POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Introducció

La informació constitueix un actiu essencial per a les organitzacions, ja que és imprescindible per a la prestació dels serveis que ofereixen. Les tecnologies de la informació i la comunicació (TIC) permeten el seu tractament eficient, però també introdueixen nous riscos.
Per aquest motiu, és necessari establir mesures adequades per protegir la informació i els serveis associats, reduint els riscos a nivells acceptables.
Aquest document estableix la Política de Seguretat de la Informació de l'**Associació de Ciberseguretat de Catalunya (ASCICAT)**, amb l'objectiu que tot el personal i col·laboradors coneguin i apliquin les mesures de seguretat definides.

1. Missió i objectius

ASCICAT adopta un model de gestió de la seguretat alineat amb el Esquema Nacional de Seguretat (ENS), regulat pel Reial decret 311/2022, reconeixent la informació i els sistemes que la suporten com a actius estratègics.
Els objectius principals són:

- Contribuir al compliment de la missió i objectius de l'organització
- Garantir el compliment de la normativa aplicable
- Assegurar la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de la informació
- Garantir la continuïtat dels serveis
- Protegir els actius davant amenaces internes i externes

ASCICAT manté un compromís continu amb la gestió de riscos (metodologia ENS - MAGERIT) i la millora contínua.

2. Abast

Aquesta política s'aplica a tots els actius d'informació i a totes les persones que hi tenen accés.

3. Marc normatiu

La política es basa en:

- Reial decret 311/2022 (Esquema Nacional de Seguretat)
- Reglament (UE) 2016/679 (RGPD)
- Llei Orgànica 3/2018 (Protecció de Dades)
- Llei 34/2002 (LSSI-CE)

4. Organització de la seguretat

ASCICAT defineix els rols següents:

- Responsable de la informació
- Responsable del servei
- Responsable de seguretat
- Responsable del sistema

5. Gestió de riscos

Es realitzen anàlisis de riscos periòdics per identificar amenaces i aplicar mesures adequades.

6. Principis de seguretat

- Seguretat per defecte
- Principi de mínim privilegi
- Protecció de la informació en repòs i en trànsit
- Registre d'activitat
- Control d'interconnexions

7. Control d'accessos

L'accés està limitat a usuaris autoritzats, amb mecanismes d'autenticació i control.

8. Gestió d'incidents

Es disposa de procediments per detectar, analitzar i resoldre incidents de seguretat.

9. Continuïtat del servei

S'implementen mesures de còpia de seguretat i recuperació davant incidents.

10. Relacions amb tercers

Els tercers han de complir les mesures de seguretat establertes per ASCICAT.

11. Millora contínua

ASCICAT revisa i millora contínuament el seu model de seguretat.

Classificació

Aquest document està classificat com a ús públic.