Govern d'Andorra

Presentació

Desplegament reglamentari de la Llei 22/2022 de ciberseguretat

- Reglament de l'Esquema Nacional de Seguretat (ENS-AD)
- Reglament de les Infraestructures Crítiques (RIC-AD)

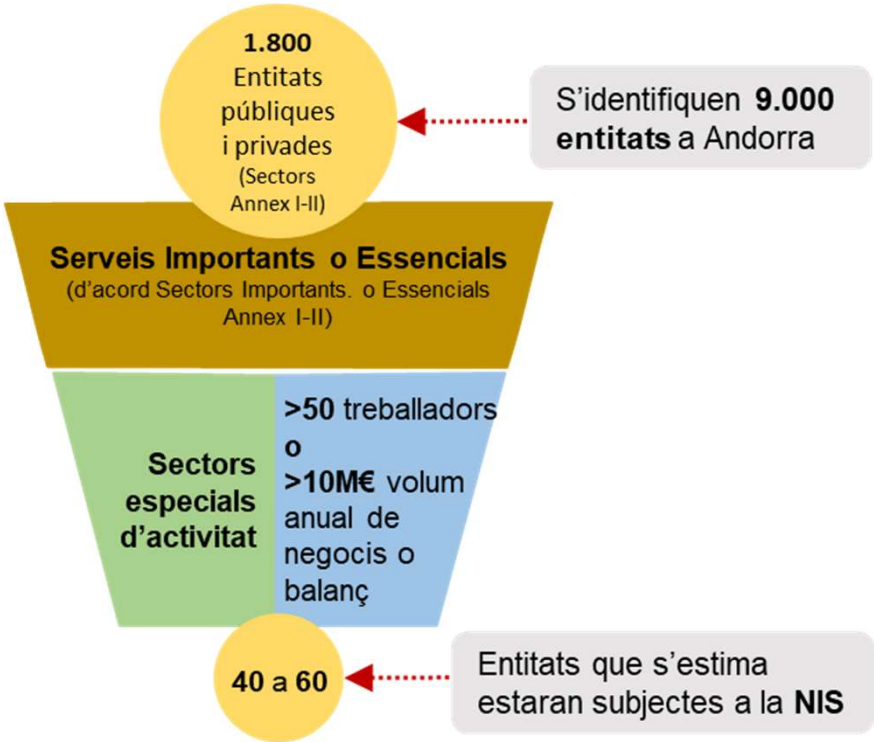
