Pla director de seguretat de l'Organització

Eugeni Platas Sirvent

Maig de 2022

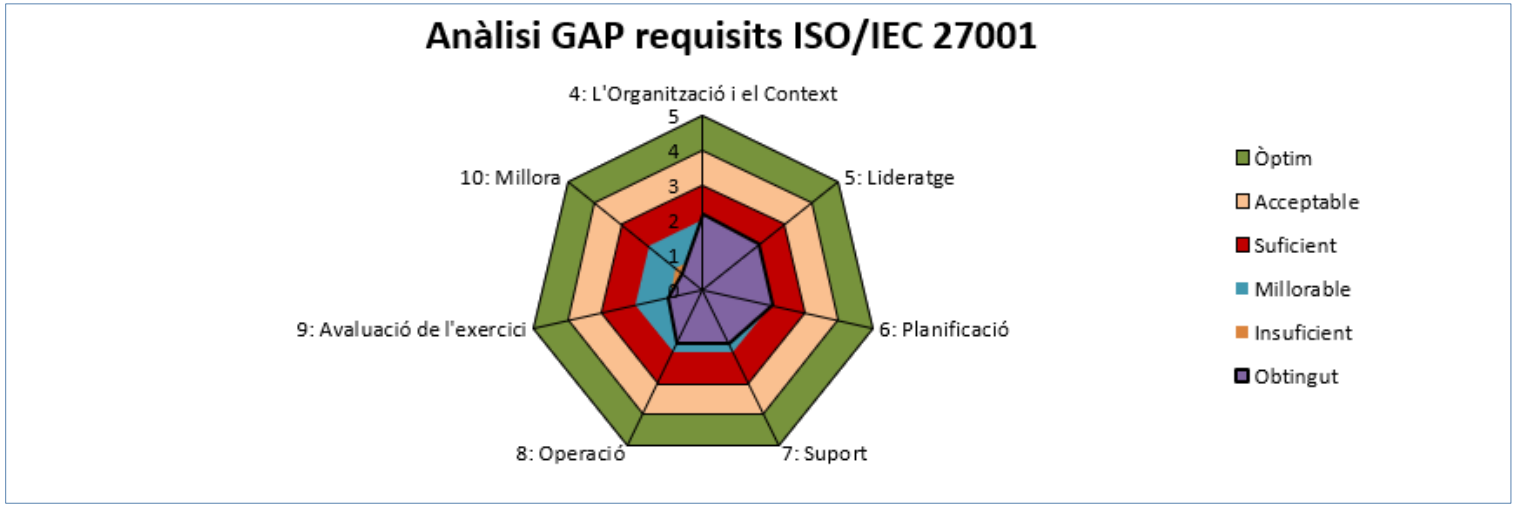
Índex

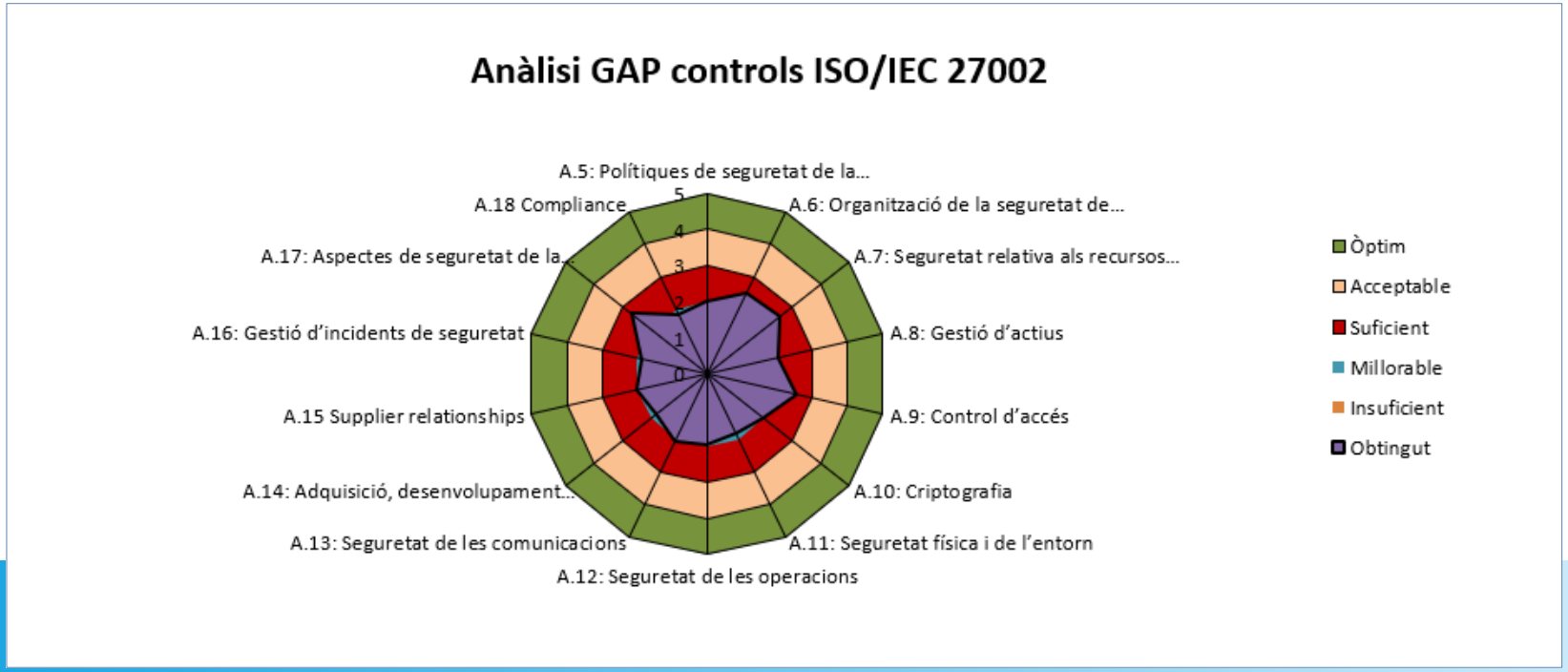
- Contextualització i anàlisi de compliment inicial
- Esquema documental ISO/IEC 27001
- Anàlisi de riscos
- Proposta de projectes
- Auditoria de compliment

