Introducció

Pla de Qualificació en Tecnologia Mòbil

Organitza: CIFO · SOC Servei d'Ocupació de Catalunya · Generalitat de Catalunya · Unió Europea Fons Social Europeu L'FSE inverteix en el teu futur

Imparteix: UOC Universitat Oberta de Catalunya

Col·labora: MOBILE WORLD CAPITAL BARCELONA

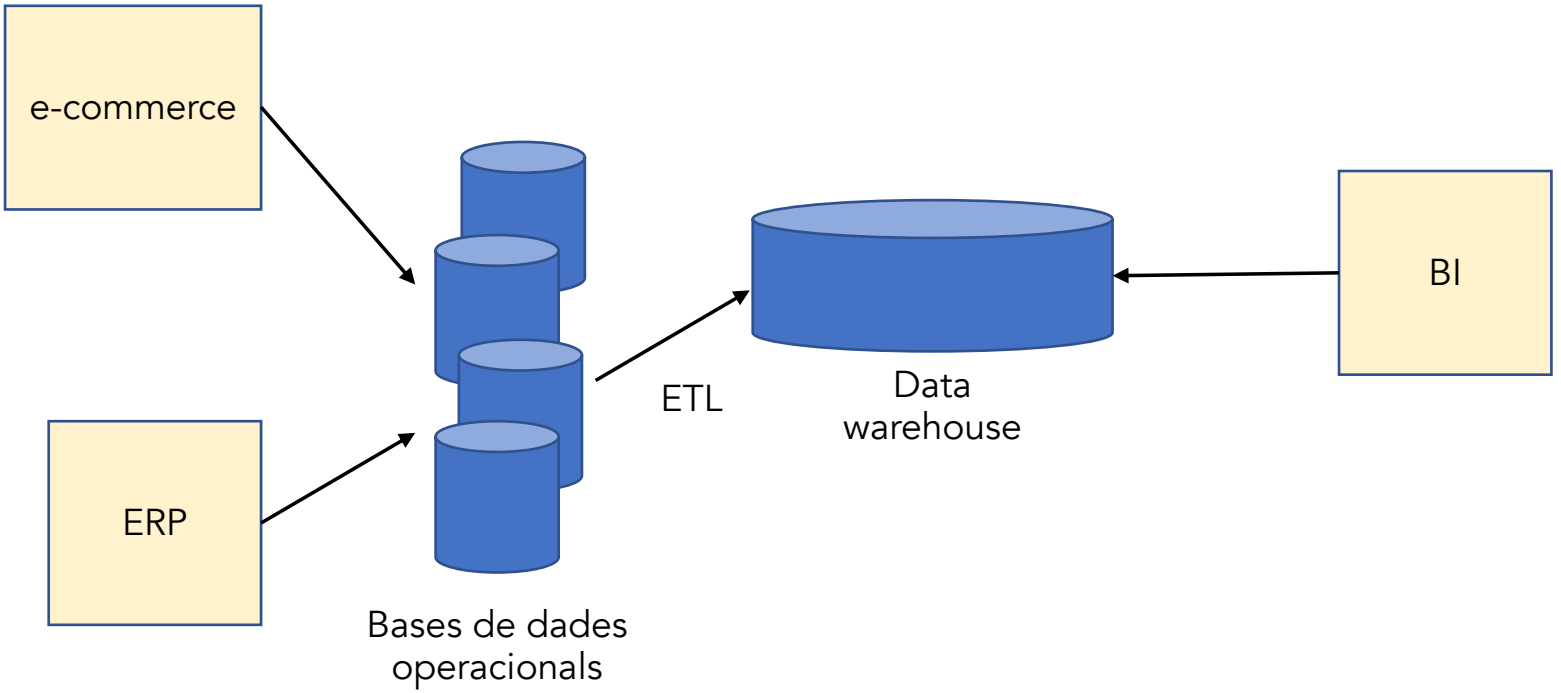
Empreses, organitzacions i "informàtica"

- Les dades són un valor per a l'empresa:
  - Servidors de dades, de documents, de còpies de seguretat...
  - Funcionament de l'empresa: *Enterprise Resource Planning* (ERP)
  - Model de negoci i e-commerce
  - Dades històriques: extreure coneixements, Big Data, Deep Learning, Data Mining, Process Mining... **DATA WAREHOUSE (magatzem de dades), ajuda a la presa de decisions, business intelligence, GIS...**

Empreses, organitzacions i "informàtica"

- Les dades són un valor per a l'empresa:
  - Els magatzems de dades proporcionen una eina per a la presa de decisions, des d'una perspectiva global de la informació de què disposa l'empresa.
  - Facilita usar tècniques estadístiques d'anàlisi i modelització per trobar relacions "ocultes".
  - Predicció de situacions futures o detecció d'escenaris i probabilitats que ocorrin.
  - etc.