12 d'octubre 2022

ANDORRA DIGITAL

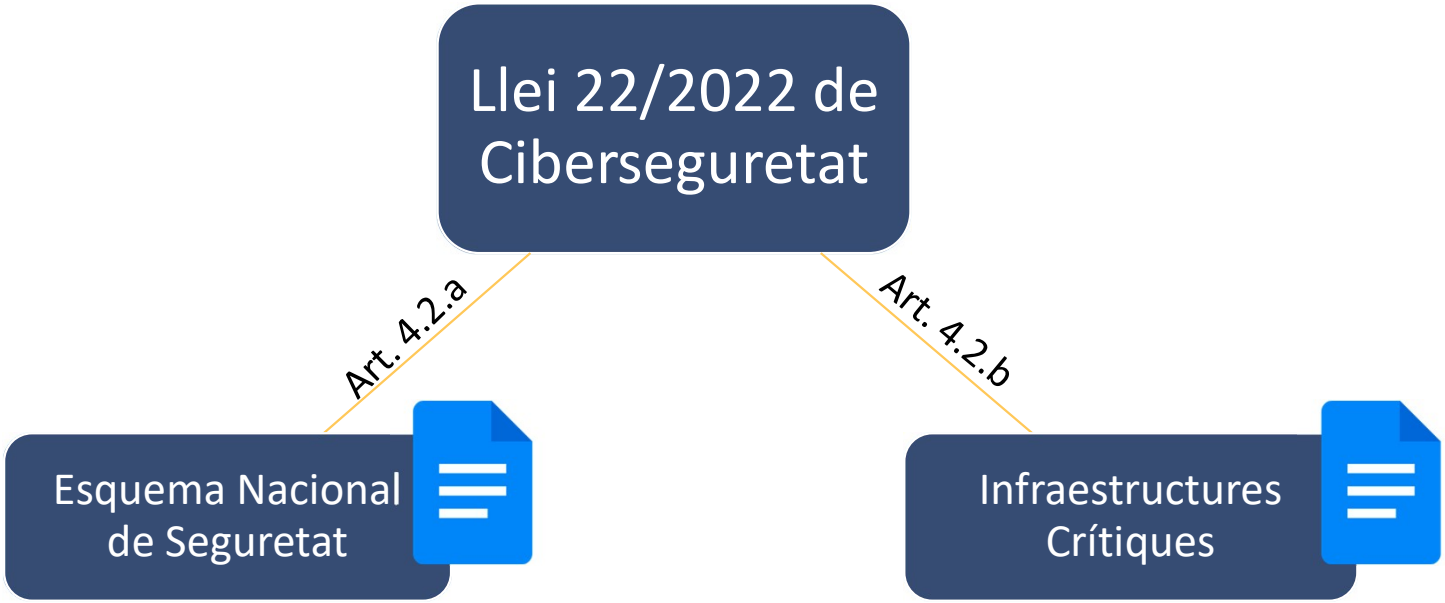
ANC-AD

Llei 22/2022 de ciberseguretat

Entitats afectades



Llei 22/2022 de ciberseguretat



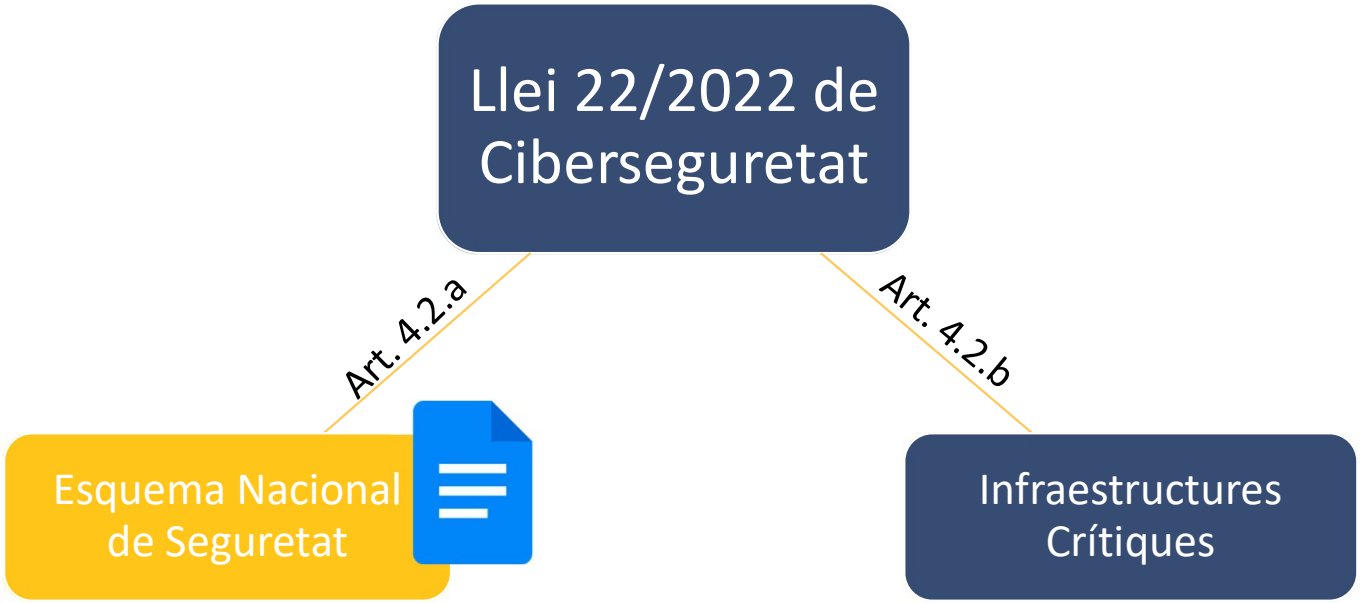
Objectiu:

