



ORG-01v00

Política de Seguretat



Doc. original signat per:
Alex Tablado Vergara
17/03/2026,
Isaías Táboas Suárez
17/03/2026,
Núria López Rodríguez
19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ



001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
15/06/2026 12:49:43

Pàgina 1 de 23



infraestructures.cat



GESTIÓ DEL DOCUMENT

PREPARAT

NTT DATA

REVISAT

ALEX TABLADO
CAP DE LA GERÈNCIA DE PROJECTES I SERVEIS TIC

APROVAT

ISAÍAS TÁBOAS
PRESIDENT I CONSELLER DELEGAT D'INFRAESTRUCTURES.CAT

CONTROL DOCUMENTAL

NÚRIA LÓPEZ
CAP DE DIVISIÓ DE GABINET TÈCNIC
RESPONSABLE DEL SISTEMA INTEGRAT DE GESTIÓ CORPORATIU (SIGC)

	Doc. original signat per: Alex Tablado Vergara 17/03/2026, Isaías Táboas Suárez 17/03/2026, Núria López Rodríguez 19/03/2026	Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029	Data creació còpia: 15/06/2026 12:49:43
		Original electrònic / Còpia electrònica autèntica	
		CODI SEGUR DE VERIFICACIÓ	Pàgina 2 de 23
			
		001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ	



CONTROL DE VERSIONS

Versió	Data	Pàgines revisades	Contingut de la modificació
00	09/03/2026	-	Creació del document.



Doc. original signat per:
 Alex Tablado Vergara
 17/03/2026,
 Isaias Táboas Suárez
 17/03/2026,
 Núria López Rodríguez
 19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ



001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
 15/06/2026 12:49:43

Pàgina 3 de 23



INDEX

1.	OBJECTIU DEL DOCUMENT	7
2.	TÍTOL PRELIMINAR. ÀMBIT D'APLICACIÓ I DISPOSICIONS GENERALS	8
	Capítol primer. Disposicions comunes	8
	Article 1. Objecte	8
	Article 2. Definicions	8
	Article 3. Abast	8
	Article 4. Àmbit subjectiu d'aplicació	8
	Capítol segon. Missió i marc legal	9
	Article 5. Missió	9
	Article 6. Marc legal	9
3.	TÍTOL PRIMER. PRINCIPIS DE SEGURETAT	10
	Capítol primer. Principis Comuns	10
	Article 7. Accés a la informació	10
	Article 8. Metodologia de seguretat de la informació	10
	Article 9. Mesures de protecció de la informació	11
4.	TÍTOL SEGON. ORGANITZACIÓ DE LA SEGURETAT	13
	Capítol primer. Principis generals	13
	Article 10. Agents rellevants per a la implementació de la Política de Seguretat de la Informació	13



Doc. original signat per:
Alex Tablado Vergara
17/03/2026,
Isaías Táboas Suárez
17/03/2026,
Núria López Rodríguez
19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ



001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
15/06/2026 12:49:43

Pàgina 4 de 23



Article 11. Responsabilitat general i específica	14
Article 12. Resolució de conflictes.....	14
Capítol segon. Figures de naturalesa unipersonal.....	14
Article 13. Responsable de la informació	14
Article 14. Responsable del servei	15
Article 15. Responsable de seguretat.....	15
Article 16. Responsable dels sistemes informàtics	17
Article 17. Administració de seguretat TIC	17
Capítol tercer. Comitè de Seguretat TIC	18
Article 18. Comitè de Seguretat TIC.....	18
Article 19. Funcions del Comitè de Seguretat TIC	18
Article 20. Règim de funcionament del Comitè de Seguretat TIC	19
5. TÍTOL TERCER. DESENVOLUPAMENT I MODIFICACIÓ DE LA POLÍTICA DE SEGURETAT	20
Capítol primer. Instruments de desenvolupament.....	20
Article 21. Desenvolupament normatiu.....	20
Article 22. Nivell A	21
Article 23. Nivell B	21
Article 24. Nivell C	21
Capítol segon. Competències de desenvolupament	22
Article 25. Assignació de competències de desenvolupament.....	22



Doc original signat per:
 Alex Tablado Vergara
 17/03/2026,
 Isaías Táboas Suárez
 17/03/2026,
 Núria López Rodríguez
 19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ

001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
 15/06/2026 12:49:43

Pàgina 5 de 23



Article 26. Instruments de nivell A i B22

Article 27. Instruments de nivell C22

Capítol tercer. Manteniment de la Política i Millora contínua..... 22

Article 28. Actualització permanent22

Article 29. Auditoria i millora contínua23



Doc. original signat per:
 Alex Tablado Vergara
 17/03/2026,
 Isaias Táboas Suárez
 17/03/2026,
 Núria López Rodríguez
 19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ



001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
 15/06/2026 12:49:43

Pàgina 6 de 23



1. OBJECTIU DEL DOCUMENT

El present document estableix la Política de Seguretat de la Informació de l'Organització, d'acord amb el Reial decret 311/2022 (Esquema Nacional de Seguretat), i defineix els principis, l'organització i les directrius generals per protegir la informació i els serveis electrònics.

L'objectiu és garantir, de manera proporcional el risc, la confidencialitat, la integritat, la disponibilitat, l'autenticitat i la traçabilitat de la informació i dels serveis, així com assegurar la continuïtat dels serveis i el compliment de la normativa aplicable (ENS, protecció de dades, transparència i altres obligacions sectorials).

La Política és d'aplicació a tots els sistemes d'informació, serveis i processos que suporten l'activitat d'Infraestructures.cat, inclosos els recursos externalitzats o gestionats per tercers quan tractin informació o prestin serveis per compte d'Infraestructures.cat.

Aquesta Política constitueix el marc de referència per al desplegament de les Normes, Procediments Operatius i Guies de Seguretat (nivells A, B i C), així com per a l'anàlisi i gestió de riscos i la categorització de sistemes.

