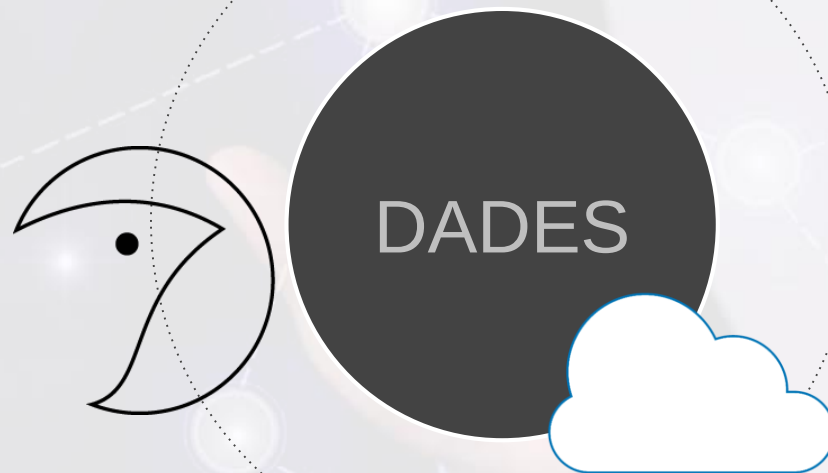


Cas pràctic d'adaptació d'una empresa a la normativa GDPR

ENGISOFT

www.engisoftcloud.com

ENGISOFT



ENGISOFT
CLOUD
SERVICES



Standard
Consulting
Partner



IoT CATALAN
ALLIANCE

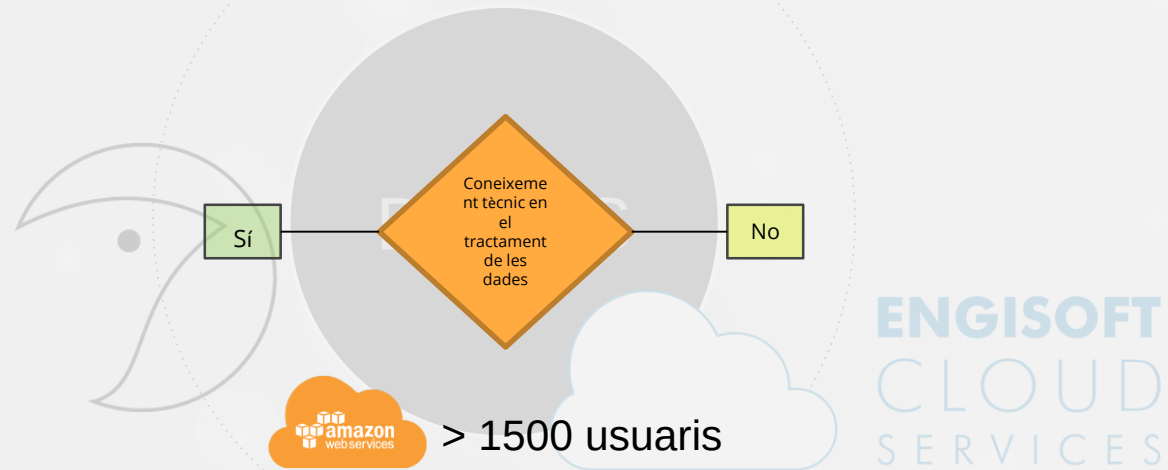
Microsoft
Partner

ENGISOFT



> 1500 usuaris

ENGISOFT



EQUIP

Reunions setmanals des de fa 1 any



Standard
Consulting
Partner



IoT

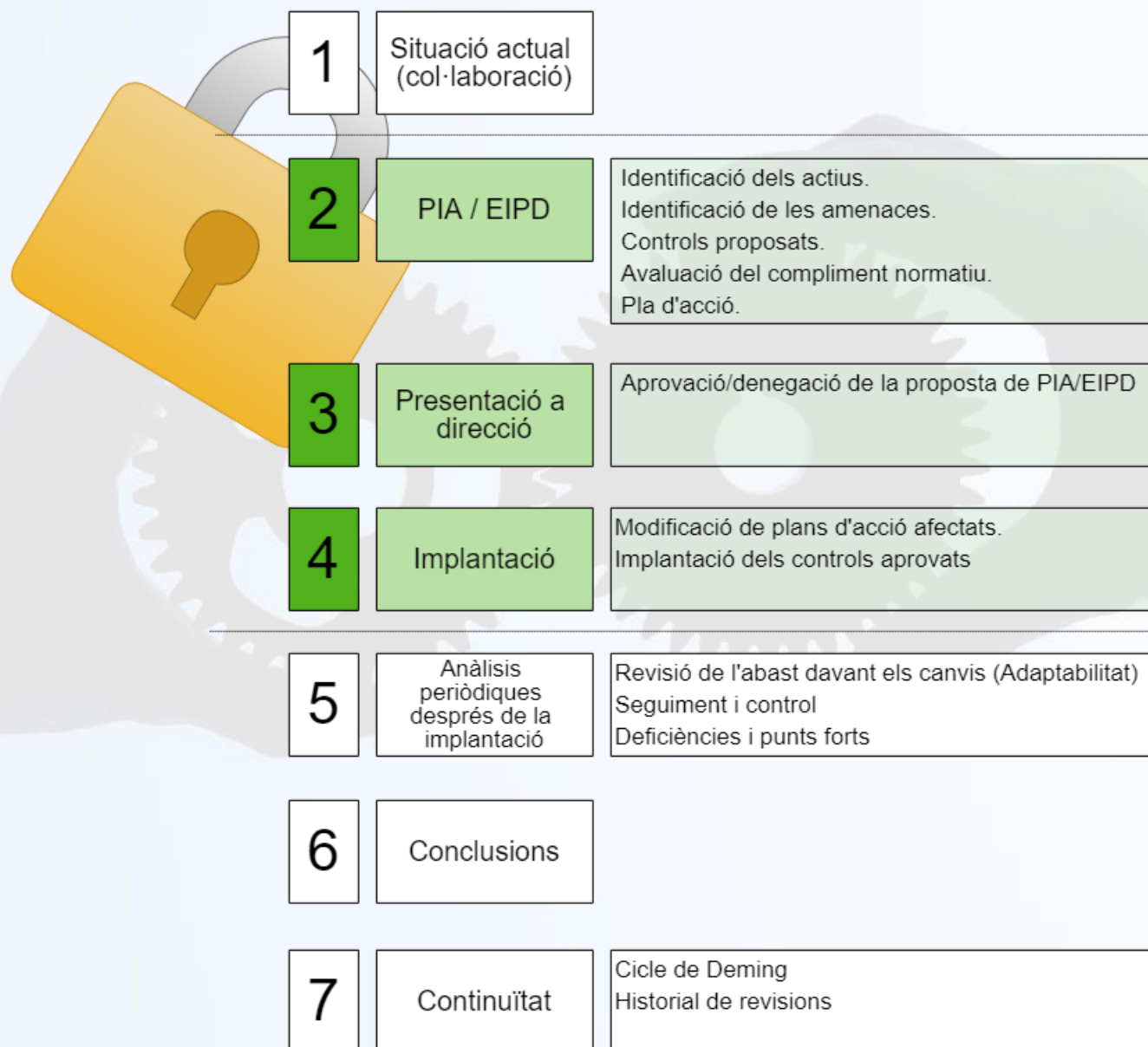
CATALAN
ALLIANCE

Microsoft
Partner

