Índex
Descripció i situació inicial
Sistema de Gestió Documental
Anàlisis de Riscos
Propostes de projectes
Auditoria de compliment
Conclusions

Sistemes de Gestió de la Seguretat de la Informació

Iván Arocas Martínez

6 de Juny de 2016

1 Descripció i situació inicial
- Descripció de l'organització
- Pla director de seguretat
- Anàlisi de compliment inicial

2 Sistema de Gestió Documental

3 Anàlisis de Riscos
- Inventari i valoració d'actius
- Anàlisi d'amenaces
- Impacte i risc

4 Propostes de projectes

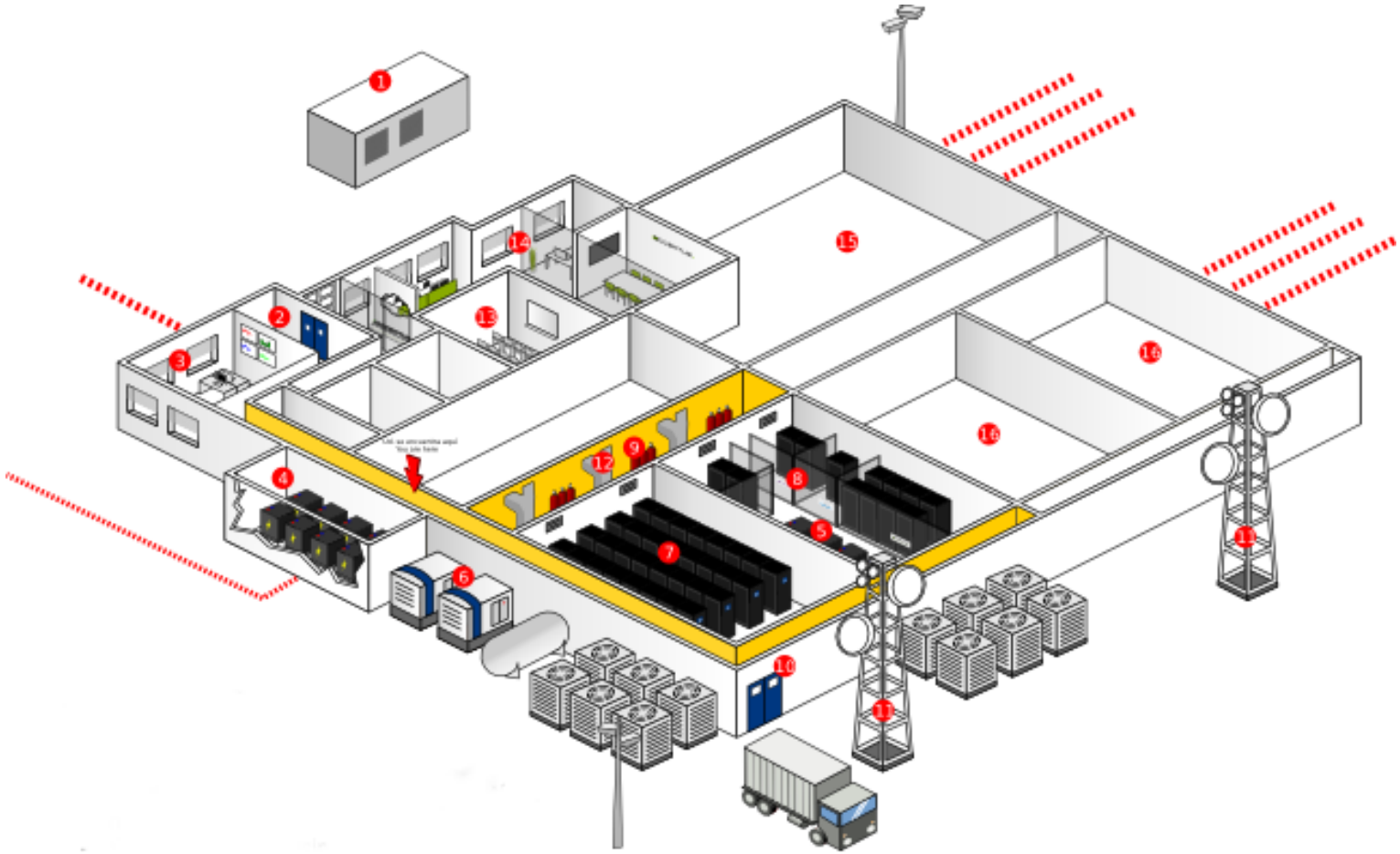
5 Auditoria de compliment

6 Conclusions

L'organització

- Serveis de tipus IaaS
- Gestió de infraestructures virtualitzades
- Serveis de assessorament per iniciar nous projectes
- Capacitat de escalat dinàmic
- Creació i manteniment de sistemes distribuïts