La Direcció i el Comitè de Seguretat TIC es comprometen a dotar a Infraestructures.cat dels recursos necessaris, promoure la formació i la conscienciació, i impulsar la millora contínua del sistema de gestió de seguretat de la informació.

Qualsevol persona usuària, empleada o col·laboradora que utilitzi o tingui accés als sistemes d'informació d'infraestructures.cat ha de conèixer i complir aquesta Política i la normativa que la desplega.

	Doc. original signat per: Alex Tablado Vergara 17/03/2026, Isaías Táboas Suárez 17/03/2026, Núria López Rodríguez 19/03/2026	Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029	Data creació còpia: 15/06/2026 12:49:43
	Original electrònic / Còpia electrònica autèntica CODI SEGUR DE VERIFICACIÓ 		Pàgina 7 de 23
001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ			



2. TÍTOL PRELIMINAR. ÀMBIT D'APLICACIÓ I DISPOSICIONS GENERALS

Capítol primer. Disposicions comunes

ARTICLE 1. OBJECTE

1. El present reglament té per objecte definir i regular, a l'àmbit d'Infraestructures.cat, la Política de Seguretat aplicable als sistemes d'informació que intervinguin en la recollida, processament, tractament, emmagatzemament i difusió de la informació que resulti necessària per a l'exercici de les seves competències.
2. El manteniment i gestió de la seguretat dels sistemes d'informació va intrínsecament lligat a l'establiment d'una organització de seguretat.
3. Aquesta organització s'estableix mitjançant la identificació i definició de les diferents activitats i responsabilitats en matèria de gestió de la seguretat dels sistemes d'informació i la implantació d'una estructura que els doni suport.

ARTICLE 2. DEFINICIONS

Als efectes de la present disposició, s'entendrà per:

- **SGSI:** sistema de gestió de seguretat de la informació.
- **Visita:** Presència motivada per amicitat, cortesia fins promocionals, comercials, científics o culturals, de durada escassa no superior a la jornada laboral.
- **Persona autoritzada:** Presència facultada per accedir als locals d'Infraestructures.cat.
- **DVD:** Digital Versàtil Disk. Disc òptic per emmagatzemar dades.

ARTICLE 3. ABAST

Aquesta Política s'aplica a tots els sistemes informàtics que siguin titularitat d'Infraestructures.cat segons la gestió o responsabilitat que tingui encomanada. Quan la titularitat, gestió o responsabilitat de la informació correspongui a Infraestructures.cat i aquesta es trobi o es tracti en entorns aliens, Infraestructures.cat o ens que en depenen exigiran les mateixes garanties i requisits que les determinades a la present Política.

ARTICLE 4. ÀMBIT SUBJECTIU D'APLICACIÓ

Les presents disposicions són d'aplicació a tot el personal d'Infraestructures.cat, així com als ens dependents que adoptaran les presents prescripcions.



Doc. original signat per:
Alex Tablado Vergara
17/03/2026,
Isaías Táboas Suárez
17/03/2026,
Núria López Rodríguez
19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ



001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
15/06/2026 12:49:43

Pàgina 8 de 23



Capítol segon. Missió i marc legal

ARTICLE 5. MISSIÓ

Infraestructures.cat és un ens integrant del sector públic de la Generalitat de Catalunya, amb personalitat jurídica pròpia i capacitat funcional plena per l'assoliment de les seves funcions amb sotmetiment a les lleis i als tribunals, les competències de la qual estan identificades a l'article 2.1 dels seus Estatuts.

La missió d'aquesta Política de Seguretat de la Informació (PSI) és establir el marc de govern i les directrius necessàries per protegir la informació i els serveis de l'organització, garantint el compliment del Reial decret 311/2022 (ENS) i de la normativa aplicable, inclosa la de protecció de dades personals, així com els requisits legals, contractuals i interns.

ARTICLE 6. MARC LEGAL

Infraestructures.cat és una persona jurídica de caràcter privat que forma part de l'administració pública i duu a terme les competències que li són pròpies i les que té encomanades amb ple sotmetiment a l'ordenament jurídic en general, i en especial en la utilització de mitjans tecnològics per al desenvolupament de les seves activitats, li són d'especial aplicació:

- 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 311/2022 de 3 de maig de l'Esquema Nacional de Seguretat.
- Les guies de seguretat del CCN que desenvolupen l'ENS, en particular, la CCN-STIC-805 sobre política de seguretat de la informació.
- Reial Decret 4/2010 de 8 de gener de l'Esquema Nacional d'Interoperabilitat.
- Reial Decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics.
- Decret 76/2020, de 4 d'agost, d'Administració digital.
- Llei 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya.
- Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.
- Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personal i garantia dels drets digitals o LOPDGDD.
- Llei 19/2014, del 29 de desembre, de transparència, accés a la informació pública i bon govern i Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern.
- Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades o RGPD.

	Doc. original signat per: Alex Tablado Vergara 17/03/2026, Isaías Táboas Suárez 17/03/2026, Núria López Rodríguez 19/03/2026	Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029	Data creació còpia: 15/06/2026 12:49:43
	Original electrònic / Còpia electrònica autèntica CODI SEGUR DE VERIFICACIÓ 	001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ	Pàgina 9 de 23



3. TÍTOL PRIMER. PRINCIPIS DE SEGURETAT

Capítol primer. Principis Comuns

ARTICLE 7. ACCÉS A LA INFORMACIÓ

1. L'accés a la informació es regirà pels següents principis:
 - 1.1. Mínim privilegi. Els privilegis de cada persona usuària es reduiran al mínim estrictament necessari per a complir les seves obligacions.
 - 1.2. Necessitat de conèixer. Els privilegis de cada persona usuària es limitaran de forma que només tindran el coneixement d'aquella informació requerida per a complir les seves obligacions.
 - 1.3. Capacitat d'autoritzar. Sols i exclusivament el personal amb la competència atribuïda podrà concedir, alterar o anul·lar l'autorització d'accés als recursos, conforme als criteris establerts pel seu responsable.
2. Als efectes de la present Política de seguretat la informació es classificarà segons els següents graus, en ordre decreixent de restricció:
 - 2.1. Confidencial. Documentació accessible únicament als seus autors i a les persones amb privilegis d'accés a informació confidencial.
 - 2.2. Restringida. Documentació accessible únicament a les persones que pertanyen a àrees que tenen competència sobre els processos de negoci associats.
 - 2.3. Lliure accés. Documentació accessible a qualsevol membre de l'organització.
 - 2.4. Accés Públic. Documentació pública, accessible a qualsevol persona de dins o fora de l'organització.
3. Als efectes de la present Política de seguretat la informació de caràcter personal es classificarà en informació sensible o no d'acord amb l'article 9 del RGPD i de la LOPDGDD.

