AUDITORIA INTERNA DE SEGURETAT INFORMÀTICA APLICABLE A QUALSEVOL ORGANITZACIÓ

Grau d'Enginyeria Informàtica

Àrea TFG: Administració de xarxes i sistemes operatius

Autora: *Mª Teresa Muñoz Siles*

Professor Consultor: *José Manuel Castillo Pedrosa*

Professorat Responsable: *David Bañeres Besora*

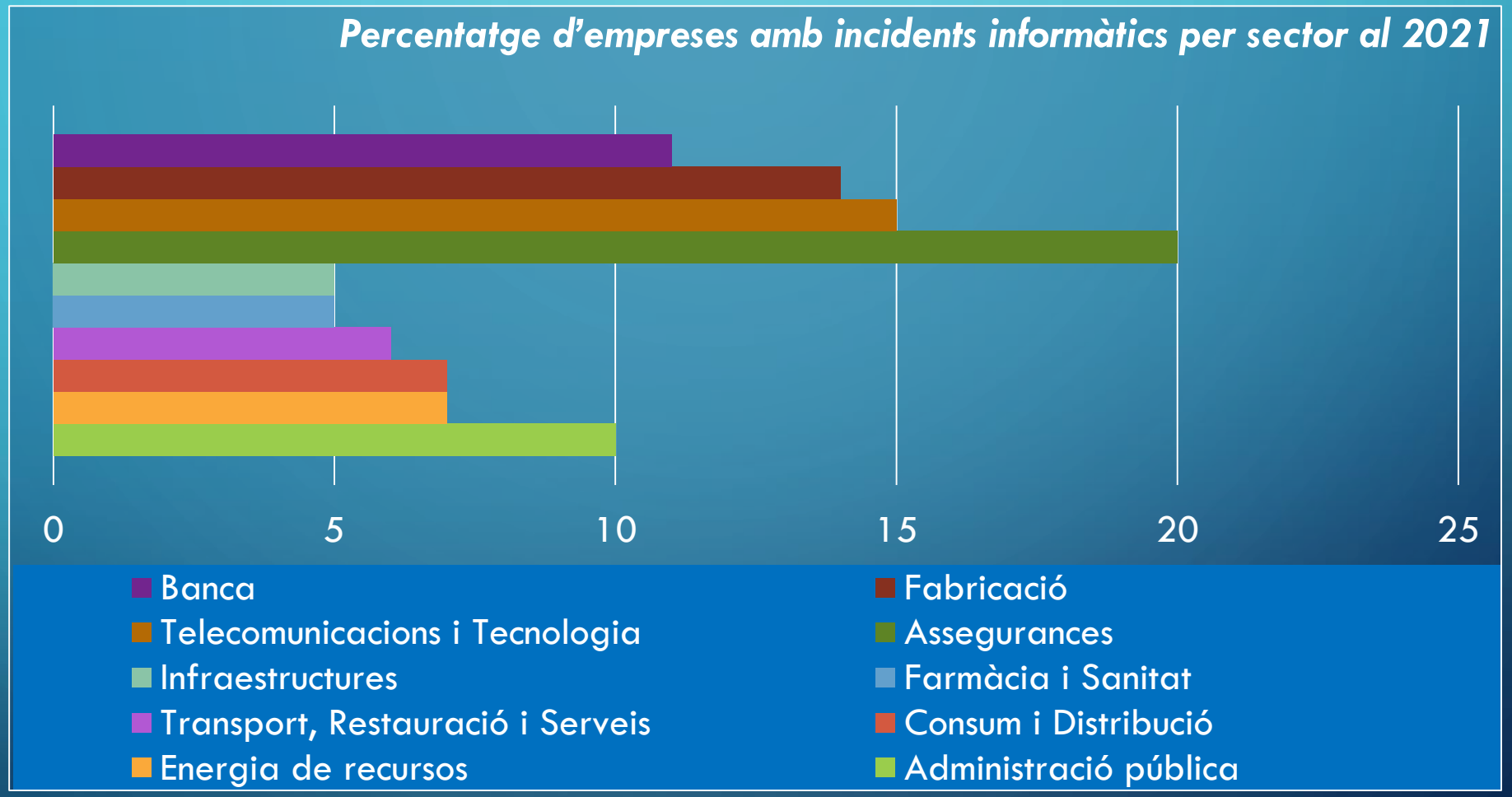
Montse Serra Vizern

SUMARI

INTRODUCCIÓ

Riscos per deficiències de la seguretat informàtica

JUSTIFICACIÓ DEL TREBALL