Contextualització (1/2)

- Organització
  - Internacional, recerca en varis àmbits
  - Gran volum de dades
  - Confidencialitat, integritat, disponibilitat
  - Processament i arxivament: local i deslocalitzat
  - Personal intern i extern
- Abast:
  - Processos d’adquisició
  - Processos de tractament i emmagatzematge
  - Processos de publicació

Contextualització (2/2)





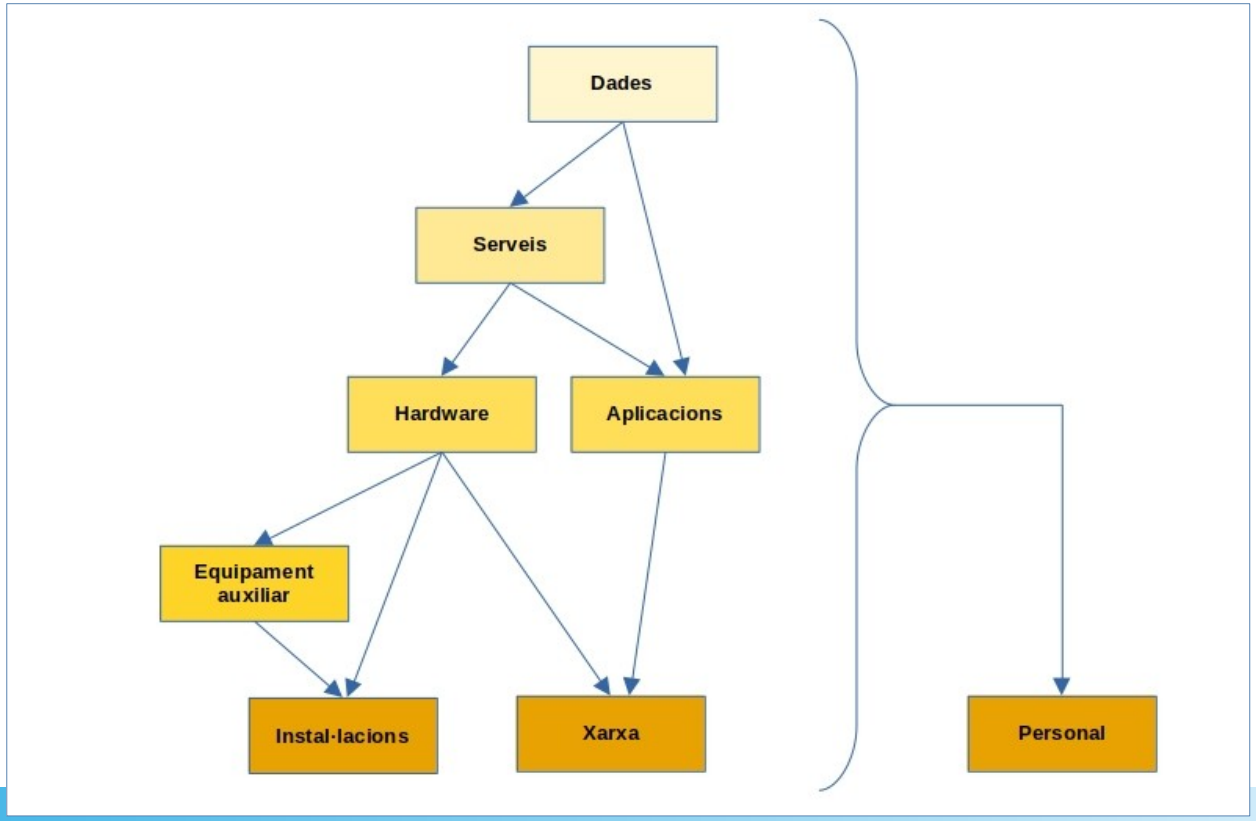
Esquema documental ISO/IEC 27001

- Política de Seguretat
- Procediment d'Auditories Internes (nou)
- Gestió d'Indicadors (nou)
- Procediment de Revisió per Direcció (nou)
- Gestió de Rols i Responsabilitats
- Metodologia d'Anàlisi de Riscos (nou)
- Declaració d'Aplicabilitat (nou)

Anàlisi de riscos (1/2)

magerit
METHODOLOGY FOR INFORMATION SYSTEMS RISK ANALYSIS AND MANAGEMENT

1) Inventari d'actius amb propietari i valoracions. Arbre de dependències



Anàlisi de riscos (2/2)

2) Anàlisi d'amenaces

- Impacte i vulnerabilitat

3) Impacte potencial

- Degradació per amenaça, al conjunt de l'Organització

4) Risc

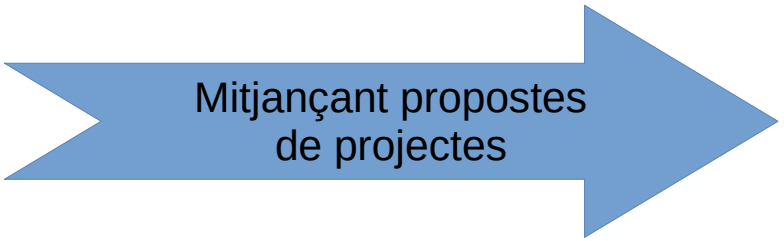
- Impacte * vulnerabilitat
- Risc residual respecte controls existents inicialment