Qualsevol empresa necessita saber quines dades té i si les està tractant correctament

- EIPD - Avaluació d'Impacte en la Protecció de Dades.
(PIA) – Privacy Impact Assessments
 - Anàlisi de risc.
 - Registre d'activitats del tractament.

PDS – Pla Director de Seguretat

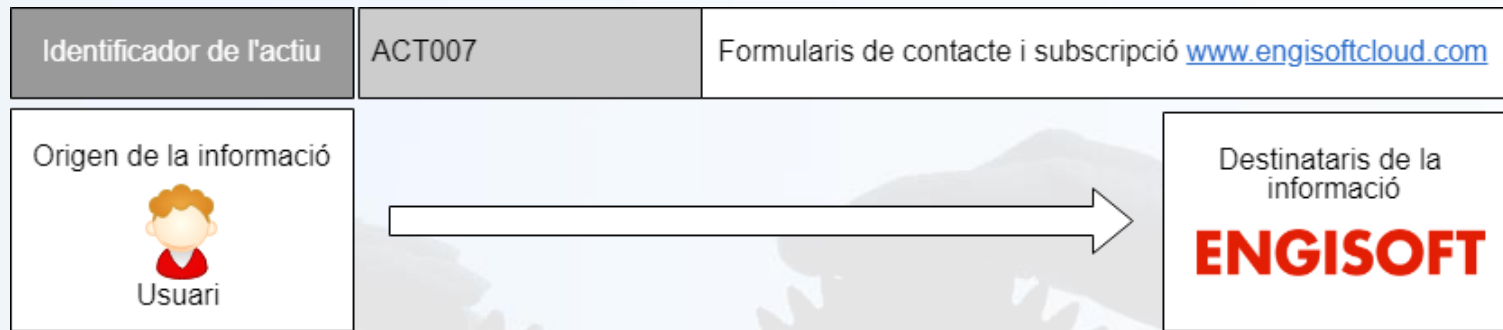


PIA – Identificació d'actius - Exemple

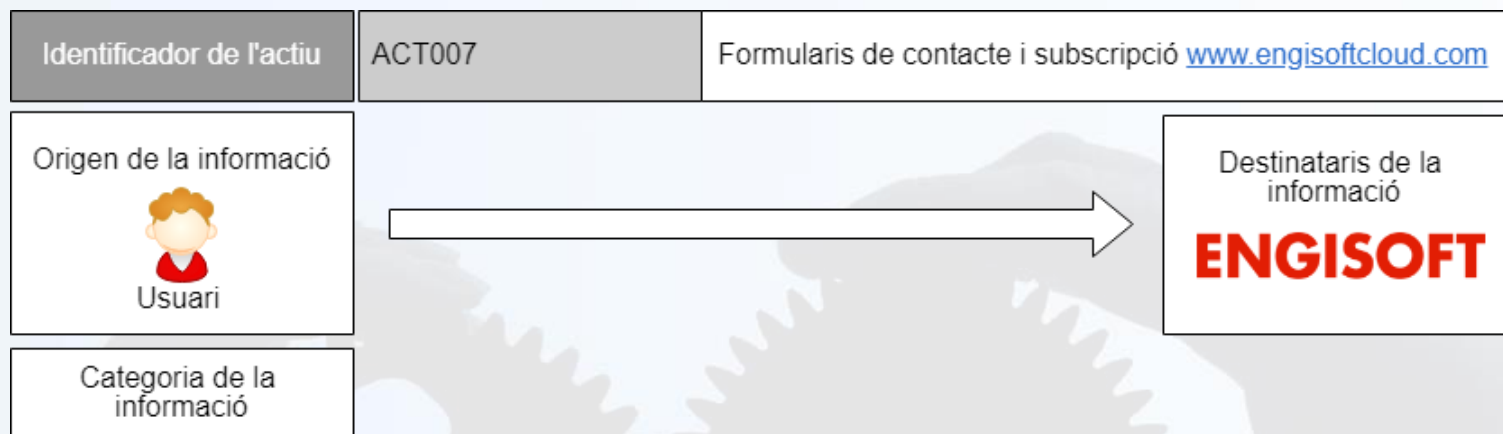
Identificador de l'actiu	ACT007	Formularis de contacte i subscripció www.engisoftcloud.com
--------------------------	--------	---