Elaborat a partir de 'El estado de la ciberseguridad en España" de Deloitte

OBJECTIUS

Auditoria interna

Mesures correctores / preventives

Pla de millora de la seguretat informàtica

Imatges obtingudes a: https://pixabay.com

AUDITORIES INFORMÀTIQUES

TIPOLOGIES

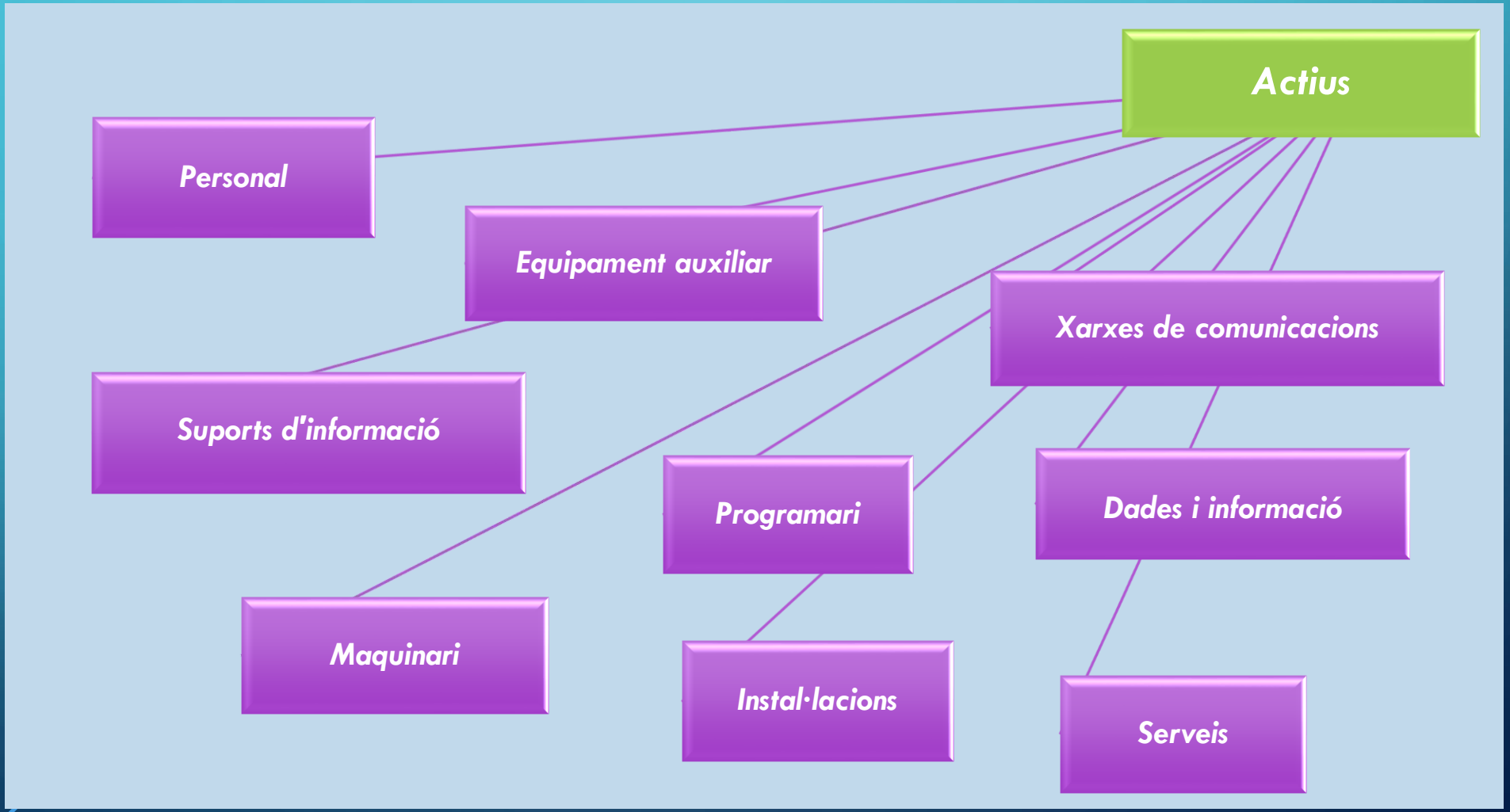
Interna

- Auditoria de primera part.
- Auditor de la mateixa organització.
- Pot incloure col·laboradors externs.
- Base per demanar la certificació.

