Projecte de decret pel qual s'aprova la Política de Seguretat de la Informació de l'Administració de la Comunitat Autònoma de les Illes Balears

L'article 29 de l'Estatut d'Autonomia encomana als poders públics impulsar l'accés a les noves tecnologies, a la plena integració en la societat de la informació i a la incorporació dels processos d'innovació.

Són aquests poders públics els responsables de generar la confiança dels ciutadans i ciutadanes en l'ús dels mitjans tecnològics en les seves relacions amb les administracions de les Illes Balears. Per aconseguir aquesta confiança, els mitjans tecnològics utilitzats han de ser segurs.

Amb aquest objectiu, el Decret 97/2006, de 24 de novembre, va crear dins l'àmbit de l'Administració de la Comunitat Autònoma de les Illes Balears la Comissió Directora i la Comissió Tècnica de la Seguretat de la Informació encarregades de garantir, dins les respectives funcions, la seguretat dels sistemes d'informació.

Posteriorment, la Llei 4/2011, de 31 de març, de la bona administració i del bon Govern de les Illes Balears reconeix el dret dels ciutadans i les ciutadanes a fer tràmits i rebre informació per mitjans electrònics com un principi informador de la bona administració i dedica l'article 7 als mitjans electrònics, informàtics i telemàtics.

La consolidació del dret de la ciutadania a relacionar-se amb les administracions per mitjans electrònics l'estableix la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques i la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic amb la implantació definitiva de l'ús de les tecnologies de la informació i de les comunicacions dins les administracions públiques, tant per millorar l'eficiència en la gestió com per afavorir les relacions de col·laboració i cooperació entre elles.

Ambdues Lleis juntament amb el Reglament d'actuació i funcionament del sector públic per mitjans electrònics, aprovat pel Reial Decret 203/2021, de 30 de març, determinen el marc jurídic per al funcionament electrònic de l'Administració. En aquest context, la digitalització de l'actuació administrativa com a forma habitual de relació amb la ciutadania i entre les administracions demanda una exigència de fiabilitat a fi que la ciutadania pugui realitzar els seus tràmits administratius de manera segura. La confiança en els sistemes d'informació s'ha d'estendre a les garanties sobre els comunicacions, el tractament i el magatzematge de la informació.

Així mateix, la Llei 39/2015, d'1 d'octubre, entre els drets de les persones en les seves relacions amb les administracions públiques que preveu l'article 13, inclou el relatiu a la protecció de les dades personals i, en particular, a la seguretat de les dades que figuren en els fitxers, sistemes i aplicacions de les administracions públiques.

D'altra banda, la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic estableix en l'article 156 que l'Esquema Nacional de Seguretat, té per objecte establir la política de seguretat en la utilització de mitjans electrònics i l'incorpora com a part essencial en la configuració de l'arxiu electrònic dels documents que regula en l'article 46 i en el règim de relacions electròniques i transferències de tecnologia entre les administracions públiques, tal

com estableix l'article 158.

El Reial Decret 311/2022, de 3 de maig, regula l'Esquema Nacional de Seguretat com a conjunt de principis bàsics i requisits mínims necessaris per a una protecció adequada de la informació tractada i els serveis que presten les entitats que, d'acord amb l'article 2 de la Llei 40/2015, d'1 d'octubre, integren el sector públic amb l'objectiu d'assegurar l'accés, la confidencialitat, la integritat, la traçabilitat, l'autenticitat, la disponibilitat i la conservació de les dades, la informació i els serveis utilitzats per mitjans electrònics que gestionen en l'exercici de les seves competències.

En aquest marc, les tecnologies de la informació i les comunicacions constitueixen un instrument estratègic i necessari de digitalització de l'Administració de la Comunitat Autònoma de les Illes Balears i el seu sector públic autonòmic. Per tant, és imprescindible que els sistemes d'informació i comunicacions s'administrin amb diligència i comptin amb les mesures adequades per protegir-se de qualsevol amenaça amb potencial per incidir en la confidencialitat, la integritat i la disponibilitat de la informació i dels serveis.

