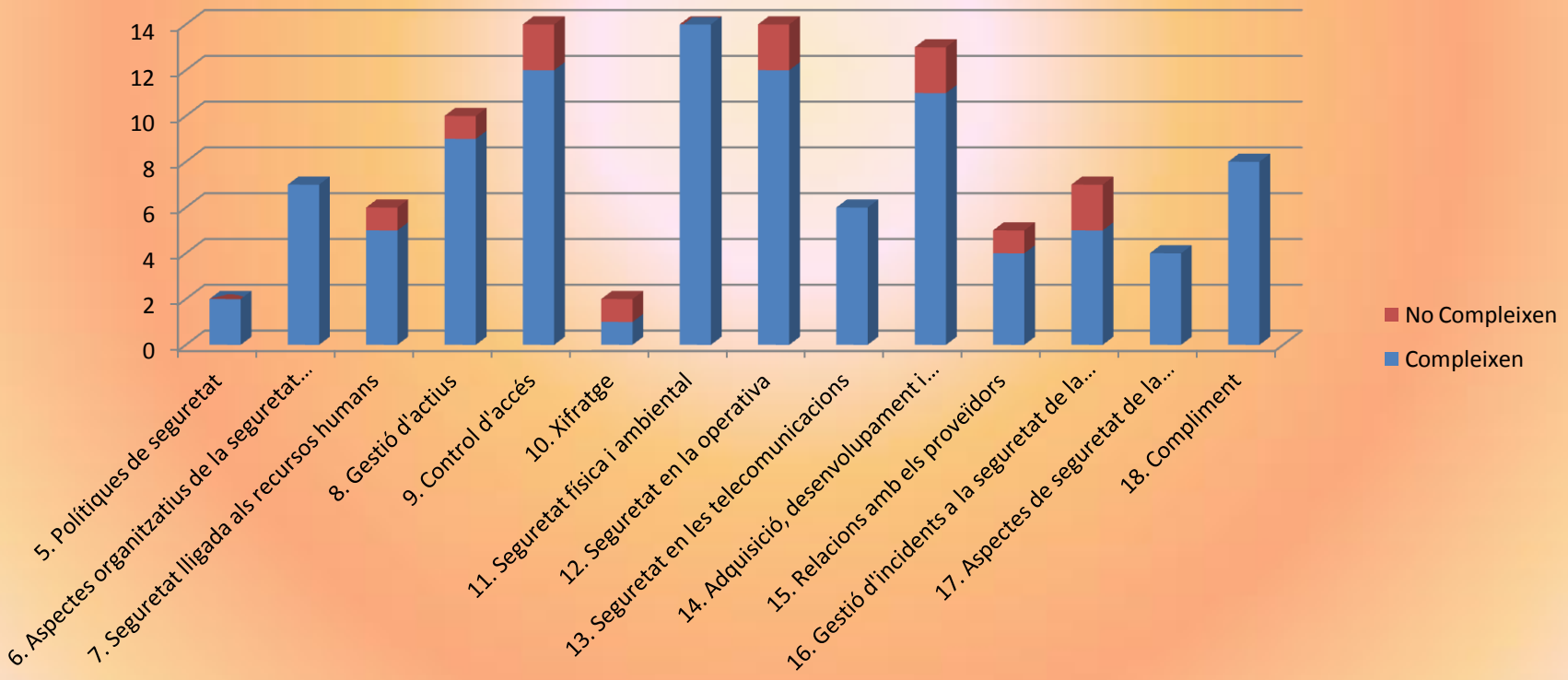
Auditoria de compliment II: No conformitats

Es troben les següents no conformitats en l'auditoria de compliment d'INGENSA, S.L.:

- NC-01: Seguretat lligada als recursos humans.
- NC-02: Gestió d'actius.
- NC-03: Control d'accés.
- NC-04: Xifratge.
- NC-05: Seguretat en l'operativa.
- NC-06: Adquisició, desenvolupament i manteniment dels sistemes d'informació.
- NC-07: Relacions amb subministradors.
- NC-08: Gestió d'incidents a la seguretat de la informació.

Compliment de controls ISO/IEC 27002:2013 per dominis

En aplicar els projectes proposats millora la maduresa dels dominis de la ISO/IEC 27002:2013 i s'incrementen el nombre de controls que compleixen la norma.



Conclusions

- Amb l'SGSI obtenim una reducció de riscos evitant pèrdua d'actius i d'activitat econòmica.
- L'SGSI permet l'obtenció de certificació de seguretat.
- Falta informe de compliment de la legislació vigent aplicable.
- S'haurà de realitzar un seguiment de les no conformitats.
- Evolució del SGSI per futures modificacions o millores.

Gràcies per la seva atenció.