Acords

Acord del 4-12-2024 d'aprovació del Reglament de la política de seguretat de la informació del Consell Superior de la Justícia, de creació del Comitè i d'identificació dels rols de seguretat de la informació.

Exposició de motius

La seguretat de la informació és un repte que cal tenir en compte en la gestió del risc. La manca de protecció adequada i de gestió de les amenaces que afecten la seguretat de la informació comporta un perill de manca de protecció de dades per als administrats, així com una reducció de la confiança del ciutadà envers la justícia.

Els processos de l'Administració de justícia i del Consell Superior de la Justícia (CSJ) tenen una alta dependència dels sistemes de tecnologies de la informació i la comunicació (TIC). Aquests sistemes han de ser administrats amb diligència i s'han de prendre les mesures adequades per protegir-los davant danys accidentals o deliberats que puguin afectar la disponibilitat, la integritat o la confidencialitat de la informació tractada o els serveis prestats.

Els processos del CSJ han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, la integritat, la disponibilitat, l'ús previst i el valor de la informació i els serveis. Per defensar-se d'aquests perills, es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació contínua dels serveis. Això implica que les parts que es relacionin amb el CSJ han d'aplicar les mesures mínimes de seguretat exigides per aquesta política, així com fer un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

Els òrgans i les estructures del Consell Superior de la Justícia, de l'Administració de justícia i els mateixos òrgans jurisdiccionals s'han de cerciorar que la seguretat de les TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la seva retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes i en plecs de licitació. Els òrgans i les estructures ans esmentades han d'estar preparats per prevenir i detectar incidents, per reaccionar-hi i per recuperar-se d'aquests incidents.

El marc legislatiu actual relatiu a la seguretat de la informació, liderat per la Llei 22/2022, del 9 de juny, de mesures per a la seguretat de les xarxes i dels sistemes d'informació (NIS-AD), ha estat desenvolupat pel Decret 417/2022, del 12-10-2022, pel qual s'aprova el Reglament de l'Esquema nacional de seguretat del Principat d'Andorra (ENS-AD), i el Decret 418/2022, del 12-10-2022, pel qual s'aprova el Reglament d'infraestructures crítiques del Principat d'Andorra (RIC-AD).

L'ENS-AD requereix l'establiment d'un sistema de gestió de la seguretat de la informació (SGSI), que de forma alineada amb l'estàndard internacional de seguretat de la informació ISO27001 exigeix l'aprovació d'una política de seguretat de la informació per garantir la confidencialitat, la integritat i la disponibilitat de la informació.

L'eficiència i l'eficàcia de la política de seguretat de la informació va requerir la creació del Comitè de Seguretat de la Informació com a òrgan de gestió i supervisió de la política de seguretat, així com de identificació i definició dels rols partícips d'aquesta política.

Dipòsit legal: AND.2-2015

Aquestes estructures del Sistema de Gestió de la Seguretat de la Informació van ser aprovades pel Consell Superior de la Justícia per acord de 6 de desembre del 2023, tanmateix, esdevé necessària la seva actualització i publicació.

D'acord amb aquestes consideracions, el Consell Superior de la Justícia, en la sessió del 4 de desembre del 2024, acorda el següent:

Article únic
S'aprova el Reglament de la política de seguretat de la informació del Consell Superior de la Justícia, de creació del Comitè i d'identificació dels rols de seguretat de la informació, que entrarà en vigor l'endemà de publicar-se al *Butlletí Oficial del Principat d'Andorra*.

Reglament de la política de seguretat de la informació del Consell Superior de la Justícia, de creació del Comitè i d'identificació dels rols de seguretat de la informació

Capítol primer. Disposicions generals

Article 1. *Objecte*
Aquest Reglament té per objecte establir les bases de la política de seguretat de la informació del Consell Superior de la Justícia i la creació del Comitè de Seguretat de la Informació, i les seves normes d'organització i funcionament. Igualment, identifica els rols participants en la seguretat de la informació.

Article 2. *Objectiu de la seguretat de la informació*
L'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb prestesa als incidents.

Article 3. *Àmbit d'aplicació*
1. La política de seguretat de la informació i els procediments relacionats són aplicables a tots els òrgans jurisdiccionals i les estructures del Consell Superior de la Justícia i de l'Administració de justícia.

2. Aquesta política s'aplica especialment als sistemes d'informació del Consell Superior de la Justícia que estan relacionats amb l'exercici dels drets per mitjans electrònics, amb el compliment dels deures per mitjans electrònics, amb l'accés a la informació o al procediment administratiu i en general a tots els sistemes que donin suport a la prestació dels serveis públics gestionats pel Consell Superior de la Justícia.

Capítol segon. Sistema de gestió de la seguretat de la informació (SGSI)

Secció primera. Organització de la seguretat de la informació

Article 4. *Objectius del sistema de gestió de la seguretat de la informació (SGSI)*
Són objectius bàsics de la política de seguretat de la informació del CSJ els següents:

1. Confidencialitat: protegir la confidencialitat dels actius d'informació mitjançant la implementació de controls d'accés i mecanismes de protecció de dades adequats.

2. Integritat: garantir la integritat dels actius d'informació mitjançant la implementació de controls per evitar la modificació, la supressió o la destrucció no autoritzada de dades.

3. Disponibilitat: assegurar la disponibilitat dels actius d'informació mitjançant la implementació de mesures adequades de còpia de seguretat i recuperació de desastres, i minimitzar l'impacte dels incidents.

4. Compliment: garantir el compliment de les lleis, les regulacions i les obligacions contractuals aplicables relacionades amb la seguretat de la informació.