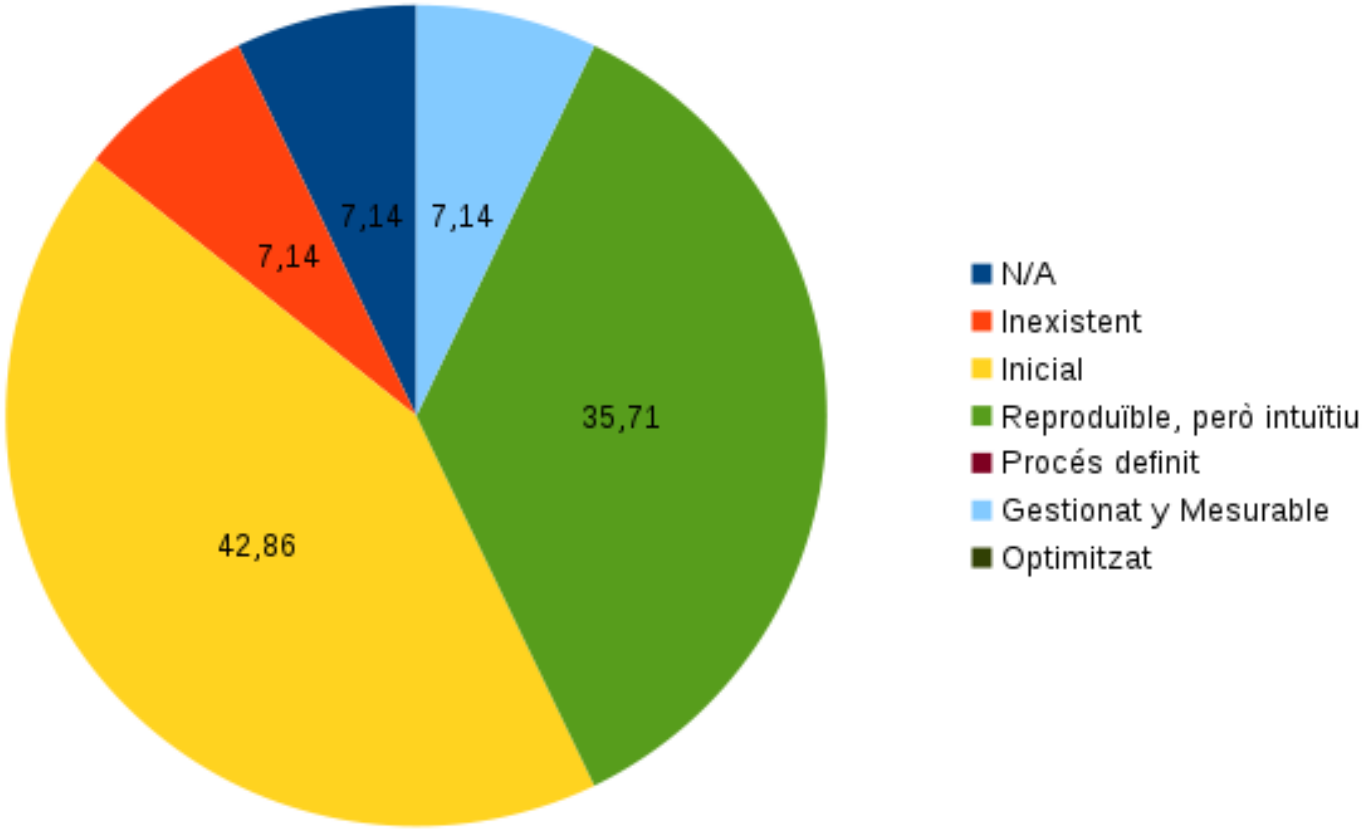
Infraestructura



Objectius

- Assegurar la confidencialitat, integritat i disponibilitat de les dades
- Complir els requisits legals aplicables a l'organització
- Tenir un pla de continuïtat de negoci
- Protegir els elements essencials de l'organització
- Crear un pla de formació en matèria de seguretat
- Crear plans de millora de la seguretat de la informació