L'apartat 1 de l'article 12 del Reial Decret 311/2022 abans esmentat, defineix la política de seguretat de la informació com el conjunt de directrius que regeixen la forma en què una organització gestiona i protegeix la informació que tracta i els serveis que presta. I en l'apartat 2 d'aquest mateix article 12 exigeix que cada administració pública disposi d'una política de seguretat aprovada formalment per l'òrgan competent. Pel que fa als ens del sector públic instrumental, l'article esmentat preveu que es puguin incloure en l'àmbit de la política de seguretat que aprovi l'Administració amb què guardin relació de vinculació, dependència o adscripció, quan així ho determinin els òrgans competents en l'exercici de les potestats d'autoorganització.

L'Administració de la Comunitat Autònoma de les Illes Balears compleix aquest mandat amb l'aprovació d'aquest Decret. La política de seguretat que s'aprova és l'instrument que ha de servir de suport de l'Administració per aconseguir els seus objectius en la utilització segura dels sistemes d'informació i comunicacions, defensar-se de les amenaces, garantir la continuïtat dels sistemes de la informació, minimitzar els riscs de dany i assegurar el compliment eficient dels seus objectius. A tal fi, el Decret determina les mesures de seguretat de naturalesa organitzativa, física i lògica per protegir cada sistema d'informació en l'àmbit de l'Administració de la Comunitat Autònoma, atès que la seguretat, entesa com a procés integral i de millora contínua, comprèn tots els elements tècnics, humans, materials i organitzatius relacionats amb els sistemes d'informació i les comunicacions. Per això, la política de seguretat s'aplica en l'àmbit de l'Administració autonòmica i dels ens del sector públic que no tenguin aprovada una de pròpia i s'hi adhereixin, i a tots els actius de la informació dels quals en siguin titular o gestor.

La política de seguretat de l'Administració de la Comunitat Autònoma constitueix el marc de referència orientat a facilitar la gestió, l'administració i la implementació dels mecanismes i procediments de seguretat que estableix l'Esquema Nacional de Seguretat. Estableix els pilars del cos normatiu de seguretat d'aquesta Administració i l'estructura organitzativa que ha de vetllar pel seu compliment, i identifica els deures que tenen els distints responsables que s'integren en aquesta estructura.

També, en la configuració de la política de seguretat que aprova aquest Decret s'han tengut en consideració les guies del Centre Criptològic Nacional (CNN), especialment, les guies CCN-

STIC-801 i CCN-STIC-805 les quals orienten a les administracions públiques no solament a tenir models de polítiques de la seguretat de la informació, sinó també a determinar les responsabilitats i funcions dels distints òrgans de la gestió de la seguretat de la informació, entre els quals hi ha l'establiment d'un comitè a molt alt nivell, atès que la seguretat de la informació és un procés que pot implicar distints àmbits, fora dels exclusivament tecnològics, com ara, els operatius, pressupostari, legal o de relacions amb les forces de seguretat. Addicionalment i, tenint en compte la possibilitat no menyspreable que en algun moment, malgrat les proteccions que es vagin desenvolupant, ocorrin incidents de seguretat que poden arribar a ser greus o crítics, el Decret crea uns òrgans de crisi amb unes funcions acordes amb la guia del CCN -CERT BP/ 20 de bones pràctiques en la gestió de cibercrisis.

Al seu torn, el Reial decret 311/2022, de 3 de maig, determina que la política de seguretat ha de ser coherent amb el que estableix el Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques respecte del tractament de dades personals i la normativa vigent en aquesta matèria, la qual té caràcter prevalent amb relació a la protecció de dades de caràcter personal en cas de discrepància.

En l'elaboració del Decret s'han observat els principis de bona regulació de l'article 49 de la Llei 1/2019, de 31 de gener, del Govern de les Illes Balears. En concret, s'adequa als principis de necessitat i eficàcia, atès que amb l'aprovació de la Política de Seguretat de la Informació l'Administració de la Comunitat Autònoma es dotarà d'un marc de protecció en l'ús dels sistemes de la informació dins l'àmbit de l'Administració autonòmica i la seva regulació, que adopta la forma i el rang de Decret, és la idònia per assolir els objectius que es volen aconseguir. Així mateix, s'adequa al principi de proporcionalitat perquè inclou el contingut imprescindible que exigeix l'Esquema Nacional de Seguretat a fi d'assolir l'objectiu perseguit. D'acord amb el principi d'eficiència, la norma no compta amb càrregues administratives innecessàries o accessòries. S'ha garantit la transparència en la tramitació de la norma i s'ha assegurat la participació de les persones interessades. Igualment, s'ajusta al principi de seguretat jurídica, atès que estableix regles clares amb la finalitat de garantir la millor protecció dels sistemes de la informació i és coherent amb la resta de l'ordenament jurídic, i també al principis de qualitat i simplificació en la mesura que en l'elaboració d'aquest decret s'ha seguit el procediment establert legalment, amb respecte als principis de bona regulació i s'ajusta a les directrius que són d'aplicació en relació amb la forma i estructura dels texts normatius.