Dipòsit legal: AND.2-2015

Article 5. *Estructura del sistema de gestió de la seguretat de la informació (SGSI)*
1. El conjunt de documents de la política de seguretat de la informació del CSJ està estructurat en el model jeràrquic següent, de quatre tipologies d'estàndards normatius:

a) El Reglament de la política de seguretat de la informació: aquest estàndard manifesta els principis de seguretat de la informació que s'han de desenvolupar als documents dels nivells jeràrquics següents.

b) Normatives internes: estàndards de caràcter regulador en els quals es defineixen els objectius de control, desenvolupant cadascun dels principis de seguretat de la informació detallats en aquest política.

c) Procediments interns: estàndards que determinen les actuacions concretes que s'han de seguir per implantar els objectius de control definits a la normativa. Aquests estàndards emanen de les normatives o altres procediments.

d) Instruccions tècniques internes: estàndards que determinen com implantar els requeriments en matèria de seguretat de la informació. Aquesta categoria inclou també manuals, formularis i models, entre d'altres. Aquests estàndards emanen dels procediments o altres instruccions tècniques.

2. Tots els estàndards normatius són de compliment obligat.

3. No tenen validesa les disposicions que en contradiguin una altra de rang superior.

Article 6. *Finalitat de la política de seguretat de la informació*
1. La política de seguretat de la informació pretén identificar els requisits de protecció de la informació per assegurar que tots els òrgans jurisdiccionals i estructures del Consell Superior de la Justícia i l'Administració de justícia protegeixen la informació, seguint les normatives legals i reguladores aplicables al Principat d'Andorra.

2. Igualment, la política de seguretat de la informació defineix les línies d'actuació que formen part de l'estratègia en matèria de seguretat de la informació i desenvolupa les directrius per a la gestió i la protecció dels actius d'informació del Consell Superior de la Justícia i l'ús adequat d'aquests actius.

Article 7. *Organització interna de la seguretat de la informació*
1. Per garantir el compliment i l'adaptació de les mesures exigides reglamentàriament, es creen els rols o perfils de seguretat següents i es designen els càrrecs o òrgans que els han d'ocupar, que es defineixen al capítol quart.

a) Responsable de sistemes d'informació (RSI).

b) Delegat de la seguretat de la informació (DSI).

c) Delegat de protecció de dades (DPD).

2. S'han d'implementar mesures tècniques i organitzatives per assegurar el principi de separació de les funcions següents:

a) Aprovació de canvis en els usuaris (autorització o validació).

b) Operacions de gestió d'usuaris (afegir, modificar o treure usuaris o permisos i autoritzacions, així com canvi de contrasenyes).

c) Auditories de seguretat de la informació i revisió i implementació de controls per reduir el risc existent.

Article 8. *Responsable de sistemes d'informació (RSI)*
1. El responsable de sistemes d'informació és la persona responsable de la planificació, la implementació i la gestió de les TIC en el CSJ.

2. Les seves funcions estan definides al capítol quart.

Dipòsit legal: AND.2-2015

Article 9. *Delegat de la seguretat de la informació (DSI).*
1. El delegat de la seguretat de la informació és la persona encarregada que es porti a terme l'anàlisi de riscos i d'identificar mancances i debilitats i de posar-les en coneixement del Comitè de Seguretat de la Informació. És responsable d'establir i supervisar l'estratègia de seguretat del Consell Superior de la Justícia, així com de garantir que els seus sistemes i dades estiguin protegits d'atacs i pèrdues.

2. Les funcions d'un DSI estan definides al capítol quart.

Article 10. *Delegat de protecció de dades (DPD)*
1. El delegat de protecció de dades s'encarrega de garantir el compliment de la normativa de protecció de dades, així com del manteniment i de l'actualització del registre d'activitats del tractament, i del seguiment de la legislació de privacitat que afecti el Consell Superior de la Justícia.

2. Les funcions del DPD són les establertes al capítol quart.

Article 11. *Consell Superior de la Justícia (CSJ)*
1. El Consell Superior de la Justícia (CSJ) és l'òrgan de representació, govern i administració de l'organització judicial al Principat d'Andorra que vetlla pel bon funcionament de la justícia.

2. Les seves funcions en matèria de la seguretat de la informació són:

a) Liderar i proveir l'estructura de gestió i els recursos necessaris per implementar aquesta política.

b) Assegurar-se del compliment dels requisits de seguretat de la informació en tots els processos.

c) Participar en la revisió de les polítiques i les activitats de seguretat de la informació i aprovar la normativa d'aplicació de l'SGSI a proposta del CSI.

d) Aportar el finançament de les activitats de seguretat de la informació.

3. El Consell Superior de la Justícia ha de ser informat i consultat sobre:

a) Les propostes de modificació de la política de la seguretat de la informació.

b) La implementació d'aquesta política en els òrgans i les estructures del Consell Superior de la Justícia i l'Administració de justícia.

Article 12. *Comitè de Seguretat de la Informació (CSI)*
1. El Comitè de Seguretat de la Informació és el responsable d'impulsar, assessorar, gestionar i supervisar la seguretat de la informació i de vetllar per ella.

2. La composició, les funcions i l'organització del CSI es regulen al capítol tercer.

Secció segona. Requeriments de seguretat

Article 13. *Requeriments de seguretat*
El Consell Superior de la Justícia, per assolir els principis bàsics i els requisits mínims de seguretat, ha d'implementar diverses mesures de seguretat proporcionals a la naturalesa de la informació i els serveis que cal protegir, tenint en compte la categoria dels sistemes afectats.

Article 14. *La seguretat com un procés integral*
1. La seguretat constitueix un procés integrat per tots els elements tècnics, humans, materials i organitzatius relacionats amb el sistema. L'aplicació de la política de seguretat del CSJ està presidida per aquest principi, que exclou qualsevol actuació puntual o tractament conjuntural.