Empreses, organitzacions i "informàtica"



Empreses, organitzacions i "informàtica"

- Seguretat TIC
  - Servidors, estacions de treball, portàtils... mecanismes d'accés i control del que es fa amb els recursos i les dades. Evitar/detectar intrusions.
  - Còpies de seguretat: bona política de recuperació de dades, gestió àgil de les incidències, detecció ràpida de fallades, etc.
  - Fallades físiques, fallades lògiques i errades humanes.
  - Confidencialitat, accessibilitat/disponibilitat, integritat.

Empreses, organitzacions i "informàtica"

- El/la responsable d'informàtica
  - Gestiona els recursos del departament d'informàtica i fa d'unió entre el departament i l'organització.
  - Es menja marrons...
  - Apaga focs...

  - **Les organitzacions destinen prou recursos a les TIC?**

Empreses, organitzacions i "informàtica"

- En què pensem quan diem "ciberseguretat"?

La seguretat informàtica és una branca de la informàtica que estudia com assegurar que els recursos dels sistemes informàtics siguin utilitzats de la forma en què es van definir. El seu objectiu és la creació de plataformes segures en què els agents que hi interaccionen (programes i usuaris) només puguin realitzar les accions que hi hagin estat autoritzades.

Els experts en seguretat informàtica acostumen a afirmar que un sistema 100% segur no existeix.

Wikipedia

Empreses, organitzacions i "informàtica"

- En què pensem quan diem "ciberseguretat"?
  - Pensem en intrusions, en denegació de serveis, en honeypots, en trencar contrasenyes...

Però la seguretat informàtica va més enllà: va de polítiques de seguretat, va de formació de persones, etc.

Dimensions de la seg. de la informació

- **Confidencialitat**
  - Només les persones autoritzades tenen l'accés a la informació sensible o privada.
  - Control d'accés, xifratge.
- **Integritat**
  - La informació i els mètodes de processament d'aquesta informació són exactes i complets, i no s'han de manipular sense autorització.
- **Disponibilitat**
  - Els usuaris que hi estan autoritzats poden accedir a la informació quan ho necessitin.

Dimensions de la seg. de la informació

- **Autenticitat i no-repudi**
  - Hi ha garantia de la identitat dels usuaris o processos que tracten la informació i de l'autoria d'una determinada acció.
- **Traçabilitat**
  - És possible reproduir un històric o seqüència d'accions sobre un determinat procés i determinar qui ha estat l'autor de cada acció.
- **Privadesa**
  - Accés a la informació de caràcter personal.

Dimensions de la seg. de la informació

Nòmines d'una empresa	Confidencialitat, integritat
Web e-commerce	Disponibilitat, integritat
Tràmits electrònics amb l'administració	Disponibilitat, integritat, traçabilitat
Sistema de comunicació d'emergències	Disponibilitat

Gestió de la seguretat

Pla de Qualificació en Tecnologia Mòbil

Organitza: CIFO · SOC Servei d'Ocupació de Catalunya · Generalitat de Catalunya · Unió Europea Fons Social Europeu L'FSE inverteix en el teu futur