Externa

- Auditoria de segona part → part externa amb interès en l'organització.
- Auditoria de tercera part → empresa auditora independent (ex. certificació).
- Auditor independent de l'organització.
- Superació de l'auditoria → Certificació.

CLASSIFICACIÓ DELS ACTIUS



BENEFICIS DE L'AUDITORIA INTERNA

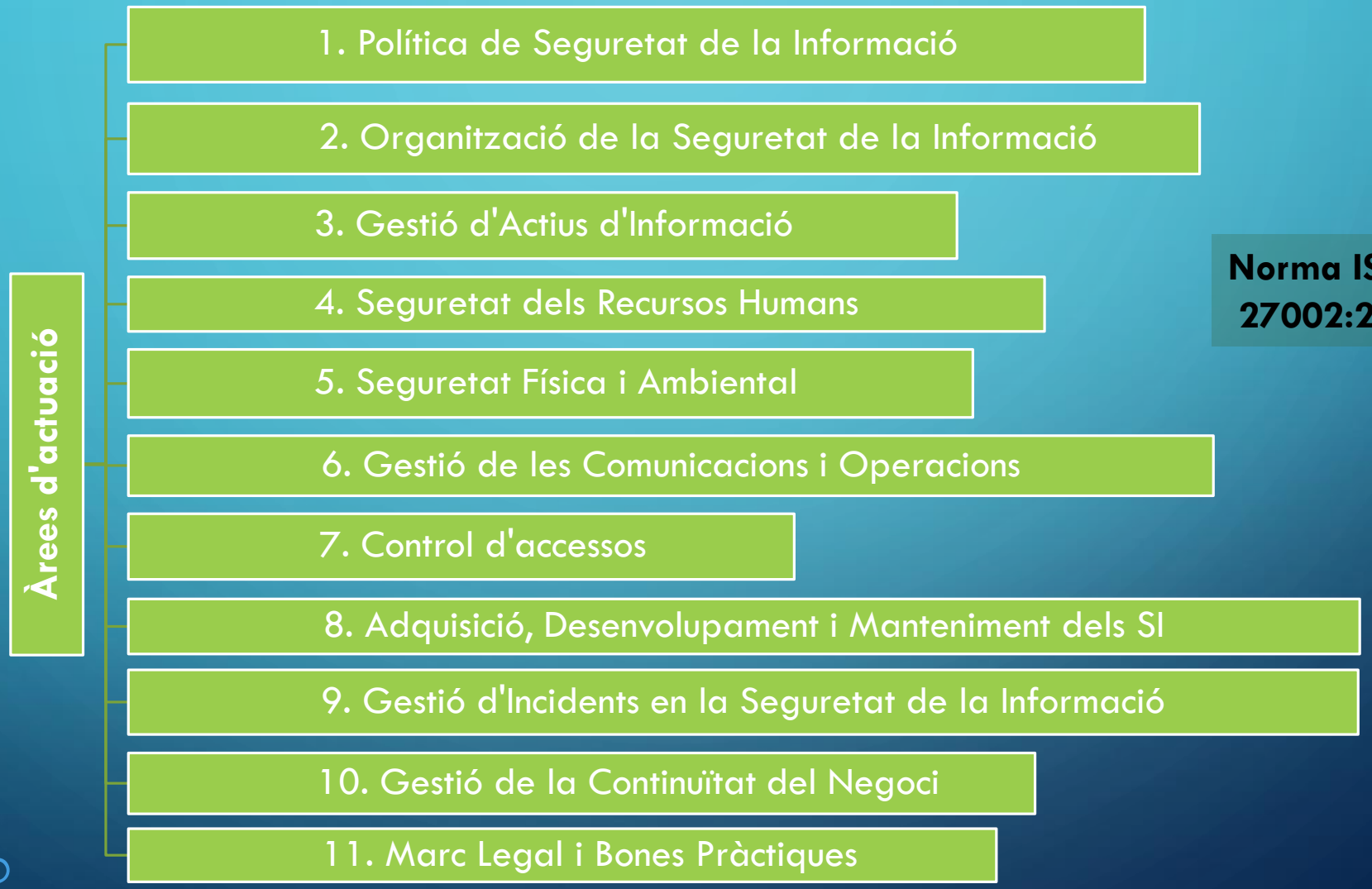
- Informe d'auditoria final ⟶ pla de millora de la seguretat de les TIC
- Reducció de l'impacte financer, legal i operatiu d'una protecció insuficient
- Cultura empresarial més conscienciada de la importància de la seguretat
- Informació útil i de qualitat (disponibilitat, confidencialitat, integritat,...)
- Compliment de la normativa i la legislació vigent (protecció de dades,...)
- Detecció de possibles vulnerabilitats i prevenció d'amenaces
- Increment de l'eficiència dels sistemes informàtics
- Preparació per obtenir la certificació
- Millora de la imatge de l'organització
- Millora de la presa de decisions
- Augment de la productivitat
- i molts més...