2. S'ha de prestar la màxima atenció a les persones que intervenen en el procés i als seus responsables jeràrquics, perquè la consciència, l'organització i la coordinació, juntament amb instruccions adequades, garanteixin la seguretat en tot moment.

Dipòsit legal: AND.2-2015

Article 15. *Principi de mínim privilegi*
Els sistemes s'han de dissenyar de manera que garanteixin la seguretat per defecte, de la manera següent:

a) El sistema ha de proporcionar la mínima funcionalitat requerida per a la prestació dels serveis.

b) Les funcions d'operació, administració i registre d'activitat han de ser les mínimes necessàries, i s'ha d'assegurar que només són accessibles per les persones o des d'emplaçaments o equips, autoritzats: si escau, es poden exigir restriccions d'horari i punts d'accés facultats.

c) En un sistema d'explotació s'han d'eliminar o desactivar, mitjançant el control de la configuració, les funcions que siguin innecessàries o inadequades a la fi que es persegueix. L'ús ordinari del sistema ha de ser senzill i segur, de manera que una utilització insegura requereixi un acte conscient per part de l'usuari. S'han d'aplicar guies de configuració de seguretat per a les diferents tecnologies, adaptades a la categorització del sistema, a aquest efecte.

Article 16. *Vigilància contínua, reavaluació periòdica i integritat, actualització del sistema i millora contínua del procés de seguretat*
1. La vigilància contínua permet la detecció d'activitats o comportaments anòmals i una resposta oportuna.

2. L'avaluació permanent de l'estat de la seguretat dels actius permet mesurar la seva evolució, detectant vulnerabilitats i identificant deficiències de configuració.

3. Les mesures de seguretat s'han de reavaluar i actualitzar periòdicament, adequant la seva eficàcia a l'evolució dels riscos i els sistemes de protecció. Es pot arribar a un replantejament de la seguretat, si és necessari.

4. La inclusió de qualsevol element físic o lògic en el catàleg actualitzat d'actius del sistema, o la seva modificació, requereix autorització formal prèvia.

5. L'avaluació i el monitoratge permanents permeten adequar l'estat de seguretat dels sistemes atenent les deficiències de configuració, les vulnerabilitats identificades i les actualitzacions que els afecten, així com la detecció inicial de qualsevol incident que tingui lloc sobre aquests sistemes.

6. El procés integral de seguretat implantat ha de ser actualitzat i millorat de forma contínua. Per a això, s'han d'aplicar els criteris i els mètodes reconeguts en la pràctica nacional i internacional relatius a la gestió de la seguretat de les tecnologies de la informació.

7. Així mateix, s'ha de demanar la revisió periòdica per part de tercers per tal d'obtenir una avaluació independent.

Article 17. *Seguretat relativa als recursos humans*
1. El Consell Superior de la Justícia té un pla de seguretat de la informació que inclou mesures durant tota la relació laboral dels empleats:

a) Abans de la contractació:
- El Consell Superior de la Justícia ha de fer les comprovacions de seguretat dels candidats.

b) Durant la relació de treball:
- Els empleats han de rebre formació en seguretat de la informació.
- Els responsables de cada estructura organitzativa s'encarreguen de garantir que els empleats compleixen les polítiques de seguretat.
- Es compta amb un pla de teletreball per protegir les dades quan els empleats treballen fora de l'oficina.
- Se segueix un procés disciplinari per als incompliments de la seguretat de la informació.

c) Finalització o canvi en la relació laboral:
- En finalitzar la relació laboral, s'eliminen els accessos i les credencials dels empleats.
- Els responsables de cada estructura han de revisar periòdicament les identitats i les autoritzacions dels empleats.

Dipòsit legal: AND.2-2015

2. La seguretat dels sistemes d'informació és atesa i revisada i auditada per personal qualificat, dedicat i instruït en totes les fases del seu cicle de vida: planificació, disseny, adquisició, construcció, desplegament, explotació, manteniment, gestió d'incidències i desmantellament.

3. De manera objectiva i no discriminatòria, el Consell Superior de la Justícia exigeix que les organitzacions que li proporcionen serveis comptin amb professionals qualificats i amb uns nivells idonis de gestió i maduresa dels serveis prestats.

Article 18. *Gestió d'actius*

1. La gestió d'actius de l'SGSI és el procés d'identificar, classificar, inventariar, protegir, monitorar i controlar els actius d'informació del Consell Superior de la Justícia i de l'Administració de justícia. Aquest procés és essencial i permet identificar els actius més valuosos i prendre les mesures necessàries per protegir-los.

2. Els punts més importants que s'inclouen en aquest procediment són:

a) Inventari d'actius.

b) Propietat dels actius.

c) Anàlisi de riscos.

d) Classificació de la informació.

e) Gestió de mitjans.

Article 19. *Gestió de la seguretat basada en els riscos i anàlisi i gestió de riscos*

1. L'anàlisi i la gestió dels riscos és part essencial del procés de seguretat i ha de ser una activitat contínua i permanentment actualitzada.

2. La gestió dels riscos permet mantenir un entorn controlat i minimitzar els riscos a nivells acceptables. La reducció a aquests nivells s'ha de fer mitjançant una aplicació de mesures de seguretat apropiada, de manera equilibrada i proporcionada a la naturalesa de la informació tractada, dels serveis que cal prestar i dels riscos als quals estiguin exposats.

3. Tots els sistemes afectats per aquesta política de seguretat i tots els tractaments de dades personals han de ser objecte d'una anàlisi de riscos, avaluant les amenaces i els riscos als quals estan exposats. Aquesta anàlisi s'ha de fer:

a) Regularment, almenys una vegada a l'any.

b) Quan canviïn els serveis prestats o la informació tractada de manera significativa.

c) Quan s'esdevingui un incident greu de seguretat o es detectin vulnerabilitats greus.