Imparteix: UOC Universitat Oberta de Catalunya

Col·labora: MOBILE WORLD CAPITAL BARCELONA

Gestió de la seguretat

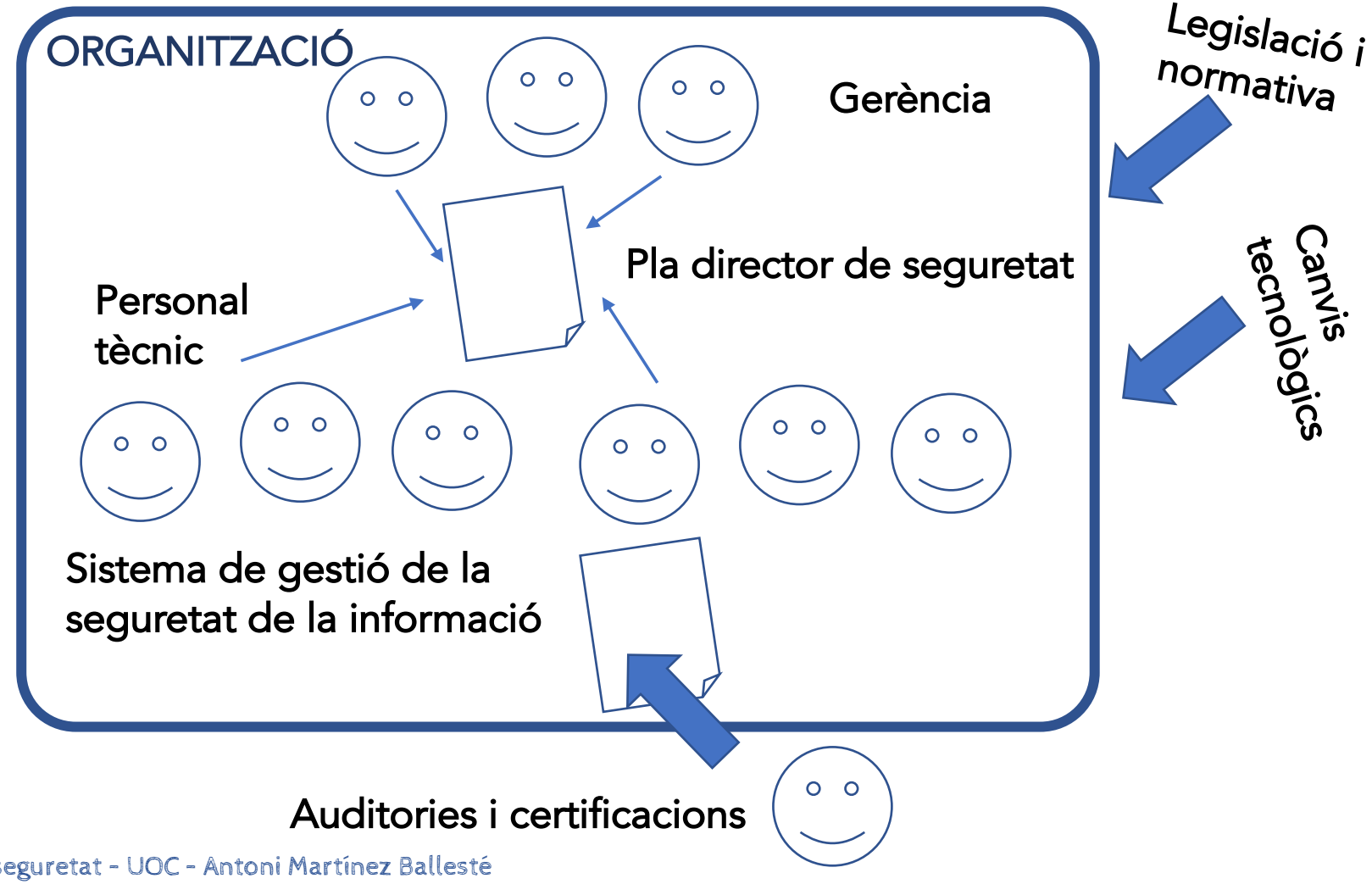
- Les organitzacions han de tenir **un pla de seguretat director de seguretat**

Aquests plans directors impliquen la direcció de l'empresa, recursos, estratègies, etc. Després hi haurà la concreció en el propi sistema de gestió de la seguretat de la informació que tingui l'empresa.

Gestió de la seguretat

- **Pla director de seguretat**
  - **Cal protegir els actius** dels sistemes d'informació de les organitzacions perquè aquestes funcionin correctament i s'assoleixin els seus objectius.
  - **Cal estar preparats pel risc** que una **amenaça** es materialitzi i es desencadeni un dany.
  - **Cal conèixer l'impacte** si una amenaça es materialitza.
  - **Cal establir controls** per reduir el nivell de risc.