Per tot això, a proposta del conseller d'Economia, Hisenda i Innovació, d'acord/oït el Consell Consultiu de les Illes Balears i havent-ho considerat el Consell de Govern de les Illes Balears en la sessió de ...

DECRET

CAPÍTOL I

Disposicions generals

Article 1
Objecte

1. El Decret té per objecte aprovar la Política de Seguretat de la Informació de l'Administració de la Comunitat Autònoma de les Illes Balears (en endavant, PSI-CAIB), així com el seu marc

organitzatiu i de gestió.

Article 2
Àmbit d'aplicació

1. Aquest Decret s'aplica a l'Administració de la Comunitat Autònoma de les Illes Balears.

2. Els ens del sector públic autonòmic han d'aprovar la seva política de seguretat pròpia, que ha de ser coherent amb la PSI-CAIB i ha de respectar els principis fonamentals que estableix l'article 4 del Decret.

No obstant, es podran adscriure a la PSI-CAIB quan així ho determinin els òrgans competents dels ens, en l'exercici de les potestats d'organització. En aquest supòsit,el secretari de l'òrgan competent de l'ens ha de trametre el certificat de l'acord d'adhesió adoptat al secretari de la Comissió Directora de la Seguretat de la Informació.

3. La PSI-CAIB s'aplica als actius de tecnologies de la informació i de les comunicacions dels quals l'Administració autonòmica n'és titular o en tingui encomanada la gestió.

4. A efectes d'aquest Decret, es remet a les definicions d'actiu i de sistema d'informació establertes en l'annex IV del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (en endavant, Esquema Nacional de Seguretat).

Article 3
Missió

1. L'Administració de la Comunitat Autònoma de les Illes Balears té com a missió servir amb objectivitat els interessos generals i actuar d'acord amb els principis constitucionals d'eficàcia, de jerarquia, de descentralització, de desconcentració i de coordinació per aconseguir els objectius que estableixen les lleis i l'ordenament jurídic.

2. Els objectius en matèria de seguretat que l'Administració de la Comunitat Autònoma pretén garantir amb la PSI-CAIB són:

- Garantir la confidencialitat, integritat i autenticitat de la informació i la continuïtat en la prestació dels serveis.

- Implementar mesures de seguretat en funció del risc.

- Formar i conscienciar a tots els nivells de l'Administració autonòmica respecte de la seguretat de la informació a fi que totes les persones que intervenen en el procés i els seus responsables jeràrquics tenguin una sensibilitat vers els riscos que poden córrer.

- Implementar mesures de seguretat que permetin la traçabilitat dels accessos i respectar, entre altres, el principi de mínim privilegi, reforçant també el deure de confidencialitat de les persones usuàries en relació amb la informació que coneixen en exercici de les seves funcions.

- Desplegar i controlar la seguretat física per tal que els actius de la informació es

trobin en àrees segures, protegits per controls d'accés, atesos els riscos detectats.

- Establir la seguretat en la gestió de les comunicacions, mitjançant els procediments necessaris, per aconseguir que la informació que es transmeti per les xarxes de comunicacions estigui degudament protegida.

- Controlar l'adquisició, desenvolupament i manteniment dels sistemes d'informació en totes les fases del cicle de vida dels sistemes de la informació, garantint la seguretat per defecte.

- Controlar el compliment de les mesures de seguretat en la prestació dels serveis i mantenir el control en l'adquisició i incorporació de nous components del sistema.

- Gestionar els incidents de seguretat per a la correcta detecció, contenció, mitigació i resolució d'aquests, adoptant les mesures necessàries per evitar que es tornin a reproduir.