Imatge obtinguda a: https://pixabay.com

NORMES ISO APLICADES A L'AUDITORIA INTERNA (I)

Norma ISO/IEC 27001:2017

NORMES ISO APLICADES A L'AUDITORIA INTERNA (II)



Norma ISO/IEC 27002:2022

LEGISLACIÓ APLICABLE

- La Carta de Drets Fonamentals de la Unió Europea
- el Tractat de Funcionament de la Unió Europea
- el Reglament (UE) 2016/679 del Parlament Europeu i del Consell
- el Reglament (UE) 2022/868 del Parlament Europeu i del Consell, de 30 de maig de 2022, relatiu a la governança europea de dades i pel qual es modifica el Reglament (UE) 2018/1724
- la Constitució Espanyola
- la Llei Orgànica de Protecció de Dades i Garantia de drets digitals (LOPDGDD)
- la Llei Orgànica 34/2002 de Serveis de la Societat de la Informació i del Comerç Electrònic (LSSI)
- la Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques (LPACAP)
- la Llei 32/2003 General de Telecomunicacions
- la Llei 17/2001 de Marques
- la Llei 59/2003 de Signatura Electrònica
- el Reial Decret Legislatiu 1/1996 de Propietat Intel·lectual
- més l'específica i pròpia per alguns sectors

Imatge obtinguda a: https://pixabay.com

ELABORACIÓ DEL PLA D'AUDITORIA

Recursos necessaris per realitzar l'auditoria (tècnics, humans, materials).

Reunions dels responsables de l'organització sol·licitants de l'auditoria.

Tasques de planificació preliminar, requeriments d'informació i proves:

- Desenvolupament del pla d'auditoria.
- Coneixements del personal auditor.
- Calendari de tasques, detall de les revisions i disseny de proves.
- Assignació de tasques als auditors.
- Normativa en què es basarà l'auditoria.
- Recollida de documentació útil.