Gestió de la seguretat



Gestió de la seguretat

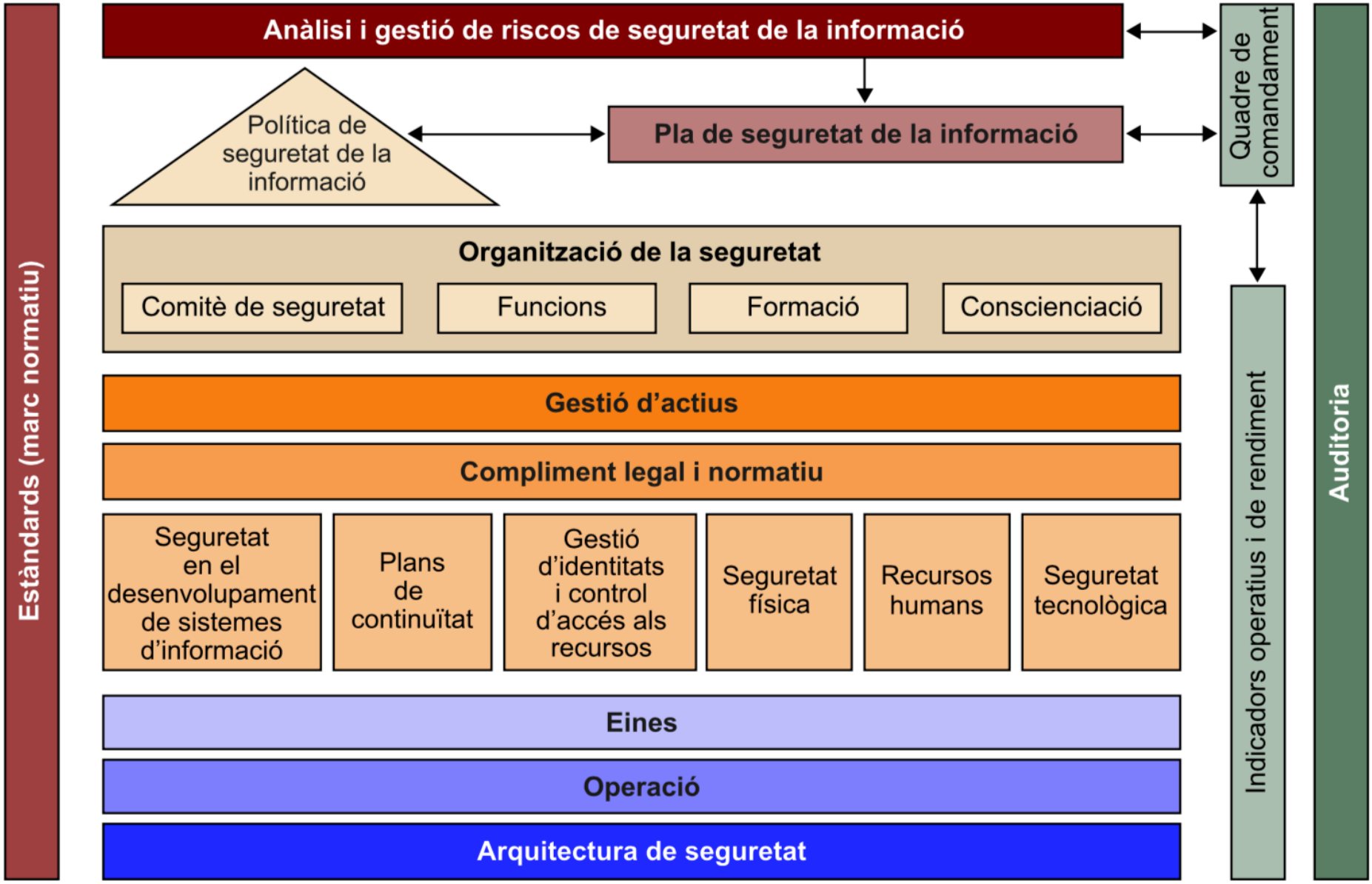
- Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia de dreta digitals.
  - Adaptació del Reglament General de la Protecció de Dades (RGPD)
- Llei 39/2015 d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
- Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica (administració pública).
- Llei 50/2003, de 19 de desembre, de signatura electrònica.
- Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a comunicacions i a les xarxes públiques de comunicacions.

Algunes d'elles tenen actualitzacions (consultar al BOE)

Gestió de la seguretat

- Cal que les organitzacions tinguin **auditories de seguretat:**
  - Anàlisi i estudi de la xarxa i sistemes d'informació.
  - Usos de les persones que s'hi relacionen, polítiques de seguretat, formació, etc.
  - Detecció de vulnerabilitats físiques, lògiques, etc.
  - Informe i documentació.