Garantir un nivell de seguretat suficient per als serveis que resulten essencials o importants per al Principat d'Andorra

Objectiu:

Reforçar la resiliència de les entitats crítiques i equivalents a crítiques

Llei 22/2022 de ciberseguretat



Objectiu:

Garantir un nivell de seguretat suficient per als serveis que resulten essencials o importants per al Principat d'Andorra

Objectiu:

Reforçar la resiliència de les entitats crítiques i equivalents a crítiques

Resum:

- Permet a les **entitats que presten serveis essencials o importants** identificar i **implementar de manera sistemàtica** i integral les **mesures de seguretat** que resulten necessàries per a assegurar la prestació dels seus serveis.

- **Facilita procediments per al desenvolupament d'un sistema de gestió per a la seguretat de la informació (SGSI)** que garanteixi un nivell de protecció proporcional al nivell de risc al qual estan exposats la informació i els serveis a protegir

Funcions de les parts

- **Procediment per l’anàlisi de riscos**

  Proporcionar un mecanisme per implantar les mesures de seguretat al conjunt d´actius de la informació.

- **Elaborar una llista d´entitats afectades i la seva publicació al BOPA**
- **Definir el catàleg d´actius i actualització anual d’aquest**

  L‘ANC-AD analitzarà els riscos i especificarà cadascú dels actius d’informació que resultin necessaris per a modelar els serveis.

- **Certificació**

  Emetre la certificació final corresponent un cop es compleixin els requisits especificats en el reglament.

- **Elaboració de material de suport**

  L´ANC-AD elaborarà els materials necessaris per tal que les entitats puguin aplicar els diferents requeriments de l´ENS-AD.

- **Formació i conscienciació**

  Les autoritats competents en col·laboració amb el CSIRT-AD i la Universitat d'Andorra, entre altres, desenvoluparan programes de sensibilització, conscienciació i formació, dirigits al personal i als òrgans de direcció de les entitats afectades per la NIS-AD

Funcions de les parts

Entitat afectada

- **Identificació de l'entitat**

  Cada entitat comunicarà a l´Autoritat Nacional competent (ANC-AD o AFA segons apliqui) la seva afectació per la Llei NIS-AD com a entitat que presta serveis importants o essencials.

- **Delegat de Seguretat de la Informació (DSI)**

  Nomenar i comunicar la figura del DSI, el qual serà el punt de contacte entre l´entitat i l´Autoritat Nacional Competent.

- **Disposar de l´inventari d´actius d´informació a modelar.**
- **Verificar sistemàticament la situació de seguretat real**
- **Auditoria de seguretat interna**