ARTICLE 8. METODOLOGIA DE SEGURETAT DE LA INFORMACIÓ

1. D'acord amb el Reial decret 311/2022 i, en particular, amb els seus annexos I (principis i requisits mínims) i II (mesures de seguretat), per a complir amb els principis bàsics i requisits mínims establerts, s'aplicaran les mesures de seguretat proporcionals a:
 - 1.1. Les dimensions de seguretat rellevants del sistema a protegir.
 - 1.2. La categoria del sistema d'informació a protegir.
2. Per tal de determinar les mesures de seguretat es seguiran els passos següents:
 - 2.1. Identificació i inventari dels actius d'informació existents.
 - 2.2. Anàlisi de riscos per a cada actiu en cadascuna de les cinc dimensions de seguretat.
 - 2.3. Classificació dels actius en funció del seu nivell de risc.



Doc. original signat per:
 Alex Tablado Vergara
 17/03/2026,
 Isaías Táboas Suárez
 17/03/2026,
 Núria López Rodríguez
 19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ

001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
 15/06/2026 12:49:43

Pàgina 10 de 23



- 2.4. Declaració d'aplicabilitat dels diferents controls previstos a l'Annex II en funció de cada actiu i dimensió.
- 2.5. Implementació dels controls.
- 2.6. Auditoria i millora continua.



Quan els actius, serveis o processos impliquin tractament de dades personals, l'anàlisi de riscos integrarà també els riscos per als drets i llibertats de les persones físiques, d'acord amb el RGPD i la LOPDGDD, i s'establiran mesures específiques de seguretat i privacitat.

Quan correspongui, es faran Avaluacions d'Impacte relatives a la Protecció de Dades (AIPD) i es consultarà el/la Delegat/Delegada de Protecció de Dades. Els registres d'activitats de tractament, els encàrrecs de tractament i la gestió de bretxes de dades personals s'alinearàn amb els procediments de seguretat i de gestió d'incidents.

- 3. La classificació del nivell de risc d'un sistema es basa en la valoració de l'impacte que tindria sobre Infraestructures.cat un incident que afecti la seguretat de la informació o dels sistemes. En aquest sentit, es tindran en compte les següents dimensions de seguretat per tal de determinar l'impacte:
 - 3.1. Disponibilitat
 - 3.2. Autenticitat
 - 3.3. Integritat
 - 3.4. Confidencialitat
 - 3.5. Traçabilitat
- 4. A més, com és d'esperar, s'observaran els següents principis bàsics recollits a l'Esquema Nacional de Seguretat (Annex I, articles 5 al 10):
 - 4.1. La seguretat com un procés integral.
 - 4.2. Gestió de la seguretat basada en els riscos.
 - 4.3. Prevenció, reacció i recuperació.
 - 4.4. Línies de defensa.
 - 4.5. Reavaluació periòdica.
 - 4.6. La seguretat com una funció diferenciada.

ARTICLE 9. MESURES DE PROTECCIÓ DE LA INFORMACIÓ

- 1. La informació classificada, regulada per la seva normativa específica, constitueix el principal actiu crític d'informació a les administracions. El seu tractament pels sistemes informàtics, requerirà l'aplicació de mesures de seguretat específiques.
- 2. Als actius d'informació d'Infraestructures.cat que no són informació classificada, ni es refereixen a activitats que pugui desenvolupar Infraestructures.cat en règim de dret privat, se'ls aplicaran les mesures de seguretat establertes en el Reial Decret 311/2022, de 3 de maig, pels que es regula

	Doc. original signat per: Alex Tablado Vergara 17/03/2026, Isaías Táboas Suárez 17/03/2026, Núria López Rodríguez 19/03/2026	Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029	Data creació còpia: 15/06/2026 12:49:43
	Original electrònic / Còpia electrònica autèntica CODI SEGUR DE VERIFICACIÓ		Pàgina 11 de 23
			
		001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ	



l'Esquema Nacional de Seguretat i a la seva normativa i guies de desplegament aplicables en l'àmbit de l'Administració Electrònica.

3. En funció de la naturalesa dels actius d'informació, els tipus de seguretat correspondran a:
 - 1.1. Protecció de les instal·lacions i infraestructures.
 - 1.2. Gestió del personal.
 - 1.3. Protecció dels equips.
 - 1.4. Protecció de les comunicacions.
 - 1.5. Protecció dels suports informàtics.
 - 1.6. Protecció de les aplicacions informàtiques.
 - 1.7. Protecció de la informació.
 - 1.8. Protecció dels serveis.