- Protegir la informació personal, adoptant les mesures tècniques i organitzatives en atenció als riscs derivats del tractament conforme a la legislació en matèria de protecció de dades.

- Supervisar de forma continuada el sistema de gestió de la seguretat, millorant i corregint les ineficiències detectades.

Article 4
Principis fonamentals

1. Els principis són directrius fonamentals de seguretat que han de tenir-se sempre presents en qualsevol activitat relacionada amb l'ús dels actius d'informació.

2. La PSI-CAIB, s'ha de desenvolupar, amb caràcter general, d'acord amb els principis següents:

a) Seguretat com a procés integral: la seguretat s'entén com un procés integral constituït per tots els elements tècnics, humans, materials, jurídics i organitzatius. La seguretat de la informació ha de considerar-se com a part de l'operativa habitual i s'ha d'aplicar des del disseny inicial dels sistemes d'informació, ha de proporcionar les funcionalitats mínimes requerides i ha de fer que l'ús ordinari del sistema sigui senzill i segur, de manera que una utilització insegura requereixi un acte conscient per part de l'usuari. A més, les especificacions de seguretat s'han d'incloure en totes les fases del cicle de vida dels serveis i sistemes, acompanyades dels corresponents procediments de control, i s'ha de conèixer en tot moment l'estat de seguretat dels sistemes, en relació amb les especificacions dels fabricants, les vulnerabilitats i les actualitzacions que els afectin, i s'ha de reaccionar amb diligència per gestionar el risc en vista de l'estat de seguretat.

b) Gestió de la seguretat basada en els riscos: l'anàlisi i gestió de riscos és part essencial del procés de seguretat i constitueix una activitat contínua i actualitzada. La gestió de riscos permet el manteniment d'un entorn controlat, minimitzant els riscos fins a nivells acceptables. La reducció d'aquests nivells es realitza mitjançant el

desplegament de mesures de seguretat, que estableixen un equilibri entre la naturalesa de les dades i els tractaments, entre l'impacte i la probabilitat dels riscos als quals estiguin exposats i entre l'eficàcia i el cost de les mesures de seguretat.

c) Prevenció, detecció, resposta i conservació: s'han de contemplar accions relatives als aspectes de prevenció, detecció i resposta, a fi de minimitzar les vulnerabilitats i aconseguir que les amenaces no es materialitzin o que, en el cas de fer-ho, no afectin greument la informació que maneja o els serveis que presta.

d) Existència de línies de defensa: el sistema d'informació ha de disposar d'una estratègia de protecció constituïda per múltiples capes de seguretat, constituïdes, al seu torn, per mesures de naturalesa organitzativa, física i lògica.

e) Vigilància contínua i reavaluació periòdica: les mesures de seguretat s'han de reavaluar i actualitzar periòdicament per a adequar la seva eficàcia a la constant evolució dels riscos i sistemes de protecció. L'avaluació permanent de l'estat de seguretat ha de servir per mesurar l'evolució del sistema de gestió de seguretat de la informació, així com per detectar vulnerabilitats, deficiències de configuració i activitats o comportaments anòmals i respondre de manera oportuna. La seguretat de la informació ha de ser atesa, revisada i auditada per personal qualificat, diferenciat, dedicat i instruït en totes les fases del cicle de vida dels sistemes d'informació.

f) Responsabilitat diferenciada: en els sistemes d'informació s'ha de diferenciar el responsable de la informació, el responsable del servei, el responsable de seguretat i el responsable del sistema. La responsabilitat de la seguretat dels sistemes d'informació ha d'estar diferenciada de la responsabilitat sobre l'explotació d'aquests sistemes d'informació.

g) Principi de proporcionalitat: la implantació de les mesures que mitiguin els riscos de seguretat dels actius de tecnologies de la informació i de les comunicacions s'ha de fer sota un enfocament de proporcionalitat, tant respecte dels costos econòmics i operatius, com respecte dels riscs i gravetat de la informació i dels serveis afectats.

h) Principi de conscienciació i formació: s'han d'articular iniciatives que permetin a les persones usuàries conèixer els seus deures i obligacions pel que fa al tractament segur de la informació. Igualment, s'ha de fomentar la formació específica en matèria de seguretat de tecnologies de la informació i de les comunicacions de totes aquelles persones que gestionen i administren sistemes d'informació i de les comunicacions.