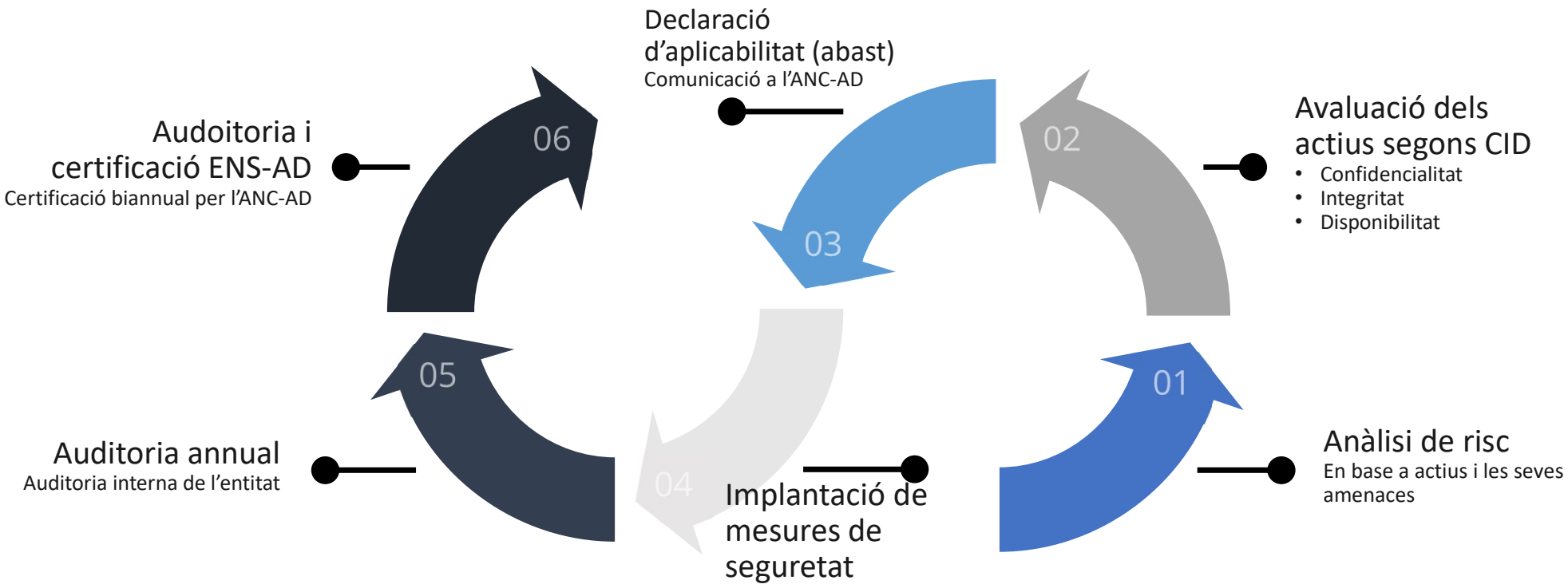
  Els actius d'informació necessaris per a la prestació dels serveis als que aplica l'ENS-AD seran objecte d'una auditoria interna ordinària anual, que verifiqui el compliment dels requeriments. Aquesta auditoria pot ser requerida per l´ Autoritat Nacional Competent.

- **Notificació d´incidents**

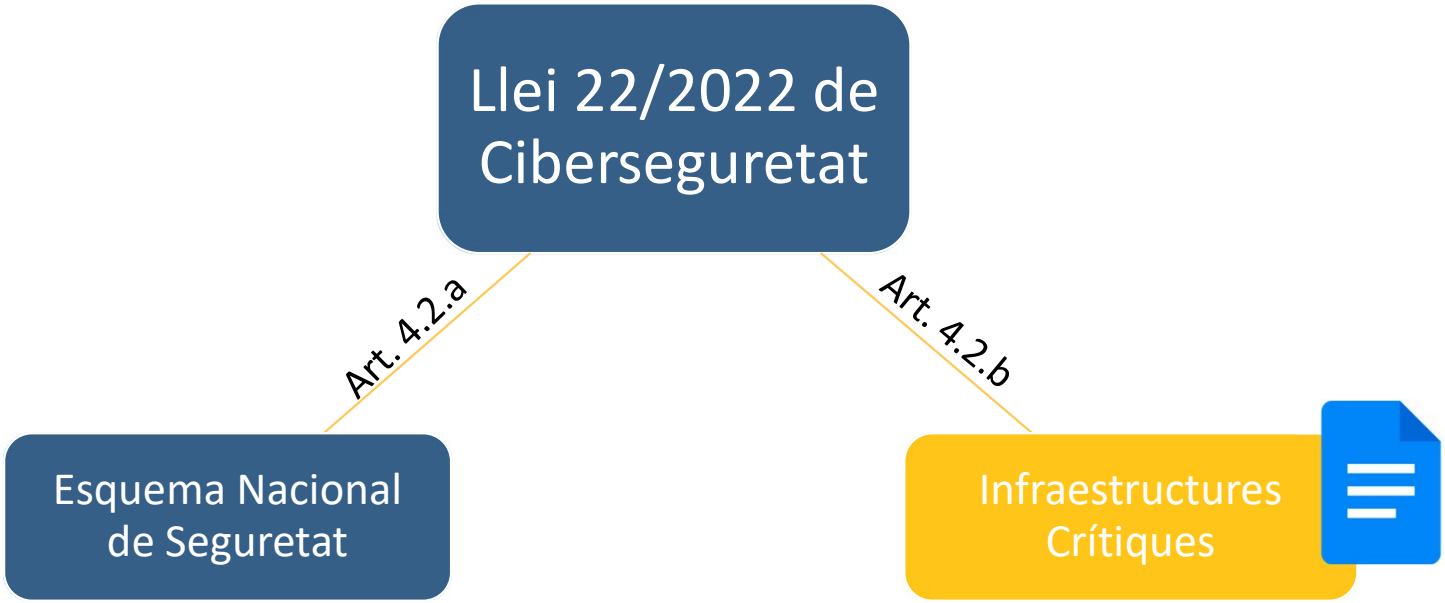
  Obligació de notificar incidents a l´Autoritat Nacional Competent en 72 hores