4. Les mesures de protecció de la informació es sotmetran a un procés de gestió basat en riscos, tal com s'expressa a l'article 14, així com es regiran pels següents principis:
 - 4.1. **Seguretat per defecte.** Els sistemes d'informació han de ser sotmesos a un procés d'anàlisi i configuració inicial, previ a la seva posada en producció, pel qual siguin considerats segurs sense que comptin amb errors coneguts i garanteixin que només el personal autoritzat podrà accedir-hi per a exercir les funcions que tinguin atribuïdes, així com donaran resposta a les funcionalitats estrictament necessàries per a la prestació dels serveis i l'exercici de les funcions d'Infraestructures.cat.
 - 4.2. **Seguretat des del disseny.** Els aspectes de seguretat es consideren en el moment de definició del servei prestat o procediment executat per Infraestructures.cat en l'exercici de les seves funcions, així com dels sistemes que hi donaran suport.
 - 4.3. **Mínima funcionalitat.** Sols estaran disponibles les funcions, protocols i serveis necessaris per a l'acompliment del requisit operacional o funcional del sistema.
 - 4.4. **Minimització de dades.** Els sistemes d'informació permetran gestionar només aquella informació necessària per a la prestació dels serveis per als quals s'han previst i serà proporcional a la finalitat perseguida per la prestació dels serveis.
 - 4.5. **Defensa en Profunditat.** Les mesures de protecció hauran d'implementar-se en la mesura del possible en diversos components, nivells o capes, i en la màxima extensió, de manera que no hi hagi una única línia (o component) de defensa.
 - 4.6. **Millora continua.** Les mesures de seguretat se sotmeten a un procés de definició, implantació i revisió per tal d'identificar i implementar possibles correccions necessàries perquè assegurin la seguretat de la informació i dels serveis i procediments dels quals és responsable Infraestructures.cat d'acord amb la seva naturalesa, abast, context i finalitat, així com de l'estat de la tècnica en cada moment.



Doc original signat per:
Alex Tablado Vergara
17/03/2026,
Isaías Táboas Suárez
17/03/2026,
Núria López Rodríguez
19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ



001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
15/06/2026 12:49:43

Pàgina 12 de 23



4. TÍTOL SEGON. ORGANITZACIÓ DE LA SEURETAT

Capítol primer. Principis generals

ARTICLE 10. AGENTS RELLEVANTS PER A LA IMPLEMENTACIÓ DE LA POLÍTICA DE SEURETAT DE LA INFORMACIÓ

1. Aquesta Política de Seguretat diferencia entre quatre figures clau:
 - 1.1. **Responsable de la informació** és la persona o òrgan dins de l'organització que té la propietat de les dades d'un sistema d'informació en concret i la responsabilitat sobre la seva correcta utilització i explotació.
 - 1.2. **Responsable de seguretat** és la persona que ha de determinar les decisions per satisfer els requisits de seguretat de la informació i dels serveis.
 - 1.3. **Responsable dels sistemes informàtics** és la persona que s'encarrega de l'explotació del sistema d'informació des de la perspectiva de la seguretat de la informació.
 - 1.4. **Responsable dels serveis** és la persona o òrgan responsable de definir les funcions i els usos a què està destinada aquesta informació i els requisits funcionals que han de complir els serveis que l'exploten.
2. La persona responsable de seguretat no pot assumir la responsabilitat de cap dels altres rols.
3. Les activitats i l'estratègia de seguretat seran coordinades a través de l'estratègia d'un Comitè pluridisciplinari denominat Comitè de Seguretat TIC.

DESIGNACIÓ, RENOVACIÓ I SUBSTITUCIÓ DE ROLS ENS

La designació dels rols ENS (Responsable de la informació, Responsable del servei, Responsable dels sistemes informàtics i Responsable de seguretat) es formalitza mitjançant resolució o acord del Comitè de Seguretat TIC i queda registrada en un llistat de rols i responsabilitats, mantingut per la persona Responsable de seguretat.

Les designacions s'han de revisar com a mínim anualment i sempre que hi hagi canvis organitzatius, canvis rellevants en els serveis/sistemes o canvis en el nivell de risc. Qualsevol cessament, substitució o delegació s'ha de documentar i comunicar a les persones interessades.

En absència temporal d'un responsable, s'establirà un substitut designat per escrit per garantir la continuïtat de les funcions.

DESIGNACIÓ ACTUAL DELS ROLS

- **Responsable de la informació (RI):** Direcció Adjunta a Presidència.
- **Responsable de seguretat (RSeg):** Cap de la Gerència de Projectes i Serveis TIC.
- **Responsable dels sistemes informàtics (RSis):** Adjudicatari del servei de sistemes i ciberseguretat.
- **Responsable del servei (RSv):** Comitè de Direcció.



Doc original signat per:
Alex Tablado Vergara
17/03/2026,
Isaías Táboas Suárez
17/03/2026,
Núria López Rodríguez
19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ

001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
15/06/2026 12:49:43

Pàgina 13 de 23



ARTICLE 11. RESPONSABILITAT GENERAL I ESPECÍFICA

1. El conjunt de persones usuàries dels sistemes d'informació d'Infraestructures.cat són responsables de la seguretat d'aquests mitjançant el seu ús correcte, així com de la seguretat de la informació i de les dades de caràcter personal que gestionin, sempre d'acord amb les seves atribucions professionals.
2. Això no obstant, el manteniment i gestió de la seguretat dels sistemes d'informació van íntimament lligats a l'establiment d'una organització. Aquesta organització s'estableix mitjançant la identificació i definició de diferents activitats en matèria de seguretat de la informació i l'establiment de responsabilitats per a la seva realització, i amb la implantació d'una estructura organitzativa que els doni suport.

ARTICLE 12. RESOLUCIÓ DE CONFLICTES

Els conflictes de competències entre els diferents agents que componen l'estructura organitzativa, els resoldrà el Comitè de Seguretat TIC. En cas de decisions a prendre de forma urgent o imminent, prevaldrà la decisió de la persona Responsable de Seguretat, que donarà compte de la seva decisió al Comitè de Seguretat TIC quan aquest es reuneixi.