4. El delegat de la seguretat de la informació és l'encarregat que es porti a terme l'anàlisi de riscos, així com d'identificar mancances i debilitats i posar-les en coneixement del Comitè de Seguretat de la Informació.

5. Aquesta gestió s'efectua per mitjà de l'anàlisi i el tractament dels riscos als quals està exposat el sistema. S'ha d'emprar alguna metodologia reconeguda internacionalment. Les mesures adoptades per mitigar o suprimir els riscos han d'estar justificades i, en tot cas, hi ha d'haver una proporcionalitat entre les mesures i els riscos.

Article 20. *Control d'accessos*

1. Ha d'establir-se un procediment en el qual es detallin els responsables del control i el monitoratge de les autoritzacions per complir els seus principis bàsics que consisteixen en la identificació, l'autenticació i l'autorització, els detalls tècnics dels tipus de credencials que cal fer servir, els accessos temporals i la caducitat d'aquestes credencials.

2. L'objectiu a l'hora d'elaborar la política de control d'accés és assignar la quantitat més baixa possible de privilegis als usuaris i només pel temps que sigui necessari per fer una tasca concreta.

Dipòsit legal: AND.2-2015

3. Els punts més rellevants que s'inclouen en aquest procediment són:

a) Accés a xarxes i serveis connectats.

b) Gestió d'accessos d'usuaris.

c) Control d'accés a sistemes i aplicacions.

Article 21. *Criptografia*
1. Tots els accessos a la informació des de l'exterior es fan amb canals xifrats i la informació s'ha d'emmagatzemar sempre de manera xifrada. Les mesures de control per a l'ús eficaç de la criptografia són importants per protegir la confidencialitat i la integritat de la informació.

2. Els procediments de criptografia es basen en dos grans principis bàsics:

a) Política d'ocupació de controls criptogràfics.

b) Gestió de claus.

Article 22. *Seguretat física de l'entorn*
S'han d'identificar i establir mesures de control físiques per protegir adequadament els actius d'informació per evitar incidents que afectin la integritat física de la informació o interferències no desitjades als serveis. En aquests termes i com a mínim:

a) Els visitants s'han d'autenticar: cal registrar la data i l'hora d'entrada/sortida.

b) L'accés físic als llocs on s'emmagatzemi informació ha d'estar restringit amb control d'accés.

c) Al personal que treballi en àrees segures se li ha d'exigir portar identificació i s'ha de notificar als empleats de seguretat si una persona no fa servir la identificació requerida.

d) Els drets d'accés s'han de revisar periòdicament i s'han de revocar segons correspongui.

e) S'ha d'aplicar la política d'escriptori i pantalla nets, que defineix la confidencialitat de documents com ara dades personals o informació financera, perquè no estiguin a la vista de persones no autoritzades en taules o taulells, per protegir la informació sensible.

Article 23. *Procediments operatius i responsabilitats*
1. La documentació dels procediments i de la política de seguretat de la informació són responsabilitat del CSI, que s'encarrega d'elaborar-la, modificar-la i custodiar-la.

2. S'han de crear procediments operatius específics sobre:

a) Protecció contra el codi maliciós.

b) Protecció contra el programari de segrest (ransomware).

c) Còpies de seguretat.

d) Monitoratge i registre d'esdeveniments.

e) Control de programari operatiu.

f) Gestió tècnica de vulnerabilitats.

Article 24. *Seguretat en les comunicacions*
1. L'Àrea de Transformació Digital ha de disposar de procediments per a la gestió segura de les xarxes. La seguretat de les comunicacions és un control de seguretat de la informació que se centra en la protecció de la confidencialitat, la integritat i la disponibilitat de la informació durant la seva transmissió i recepció.

2. Els controls de seguretat apropiats per a les comunicacions han de tenir en compte els principis següents:

a) Protecció davant d'accés no autoritzat, com missatges encriptats.

Dipòsit legal: AND.2-2015

b) Assegurar el correcte adreçament i transport dels missatges.

c) Fiabilitat i disponibilitat del servei.

d) Consideracions legals (firmes digitals).

Article 25. *Adquisició, desenvolupament i manteniment dels sistemes d'informació*
1. S'han d'establir procediments per a la gestió segura de l'adquisició, el desenvolupament i el manteniment de programari i maquinari necessari per al correcte funcionament dels serveis.

2. Els principis d'enginyeria segurs requereixen documentar procediments sobre com implementar mesures de seguretat a les tècniques de desenvolupament següents:

a) Procediments segurs per al disseny i la codificació (elaboració de codi segur).

b) Processos de disseny de mecanismes d'autenticació difícils de vulnerar.

c) Processos de somatització de variables.

d) Procediments per a l'ús correcte de la criptografia.

e) Altres.

Article 26. *Seguretat en la relació amb proveïdors*
1. S'ha de crear un procediment de revisió de la seguretat de la informació de proveïdors en què es detallin els requisits d'avaluació i el tractament de risc amb els mateixos proveïdors.

2. Aquest procediment s'ha d'adaptar als riscos generals que suposa la contractació de forma externa de l'allotjament de servidors, aplicacions de dades i serveis de comunicació.

3. La informació del Consell Superior de la Justícia ha de ser protegida pels proveïdors dels serveis. Per això, els contractes de prestació de serveis han d'incloure clàusules que especifiquin les condicions de seguretat que han de complir els proveïdors.

Article 27. *Gestió d'incidents de la seguretat de la informació*
1. Els incidents referits a l'Àrea de Transformació Digital s'han de comunicar al Consell Superior de la Justícia, que aplica les activitats detallades al procediment de gestió d'incidents.