Reglament de l'Esquema Nacional de Seguretat (ENS-AD)

Establiment de l'ENS



Llei 22/2022 de ciberseguretat



Objectiu:

Garantir un nivell de seguretat suficient per als serveis que resulten essencials o importants per al Principat d'Andorra

Objectiu:

Reforçar la resiliència de les entitats crítiques i equivalents a crítiques

Resum:

- Disposar de les **garanties d'un nivell de protecció mínim per a totes les infraestructures** que participen en la prestació dels serveis importants i essencials

- Les entitats crítiques es **dotaran d'una capacitat de recuperació enfront d'incidents (resiliència) molt major que l'exigible a la resta d'entitats**

Definicions:

Entitat crítica: una entitat que proporciona un o més serveis essencials la prestació dels quals depèn d'una o més infraestructures crítiques situades al Principat d'Andorra.

Infraestructures crítiques: infraestructures que són indispensables i no permeten solucions alternatives, pel que la seva pertorbació o destrucció, tindria efectes perjudicials significatius sobre la prestació d'un o més serveis essencials.

Funcions de les parts

- **Identificació d´infraestructures crítiques**

  L'Autoritat Nacional Competent (ANC-AD o AFA segons apliqui) elaborarà la definició d'infraestructura crítica en funció dels resultats de la seva avaluació dels riscos que poden afectar els serveis essencials de la seva competència.

- **Elaborar una llista d´entitats afectades.**
- **Comunicar dins el termini d´un mes, a les entitats afectades.**
- **Elaboració del Catàleg Nacional d´Infraestructures Crítiques (CNIC)**
- **Elaborar el Pla d´Infraestructures Crítiques (PIC):**

  Compendi de documents, confidencials en la seva majoria, que descriuen com organitzar la seguretat a nivell ampli de país, i com controlar, motivar, liderar així com prendre les decisions per aconseguir els objectius de protecció desitjats.

- **Elaboració Pla de Suport Operatiu (PSO)**

  En cas que l'ANC-AD ho consideri, es poden demanar suport per dissenyar un Pla de Suport Operatiu en cas de que existeixin amenaces sobrevingudes que requereixin afegir mesures complementàries i extraordinàries a alguna infraestructura crítica

- **Elaboració de material de suport**

  L´ANC-AD elaborarà el material necessari per tal que les entitats puguin aplicar els diferents requeriments del RIC-AD.

- **Organització d'exercicis de resiliència**

  L'ANC-AD, en col·laboració amb el CSIRT-AD i la Universitat d'Andorra, entre altres desenvoluparà materials i metodologies d'orientació, donarà suport a l'organització d'exercicis per a comprovar la resiliència de les entitats crítiques i proporcionarà formació al seu personal.

Reglament d’Infraestructures Crítiques (RIC-AD)

Funcions de les parts

Entitat afectada

- **Elaborar el Pla Estratègic Sectorial (PES-AD)**

  Descriu, en cadascun dels sectors essencials de l'Annex I de la Llei NIS-AD, quins són els serveis essencials proporcionats a la ciutadania, el funcionament general d'aquests, els seus riscos, les infraestructures crítiques per a garantir la prestació de cada servei essencial amb la qualitat requerida.

- **Pla de Seguretat de l´Entitat (PSE-AD)**

  Són els documents estratègics on es defineixen les polítiques generals d’una entitat crítica

- **Delegat de Seguretat de la Informació (DSI)**

  Designar i proporcionar la figura del DSI, el qual serà el punt de contacte entre l´entitat i l´Autoritat Nacional Competent.