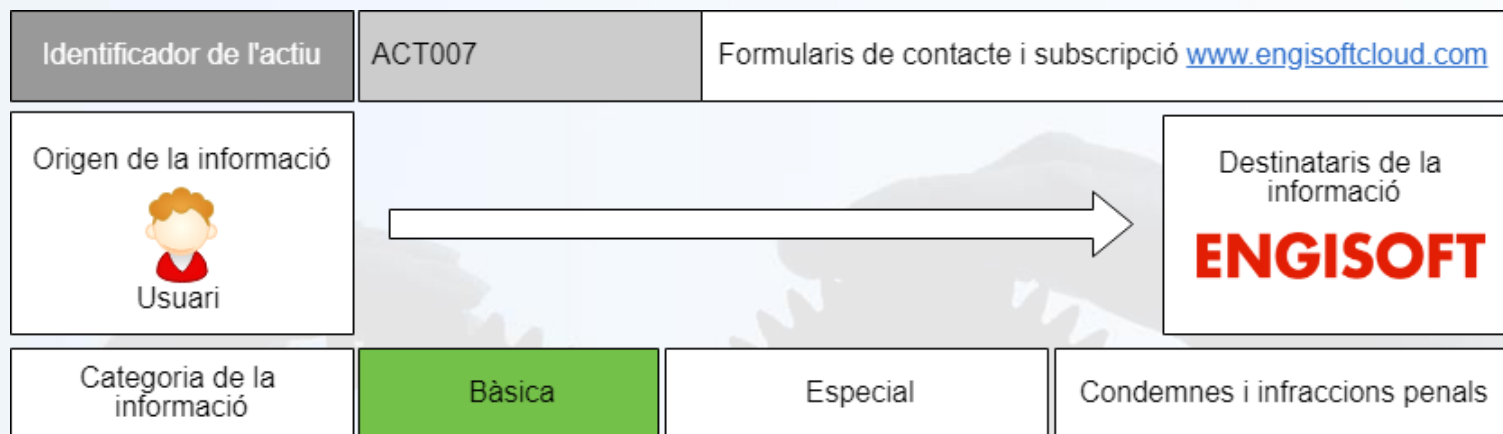
PIA – Identificació d'actius - Exemple



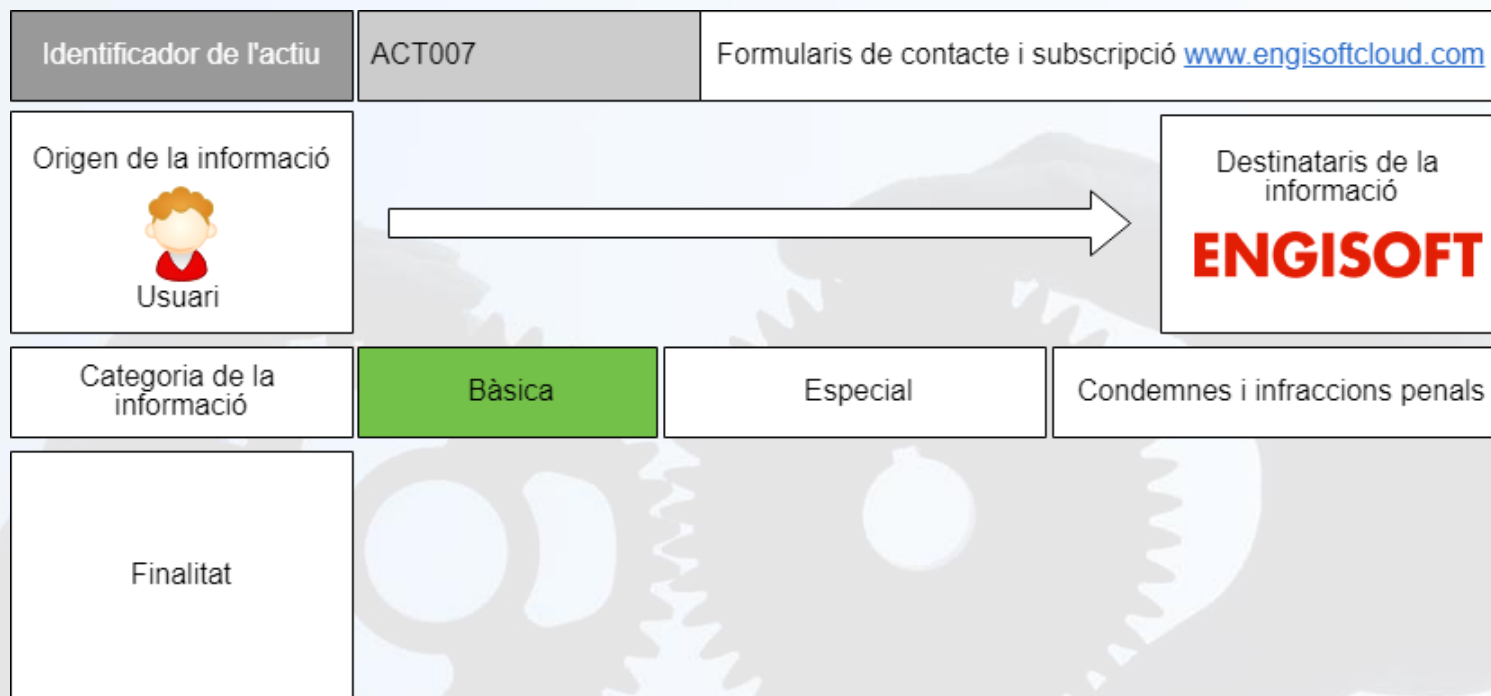
PIA – Identificació d'actius - Exemple



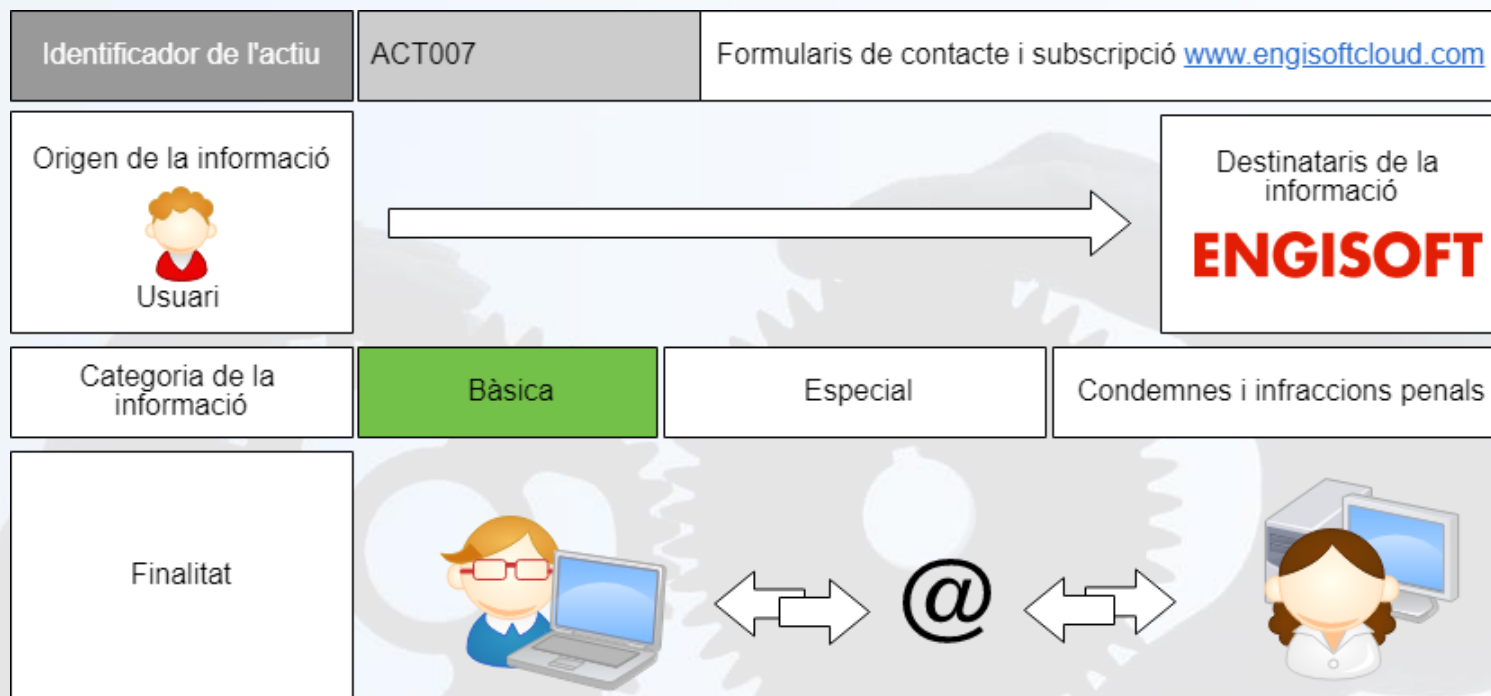
PIA – Identificació d'actius - Exemple



PIA – Identificació d'actius - Exemple



PIA – Identificació d'actius - Exemple



PIA – Identificació d'actius - Exemple



PIA – Identificació d'actius - Exemple

Identificador de l'actiu	ACT007	Formularis de contacte i subscripció www.engisoftcloud.com	
Origen de la informació  Usuari			Destinataris de la informació ENGISOFT
Categoria de la informació	Bàsica	Especial	Condemnes i infraccions penals