Gestió de la seguretat



El procés de gestió de la seguretat de la informació

Gestió de la seguretat

Cada organització ha d'analitzar quin s'adapta millor a les seves característiques.

- **Models de gestió**
  - **GESTIÓ INTERNA.** Íntegrament gestionada per personal propi. Requereix tenir un responsable de seguretat de la informació i un equip de treball (si escau).
    - **Punts forts:** Coneixement del negoci, implicació del personal.
    - **Punts febles:** Cost de la contractació, poca flexibilitat en el dimensionament dels equips.

Gestió de la seguretat

Cada organització ha d'analitzar quin s'adapta millor a les seves característiques.

- **Models de gestió**
  - **GESTIÓ EXTERNALITZADA.** Subcontractació d'una empresa de serveis informàtics, per gestionar total o parcialment la seguretat.
    - **Punts forts:** Alta especialització, experiència.
    - **Punts febles:** Possible desconfiança del personal intern.
    - És necessari un bon contracte amb les responsabilitats i tasques, així com els acords de nivell de servei (*service level agreement*).
  - **MODEL MIXT.** Personal propi (gestor) treballant amb serveis externs.

Gestió de la seguretat

Gestió de la seguretat en remot, monitoritzant la seguretat dels clients 24x7.

- **Security Operations Center**
  - Protecció contra intrusions i atacs externs.
  - Activitat dels tallafocs, sistemes de detecció i protecció d'intrusions, antivirus...
  - Configuració segura de maquinari i programari.
  - Monitoratge de disponibilitat de sistemes.
  - Auditories de seguretat i proves de penetració.
  - Assistència tècnica i capacitat de contenció en cas d'incidències.

Gestió de la seguretat

- **Tipus de controls de seguretat**
  - **Segons la naturalesa del control**
    - **Controls tècnics**
      - Antivirus, tallafoc, la configuració d'un sistema, un SAI, el xifratge de les comunicacions, etc.
    - **Controls organitzatius**
      - Polítiques, normes i procediments, plans de conscienciació, pla de continuïtat de negoci...

Gestió de la seguretat

- **Tipus de controls de seguretat**
  - **Segons allò que controlen**
    - **Controls sobre la probabilitat d'ocurrència d'una amenaça**
      - Sistema de detecció d'incendis
    - **Controls sobre l'impacte en cas de materialització de l'amenaça**
      - Sistema d'alimentació ininterrompuda
      - Generador elèctric
      - Còpies de seguretat en mirall, sistemes virtualitzats.

Gestió de la seguretat

- **Tipus de controls de seguretat**
  - **Segons la seva finalitat**
    - **De detecció**
      - Sistema de detecció d'incendis
      - Sistema de detecció d'intrusions
    - **Correctius**
      - Sistema d'extinció d'incendis
      - Còpies de seguretat

Gestió de la seguretat: fonts i marcs de treball

- **Normes ISO relatives a la seguretat de la informació** (ISO 27000) i altres normes ISO (22301, continuïtat de negoci; 31000 gestió de riscos)
- **Marc de treball Cobit** (*Control OBjectives for Information and related Technology*)
  - Alineació estratègica; Lliurament de valor; Administració de riscos; Administració de recursos; Mesurament de l'acompliment
- **Marc de treball ITIL** (*Information Technology Infrastructure Library*)
  - ... Gestió de la infraestructura de les TIC; Gestió de la seguretat

Gestió de la seguretat: ISO 27000

- **27000.** Conceptes i vocabulari que surten en els diferents estàndards de la sèrie.
- **27001.** Especificacions per implantar un sistema de gestió de la seguretat.
- **27002.** Codi de bones pràctiques.
- **27003.** Guia d'implementació dels Sistemes de Gestió de la Seguretat.
- **27004.** Mètriques i tècniques de mesura.
- **27005.** Directrius per a la gestió del risc.
- **27018.** Codi de bones pràctiques enfocades a la protecció d'informació personal en entorns cloud.
- **27032.** Codi de bones pràctiques enfocades a la ciberseguretat.
- **...**

Gestió de la seguretat: ISO 27000

- Objectius
  - Formular els requisits i objectius de seguretat de la informació.
  - Assegurar que els riscos de seguretat es gestionen de manera efectiva en termes de costos.
  - Assegurar el compliment de lleis i regulacions.
  - Implementar i gestionar els controls necessaris per a assegurar que s'aconsegueixen els objectius de seguretat que ha definit l'organització.
  - Definir nous processos de gestió de la seguretat, o identificar i aclarir els processos que ja hi ha.