Nivell de compliment inicial controls ISO/IEC 27002:2013



Documents

- Política de Seguretat
- Procediment d'Auditories Internes
- Procediment de Revisió per Direcció
- Gestió de Rols i Responsabilitats
- Metodologia de Anàlisis de Riscos
- Declaració de Aplicabilitat

Actius amb valor alt

- Routers BGP
- Switches
- Servidors
- Router Mikrotik
- Serveis web
- DNS
- Connexio Internet
- CPD
- Personal
- Direcció
- Sistemes Operatius
- Servidors web
- Servidors Base de dades
- Servidors de fitxers
- Hipervisors
- Armaris Rack

Actius amb valor mig/baix

- Hardware de recanvi
- Aplicacions internes
- Equips d'oficina
- Telèfons VoIP
- Documentació

Principals amenaces

Físiques

- Desastres naturals
- Tall del subministre elèctric
- Averíes
- Foc
- Temperatura

Principals amenaces

Lògiques

- Errors del administrador
- Denegació de servei
- Modificació de la informació
- Access no autoritzat

Calcul del risc

- A Valor del actiu
- B Impacte del actiu
- C Probabilitat d'amenaça
- Risc = (A+B+C)/3

Hardware

- Router redundat (VRRP)
- Router redundat (backup)
- Creació cloud de backup
- Noves controladores switchs

Gestió

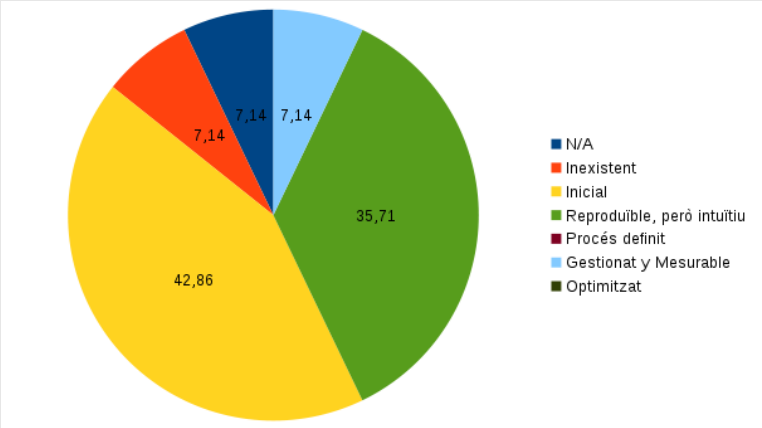
- Documentació de nous projectes
- Revisió d'instal·lacions, compliment de requisits
- Pla d'actuació front a incidents de seguretat
- Actualització del Pla de continuïtat de negoci

Altres projectes

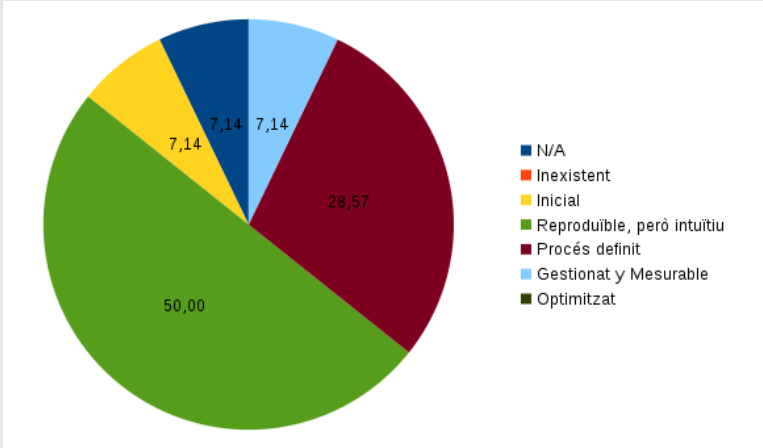
- Xifrat discos oficines
- Open Xchange
- Pen-tests interns, prevenció d'incidents

Nivell de compliment controls ISO/IEC 27002:2013

Compliment Inicial



Compliment Actual



No conformitats

- Registre centralitzat d'activitat
- Política d'actualitzacions
- Sobreasignament de recursos
- Política sobre teletreball
- Formació periòdica

Observacions

- Control de capacitat dels backups
- Evidencies de proves de recuperació

Conclusions

Punts forts

- Implicació de la direcció
- Coneixements i aptituds del personal
- Experiència

Millores

- Documentació
- Formalització de procediments
- Definició de responsabilitats