Amenaça	Impacte potencial	Vulnerabilitat o freqüència	Risc	Propietari del risc
Incendi, per causes naturals o industrials	407	1/10	40.7	*IT Manager*
Inundacions, per causes naturals o industrials	407	1/10	40.7	*IT Manager*
Averia de l'equipament o programa (físic o lògic)	489.3	1	489.3	*IT Manager*
Tall del subministre elèctric	274	1	274	*IT Manager*
Averia en el sistema de climatització	223.2	1	223.2	*IT Manager*
Incident en la xarxa de comunicacions	291.6	10	2916	*IT Manager*
Error d'ús dels sistemes	363.9	10	3639	CISO
Error d'administració dels sistemes	968.1	10	9681	CISO
Incidents deguts a software malintencionat	696	1	696	CISO
Alteració de la informació	203.6	1	203.6	CISO
Destrucció de la informació	245	1	245	CISO
Fuga d'informació	316.4	1	316.4	CISO
Error de manteniment / actualització de software	294	1	294	*IT Manager*
Error de manteniment / actualització de hardware	268	1/10	26.8	*IT Manager*
Accés no autoritzat	355.8	1	355.8	CISO
Intercepció d'informació	261.2	1	261.2	CISO

Proposta de projectes (1/3)

Objectius

- Mitigar el risc identificat
- Millorar el compliment inicial (norma i controls)

