

Altres disposicions

Decret 550/2023, del 6 de desembre del 2023

Decret 550/2023, del 6-12-2023, d'aprovació de la política de seguretat de la informació del Govern d'Andorra i de creació del Comitè Tècnic de Seguretat de la informació.

Exposició de motius

En el context d'un món digitalitzat i cada vegada més dependent dels serveis digitals, aquests han esdevingut objectiu preferent de la delinqüència. En aquest sentit, és imprescindible dotar les organitzacions de mitjans per garantir un nivell de seguretat suficient.

És amb aquest objectiu que el Govern d'Andorra desplega un paquet normatiu que establia les directrius de seguretat a complir, especialment en organitzacions que proveeixen serveis considerats crítics o essencials: el Decret 346/2021, del 20 d'octubre del 2021, de creació de l'Agència Nacional de Ciberseguretat; la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació (NIS-AD); el Decret 417/2022, del 12 d'octubre del 2022, d'aprovació del Reglament de l'Esquema Nacional de Seguretat del Principat d'Andorra (ENS-AD), i el Decret 418/2022 d'aprovació del Reglament d'infraestructures crítiques del Principat d'Andorra (RIC-AD).

En aquest sentit, l'ENS-AD requereix l'establiment d'un sistema de gestió de seguretat de la informació (SGSI), que de forma alineada a l'estàndard internacional de seguretat de la informació ISO27001 exigeix l'aprovació d'una política de seguretat de la informació, que estableix el compromís del Govern d'Andorra per garantir la confidencialitat, la integritat i la disponibilitat de la informació, així com la creació d'un òrgan consultiu i de supervisió, el Comitè Tècnic de Seguretat de la Informació.

A proposta del cap de Govern, el Govern, en la sessió de 6 de desembre 2023, aprova aquest Decret amb el contingut següent:

Article 1. *Abast*

La política de seguretat de la informació (en endavant, "PSIGdA"), és d'aplicació per a tots els departaments de Govern d'Andorra i per a tot el personal que intervingui en el tractament de la informació amb independència de quina sigui la seva condició o relació laboral.

La Secretaria d'Estat de Transformació Digital i Telecomunicacions és responsable de gestionar, elaborar i assegurar que es mantingui el cos normatiu de seguretat del Govern d'Andorra, segons el que estableixi l'Esquema Nacional de Seguretat i el Reglament d'infraestructures crítiques vigents.

Article 2. *Descripció de la política de seguretat de la informació*

1. La política de seguretat de la informació del Govern d'Andorra és una norma, de compliment obligat dins l'organització, que estableix les directrius i principis bàsics per a la protecció dels sistemes d'informació amb l'objectiu de garantir la confidencialitat, la integritat i la disponibilitat de les dades.
2. De la PSIGdA, en depenen la resta de normes de seguretat que emanen del sistema de gestió de la seguretat de la informació.

Article 3. *Principis bàsics de la seguretat de la informació*

1. La seguretat s'entén com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius relacionats amb les tecnologies de la informació i les comunicacions (TIC).

2. La seguretat de la informació s'ha d'integrar en tots els processos de la organització i, per tant, s'ha d'aplicar tant en el del disseny inicial de les TIC com en la seva operativa, amb l'objectiu de garantir la protecció, la integritat i la disponibilitat de les dades.

3. La política de seguretat de la informació, conforme a l'ENS-AD, se sustenta en els sis principis bàsics següents:

a) Seguretat com a procés integral, que tingui en compte no només actius o elements tecnològics, sinó també personal, seguretat física i aspectes organitzatius, aquests s'aplicaran de manera sistemàtica utilitzant un sistema de gestió de la seguretat o SGSI.

Les mesures de protecció i els controls són necessaris per garantir la seguretat i la privacitat de la informació que tracta el Govern d'Andorra, tant en els paràmetres de confidencialitat, integritat i disponibilitat com en els de traçabilitat i autenticitat, a més d'assegurar l'accés i la conservació de les dades.

El cos normatiu de seguretat s'estructura de forma jeràrquica, de manera que les normes i procediments de nivell inferior s'ajusten i supediten a les de nivell superior. En aquest sentit, la política de seguretat se situa en el primer nivell o nivell més alt.