Article 5
Marc normatiu

1. El marc normatiu en què es desenvolupen les activitats de l'Administració de la Comunitat Autònoma de les Illes Balears en l'àmbit de la seguretat de la informació és el següent:

a) Reglament 2016/679 del Parlament Europeu 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 i pel qual es deroga la Directiva 95/46/CE (en endavant, Reglament general de protecció de dades).

b) Reglament 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a

la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i pel qual es deroga la Directiva 1999/93/CE.

c) Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

d) Llei 6/2020, d' 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.

e) Llei 9/2017, de 8 de novembre, de contractes del sector públic per la qual es transposen a l'ordenament jurídic espanyol les directives del Parlament Europeu i del Consell 2014/23/UE i 2014/24/UE, de 26 de febrer de 2014.

f) Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.

g) Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.

h) Llei 4/2011, de 31 de març, de la bona administració i del bon govern de les Illes Balears.

i) Llei 3/2003, de 26 de març, de règim jurídic de l'Administració de la Comunitat Autònoma de les Illes Balears.

j) Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació.

k) Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.

l) Reial decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics.

m) Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'administració electrònica.

n) Ordre PCI/487/2019, de 26 d'abril, per la que es publica l'Estratègia Nacional de Ciberseguretat 2019, aprovada pel Consell de Seguretat Nacional.

o) Decret 24/2022, d'11 de juliol, de la Comissió Superior de Sistemes d'Informació en Tecnologia i Comunicacions.

p) Decret 113/2010, de 5 de novembre, d'accés electrònic als serveis públics de l'Administració de la Comunitat Autònoma de les Illes Balears.

q) Decret 107/2006, de 15 de desembre, de regulació de l'ús de la signatura electrònica en l'àmbit de l'Administració de la Comunitat Autònoma de les Illes Balears.

r) Decret 10/2025, de 14 de juliol, de la presidenta de les Illes Balears, pel qual s'estableixen les competències i l'estructura orgànica bàsica de les conselleries de l'Administració de la Comunitat Autònoma de les Illes Balears.

s) La resta de normativa que complementi, desplegui o substitueixi les anteriors i que es trobin dins l'àmbit d'aplicació de la PSI-CAIB.

2. Igualment, formen part del marc regulador de la PSI-CAIB totes les normes a què fa referència el Capítol III.

CAPÍTOL II
Estructura organitzativa

Article 6
Organització de la seguretat de la informació

1. La preservació de la seguretat és un objectiu comú de tot el personal, òrgans i unitats de l'Administració de la Comunitat Autònoma de les Illes Balears.

2. L'estructura organitzativa de gestió de la seguretat de la informació de l'Administració de la Comunitat Autònoma està composta per:

a) Comissió Directora de la Seguretat de la Informació.

b) Comissió Tècnica de la Seguretat de la Informació.

c) Responsables de la informació.

d) Responsables del servei.

e) Responsables de seguretat.

f) Responsables del sistema.

g) Administradors de la seguretat del sistema.

Article 7
Comissió Directora de la Seguretat de la Informació

1. La Comissió Directora de la Seguretat de la Informació és l'òrgan col·legiat encarregat de donar l'impuls organitzatiu i normatiu necessari en matèria de seguretat de la informació. La Comissió s'adscriu a la Conselleria d'Economia, Hisenda i Innovació, a través de la Direcció General d'Estratègia Digital i Desenvolupament Tecnològic.

2. Aquesta Comissió té la composició següent:

a) La presidència, que ocupa el conseller d'Economia, Hisenda i Innovació.

b) La vicepresidència, que ocupa el director general d'Estratègia Digital i Desenvolupament Tecnològic.

c) Vocals:

- El secretari general de la Conselleria de Presidència, Coordinació de l'Acció de Govern i Cooperació Local.
- El director general de Funció Pública .
- El director general d'Emergències i Interior.
- El director de la Direcció de l'Advocacia de la Comunitat Autònoma.
- L'interventor general de la Comunitat Autònoma.

d) La secretaria, que ocupa el cap del Departament de Ciberseguretat i Telecomunicacions.