Finalitat	 ↔ @ ↔ 		
Causa legitimadora			

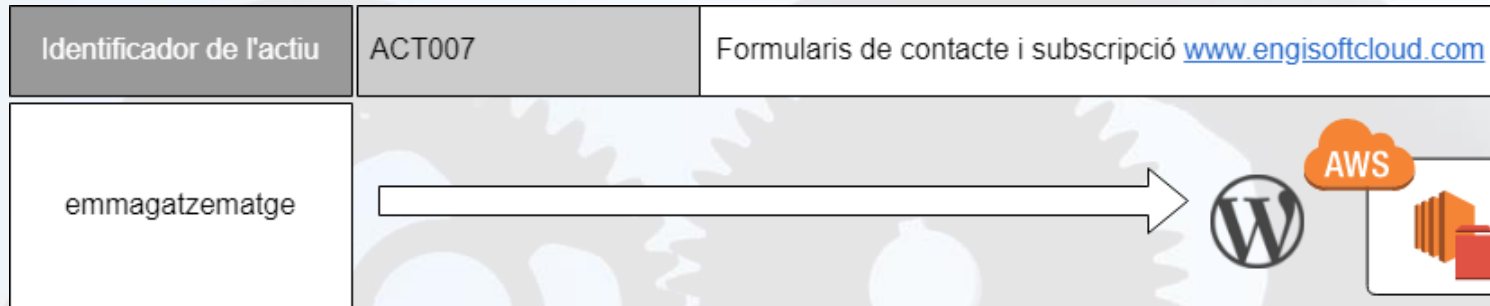
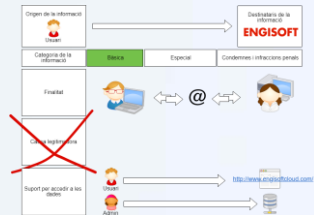
PIA – Identificació d'actius - Exemple

Identificador de l'actiu	ACT007	Formularis de contacte i subscripció www.engisoftcloud.com	
Origen de la informació  Usuari			Destinataris de la informació ENGISOFT
Categoria de la informació	Bàsica	Especial	Condemnes i infraccions penals
Finalitat	 ↔ @ ↔ 		
Causa legitimadora			
Suport per accedir a les dades			

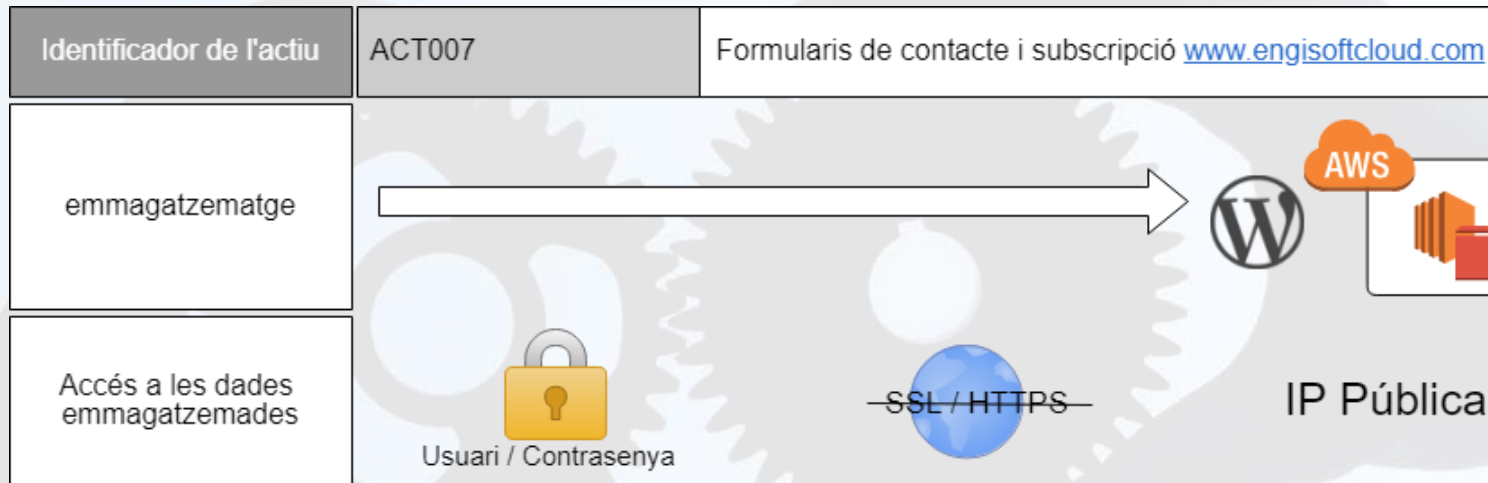
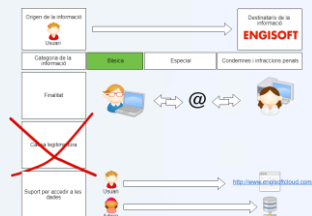
PIA – Identificació d'actius - Exemple