2. Aquest procediment té com a objectiu assegurar un enfocament coherent i eficaç per a la identificació, l'avaluació, la contenció, l'erradicació i la recuperació d'incidents de seguretat de la informació, incloent-hi la comunicació dels esdeveniments de seguretat i vulnerabilitats.

3. Els controls estan agrupats en les categories següents:

a) Establiment d'un procés de gestió d'incidents.

b) Identificació i avaluació d'incidents.

c) Contenció i erradicació d'incidents.

d) Recuperació de dades.

e) Comunicació d'incidents.

4. Hi ha d'haver un procés integral de detecció, reacció i recuperació davant de codis danyosos mitjançant el desenvolupament de procediments que cobreixin els mecanismes de detecció, els criteris de classificació i els procediments d'anàlisi i resolució, així com les vies de comunicació a les parts interessades i el registre de les actuacions. Aquest registre s'empra per a la millora contínua de la seguretat del sistema.

a) Les mesures de prevenció poden incorporar components orientats a la dissuasió o a la reducció de la superfície d'exposició, i han d'eliminar o reduir la possibilitat que les amenaces arribin a materialitzar-se.

b) Les mesures de detecció van dirigides a descobrir la presència d'un ciberincident.

Dipòsit legal: AND.2-2015

c) Les mesures de resposta es gestionen en temps oportú, estan orientades a la restauració de la informació i els serveis que poguessin haver-se vist afectats per un incident de seguretat.

d) El sistema d'informació garanteix la conservació de les dades i la informació en suport electrònic.

5. Perquè la informació i els serveis no es vegin perjudicats per incidents de seguretat, el Consell Superior de la Justícia implementa les mesures de seguretat establertes per les NIS-AD, l'ENS-AD i el RIC-AD, així com qualsevol altre control addicional que hagi identificat com a necessari, mitjançant una avaluació d'amenaces i riscos. Aquests controls, així com els rols i les responsabilitats de seguretat de tot el personal, estan clarament definits i documentats.

6. Quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com a normals, s'han d'establir els mecanismes de detecció i report necessaris perquè arribin als responsables regularment.

7. S'estableixen les mesures següents de reacció davant d'incidents de seguretat:

a) Mecanismes per respondre eficaçment als incidents de seguretat.

b) Designar un punt de contacte per a les comunicacions respecte a incidents detectats en altres departaments o en altres organismes.

c) Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en ambdós sentits, amb els equips de resposta a emergències (CERT).

d) Per garantir la disponibilitat dels serveis, el Consell Superior de la Justícia disposa dels mitjans i les tècniques necessaris que permeten garantir la recuperació dels serveis més crítics.

Article 28. *Línies de defensa i prevenció davant d'altres sistemes interconnectats*

1. El Consell Superior de la Justícia ha d'implementar una estratègia de protecció del sistema d'informació constituïda per múltiples capes de seguretat, constituïdes per mesures organitzatives, físiques i lògiques, de manera que quan una capa ha estat compromesa permeti desenvolupar una reacció adequada davant dels incidents que no s'han pogut evitar, reduint la probabilitat que el sistema sigui compromès en conjunt i minimitzar-ne l'impacte final.

2. S'ha de protegir el perímetre del sistema d'informació, especialment quan el sistema del Consell Superior de la Justícia es connecta a xarxes públiques, tal com es defineixen en la legislació vigent en matèria de telecomunicacions, i s'han de reforçar les tasques de prevenció, detecció i resposta a incidents de seguretat.

3. En tot cas, s'han d'analitzar els riscos derivats de la interconnexió del sistema amb altres sistemes i es controla el seu punt d'unió. Per a l'adequada interconnexió entre sistemes cal atenir-se al que disposa la instrucció tècnica de seguretat corresponent.

Article 29. *Continuïtat d'operacions*

1. La continuïtat d'operacions és un procés sistemàtic per identificar, avaluar i mitigar els riscos que podrien interrompre les operacions crítiques dels òrgans i les estructures de l'Administració de justícia i del Consell Superior de la Justícia. La integració de la Seguretat de la Informació garanteix que els actius d'informació es protegeixen adequadament dels incidents de seguretat, fins i tot durant una interrupció del servei.

2. Aquest procediment identifica els aspectes següents de seguretat de la informació:

a) Identificació i avaluació dels actius d'informació crítics per a la continuïtat del servei.

b) Avaluació dels riscos de seguretat de la informació que podrien afectar els actius crítics.

c) Implementació de controls de seguretat de la informació per mitigar els riscos identificats.

d) Prova periòdica dels controls de seguretat de la informació per garantir-ne l'eficàcia.

e) Planificació de la continuïtat del servei per garantir que els actius d'informació crítics estan disponibles i accessibles en cas d'una interrupció del servei.

Dipòsit legal: AND.2-2015

Article 30. *Gestió de projectes*
1. Cada nou projecte que s'ha implementar ha d'incloure un procés de revisió per assegurar el correcte compliment d'aquesta política.

2. Tots els processos de revisió que afecten la gestió de la informació del Consell Superior de la Justícia i l'Administració de justícia s'han de documentar d'acord amb les recomanacions de l'Àrea de Transformació Digital.

Article 31. *Funció diferenciada i organització i implantació del procés de seguretat*
El Consell Superior de la Justícia organitza la seva seguretat implicant-hi tots els membres i les estructures de la institució mitjançant la designació de diferents rols de seguretat amb responsabilitats clarament diferenciades, tal com es recull a l'article 7 (Organització interna de la seguretat de la informació).

Article 32. *Prestació de serveis a terceres parts per part del Consell Superior de la Justícia i l'Administració de justícia*
1. Quan el Consell Superior de la Justícia presti serveis a altres organismes o gestioni informació d'altres organismes se'ls ha de fer partícips d'aquesta política de seguretat de la informació.