3. Podran assistir, amb veu però sense vot, els òrgans directius de la conselleria o de l'ens del sector públic autonòmic promotor de la proposta en matèria de seguretat de la informació que, si n'és el cas, hagi de formar part de l'ordre del dia de la sessió.

4. El president, per iniciativa pròpia o a proposta de qualsevol dels seus membres, pot convocar, amb veu i sense vot, els òrgans directius diferents del promotor, quan es tractin assumptes que afectin les seves competències.

5. La Comissió pot nomenar els assessors que consideri oportuns, amb caràcter permanent o puntual, els quals podran ser convidats a assistir a les sessions, amb veu però sense vot.

6. El vicepresident substitueix el president en cas de vacant, absència, malaltia o qualsevol altra causa justificada.

7. En casos de vacant, d'absència, malaltia i, en general, quan es doni alguna causa justificada, el vicepresident i els vocals poden designar altres persones perquè assisteixin a les sessions amb plenes facultats per exercir les funcions pròpies d'aquests membres. La designació es pot fer entre persones funcionàries amb dependència orgànica del vicepresident o del vocal de què es tracti en cada cas, amb rang mínim de cap de servei, o entre les persones titulars dels òrgans directius de la conselleria de què es tracti.

8. En cas de vacant, absència, malaltia o qualsevol altre impediment justificat del secretari, el suplirà la persona que determini el president de la Comissió.

9. S'atribueixen a aquesta Comissió les funcions següents:

a) Aprovar la proposta de la política de seguretat de la informació i les seves modificacions, i elevar-la al conseller d'Economia, Hisenda i Innovació perquè n'impulsi la tramitació.

b) Vetllar pel compliment de la PSI-CAIB, impulsar-ne el desenvolupament i compliment normatiu, i també fer-ne difusió.

c) Elaborar l'estratègia d'evolució de l'organització respecte a la seguretat de la informació.

d) Rebre l'informe consolidat de l'estat de seguretat de l'Administració de la Comunitat Autònoma que elabori la Comissió Tècnica de Seguretat de la Informació.

e) Resoldre, en darrera instància, els conflictes de responsabilitat en els termes que s'estableixen en l'article 18.

f) Proveir els recursos i mitjans necessaris per assegurar la conscienciació i formació en matèria de seguretat de la informació de tot el personal afectat per aquest Decret.

g) Promoure la millora contínua del sistema de gestió de la seguretat de la informació.

h) Implementar les mesures organitzatives de seguretat d'acord amb els plans de millora.

10. La Comissió Directora de la Seguretat de la Informació pot encomanar a la Comissió Tècnica de la Seguretat de la Informació les tasques necessàries per al millor exercici de les seves funcions.

11. La Comissió s'ha de reunir de manera ordinària una vegada a l'any i, de manera extraordinària, a petició motivada de qualsevol membre.

12. La Comissió es regeix pel que s'estableix en aquest Decret i pel que disposen els articles 15 a 18 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, i el capítol V del títol I de la Llei 3/2003, de 26 de març, de règim jurídic de l'Administració de la Comunitat Autònoma de les Illes Balears.

Article 8
Comissió Tècnica de la Seguretat de la Informació

1. La Comissió Tècnica de la Seguretat de la Informació és l'òrgan col·legiat encarregat de coordinar i impulsar els aspectes tècnics en matèria de seguretat de la informació. La Comissió s'adscriu a la Conselleria d'Economia, Hisenda i Innovació, a través de la Direcció General d'Estratègia Digital i Desenvolupament Tecnològic.

2. Aquesta Comissió té la composició següent:

a) La presidència, que ocupa el director general d'Estratègia Digital i Desenvolupament Tecnològic.

b) La vicepresidència, que ocupa el cap del Departament de Ciberseguretat i Telecomunicacions.

c) Vocals:

- El director general d'Innovació i Transformació Digital.
- El cap del Departament de Desenvolupament Tecnològic.
- El cap del Departament d'Infraestructures Tecnològiques i Plataformes Corporatives
- El cap del Departament de l'Oficina d'Administració Digital.
- El cap del Servei Jurídic d'Administració Digital.

b) La secretaria, que ocupa el cap del Servei de Ciberseguretat.

3. El Delegat de Protecció de Dades de l'Administració de la Comunitat de les Illes Balears hi ha d'assistir amb veu però sense vot quan es tractin qüestions relatives a la protecció de dades de caràcter personal.