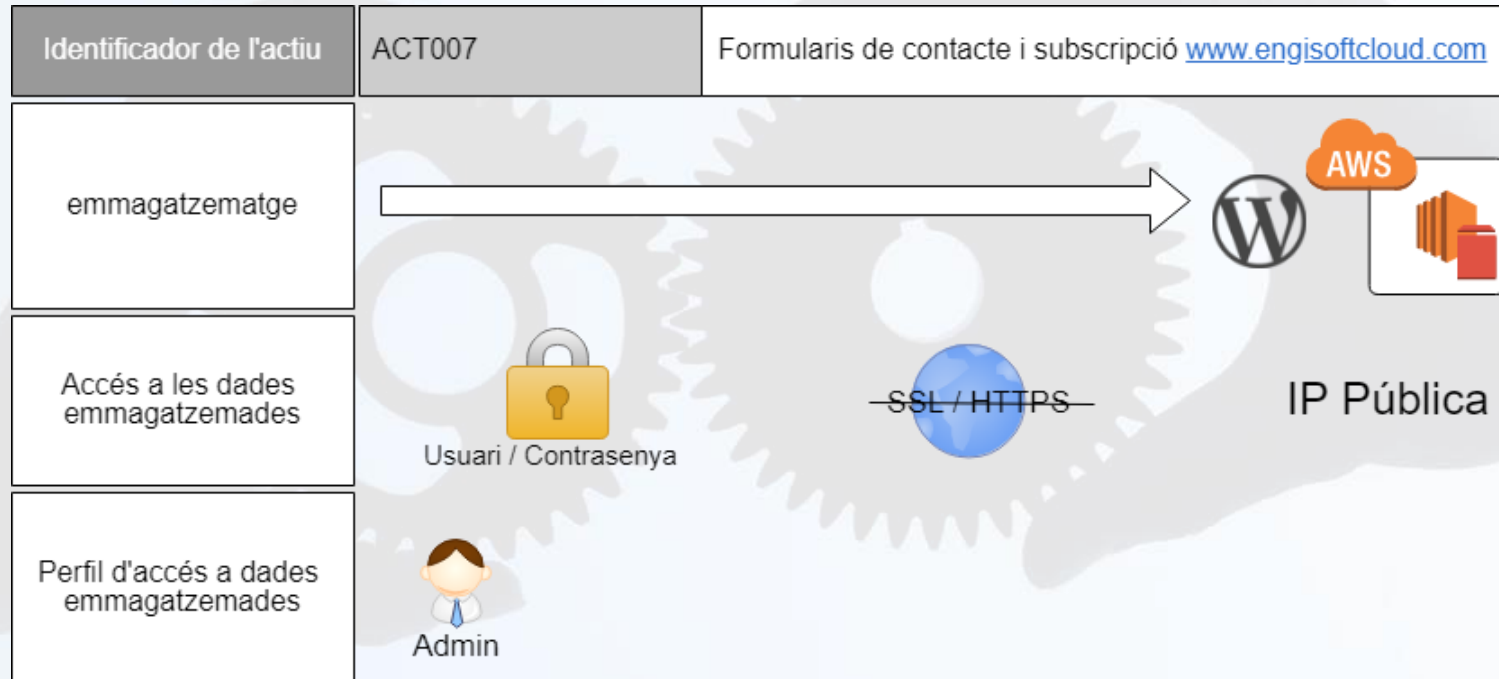
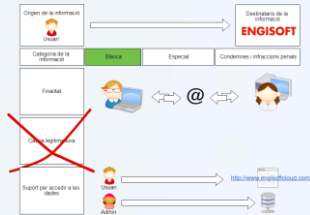
PIA – Identificació d'actius - Exemple



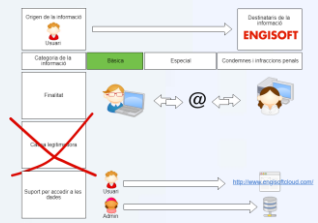
PIA – Identificació d'actius - Exemple



PIA – Identificació d'actius - Exemple

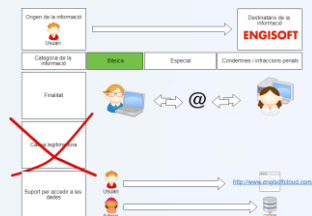


PIA – Identificació d'actius - Exemple



Identificador de l'actiu	ACT007	Formularis de contacte i subscripció www.engisoftcloud.com
emmagatzematge		
Accés a les dades emmagatzemades	 Usuari / Contrasenya	 IP Pública
Perfil d'accés a dades emmagatzemades	 Admin	
ENGISOFT	Responsable	Encarregat