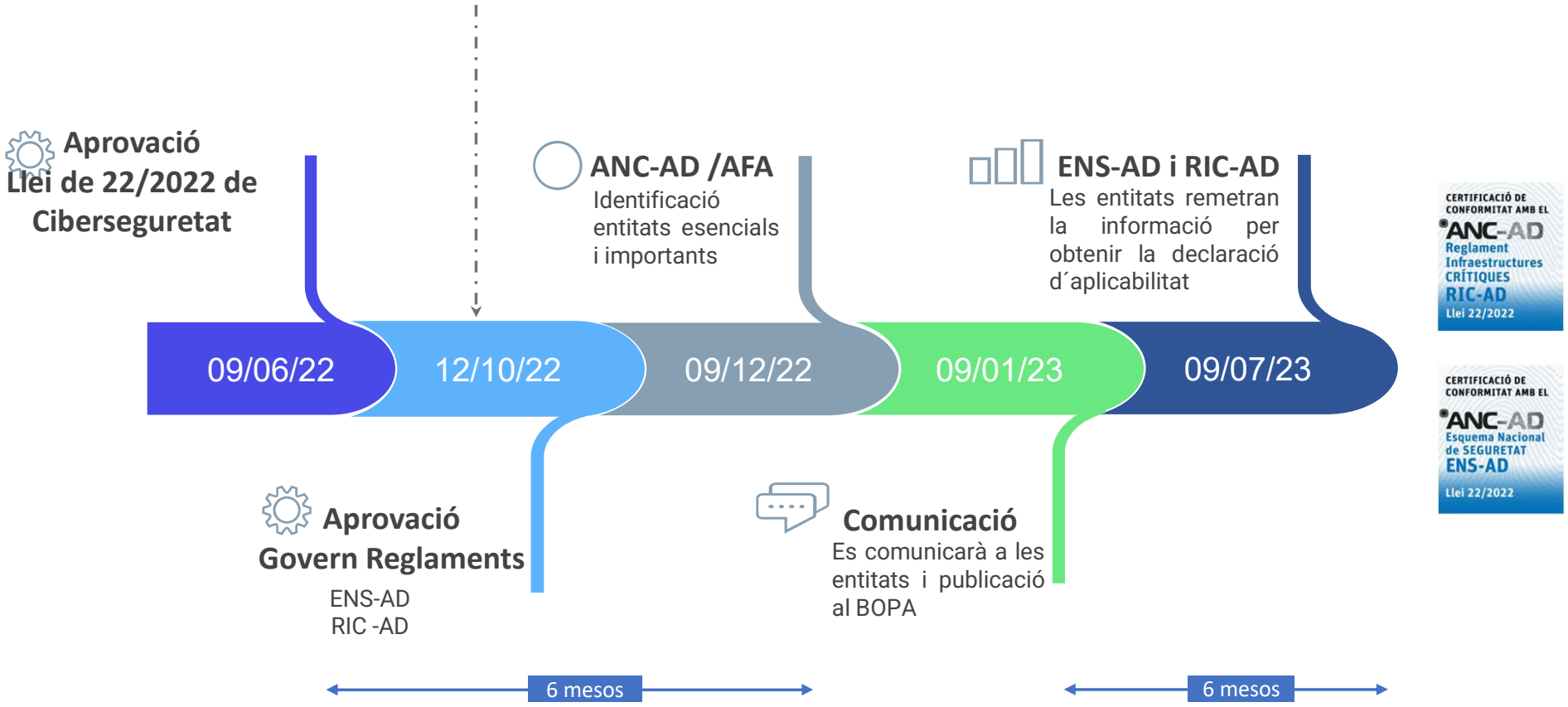
- **Auditoria de seguretat interna**

  Les entitats crítiques i les entitats equivalents a entitats crítiques seran objecte d'una auditoria interna ordinària anualment, on es verifiqui el compliment dels requeriments establerts en el reglament.

- **Notificació d´incidents**

  Obligació de notificar incidents a l´Autoritat Nacional Competent en un termini de 72 hores

Marc temporal de desplegament



Govern d'Andorra

Gràcies per la vostra atenció