2. El Consell Superior de la Justícia ha de definir i aprovar els canals per a la coordinació de la informació i els procediments d'actuació per a la reacció davant d'incidents de seguretat, així com la resta d'actuacions que dugui a terme en matèria de seguretat en relació amb altres organismes.

3. Quan el Consell Superior de la Justícia utilitzi serveis de tercers o cedeixi informació a tercers, se'ls ha de fer partícips d'aquesta política de seguretat i de la normativa de seguretat que afecta aquests serveis o informació.

Article 33. *Responsabilitat respecte de la gestió de la seguretat de la informació*
1. Tot el personal i col·laboradors interns i externs del Consell Superior de la Justícia i l'Administració de justícia són responsables d'assegurar el compliment dels principis d'aquesta política i dels documents normatius interns del Consell Superior de la Justícia que la desenvolupen, així com de les lleis i regulacions vigents en matèria de seguretat de la informació.

2. El Consell Superior de la Justícia es reserva qualsevol dret d'actuació legal o disciplinària en situacions d'incompliment d'aquesta política.

Article 34. *Revisió i aprovació de l'SGSI*
1. Les modificacions i excepcions al sistema de gestió de seguretat de la informació són aprovades pel CSJ a proposta del CSI.

2. El CSI s'encarrega de liderar la revisió anual de l'SGSI per avaluar-ne el funcionament i indicar les àrees de millora.

Article 35. *Aprovació de la política de seguretat de la informació*
1. L'SGSI del Consell Superior de la Justícia estableix els requisits concisos i mínims que han de complir totes les unitats organitzatives nomenades a aquest efecte. Aquests requisits estan dissenyats per ser fàcils d'entendre i complir.

2. Els procediments referenciats en aquesta política i les seves modificacions són responsabilitat del CSI.

Article 36. *Revisió de la política de seguretat de la informació*
El CSI s'encarrega de liderar la revisió de la política de seguretat de la informació anualment i, en cas de requerir modificacions, elabora les propostes perquè les aprovi posteriorment el Consell Superior de la Justícia.

Dipòsit legal: AND.2-2015

Capítol tercer. Comitè de la Seguretat de la Informació (CSI)

Article 37. *Naturalesa*

Es crea el Comitè de la Seguretat de la Informació com a òrgan de gestió i supervisió en matèria de seguretat del Consell Superior de la Justícia.

Article 38. *Composició*

1. El Comitè de Seguretat de la Informació està format pels membres següents:

a) President: responsable de sistemes d'informació (RSI).

b) Vicepresident: delegat de la seguretat de la informació (DSI).

c) Vocal: delegat de protecció de dades (DPD).

d) Vocal: representant elegit pel Consell Superior de la Justícia.

2. Amb caràcter opcional, altres membres del Consell Superior de la Justícia i personal tècnic especialitzat, siguin de caràcter intern, extern o mixt, poden incorporar-se a les tasques del CSI. En qualsevol cas, aquestes persones no disposen de dret de vot.

3. Són funcions del president representar el CSI, convocar, establir l'ordre del dia i presidir les sessions del CSI, així com la signatura de les actes, les certificacions d'acords, els informes o altres dictàmens.

4. Són funcions del vicepresident la substitució del president en cas d'absència, de malaltia o per qualsevol causa que li impedeixi l'exercici de les seves funcions, com també qualsevol que li sigui encomanada pel president.

5. Són funcions dels vocals les que els siguin encomanades pel president o el vicepresident.

Article 39. *Funcions del CSI*

1. Són funcions del CSI:

a) Alinear la política de seguretat de la informació amb els objectius de seguretat estratègics del Consell Superior de la Justícia.

b) Assegurar la implementació i l'execució de la política de seguretat de la informació.

c) Identificar i gestionar els riscos de seguretat.

d) Garantir la seguretat de les dades i els sistemes d'informació del Consell Superior de la Justícia i de l'Administració de justícia.

e) Coordinar els esforços de les àrees en matèria de seguretat de la informació, per assegurar que siguin consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.

f) Proposar plans de millora de la seguretat de la informació, amb la dotació pressupostària corresponent, i prioritzar les actuacions en matèria de seguretat quan els recursos siguin limitats.

g) Vetllar perquè la seguretat de la informació es tingui en compte en tots els projectes des de la seva especificació inicial fins a la posada en operació. En particular, vetllar per la creació i la utilització de serveis horitzontals que redueixin duplicitats i donin suport a un funcionament homogeni de tots els sistemes de TIC.

h) Fer un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions específiques.

i) Proposar i revisar la normativa de seguretat de la informació per aprovar-la.

j) Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de la seguretat de la informació.

k) Promoure l'elaboració de les auditories periòdiques ENS-AD i de protecció de dades que permetin verificar el compliment de les obligacions del Consell Superior de la Justícia en matèria de seguretat de la informació.

l) Altres que consideri el Consell Superior de Justícia en matèria de seguretat de la informació.

Dipòsit legal: AND.2-2015

2. Les funcions atribuïdes al CSI per un altre òrgan no poden ser delegades si bé poden ser revocades en qualsevol moment.

Article 40. *Funcionament i organització del CSI*
1. Compromís de participació activa

Per poder dur a terme les seves obligacions, els membres del CSI es comprometen a participar activament en les reunions i a aportar les seves perspectives per garantir la seguretat i la protecció de les dades del Consell Superior de la Justícia i de l'Administració de justícia.

2. Sessions

El CSI es reuneix trimestralment, o quan existeixen propostes o esdeveniments que ho justifiquin, de forma presencial, a les dependències del Consell Superior de la Justícia o bé mitjançant altres sistemes de comunicació que garanteixen la correcta participació dels membres.