Gestió de la seguretat: ISO 27000

- Objectius
  - Definir nous processos de gestió de la seguretat, o identificar i aclarir els processos que ja hi ha.
  - Fer que la direcció conegui l'estat de les activitats de gestió de la seguretat.
  - Conèixer el grau de compliment de polítiques, directives i estàndards adoptats per l'organització, per part d'auditors interns o externs.
  - Establir polítiques, directives, estàndards o procediments de seguretat de la informació en les relacions amb tercers.
  - Convertir la seguretat de la informació en un facilitador del negoci.
  - Proporcionar informació rellevant sobre l'estat de la seguretat de la informació a clients.

Gestió de la seguretat: ISO 27000

Dominis de seguretat de l'ISO 27002

5. Polítiques de seguretat de la informació (1 objectiu, 2 controls)	6. Organització de la seguretat de la información (2 objectius, 7 controls)	7. Seguretat relativa als recursos humans (3 objectius, 6 controls)	8. Gestió d'actius (3 objectius, 10 controls)
9. Control d'accés (4 objectius, 14 controls)	10. Criptografia (1 objectiu, 2 controls)	11. Seguretat física i de l'entorn (2 objectius, 15 controls)	12. Seguretat de les operacions (7 objectius, 14 controls)
13. Seguretat de les comunicacions (2 objectius, 7 controls)	14. Adquisició, desenvolupament i manteniment dels sistemes d'informació (3 objectius, 13 controls)	15. Relacions amb proveïdors (2 objectius, 5 controls)	16. Gestió d'incidents de seguretat de la informació (1 objectiu, 7 controls)
	17. Aspectes de seguretat de la informació per a la gestió de la continuïtat del negoci (2 objectius, 4 controls)	18. Acompliment (2 objectius, 8 controls)	

Dominis de seguretat de l'ISO 27002, especificant per a cada domini el nombre de controls que el componen i el nombre d'objectius de control totals per domini.

Plans directors

Pla de Qualificació en Tecnologia Mòbil

Organitza: CIFO · SOC Servei d'Ocupació de Catalunya · Generalitat de Catalunya · Unió Europea Fons Social Europeu L'FSE inverteix en el teu futur

Imparteix: UOC Universitat Oberta de Catalunya

Col·labora: MOBILE WORLD CAPITAL BARCELONA

Plans directors de seguretat

- Definició i priorització d'un conjunt de projectes en matèria de seguretat de la informació amb l'objectiu de reduir els riscos als que s'exposa l'organització, partint d'una anàlisi de la situació actual.
- Per arribar a tenir-lo cal seguir una sèrie de fases...