Capítol segon. Figures de naturalesa unipersonal

ARTICLE 13. RESPONSABLE DE LA INFORMACIÓ

1. Responsable de la informació és la persona qui té la potestat de determinar les característiques de la informació, a efecte d'establir els requisits en matèria de seguretat de la informació.
2. A la persona Responsable de la informació li correspon:
 - 1.1. La valoració de la informació en totes les dimensions de seguretat -disponibilitat, integritat, confidencialitat, traçabilitat i autenticitat- tenint en compte la naturalesa d'aquesta informació i la normativa que pugui ser-li d'aplicació.
 - 1.2. L'anàlisi de riscos de la informació que li competeixi, així com l'aprovació de la categorització del sistema d'informació i la declaració d'aplicabilitat de controls que proposi la persona responsable de seguretat.
 - 1.3. La responsabilitat última de la protecció de la informació respecte a l'ús que en facin les persones a càrrec seu, o les que depenguin de la seva direcció, o en general, les persones que estiguin autoritzades a accedir a la informació.
 - 1.4. La propietat dels riscos sobre la informació.
 - 1.5. Acceptar el risc residual sobre la informació de la qual és responsable.
 - 1.6. Autoritzar els accessos de les persones usuàries a la informació, respectant els principis de mínim privilegi i necessitat de conèixer establerts a la present Política.



Doc original signat per:
 Alex Tablado Vergara
 17/03/2026,
 Isaías Táboas Suárez
 17/03/2026,
 Núria López Rodríguez
 19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ

001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
 15/06/2026 12:49:43

Pàgina 14 de 23



- 1.7. La responsabilitat última del compliment de totes les garanties establertes per la legislació i la normativa interna d'Infraestructures.cat, especialment pel que fa a informació que contingui dades de caràcter personal.
- 1.8. La responsabilitat última de qualsevol error o negligència que derivi en un incident de seguretat en qualsevol de les seves dimensions, motivat per no atendre amb la deguda diligència el deure de vetlla del compliment de les mesures de seguretat establertes.
3. El Comitè de Seguretat TIC determinarà qui és la persona Responsable de la Informació per a cada sistema.

ARTICLE 14. RESPONSABLE DEL SERVEI

1. Responsable del servei és la persona qui té la potestat d'establir les característiques d'un servei, a l'efecte de determinar els requisits en matèria de seguretat i de la informació.
2. A la persona Responsable del servei li correspon:
 - 2.1. La valoració del servei en totes les dimensions de seguretat -disponibilitat, integritat, confidencialitat, traçabilitat i autenticitat- tenint en compte la naturalesa del servei i la normativa que pugui ser-li d'aplicació.
 - 2.2. L'anàlisi de riscos del servei que li competeixi, així com l'aprovació de la categorització del sistema d'informació i la declaració d'aplicabilitat de controls que proposi la persona responsable de seguretat.
 - 2.3. La propietat dels riscos sobre els serveis.
 - 2.4. L'acceptació del risc residual sobre els serveis que siguin de la seva competència.
3. Les persones Responsables dels serveis es determinaran en funció de les competències atribuïdes a cada àrea o departament en funció de l'organigrama corporatiu.

ARTICLE 15. RESPONSABLE DE SEGURETAT

1. La persona Responsable de seguretat és el màxim responsable de la seguretat dels sistemes d'informació d'Infraestructures.cat, sent qui determina i supervisa les mesures de seguretat que han de ser implantades d'acord amb la valoració dels serveis i de la informació per les persones responsables dels serveis i de la informació, respectivament.
2. Atès el principi de "la seguretat com a funció diferenciada", la figura Responsable de seguretat és independent de Responsable del sistema, Responsable del servei i Responsable de la informació.
3. Pel millor acompliment de les funcions relacionades amb les mesures de seguretat implantades, i especialment, per raons de complexitat o immediatesa, la persona Responsable de seguretat podrà delegar determinats aspectes de les seves funcions a altres persones de l'organització. En aquests supòsits, les diferents persones responsables de seguretat delegats actuaran ajustant-se estrictament al contingut de la delegació, la qual recollirà l'abast material i temporal, les obligacions i responsabilitats



Doc. original signat per:
Alex Tablado Vergara
17/03/2026,
Isaías Táboas Suárez
17/03/2026,
Núria López Rodríguez
19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ

001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
15/06/2026 12:49:43

Pàgina 15 de 23



de les tasques delegades. De les possibles delegacions haurà d'informar-se al Comitè de Seguretat TIC.

4. Seran funcions de la persona Responsable de seguretat:
 - 4.1. Actuar com a Secretari/a del Comitè de Seguretat TIC.
 - 4.2. Proposar a la persona President/a del Comitè de Seguretat TIC la convocatòria del Comitè, definint l'ordre del dia i recopilant la informació pertinent.
 - 4.3. Ser responsable, juntament amb els diferents responsables de seguretat delegats, d'estar al cas dels canvis normatius que puguin afectar directament o indirectament, a la seguretat dels sistemes d'informació d'Infraestructures.cat, alertant al Comitè de Seguretat TIC i proposant les accions oportunes per l'adequació al nou marc normatiu.
 - 4.4. A la persona responsable de seguretat li correspon donar suport en l'avaluació de riscos que comet als Responsables de la informació i el servei, i formular proposta de categorització dels sistemes d'informació i de declaració de l'aplicabilitat dels controls.
 - 4.5. Definir els procediments operatius de seguretat de la informació.
 - 4.6. Dur a terme periòdicament auditories per avaluar el compliment de la normativa sobre seguretat i l'efectivitat de les mesures adoptades.
 - 4.7. Ser la persona responsable de la presa de decisions dia a dia en matèria de seguretat de la informació entre les reunions del Comitè de Seguretat TIC. Aquestes decisions respectaran els principis d'unitat d'acció i coordinació d'actuacions en general i, si escau, s'elevaran al Comitè de Seguretat TIC mitjançant la convocatòria extraordinària d'aquest.
 - 4.8. Promoure la formació i conscienciació en matèria de seguretat de la informació a les persones implicades en l'ús de la informació i la prestació dels serveis protegits.
 - 4.9. Informar el Comitè de Seguretat TIC de:
 - Un resum consolidat d'actuacions en matèria de seguretat,
 - Un resum consolidat d'incidents relatius a la seguretat de la informació,
 - L'estat de la seguretat del sistema, en particular del risc residual al que el sistema està exposat.
 - 4.10. Informar a la persona Responsable del servei de les decisions i incidents en matèria de seguretat que afectin el servei del qual és responsable, en particular de l'estimació de risc residual i de les desviacions significatives de risc respecte als marges aprovats.
 - 4.11. Informar a la persona Responsable de la informació de les decisions i incidents en matèria de seguretat que afectin la informació de la qual és responsable, en particular de l'estimació de risc residual i de les desviacions significatives de risc respecte als marges aprovats.
 - 4.12. I qualsevol altra tasca que li sigui encomanada per la present Política i pel Comitè de Seguretat TIC d'Infraestructures.cat.