Els estàndards estan situats en el segon nivell i han d'estar alineats amb la política de seguretat de la informació. Les mesures de seguretat i privacitat indicades en els estàndards són de compliment obligat per als procediments de seguretat, que són els documents de més baix nivell de la piràmide jeràrquica i han d'estar alineats tant amb la política com amb els estàndards de seguretat.

La PSIGdA s'aplica a tots els processos dins l'abast del SGSI, així com al personal del Govern que hi intervé, tant propi com extern a l'organització.

En conseqüència, tant el personal del Govern, com els proveïdors i tercers han de conèixer i complir el marc normatiu en matèria de seguretat de la informació.

b) Principi de proporcionalitat: s'aplicaran les mesures de seguretat de forma proporcional, segons el nivell de risc definit per a cada servei o element.

c) Modelatge dels actius d'informació bàsics, mitjançant actius d'informació estàndard per als quals cal preveure mesures o procediments de prevenció, per eliminar o reduir la possibilitat que les amenaces arribin a materialitzar-se; de detecció, per identificar la presència d'un ciberincident; de resposta, per restaurar la informació i els serveis afectats, i de conservació i integritat de les dades i informacions en suport electrònic.

d) Estructuració de les mesures de seguretat en capes: una primera o bàsica, una segona de nivell de seguretat mitjà i una de categoria alta, de forma que es redueixi la probabilitat que la bretxa en una capa comprometi els actius d'informació que suporten els serveis als quals aplica l'ENS-AD (principi d'estratificació de les mesures).

e) Monitoratge i millora contínua, per poder respondre a atacs o amenaces de seguretat, i tenir la capacitat de modular les mesures i respostes a les situacions i riscos associats.

f) Diferenciació de responsabilitats: el responsable de la prestació del servei ha de ser una persona diferent del responsable de la seguretat dels actius que suporten el servei.

Article 4. Gestió de riscos

1. La gestió de riscos és el procés integral que implica la identificació, l'avaluació i la mitigació de les amenaces cibernètiques.

2. El delegat de la seguretat de la informació és l'encarregat d'assegurar que s'efectui l'anàlisi de riscos, així com d'identificar mancances i debilitats i de posar-les en coneixement del Comitè Tècnic de Seguretat de la Informació.

3. El procés de gestió de riscos ha de complir els requeriments establerts en l'ENS-AD i les indicacions de l'ANC-AD (Agència Nacional de Ciberseguretat d'Andorra).

4. En l'anàlisi de riscos s'ha d'utilitzar una metodologia estàndard i reconeguda en l'àmbit internacional alineada amb el que exigeix l'ENS-AD.
5. L'anàlisi i gestió de riscos és una part essencial del procés de seguretat, per assegurar el manteniment d'un entorn controlat, minimitzant els riscos fins a nivells considerats acceptables per l'organització.
6. La reducció del nivell de risc es fa desplegant mesures de seguretat i privacitat que es modulen en funció de la naturalesa de les dades i els tractaments de la informació, així com de l'impacte i la probabilitat dels riscos als quals estiguin exposats, buscant un compromís entre cost i eficàcia.

Article 5. Millora contínua i avaluació periòdica

1. La gestió de la seguretat de la informació és un procés subjecte a actualització permanent. Els canvis en l'organització, les amenaces, les tecnologies o la legislació són exemples en què és necessària una adaptació contínua dels sistemes per fer front a un entorn en constant evolució.
2. En conseqüència, cal aplicar els procediments i operativa escaients per assegurar les accions següents:
 - a) Revisió de la política de seguretat de la informació.
 - b) Revisió dels serveis i informació i la seva categorització.
 - c) Execució anual de l'anàlisi de riscos.
 - d) Realització d'auditories internes i externes.
 - e) Revisió de les mesures de seguretat.
 - f) Revisió i actualització de les normes i procediments.

Article 6. Obligacions del personal

1. Tot el personal del Govern té l'obligació de conèixer i complir aquesta política de seguretat de la informació, i és responsabilitat del Comitè Tècnic de Seguretat de la Informació disposar els mitjans necessaris perquè aquesta sigui difosa a tothom a qui apliqui.
2. El personal amb responsabilitat en l'operació o administració de sistemes TIC ha de rebre formació per aprendre a gestionar-los de manera segura. Així mateix, s'ha de promoure la conscienciació en matèria de seguretat a tot el personal del Govern d'Andorra mitjançant programes de formació, el contingut dels quals es podrà adaptar a les necessitats de cada destinatari.
3. L'incompliment de l'aquesta política de seguretat de la informació pot comportar l'adopció de les mesures disciplinàries que escaiguin, sense perjudici de les responsabilitats legals corresponents.