PIA – Identificació d'actius - Exemple

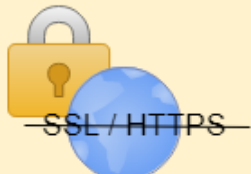


Identificador de l'actiu	ACT007	Formularis de contacte i subscripció www.engisoftcloud.com
emmagatzematge		
Accés a les dades emmagatzemades	 Usuari / Contrasenya	IP Pública
Perfil d'accés a dades emmagatzemades	 Admin	
ENGISOFT	Responsable	Encarregat
Altres		

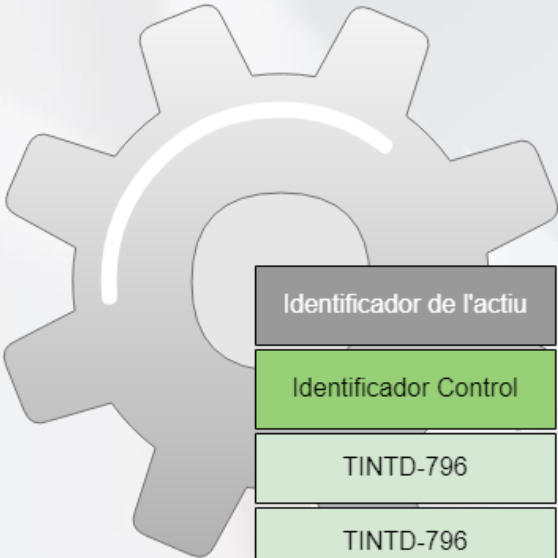
PIA – Gestió de riscos

Categories	Escala de maduresa	Nivells d'impacte	Probabilitat de materialització	Accions
Generals	Inexistent	Molt alt	Molt alta (81% - 100%)	Transferir
Legitimació dels tractaments i cessió de dades personals	Inicial	Alt	Alta (61% - 80%)	Eliminar
Transferències internacionals	Repetible	Mig	Mitjana (41% - 60%)	Assumir
Notificació dels tractaments	Definit	Baix	Baixa (21% - 40%)	Mitigar
Transparència dels tractaments	Administrat	Molt baix	Molt baixa (0% - 20%)	
Qualitat de les dades.	Optimitzat			
Dades especialment protegides				
Deure de secret.				
Tractament per encàrrec.				
Drets ARCO				
Seguretat.				

PIA – Gestió de riscos - Exemple

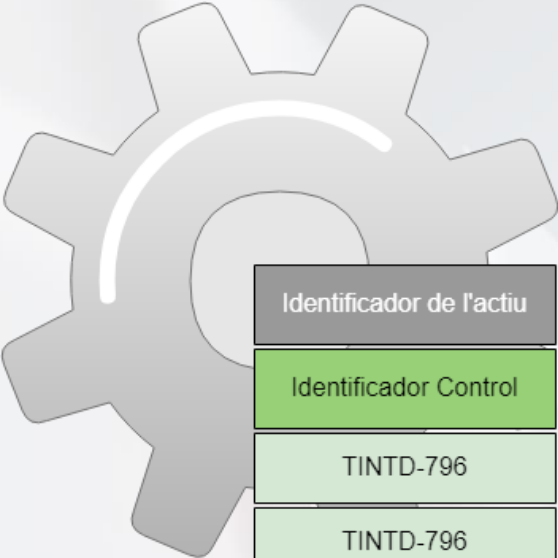
Identificador de l'actiu	ACT007		Formularis de contacte i subscripció www.engisoftcloud.com									
Descripció de riscos			 INFO Usuaris									
Grau de maduresa	Inicial											
Nivell impacte si es materialitza	Baix											
Probabilitat que es materialitzi	Baix											
Mesures proposades	 - Mitigar -		 - Mitigar -		 Versions - Mitigar -		 - Eliminar -		 - Eliminar -		 - Transferir - 	
Probabilitat que es materialitzi després de l'aplicació	Molt baix											

PIA – Controls proposats - Exemple



Identificador de l'actiu	ACT014	
Identificador Control	Controls	Prioritat
TINTD-796	2FA/MFA per usuaris administradors.	Mitja
TINTD-796	Creació usuaris nominals i tractament de super-usuari.	Alta
TINTD-797	Definició de protocol per actualitzacions i manteniment WP.	Mitja
TINTD-820	Redacció i incorporació al WEB de política de privacitat i cookies.	Alta
TINTD-788	Revisió regles d'accés remot al repositori de dades.	Alta
TINTD-827	Estudi de possibilitat de anonimització/criptació de dades en instància EC2/AWS.	Baixa
TINTD-819	Estudi viabilitat del foro.	Baixa
TINTD-798	Aplicació de certificats (SSL/HTTPS)	Alta

PIA – Controls proposats - Exemple



Identificador de l'actiu	ACT014		
Identificador Control	Controls	Prioritat	Acceptat
TINTD-796	2FA/MFA per usuaris administradors.	Mitja	
TINTD-796	Creació usuaris nominals i tractament de super-usuari.	Alta	
TINTD-797	Definició de protocol per actualitzacions i manteniment WP.	Mitja	
TINTD-820	Redacció i incorporació al WEB de política de privacitat i cookies.	Alta	
TINTD-788	Revisió regles d'accés remot al repositori de dades.	Alta	
TINTD-827	Estudi de possibilitat de anonimització/criptació de dades en instància EC2/AWS.	Baixa	
TINTD-819	Estudi viabilitat del foro.	Baixa	
TINTD-798	Aplicació de certificats (SSL/HTTPS)	Alta	

Els deures de l'empresa en la protecció de dades

Accés	Seguretat i accés físic
Manipulació	Seguretat i accés virtual
Emmagatzematge	Seguretat en transferència