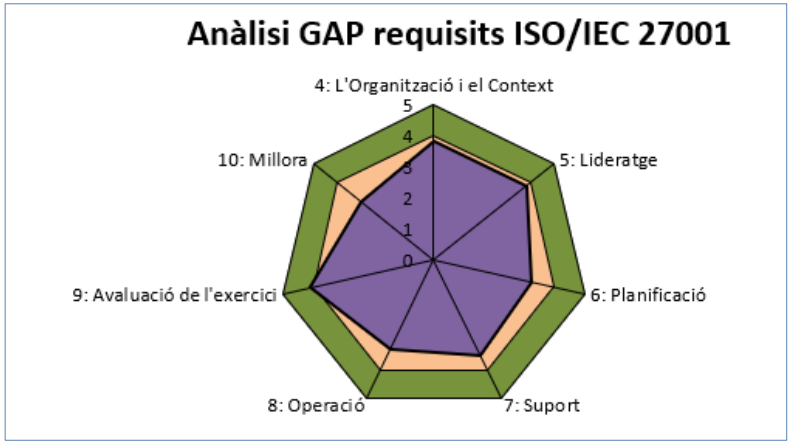


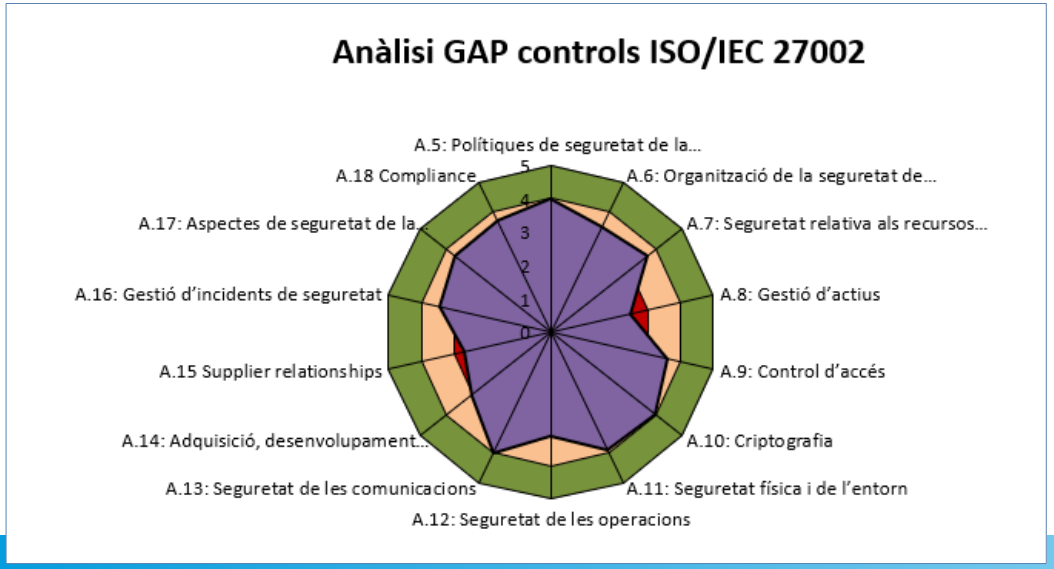
- Descripció i fases
- Planificació temporal
- Valoració econòmica
- Millores: risc, norma, controls

Proposta de projectes (2/3)

- Projecte 1: Campanyes de difusió i conscienciació
  - Tots els empleats, subcontractistes i altres tercers
- Projecte 2: Implementació i gestió d'indicadors
  - Imprescindible per assolir nivell 4 de maduresa
- Projecte 3: Establiment de revisions periòdiques
  - Per la direcció, auditories internes, auditories externes
- Projecte 4: Adopció de *Security by Design*
  - La seguretat com a part dels requisits
- Millores intrínseques del pla director de seguretat

Proposta de projectes (3/3)





Amenaça	Impacte potencial	Vulnerabilitat o freqüència	Risc	Projectes que el redueixen
Incendi, per causes naturals o industrials	325.6*	1/10	32.56*	2, 3
Inundacions, per causes naturals o industrials	325.6*	1/10	32.56*	2, 3
Averia de l'equipament o programa (físic o lògic)	391.4*	1/10*	39.14*	2, 3, 4
Tall del subministre elèctric	219.2*	1	219.2*	2, 3
Averia en el sistema de climatització	178.6*	1	178.6*	2, 3
Incident en la xarxa de comunicacions	174.96*	10	1749.6*	2, 3, 4
Error d'ús dels sistemes	291.1*	1*	291.1*	1, 2, 3, 4
Error d'administració dels sistemes	774.5*	1*	774.5*	1, 2, 3, 4
Incidents deguts a software malintencionat	417.6*	1/10*	41.76*	1, 2, 3, 4
Alteració de la informació	122.16*	1/10*	12.22*	1, 2, 3, 4
Destrucció de la informació	147*	1/10*	14.7*	1, 2, 3, 4
Fuga d'informació	189.84*	1/10*	18.98*	1, 2, 3, 4
Error de manteniment / actualització de software	235.2*	1	235.2*	2, 3
Error de manteniment / actualització de hardware	214.4*	1/10	21.44*	2, 3
Accés no autoritzat	284.6*	1	284.6*	2, 3
Intercepció d'informació	156.72*	1/10*	15.67*	1, 2, 3, 4

*: valor reduït gràcies als projectes

Auditoria de compliment (1/2)

- Auditoria interna, després de projectes
- Informe d'auditoria:
  - Compliment controls ISO/IEC 27002 aplicables
  - Compliment requisits ISO/IEC 27001
  - Compliment objectius de seguretat de l'Organització
  - No-conformitats
  - Recomanacions de millora

Auditoria de compliment (2/2)

- ✓ Compliment dels objectius de seguretat
- ✓ Cap no-conformitat major detectada

- ➡ No-conformitats menors
  - Requisits/controls amb nivells < 3
- ➡ Recomanacions de millora:
  - Continuar amb les revisions i avaluacions
  - Estandardització de procediments
  - Adopció de bones pràctiques ITIL

Moltes gràcies per l’atenció