Doc. original signat per:
Alex Tablado Vergara
17/03/2026,
Isaías Táboas Suárez
17/03/2026,
Núria López Rodríguez
19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ



001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
15/06/2026 12:49:43

Pàgina 16 de 23



ARTICLE 16. RESPONSABLE DELS SISTEMES INFORMÀTICS

1. En matèria de seguretat de la informació, correspondrà a la persona Responsable dels sistemes informàtics:
 - 1.1. Tenir en compte la Política de seguretat i els procediments que la desenvolupin, en les seves tasques naturals de desenvolupament, operació i manteniment dels sistemes informàtics.
 - 1.2. Tenir en compte la Política de seguretat a l'hora de contractar serveis externs i especificar-ne els requisits, imposant a les empreses proveïdores les obligacions corresponents.
 - 1.3. Definir l'estratègia de gestió dels sistemes d'informació i l'arquitectura d'aplicacions i sistemes tenint en compte els principis d'aquesta política i els procediments que la desenvolupen.
 - 1.4. Assegurar-se que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.
 - 1.5. Acordar la suspensió del tractament d'una certa informació o la prestació d'un determinat servei si s'assabenta de deficiències greus de seguretat que poguessin afectar a la satisfacció dels requisits establerts. Aquesta decisió haurà de ser acordada amb la persona Responsable de la informació afectada, del servei afectat i amb la persona Responsable de seguretat abans de ser executada.
2. La persona Responsable dels sistemes informàtics informa a la persona Responsable de seguretat:
 - 2.1. De les actuacions en matèria de seguretat, en particular de tot el relatiu a decisions d'arquitectura del sistema.
 - 2.2. El resum consolidat dels incidents de seguretat.
 - 2.3. De l'eficàcia de les mesures de protecció que estiguin implantades.

ARTICLE 17. ADMINISTRACIÓ DE SEGURETAT TIC

1. La funció d'Administració de seguretat TIC és responsable de la implantació, gestió i manteniment de les mesures de seguretat aplicables als sistemes informàtics i de comunicacions.
2. Tindrà aquest rol l'empresa que tingui adjudicats els serveis d'administració de sistemes i suport a les persones usuàries.
3. Correspondrà a la figura d'Administració de Seguretat TIC:
 - 3.1. La implementació, gestió i manteniment de les mesures de seguretat aplicables.
 - 3.2. La gestió, configuració i actualització, si escau, del maquinari i programari en els que es basen els mecanismes i serveis de seguretat del sistema d'informació.
 - 3.3. La gestió de les autoritzacions concedides a les persones usuàries del sistema, en particular al Sistema d'Informació.



Doc. original signat per:
 Alex Tablado Vergara
 17/03/2026,
 Isaías Táboas Suárez
 17/03/2026,
 Núria López Rodríguez
 19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ

001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
 15/06/2026 12:49:43

Pàgina 17 de 23



- 3.4. L'aplicació dels Procediments Operatius de Seguretat de la informació.
- 3.5. Cal assegurar que els controls de seguretat establerts s'apliquen estrictament.
- 3.6. Aplicar els procediments de seguretat aprovats i proposar-ne millores i ampliacions encaminades a garantir la seguretat de la informació.
- 3.7. Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
- 3.8. Mantenir actualitzats els sistemes d'informació en matèria de seguretat de la informació.
- 3.9. Monitorar l'estat de seguretat del sistema, proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica implementats al sistema.
- 3.10. Informar a les persones Responsables de la seguretat i del sistema de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
- 3.11. Col·laborar en la investigació i resolució d'incidents de seguretat, des de la seva detecció fins a la seva resolució.

Capítol tercer. Comitè de Seguretat TIC

ARTICLE 18. COMITÈ DE SEGURETAT TIC

1. Es crea el Comitè de Seguretat TIC d'Infraestructures.cat, com un òrgan col·legiat de caràcter horitzontal (les persones participants hi intervenen en peu d'igualtat, independentment del seu lloc a l'organigrama), que es regirà en el seu funcionament per aquesta Política.
2. El Comitè de Seguretat TIC és l'òrgan que gestiona i coordina la seguretat dels sistemes informàtics a Infraestructures.cat.
3. El Comitè de Seguretat TIC està format per:
 - 3.1. **Responsable de la informació**, que presidirà el Comitè de Seguretat TIC.
 - 3.2. **Responsable de seguretat**, que serà el/la secretari/a del Comitè de Seguretat TIC.
 - 3.3. **Responsable dels sistemes informàtics**.
 - 3.4. **Responsable dels serveis**.

ARTICLE 19. FUNCIONS DEL COMITÈ DE SEGURETAT TIC

1. El Comitè de Seguretat TIC desenvoluparà les següents funcions:
 - 1.1. Coordinar totes les funcions de seguretat i en particular, resoldre els conflictes de competència que poguessin sorgir entre els diferents responsables i/o entre diferents àrees d'Infraestructures.cat.
 - 1.2. Vetllar pel compliment de la normativa d'aplicació legal, regulatòria i sectorial amb impacte en la seguretat de la informació.