Article 7. Organització de la seguretat de la informació

1. El Govern d'Andorra disposa d'estructura organitzativa per a la gestió de la seguretat dels sistemes d'informació, composta pels perfils següents:
 - a) Responsables tècnics de sistemes d'informació
 - b) Responsables de serveis TIC
 - c) Responsables del tractament de dades
 - d) Delegat de protecció de dades
 - e) Responsables de desenvolupament
 - f) Delegat de la seguretat de la informació
 - g) Responsables de control d'accés, energia i refrigeració dels centre de dades
2. Aquesta estructura ha de completar-se amb el Comitè Tècnic de Seguretat de la Informació, segons s'estableix en el marc de referència internacional ISO/IEC27001, com a supervisor i govern per assegurar

la correcta i efectiva implementació del PSIGdA i del conjunt de normes de seguretat de la informació associades.

Article 8. *Composició del Comitè Tècnic de Seguretat de la Informació*

1. El Comitè Tècnic de Seguretat de la Informació està format per:

- a) President: secretari d'Estat de Transformació Digital i Telecomunicacions
- b) Vicepresident: director del Departament de Transformació Digital
- c) Secretari: tècnic nomenat pel Departament de Transformació Digital
- d) 4 vocals: el director d'Ensenyament Superior, Recerca i Innovació Tecnològica, el delegat de Seguretat de la Informació del cos de Policia, el delegat de Seguretat de la Informació del Govern i el responsable de Seguretat del Departament de Transformació Digital.

2. El Comitè Tècnic de Seguretat de la Informació pot requerir l'assessorament de tècnics i experts o de qualsevol altre actor, en tots els casos interns a l'organització, que es consideri escaient per part de la presidència o les direccions. Aquests tècnics o experts només participen a títol consultiu.

Article 9. *Creació, funcions i responsabilitats del Comitè Tècnic de Seguretat de la Informació*

1. Es crea el Comitè Tècnic de Seguretat de la Informació (CTSI).

2. Són funcions i responsabilitats del Comitè Tècnic de Seguretat de la Informació:

- a) Emetre informes al Govern sobre qüestions de seguretat de la informació.
- b) Proposar directrius i recomanacions, que seran recollides en les corresponents actes de les reunions del Comitè, a les quals el seu president haurà de donar resposta.
- c) Estar informat de les normatives vigents en matèria de seguretat de la informació.
- d) Promoure i impulsar el desenvolupament de projectes de seguretat.
- e) Coordinar els esforços dels diferents actors implicats en la seguretat de la informació per assegurar-ne l'eficàcia i l'alineació amb els objectius del Govern d'Andorra i del mateix Comitè.
- f) Promoure la sensibilització sobre i la difusió de la seguretat de la informació.
- g) Assessorar en matèria de seguretat de la informació qui li ho requereixi.
- h) Revisar la política de seguretat de la informació prèvia elevació a aprovació.
- i) Validar i aprovar les normes del SGSI que li són elevades.
- j) Fer el seguiment dels principals riscos i incidents de seguretat, així com recomanar possibles accions de millora.
- k) Facilitar la comunicació en matèria de seguretat de la informació a tota la organització.
- l) Altres funcions considerades inherents a la natura del Comitè.
- m) Altres funcions que li assigni la legislació vigent.

Article 10. *Funcionament i organització del Comitè Tècnic de Seguretat de la Informació*

1. El Comitè Tècnic de Seguretat de la Informació es reuneix almenys una vegada a l'any i sempre que el president el convoqui.

2. El CTSI podrà fer les reunions de forma presencial o telemàtica.

3. Són funcions de president:

- a) Representar el Comitè Tècnic de Seguretat de la Informació.
- b) Convocar, establir l'ordre del dia i presidir les sessions.