Les sessions del CSI les convoca el president. Les convocatòries han d'incloure l'ordre del dia i la documentació que s'ha de tractar.

3. Ordre del dia

Els punts de l'ordre del dia d'una reunió del CSI han d'incloure els temes següents:

a) Lectura i aprovació de l'acta de la reunió anterior.

b) Seguiment de projectes.

c) Discussió d'amenaces i vulnerabilitats.

d) Revisió de mètriques de seguretat per avaluar el rendiment del programa de seguretat.

e) Altres temes depenent de les circumstàncies concurrents, com els plans de resposta d'incidents amb l'avaluació dels danys i fórmules de mitigació dels atacs o les revisions de resultats de les auditories per identificar i abordar les vulnerabilitats.

4. Quòrum

El CSI queda vàlidament constituït amb l'assistència de tres dels quatre membres en primera convocatòria i de la meitat dels membres en segona convocatòria.

El CSI també queda vàlidament constituït sense convocatòria prèvia si es reuneixen tots els membres i acorden per unanimitat constituir-se en sessió.

5. Acords del Comitè de Seguretat de la Informació

Els acords del CSI es prenen per majoria simple dels membres. El vot del president és diriment en cas d'empat. Amb caràcter extraordinari, les accions que no hagin estat acordades amb anterioritat, que tinguin com a finalitat la protecció dels interessos del CSJ i de l'Administració de justícia, i que requereixin una immediatesa en la presa de decisions poden ser aprovades pel president o, si no hi és, el vicepresident, i necessiten la confirmació posterior del CSI.

Queda prohibida la delegació de vots al CSI.

Els membres que discrepin dels acords adoptats poden fer constar a l'acta la seva discrepància.

6. Actes

De cada sessió s'ha d'aixecar l'acta corresponent, que inclou els temes tractats i els acords presos. Les actes, signades pel president, han de ser trameses als membres del CSI.

Qualsevol membre del CSI o del Consell Superior de la Justícia té dret a sol·licitar i a obtenir una còpia, total o parcial, de les actes de les reunions del CSI. El president ha de certificar aquestes còpies.

Dipòsit legal: AND.2-2015

7. Grups de treball

Per desenvolupar les funcions del CSI es poden constituir grups de treball per dur a terme tasques específiques i de temàtica concreta i especialitzada.

La composició dels grups de treball pot estar integrada per persones empleades del Consell Superior de la Justícia o bé per especialistes externs al CSJ, si bé la presidència ha de recaure sempre en un membre del CSI.

Les funcions, la composició i el règim de funcionament d'aquests grups es defineixen en l'acord de constitució aprovat pel CSI.

Capítol quart. Rols de la seguretat de la informació

Article 41. *Designació de rols en seguretat de la informació*

1. Els rols de seguretat i la descripció dels llocs que els ocupen són els següents:

a) Responsable de sistemes d'informació (RSI).

b) Delegat de la seguretat de la informació (DSI).

c) Delegat de protecció de dades (DPD).

2. Les competències atribuïdes als rols, si estan assignades a personal que forma part de l'estructura del Consell Superior de la Justícia, s'integren en la descripció de funcions d'aquests llocs de treball.

Article 42. *Responsable de sistemes d'informació (RSI)*

1. El responsable de sistemes d'Informació ha d'ocupar un lloc de responsabilitat i comandament dins l'estructura del CSJ.

2. El responsable de sistemes s'estableix a escala operativa. Tanmateix, es poden designar delegats d'aquest responsable d'acord amb la política de seguretat del Consell Superior de la Justícia.

3. Són funcions generals del responsable de sistemes d'informació les següents:

a) Definir la política de TIC del Consell Superior de la Justícia i de l'Administració de justícia.

b) Planificar i implementar els projectes de TIC.

c) Gestionar els recursos de TIC.

d) Proporcionar suport tècnic als usuaris.

e) Garantir la seguretat i la privadesa de les dades.

4. Són funcions específiques del responsable de sistemes d'informació les següents:

a) Identificar necessitats de seguretat de la informació: l'RSI ha de treballar amb els òrgans jurisdiccionals i les estructures del Consell Superior de la Justícia i de l'Administració de justícia per identificar les necessitats de seguretat de la informació del Consell Superior de la Justícia. Aquestes necessitats poden variar en funció de la naturalesa de les dades que gestiona el Consell Superior de la Justícia.

b) Planificar i desenvolupar la infraestructura de TIC del Consell Superior de la Justícia. Això inclou la planificació de la compra de nous equips i programari, la implementació de noves tecnologies, la resolució de problemes, la prevenció de caigudes, la supervisió del rendiment dels sistemes i la gestió dels sistemes existents.

c) Gestionar les incidències de seguretat: això implica investigar la causa de l'incident, identificar les dades compromeses i prendre mesures correctives.

d) Col·laborar amb els òrgans jurisdiccionals i les estructures del Consell Superior de la Justícia i de l'Administració de justícia per garantir la seguretat de la informació i l'èxit de qualsevol programa de seguretat de la informació.

Dipòsit legal: AND.2-2015

5. Quan la complexitat del sistema ho justifiqui, l'RSI pot proposar al CSI la designació dels responsables del sistema delegats que consideri necessaris, que tenen dependència funcional directa de l'RSI i han de ser responsables en el seu àmbit de totes les accions que els delegui el mateix RSI.

Article 43. *Delegat de la seguretat de la informació (DSI)*

1. El delegat de la seguretat de la informació determina les decisions per satisfer els requisits de seguretat del Consell Superior de la Justícia.