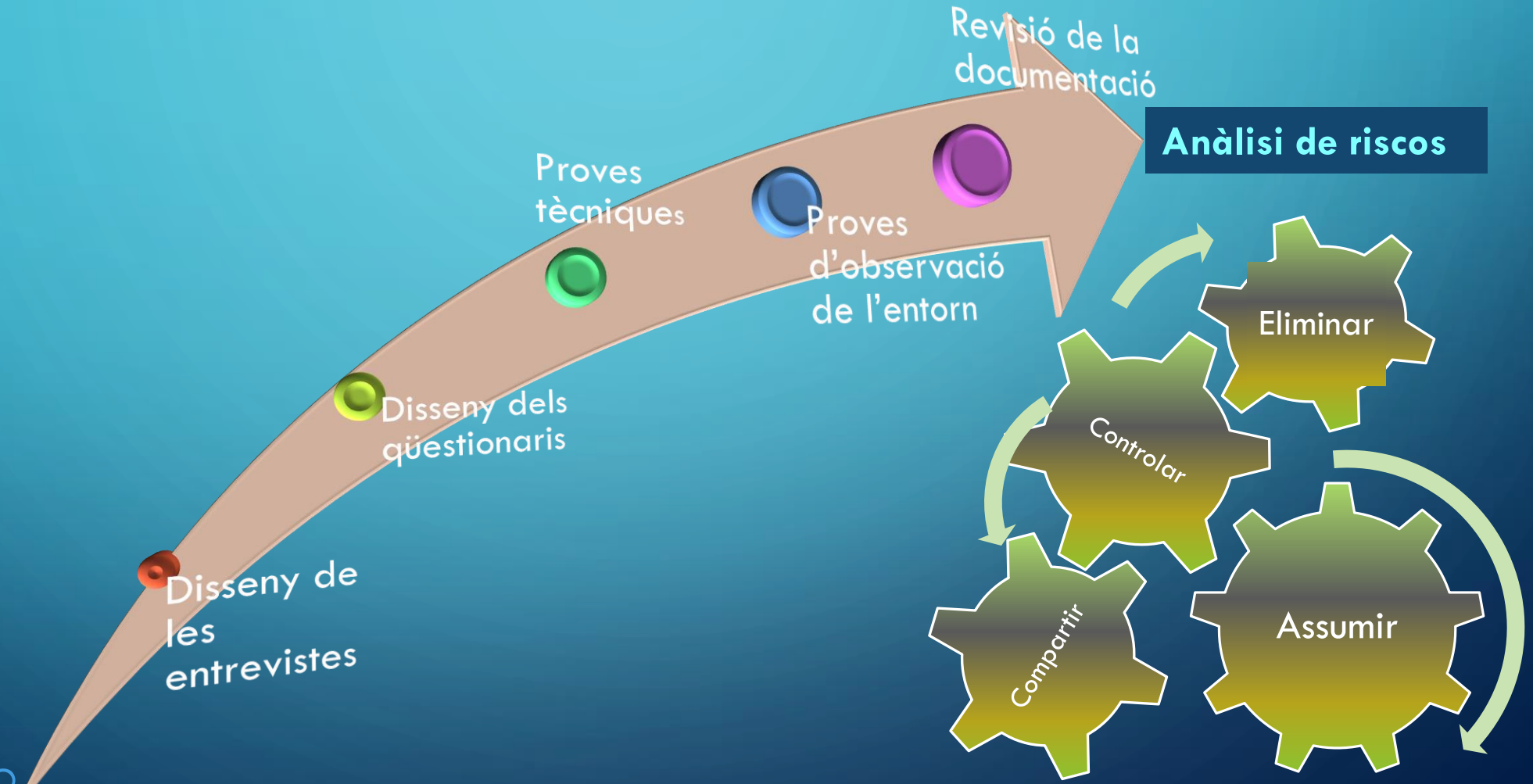
Establiment del pla d'auditoria: execució d'activitats, revisions, proves

Avaluació global dels resultats de l'auditoria.

Redacció i presentació de l'informe final d'auditoria.

Control de seguiment de la millora aconseguida amb les mesures aplicades.