- c) Dirimir els empats amb el seu vot.
 - d) Signar les actes, les certificacions d'acords, els informes, les autoritzacions d'inspecció i els dictàmens.
4. Són funcions del vicepresident:
- a) Substituir el president en cas d'absència, de malaltia o per qualsevol altra causa que li impedeixi l'exercici de les seves funcions.
 - b) Encarregar-se del despatx i dels assumptes que li delegui el president.
5. Són funcions del secretari:
- a) Assistir administrativament el president.
 - b) Estendre les actes de les sessions del CTSI, signar-les i sotmetre-les al vistiplau del president.
 - c) Presentar anualment un informe sobre el funcionament del CTSI.
 - d) Qualsevol altra que li encomani el president.

Article 11. Sessions

1. Les sessions del CTSI, les convoca el president amb una antelació mínima de cinc dies, amb indicació del dia, el lloc i l'hora de la reunió, i de l'ordre del dia. La convocatòria pot incloure la previsió d'una segona convocatòria de la sessió.
2. El president fixa l'ordre del dia de les sessions. Abans que es convoqui la sessió corresponent, tres membres del CTSI poden demanar al president que inclogui un assumpte determinat en l'ordre del dia.
3. No es pot deliberar, votar ni adoptar acords sobre temes no inclosos en l'ordre del dia de la reunió, llevat que hi siguin presents tots els membres del CTSI i ho decideixin així per unanimitat.
4. Per a la constitució vàlida d'una reunió de la CTSI cal que hi siguin presents tres dels seus membres, entre els quals hi ha d'haver, com a mínim, el president o el vicepresident.
5. El secretari estén acta de les sessions, en què fa constar el dia, l'hora i el lloc de la reunió, l'ordre del dia, els assistents, els acords adoptats i les qüestions principals que s'hagin deliberat. L'acta de la sessió, l'ha d'aprovar el CTSI en una sessió posterior i l'ha de signar el president.

Article 12. Règim de decisió

1. El CTSI decideix per majoria simple dels seus membres.
2. En cas d'empat, dirimeix el vot del president.
3. Els membres que discrepin dels acords adoptats poden fer constar a l'acta la seva discrepància i poden adjuntar vots particulars als acords.

Article 13. Procediment d'emissió d'informes i dictàmens

1. Un cop rebuda la petició d'un informe o un dictamen, el president la trasllada a tots els membres del Comitè Tècnic de Seguretat de la Informació i, en un termini de tres dies hàbils i una vegada ha escoltat el vicepresident, nomena una ponència.
2. Els ponents han de presentar el projecte d'informe o de dictamen en un termini de deu dies hàbils des del seu nomenament. El president, quan la naturalesa de l'assumpte ho requereixi, pot prorrogar aquest termini fins a deu dies hàbils més. En cas d'urgència, aquest termini es pot reduir a cinc dies hàbils.
3. El projecte d'informe o de dictamen elaborat pels ponents es distribueix entre els membres del Comitè Tècnic de Seguretat de la Informació en un termini de tres dies hàbils des del seu lliurament.
4. El projecte d'informe o de dictamen se sotmet a la deliberació i a l'aprovació del Comitè Tècnic de Seguretat de la Informació en un termini no inferior a cinc dies hàbils ni superior a quinze, a comptar del seu lliurament.



5. En tot cas, l'emissió de l'informe o el dictamen té lloc dins del termini de dos mesos a comptar de la sol·licitud.

6. Els membres del Comitè Tècnic de Seguretat de la Informació que discrepin poden adjuntar vots particulars als informes i els dictàmens aprovats. A aquest efecte, disposen de dos dies hàbils per lliurar al secretari el seu vot particular, a comptar del moment en què quedi fixada la redacció definitiva de l'informe o del dictamen.

Si se sobrepassen els dos mesos de termini màxim per emetre l'informe o el dictamen, aquest informe o dictamen s'envia al sol·licitant tot indicant que s'hi ha formulat un o diversos vots particulars. El secretari del Comitè Tècnic de Seguretat de la Informació els trameta al sol·licitant tan bon punt els rebi.

Disposició final

Aquest Decret entra en vigor l'endemà de la seva publicació al *Butlletí Oficial del Principat d'Andorra*.

Cosa que es fa pública per a coneixement general.

Andorra la Vella, 6 de desembre del 2023

Xavier Espot Zamora
Cap de Govern