2. El responsable de seguretat exerceix les funcions que li encomana la Llei de mesures per a la seguretat de les xarxes i dels sistemes d'informació i la normativa que la desenvolupa; en concret, són les següents:

a) Dirigir i coordinar el desenvolupament i la implementació de l'SGSI: garanteix que l'SGSI estigui dissenyat i implementat de manera efectiva per protegir la informació del Consell Superior de la Justícia i l'Administració de justícia.

b) Garantir que el Consell Superior de la Justícia i l'Administració de justícia compleixen les normatives i requisits de seguretat aplicables.

c) Informar i formar els treballadors sobre la importància de la seguretat de la informació i com protegir la informació del Consell Superior de la Justícia i de l'Administració de justícia.

d) Elaborar auditories i avaluacions periòdiques de la seguretat de la informació per identificar i resoldre els riscos de seguretat.

e) Recopilar i mantenir un inventari de tots els actius d'informació del Consell Superior de la Justícia i de l'Administració de justícia. Aquest inventari ha de contenir informació sobre la classe de seguretat de cada actiu, la seva ubicació, els seus propietaris i els riscos associats.

f) Formar i sensibilitzar el personal sobre la seguretat informàtica. Aquesta formació ha de cobrir temes de bones pràctiques, com la seguretat de les contrasenyes, l'ús de programari segur i la detecció d'atacs, entre altres.

g) Elaborar i implementar una política de seguretat de la informació. La política de seguretat de la informació defineix els objectius, les mesures i els procediments de seguretat del Consell Superior de la Justícia. L'RSI és responsable de l'elaboració i la implementació d'aquesta política.

h) Supervisar el compliment de la política de seguretat de la informació.

i) Fer una avaluació de riscos de seguretat per identificar i prioritzar els riscos a què estan exposats el Consell Superior de la Justícia i l'Administració de justícia. Aquesta avaluació ha de servir per definir i implementar les mesures de seguretat necessàries per mitigar els riscos identificats.

j) Gestionar la seguretat dels sistemes. Determinar la categoria de cada sistema, elaborar la declaració d'aplicabilitat i decidir sobre les mesures de seguretat addicionals que s'han d'aplicar. També aprovar els procediments operatius de seguretat elaborats per l'RSI i verificar l'estat de la seguretat del sistema monitorat pel DPD.

k) Gestionar la seguretat de la informació. Promoure la formació i la conscienciació sobre la seguretat de la informació entre els treballadors del Consell Superior de la Justícia i de l'Administració de justícia. També validar els plans de continuïtat elaborats per l'RSI i rebre els informes sobre el grau d'implantació i eficàcia de les mesures de seguretat físiques.

l) Gestionar la seguretat dels usuaris. Protegir els sistemes d'informació dels usuaris no autoritzats.

m) Determinar els requisits de seguretat de la informació, així com garantir que es compleixen. També determinar els nivells de seguretat de la informació i participar en l'acceptació final del risc residual.

3. El delegat de seguretat de la informació, en funció de la complexitat de l'organització, pot proposar delegats de les seves funcions per a àrees diferenciades. Aquests delegats són designats pel CSI amb dependència funcional directa del DSI i han d'actuar sota la responsabilitat del DSI.

Dipòsit legal: AND.2-2015

Article 44. *Delegat de protecció de dades (DPD)*

1. Les funcions del delegat de protecció de dades són les establertes a la Llei de protecció de dades personals i normativa que la desenvolupa, i abasten l'assessorament i la supervisió.

2. Abast de les funcions d'assessorament:

a) Aconsellar i assessorar el Consell Superior de la Justícia sobre les seves obligacions en matèria de protecció de dades.

b) Assessorar el responsable o l'encarregat del tractament i els empleats que s'ocupin del tractament de les obligacions de la normativa aplicable en protecció de dades.

c) Informar el responsable o l'encarregat del tractament de les possibles bretxes de seguretat que s'hagin detectat.

d) Mantenir i actualitzar el fitxers a l'Agència Andorrana de Protecció de Dades i fer el seguiment de la legislació de privacitat que afecti el Consell Superior de la Justícia.

e) Assistir al Consell Superior de la Justícia en cas de sol·licituds d'accés, rectificació, supressió, oposició i limitació del tractament, així com en cas de vulneració de la seguretat dels sistemes de tractament de dades.

3. Abast de les funcions de supervisió:

a) Supervisar el compliment de la normativa aplicable en protecció de dades i de les polítiques del responsable o encarregat del tractament en aquesta matèria.

b) Revisar les operacions de tractament de dades personals.

c) Avaluar els riscos que impliquen les operacions de tractament de dades personals.

d) Gestionar operacions que puguin donar lloc a un risc alt.

e) Dur a terme auditories de protecció de dades.

f) Identificar els possibles riscos de seguretat del sistema, avaluar-los i prendre mesures per mitigar-los.

g) Col·laborar amb les autoritats de control.

Disposició addicional

A les entitats que en l'àmbit d'una relació laboral o comercial tractin informació que sigui titularitat del Consell Superior de la Justícia o que estigui sota la seva responsabilitat, se'ls ha d'exigir l'adhesió a aquest sistema de gestió de la seguretat de la informació i el compromís de complir-lo.

Disposició final

El CSI ha de desenvolupar aquest document i proposar per a aprovació del CSJ les normes que siguin necessàries per assegurar l'objectiu de la seguretat de la informació. De forma no limitada, s'han d'elaborar les normes següents:

- Normativa de gestió de riscos.
- Normativa d'ús acceptable.
- Normativa de còpies de seguretat.
- Normativa de gestió d'actius.
- Normativa de gestió del canvi.

Cosa que es fa pública per a coneixement general.

Andorra la Vella, 4 de desembre del 2024

Josep Maria Rossell Pons
President

Dipòsit legal: AND.2-2015