4. Podran assistir, amb veu però sense vot, els òrgans directius de la conselleria o de l'ens del sector públic autonòmic promotor de la proposta en matèria de seguretat de la informació que, si n'és el cas, hagi de formar part de l'ordre del dia de la sessió.

5. El president, per iniciativa pròpia o a proposta de qualsevol dels seus membres, pot convocar, amb veu i sense vot, els òrgans directius diferents del promotor, quan es tractin assumptes que afectin les seves competències.

6. La Comissió pot nomenar els assessors que consideri oportuns, amb caràcter permanent o puntual, i els pot convidar a assistir a les sessions, amb veu però sense vot.

7. El vicepresident substitueix el president en cas de vacant, absència, malaltia o qualsevol altra causa justificada.

8. En casos de vacant, absència, malaltia i, en general, quan es doni alguna causa justificada, el vicepresident i els vocals poden designar altres persones perquè assisteixin a les sessions amb plenes facultats per exercir les funcions pròpies d'aquests membres. La designació es pot fer entre persones funcionàries amb dependència orgànica del vicepresident o del vocal de què es tracti en cada cas, amb rang mínim de cap de secció.

9. En cas d'absència o qualsevol altre impediment justificat del secretari, l'ha de suplir la persona que determini el president de la Comissió.

10. S'atribueixen a aquesta Comissió les funcions següents:

a) Elevar la proposta de la política de seguretat de la informació de l'Administració de la Comunitat Autònoma de les Illes Balears a la Comissió Directora de la Seguretat de la Informació, revisar-la anualment i proposar-ne les modificacions.

b) Revisar, si escau, les propostes de les polítiques de seguretat de la informació dels ens del sector públic autonòmic i assabentar-ne la Comissió Directora de Seguretat de la Informació.

c) Proposar les normes de segon nivell d'acord amb l'article 13.

d) Proposar a la Comissió Directora de la Seguretat de la Informació les mesures organitzatives a implementar d'acord amb els plans de millora de la seguretat de la informació.

e) Prioritzar les actuacions en matèria de seguretat quan els recursos siguin limitats.

f) Realitzar les tasques de suport encomanades per la Comissió Directora de la Seguretat de la Informació d'acord amb l'apartat 10 de l'article 7.

g) Elaborar l'informe consolidat de l'estat de seguretat de la informació de l'Administració de la Comunitat Autònoma amb base als informes dels responsables de seguretat, i elevar-lo a la Comissió Directora de Seguretat de la Informació.

h) Vetllar perquè la creació i utilització de serveis horitzontals permetin la reducció de duplicitats i tenguin un funcionament homogeni als sistemes d'informació.

i) Monitorar els principals riscs residuals que assumeixen els responsables del servei i responsables de la informació i recomanar possibles actuacions.

j) Promoure auditories periòdiques i/o autoavaluacions que permetin verificar el compliment de les obligacions de la l'Administració de la Comunitat Autònoma en matèria de seguretat de la informació.

k) Resoldre els conflictes de responsabilitat en els termes que s'estableixen a l'article 18.

l) Aprovar els plans de millora i de continuïtat de la seguretat.

11. La Comissió s'ha de reunir de manera ordinària cada tres mesos i, de manera extraordinària, a petició motivada de qualsevol membre.

12. Els acords s'han d'adoptar per majoria de vots. En cas d'empat, el president té vot de qualitat.

13. La Comissió es regeix pel que s'estableix en aquest Decret i pel que disposen els articles 15 a 18 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, i el capítol V del títol I de la Llei 3/2003, de 26 de març, de règim jurídic de l'Administració de la Comunitat Autònoma de les Illes Balears.

Article 9
Responsables de la informació

1. El responsable de la informació és la persona que determina els requisits de seguretat de la informació.

2. Aquesta responsabilitat recau en els òrgans directius de les conselleries respecte de la

informació tractada en l'àmbit de les seves competències.