Doc original signat per:
Alex Tablado Vergara
17/03/2026,
Isaías Táboas Suárez
17/03/2026,
Núria López Rodríguez
19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ

001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
15/06/2026 12:49:43

Pàgina 18 de 23



- 1.3. Proposar les modificacions o revisions de la present Política de Seguretat que consideri oportunes, donant trasllat de les mateixes per la seva presa en consideració.
- 1.4. Aprovar la normativa de seguretat de la informació proposada per la persona Responsable de seguretat.
- 1.5. Recollir de la persona Responsable de seguretat informes regulars de l'estat de la seguretat de l'Organització i dels possibles incidents i proposar mesures encaminades a la millora de la seguretat.
- 1.6. Coordinar i donar resposta a les qüestions plantejades per la persona Responsable de seguretat, així com prendre raó de les decisions adoptades per aquest en el desenvolupament de les seves funcions.
- 1.7. Aprovar les propostes d'activitats formatives necessàries per al personal de l'empresa en l'àmbit de la seguretat, canalitzades per la persona Responsable de seguretat.
- 1.8. Vetllar per la disponibilitat de recursos per atendre les necessitats de seguretat dels sistemes d'informació, promovent inversions de caràcter horitzontal.
- 1.9. Monitorar el desenvolupament dels processos de gestió d'incidents de seguretat i recomanar possibles actuacions al respecte. En particular, vetllar per la coordinació de les diferents àrees de seguretat en la gestió d'incidents de seguretat de la informació.
- 1.10. Prioritzar les actuacions en matèria de seguretat quan els recursos siguin limitats.
- 1.11. Promoure la millora continua del sistema de gestió de la seguretat de la informació.
- 1.12. Qualsevol altra responsabilitat que li sigui encarregada per la present Política de Seguretat de la informació o per la Direcció d'Infraestructures.cat.

ARTICLE 20. RÈGIM DE FUNCIONAMENT DEL COMITÈ DE SEGURETAT TIC

1. El Comitè de seguretat TIC es reunirà amb caràcter ordinari, almenys una vegada per trimestre i amb caràcter extraordinari sempre que ho requereixi algun dels seus membres o en atenció als incidents de seguretat que succeeixin.
2. Les reunions tindran lloc dins de la jornada de treball d'Infraestructures.cat.
3. Per raons d'urgència podrà reunir-se sempre que la Presidència del Comitè ho estimi convenient, inclús fora de la jornada de treball habitual.
4. El Comitè podrà acordar la incorporació de persones expertes en les diferents matèries, l'elaboració d'estudis, informes i dur a terme qualsevol altra gestió que la seva complexitat tècnica ho requereixi.
5. El Comitè de seguretat TIC podrà regular el seu propi règim de funcionament, el qual haurà de respectar, en qualsevol cas, el dispostat a la present disposició i la normativa que resulti d'aplicació.



Doc original signat per:
 Alex Tablado Vergara
 17/03/2026,
 Isaías Táboas Suárez
 17/03/2026,
 Núria López Rodríguez
 19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ

001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
 15/06/2026 12:49:43

Pàgina 19 de 23

5. TÍTOL TERCER. DESENVOLUPAMENT I MODIFICACIÓ DE LA POLÍTICA DE SEGURETAT

Capítol primer. Instruments de desenvolupament

ARTICLE 21. DESENVOLUPAMENT NORMATIU

1. El desenvolupament de la present Política es durà a terme mitjançant instruments pertanyents als tres nivells, anomenats:
 - a. A. Normes de Seguretat.
 - b. B. Procediments Operatius de Seguretat.
 - c. C. Guies de Seguretat.
2. Quan s'aprovi un instrument de desenvolupament haurà d'especificar-se a quin nivell pertany.

GESTIÓ I ACCÉS A LA DOCUMENTACIÓ DE SEGURETAT

La documentació de seguretat (Política, Normes, Procediments, Guies, inventari d'actius, anàlisi i tractament del risc, Declaració d'Aplicabilitat, registres d'incidents, informes d'auditoria i evidències associades) es mantindrà en un repositori corporatiu centralitzat amb control de versions i còpies de seguretat.



L'accés al repositori estarà restringit d'acord amb el principi de necessitat de conèixer i el mínim privilegi. Com a mínim hi tindran accés la persona Responsable de seguretat i les persones Responsables dels sistemes informàtics, responsables del servei i de la informació hi accediran quan sigui necessari per a les seves funcions. L'accés i les modificacions quedaran registrats.

La Política i les Normes de Seguretat vigents es difondran a tot el personal mitjançant els canals interns establerts, i s'assegurarà que el personal de tercers amb accés als sistemes en conegui el contingut i assumeixi el compromís de compliment.

REFERÈNCIA ALS REQUISITS MÍNIMS I DOCUMENTACIÓ DE DESPLEGAMENT (ENS)

Sense perjudici del desenvolupament detallat mitjançant instruments de nivell A/B/C, els següents àmbits han d'estar coberts com a mínim per normes, procediments o guies específiques, d'acord amb l'ENS (art. 12.6 RD 311/2022):

- Gestió d'actius, inventari i categorització de sistemes.
- Anàlisi i tractament del risc (inclosa la Declaració d'Aplicabilitat).
- Control d'accés, gestió d'identitats i privilegis.
- Registre d'activitat, monitoratge i gestió d'esdeveniments de seguretat.
- Gestió d'incidents de seguretat i notificació de bretxes (incloses bretxes de dades personals).
- Continuitat del servei i recuperació davant desastres.
- Gestió de canvis, configuració, vulnerabilitats i actualitzacions.

	Doc. original signat per: Alex Tablado Vergara 17/03/2026, Isaías Táboas Suárez 17/03/2026, Núria López Rodríguez 19/03/2026	Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029	Data creació còpia: 15/06/2026 12:49:43
	Original electrònic / Còpia electrònica autèntica CODI SEGUR DE VERIFICACIÓ		Pàgina 20 de 23
		 001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ	



- Contractació i gestió de les empreses proveïdores/tercers amb requisits de seguretat.
- Còpies de seguretat i restauració.
- Formació i conscienciació en seguretat de la informació

ARTICLE 22. NIVELL A

1. Pertanyen al nivell A, les Normes de Seguretat, conformades pel conjunt de regles i directrius de caràcter obligatori que desenvolupen directament el contingut de la present Política o traslladen a l'ordre intern, mitjançant les corresponents normes, el compliment de la normativa legal aplicable en la matèria.
2. S'integrarà en aquest nivell qualsevol normativa interna relacionada amb la seguretat que la persona Responsable de la Seguretat elabori i consideri necessària per complir els objectius exposats a l'article anterior, i que sigui aprovada pel Comitè de Seguretat TIC.