Plans directors de seguretat

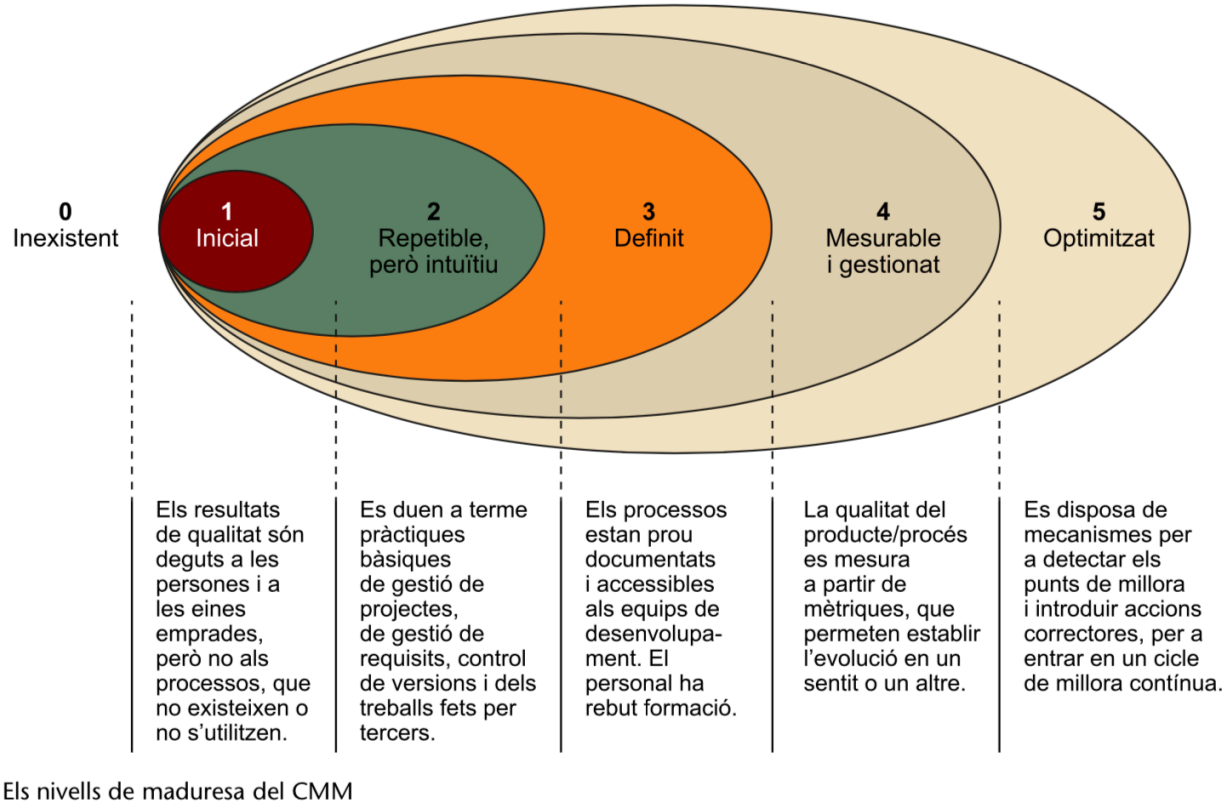
- Fases
  - 1) Conèixer la situació actual
  - 2) Conèixer l'estratègia de l'organització
  - 3) Definir projectes i iniciatives
  - 4) Classificació i priorització
  - 5) Aprovació per part de la direcció
  - 6) Implementació

Plans directors de seguretat

- 1) Conèixer la situació actual
  - Quins actius i processos cal protegir? O cal prioritzar-ne la protecció?
  - Podem usar les bones pràctiques de la ISO 27002 per fer una avaluació inicial. Contempla qüestions tècniques, legals i organitzatives.
  - Quin model de maduresa té l'empresa envers la seguretat TIC?

Plans directors de seguretat

- Marc de treball **Capability Maturity Model**, per a la millora de processos. Nivells de maduresa:



Els nivells de maduresa del CMM

Plans directors de seguretat

- 1) Conèixer la situació actual
  - Caldrà fer reunions amb els actors.
  - Caldrà conèixer les instal·lacions, registrant problemes i evidències.
  - Després caldrà analitzar els resultats.
  - També cal fer una anàlisi dels riscos i impacte.

Plans directors de seguretat

- 2) Conèixer l'estratègia de l'organització
  - És la seguretat una prioritat?
  - Hi ha recursos?
  - L'organització ha de canviar, créixer...

Plans directors de seguretat

- 3) Projectes i iniciatives. 4) Priorització

ID	Proyecto	Descripción
01	Desarrollar e implementar una política de seguridad	Desarrollar e implementar una política de seguridad que contenga al menos los siguientes aspectos: • Compromiso de la Dirección. • Utilización del e-mail e Internet. • Utilización de dispositivos móviles. • Aspectos de protección de datos.
02	Desplegar un plan de concienciación en materia de seguridad de la información.	Llevar a cabo sesiones de formación para y concienciación que cubran tanto el personal de los departamentos operativos como la Dirección.
03	Mejora en la gestión de incidentes y atención al usuario	Definir, documentar e implantar un proceso para la gestión de los incidentes de seguridad.
04	Adecuación al RGPD	Llevar a cabo un proyecto para adaptar la organización al RGPD.

https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

Plans directors de seguretat

- 5) Aprovació per part de la direcció
  - Possiblement caldrà revisions i modificacions... potser cal repetir-ho de forma cíclica.

Serà interessant calcular el cost.

- 6) Posada en marxa
  - Presentació davant l'organització
  - Assignar responsables
  - Seguiment i la seva periodicitat
  - Fites de la posada en marxa i calendari