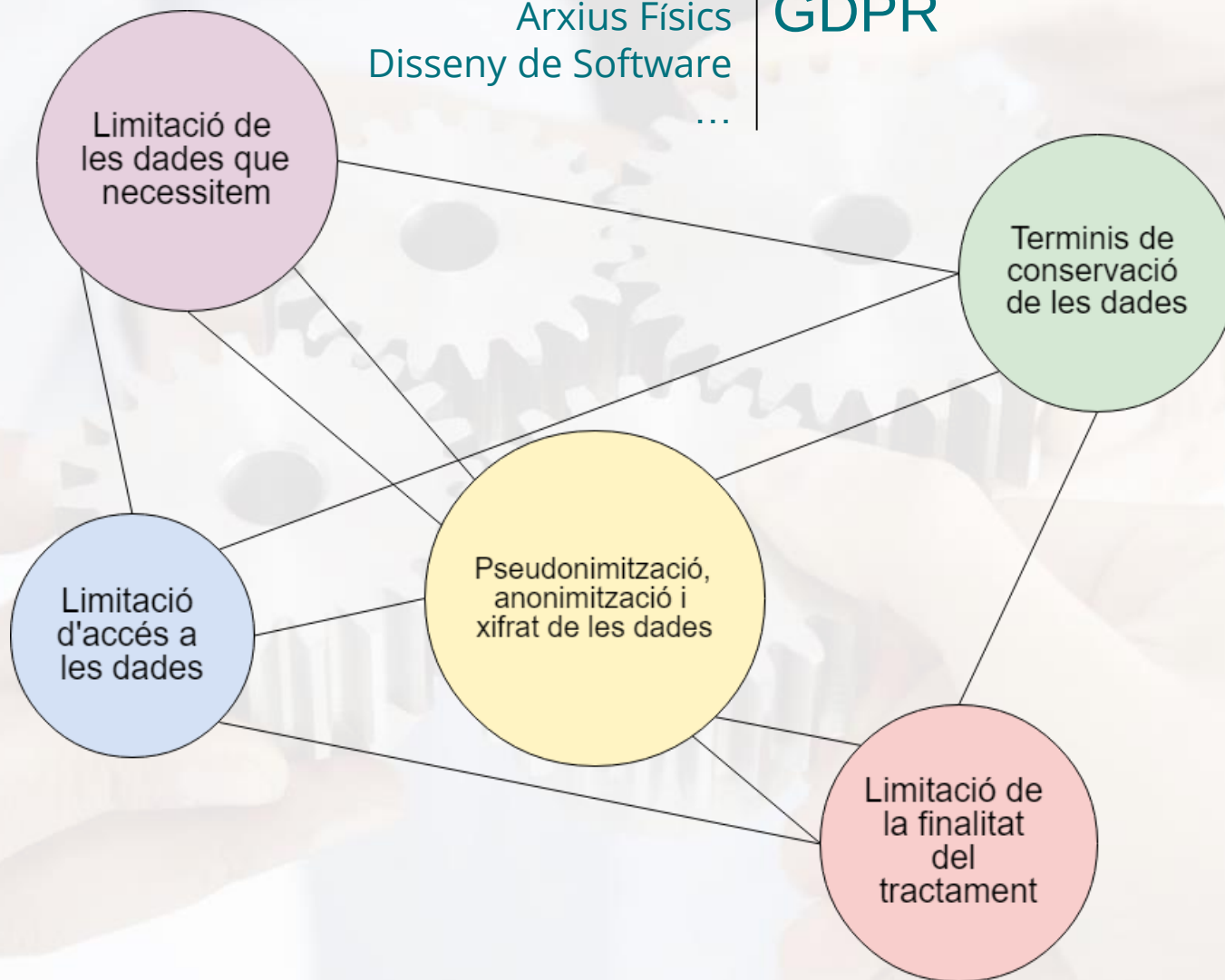
DMZ i seguretat perimetral	Perfils i polítiques <i>blacklist/whitelist</i>	Gestor contrasenyes / SSO
IDS/IPS	VPN	
Antivirus	Actualitzacions	Encriptació / Xifrat
Còpies de seguretat i PRC	Conscienciació i formació	

Privacitat i protecció de dades des del disseny i per defecte

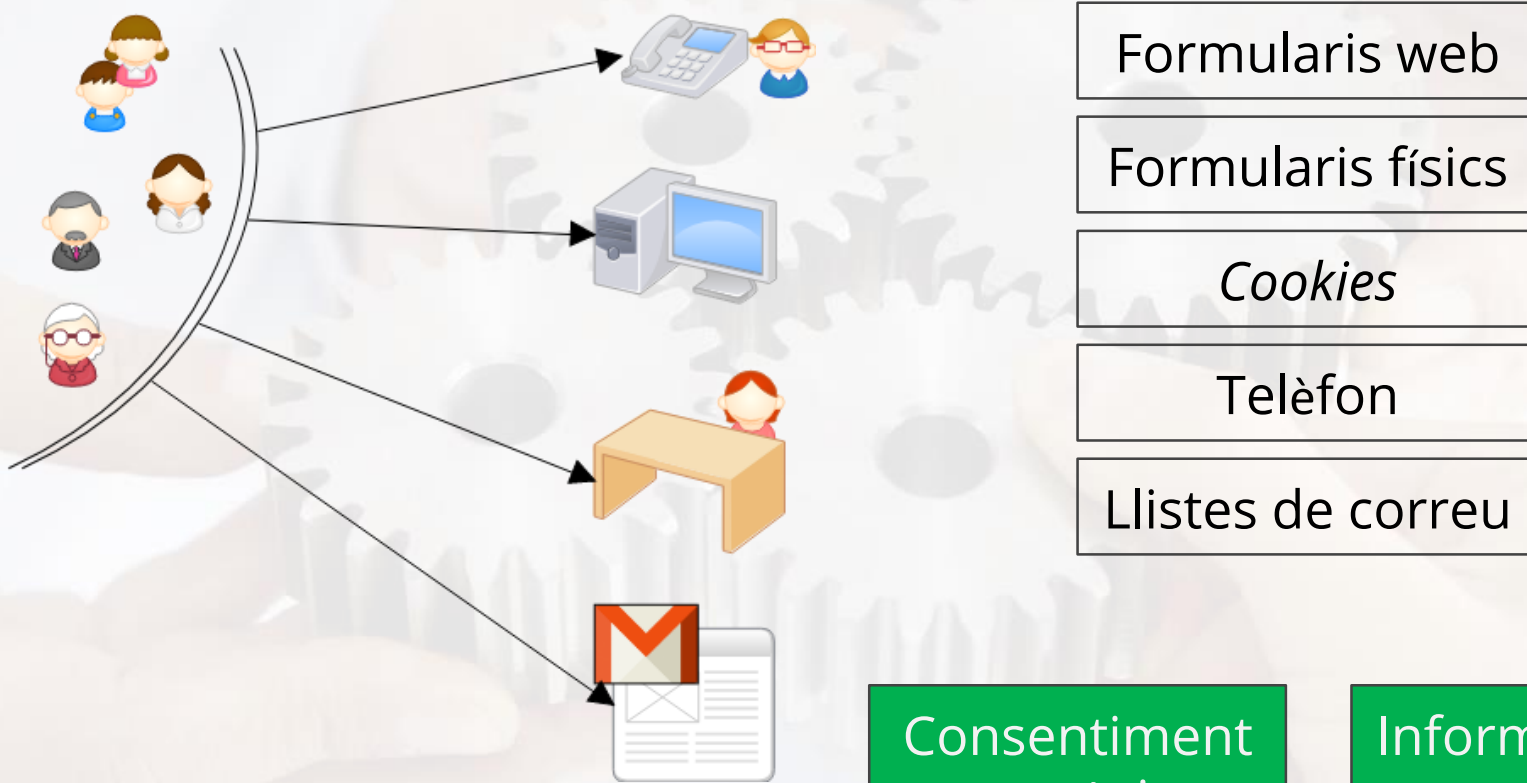
(SPD - Security and Privacy by Design)