ARTICLE 23. NIVELL B

1. Pertanyen a aquest nivell els anomenats Procediments Operatius de Seguretat, constituïts pel conjunt de procediments tècnics de caràcter obligatori orientats a resoldre les tasques, processos de treball o modes d'actuació considerats més rellevants atenent el perjudici que causaria una actuació inadequada de seguretat, desenvolupament, manteniment o explotació dels sistemes d'informació o per venir imposats per la normativa aplicable.
2. S'integraran en aquest nivell qualsevol procediment relacionat amb l'àmbit de la seguretat que la persona Responsable del Sistema elabori i consideri necessària per complir els objectius exposats en el present article, i que sigui aprovada per la mateixa persona Responsable de Seguretat.

ARTICLE 24. NIVELL C

1. Pertanyen al nivell C les anomenades Guies de Seguretat, formades pel conjunt de recomanacions i especificacions tècniques i jurídiques, de caràcter interpretatiu o orientatiu, destinades a il·lustrar amb més grau de detall o a fixar posicions, respecte aspectes concrets de la seguretat. El seu objectiu últim és el d'ajudar a la correcta aplicació de les normes i procediments recollits en els nivells A i B, o a complementar el seu contingut, així com a complementar el seu contingut, contribuint a una millor informació i difusió d'aquestes.
2. S'integren en aquest nivell:
 - a. Les Guies Tècniques de Seguretat.
 - b. Els Manuals, informes, monografies, quaderns, estudis tècnics i recomanacions.



Doc. original signat per:
 Alex Tablado Vergara
 17/03/2026,
 Isaías Táboas Suárez
 17/03/2026,
 Núria López Rodríguez
 19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ

001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
 15/06/2026 12:49:43

Pàgina 21 de 23



Capítol segon. Competències de desenvolupament

ARTICLE 25. ASSIGNACIÓ DE COMPETÈNCIES DE DESENVOLUPAMENT

Les competències per l'elaboració i aprovació dels instruments de desenvolupament de la present Política s'assignen en funció dels diferents nivells en què s'enquadren, de conformitat amb el Títol segon de la Política de Seguretat.

ARTICLE 26. INSTRUMENTS DE NIVELL A I B

1. La competència per l'aprovació de les Normes de Seguretat correspon al Comitè de Seguretat TIC, a proposta de la persona Responsable de Seguretat.
2. La competència per l'aprovació dels Procediments operatius de Seguretat correspon a la persona Responsable de Seguretat i es donarà compte al Comitè de Seguretat TIC
3. La persona Responsable de Seguretat, la persona Responsable dels sistemes informàtics o la figura d'Administració de Seguretat TIC, cadascun en el marc de les seves competències, formularan les propostes que considerin més adequades per al desenvolupament de les normatives de nivell A i B.

ARTICLE 27. INSTRUMENTS DE NIVELL C

Correspon a la persona Responsable de Seguretat, a la persona Responsable dels sistemes informàtics o a la figura d'Administració de Seguretat TIC, cadascun en el marc de les seves competències l'elaboració i/o aprovació de les Guies de seguretat.

Capítol tercer. Manteniment de la Política i Millora contínua

ARTICLE 28. ACTUALITZACIÓ PERMANENT

1. La present Política haurà de mantenir-se permanentment actualitzada per adequar-se als progressos i avenços de l'Administració Electrònica, a l'evolució tecnològica, al desenvolupament de la societat de la informació i als canvis normatius que la puguin afectar.
2. L'actualització l'haurà d'aprovar el Comitè de Seguretat TIC, a proposta de la persona responsable de seguretat.
3. La persona responsable de seguretat haurà de verificar la vigència de la política, com a mínim una vegada a l'any i, en tot cas, quan es produeixin canvis en els serveis o es produeixin incidents de seguretat de nivell alt que puguin fer replantejar algun aspecte de la Política.



Doc. original signat per:
Alex Tablado Vergara
17/03/2026,
Isaías Táboas Suárez
17/03/2026,
Núria López Rodríguez
19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ

001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
15/06/2026 12:49:43

Pàgina 22 de 23



ARTICLE 29. AUDITORIA I MILLORA CONTÍNUA

1. La correcta aplicació dels procediments i les mesures de seguretat que s'estableixen en la present Política seran objecte d'una auditoria regular ordinària, com a mínim cada dos anys, que verifiqui el compliment dels requisits de l'Esquema Nacional de Seguretat.

A més, es realitzaran auditories extraordinàries quan es produeixin canvis substancials en els sistemes o serveis, canvis rellevants en l'arquitectura o en l'externalització, variacions significatives del nivell de risc, o després d'incidents greus de seguretat que ho aconsellin.

2. L'informe d'auditoria determinarà el grau de compliment de la present Política a l'Esquema Nacional de Seguretat identificant les deficiències i suggerint possibles mesures correctores, així com les recomanacions que es considerin adients. Haurà d'incloure els criteris metodològics utilitzats durant l'auditoria i l'objectiu d'aquesta, i les dades, fets i observacions en què es basin les conclusions formulades.
3. Els informes d'auditoria els presentarà la persona Responsable de seguretat i les persones Responsable dels sistemes d'informació competents.



Doc. original signat per:
Alex Tablado Vergara
17/03/2026,
Isaías Táboas Suárez
17/03/2026,
Núria López Rodríguez
19/03/2026

Document electrònic garantit amb signatura electrònica. Podeu verificar la seva integritat al web csv.gencat.cat fins al 15/06/2029

Original electrònic / Còpia electrònica autèntica

CODI SEGUR DE VERIFICACIÓ



001CYTJ6ZNELDZ7JP4FNSGDIS41GT8SQ

Data creació còpia:
15/06/2026 12:49:43

Pàgina 23 de 23