PLA DE TREBALL DE L'AUDITORIA INTERNA



ANÀLISI DE RISCOS

ISO 27001

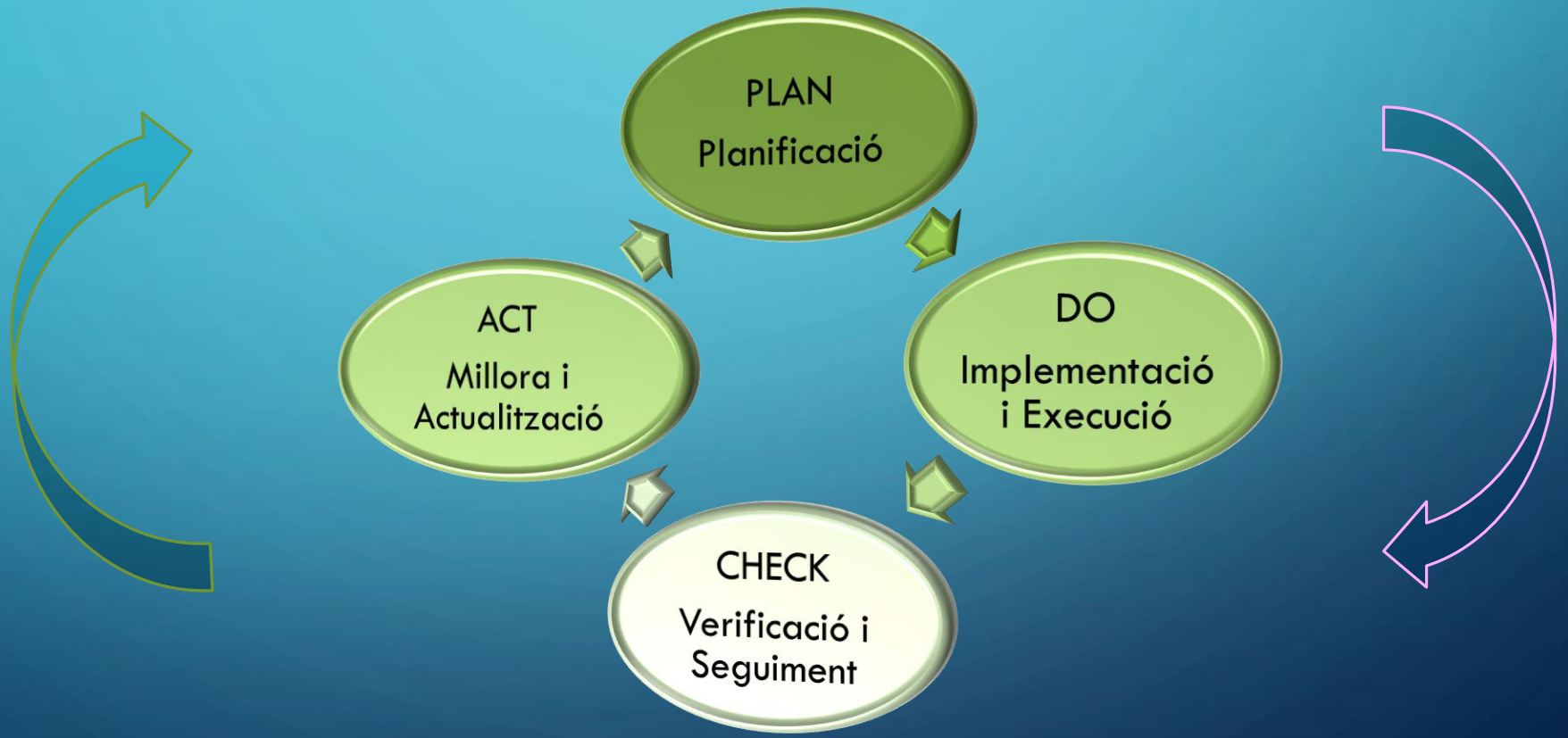
- Identificació dels actius, requisits legals i processos de negoci
- Valoració dels actius crítics
- Determinació de les amenaces i les vulnerabilitats que poden afectar els actius
- Estimació de l'impacte sobre els actius degut a una vulnerabilitat
- Avaluació del risc de de les amenaces i les vulnerabilitats segons les mesures existents
- Càlcul del nivell de risc

INFORME FINAL DE L'AUDITORIA

- ✓ Dates de l'auditoria i d'emissió de l'informe
- ✓ Abast, limitacions i objectius
- ✓ Període de cobertura
- ✓ Identificació dels sistemes auditats
- ✓ Metodologia aplicada i documentació auditada
- ✓ Punts forts, debilitats i oportunitats de millora
- ✓ Grau de compliment i recomanacions basades en els riscos
- ✓ Annexos: resultats de les proves, restriccions i accions de millora
- ✓ Signatura de l'auditor intern

IMPLEMENTACIÓ DE L'AUDITORIA

Segueix la metodologia PDCA *(Plan-Do-Check-Act)* en la qual es basa la norma ISO 27001



CONCLUSIONS

AUDITORIA INTERNA DE SEGURETAT INFORMÀTICA APLICABLE A QUALSEVOL ORGANITZACIÓ

L'AUDITORIA INTERNA DE SEGURETAT INFORMÀTICA, UNA GRAN OBLIDADA, PERÒ UNA EXCEL·LENT ALIADA DE LES ORGANITZACIONS

Aquest treball final de grau es centra en donar rellevància a l'important paper de l'auditoria interna de la seguretat informàtica de qualsevol organització, amb independència del sector al que pertany o del seu tamany.

Es segueix una planificació prèvia que inclou tots els recursos necessaris, i que a més, contempla la legislació vigent i es basa en normes estàndard internacionals tan imprescindibles com són la ISO 27001 i la ISO 27002.

Tot això, en conjunt, constitueix un procés de millora contínua beneficiós per l'organització al reduir en la mesura del possible l'efecte de les amenaces que planen permanentment sobre els actius d'informació, ajudant-li a assolir, fins i tot, la seva certificació ISO 27001.

Moltes gràcies