Productes propis
Disseny de BBDD
Arxius Físics
Disseny de Software
...

GDPR



Com recollir dades personals de clients o contactes



Dret d'usuari, clients o contactes sobre les seves dades

ARCO

Accés

Rectificació

Cancel·lació

Oposició

GDPR

Limitació

Portabilitat

Supressió (oblit)

<https://www.engisoftcloud.com/>

Els treballadors

Educació i conscienciació mèdica i
sostenible

Pòsters

Tríptics

Sessions

Exemples:

- Atacs controlats
- Enginyeria Social
 - Notícies
 - Etc.

AEPD

BYOD, documents compartits i correu electrònic



Centralització
de
repositoris

Limitació
d'accés

Document
a signar

Perfils

Antivirus

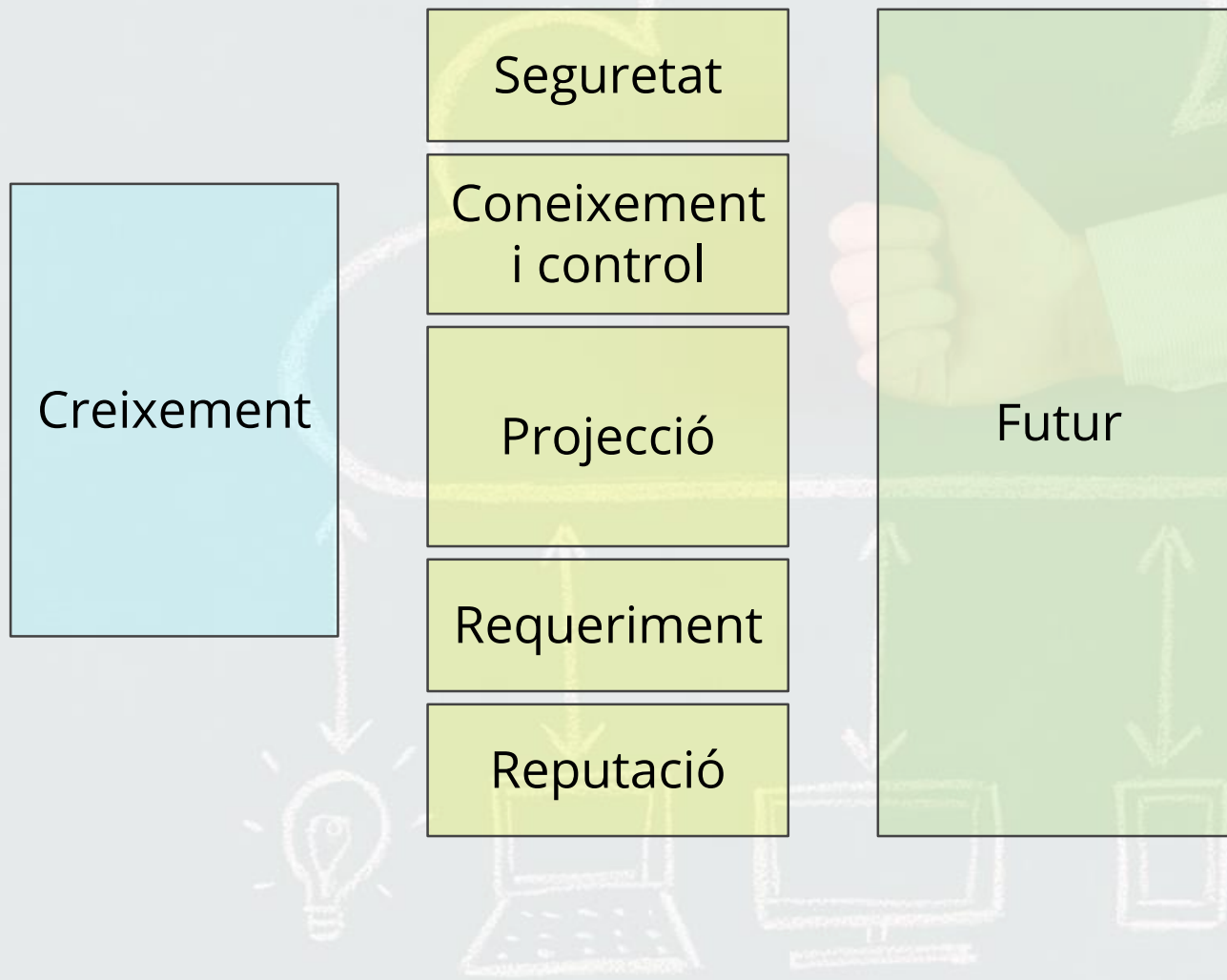


Violacions de seguretat i el deure d'informar

72h

Protocol	Responsable d'informar	Assegurança ciber-risc
	Responsable en prendre decisions	
	Plantilles de comunicació afectats	
	Canals de comunicació i seguiment	Conseqüències
	Comunicació autoritat competent	
	Documentació	

Conclusió



ENGISOFT

Cas pràctic d'adaptació d'una empresa a la normativa GDPR

Xavi Fernández

CISO – R+D

x.fernandez@engisoft.com

Gràcies!