3. Són funcions dels responsables de la informació:

a) Aprovar els nivells de seguretat de la informació, valorant els impactes dels incidents que afectin la seguretat de la informació en cadascuna de les dimensions de seguretat que estableix l'Esquema Nacional de Seguretat. Per a aquesta aprovació pot obtenir una proposta del responsable de la seguretat i, si escau, del responsable del sistema.

b) Assignar els recursos econòmics i humans necessaris per dur a terme els anàlisis de riscos i els seus controls compensatoris.

c) Acceptar, juntament amb els responsables del servei, els riscos residuals calculats a l'anàlisi de riscos i realitzar-ne el seguiment i control, sens perjudici de la possibilitat de delegar aquesta darrera tasca.

d) Proposar al responsable de seguretat la suspensió del tractament de la informació o la prestació del servei corresponent si s'aprecien deficiències greus de seguretat.

e) Aprovar les normes de tercer nivell d'acord amb l'article 16.

f) Exercir qualsevol altra funció prevista per la normativa de seguretat.

Article 9
Responsables del servei

1. El responsable del servei és la persona que determina els requisits de seguretat dels serveis prestats.

2. Aquesta responsabilitat recau en els òrgans directius de les conselleria que gestionin els procediments o tràmits del servei prestat dins l'àmbit de les seves competències.

3. Són funcions dels responsables del servei:

a) Aprovar els nivells de seguretat del servei prestat, valorant els impactes dels incidents que afectin la seguretat de la informació en cadascuna de les dimensions de seguretat que estableix l'Esquema Nacional de Seguretat. Per a la seva aprovació pot obtenir una proposta del responsable de la seguretat i, si escau, del responsable del sistema.

b) Assignar els recursos econòmics i humans necessaris per dur a terme els anàlisis de riscos i els seus controls compensatoris

c) Acceptar, juntament amb els responsables de la informació, els riscos residuals calculats a l'anàlisi de riscos i de realitzar el seu seguiment i control, sense perjudici de la possibilitat de delegar aquesta darrera tasca.

d) Proposar al responsable de seguretat la suspensió de tractament de la prestació del servei si s'aprecien deficiències greus de seguretat.

e) Aprovar les normes de tercer nivell d'acord amb l'article 16.

f) Exercir qualsevol altra funció prevista per la normativa de seguretat.

Article 10
Responsables de seguretat

1. El responsable de seguretat és la persona que determina les decisions per satisfer els requisits de seguretat de la informació i dels serveis, supervisa la implantació de mesures necessàries per garantir que se satisfan els requisits i informa sobre aquests aspectes.
2. El responsable de cada servei ha de nomenar el responsable de seguretat. Quan la gestió de la seguretat d'un sistema d'informació l'assumeixi per raó de competència la Direcció General d'Estratègia Digital i Desenvolupament Tecnològic, el responsable de seguretat serà el cap del Departament de Ciberseguretat i Telecomunicacions d'aquesta Direcció General, que podrà delegar aquesta funció en els caps de servei adscrits a aquest Departament.
3. El càrrec de responsable de seguretat és incompatible amb els càrrecs de responsable del sistema, del servei i de la informació. En tot cas, no pot haver-hi dependència jeràrquica entre el responsable de seguretat i el responsable del sistema. Aquesta restricció no és aplicable als sistemes d'informació l'objecte principal dels quals sigui la prestació de serveis de seguretat de la informació.
4. Són funcions del responsable de seguretat:

    a) Vetllar perquè la seguretat s'apliqui en tots els sistemes d'informació durant tot el seu cicle de vida.

    b) Vetllar pel compliment del cos normatiu definit en l'article 13.

    c) Col·laborar en l'elaboració de les normes de segon i tercer nivell definides en l'article 13.

    d) Aprovar les normes de tercer nivell d'acord amb l'article 13.

    e) Promoure la seguretat de la informació manejada i dels serveis electrònics prestats pels sistemes d'informació.

    f) Mantenir la documentació de seguretat organitzada i actualitzada, i gestionar els mecanismes per accedir-hi, juntament amb el responsable del sistema.

    g) Proposar les activitats de conscienciació i formació en matèria de seguretat.

    h) Coordinar i fer el seguiment de l'adequació a l'Esquema Nacional de Seguretat.

    i) Supervisar el funcionament les mesures de seguretat de la informació, ja siguin de caràcter tecnològic o organitzatiu, i realitzar controls per comprovar-ne l'efectivitat.

    j) Realitzar auditories periòdiques per verificar el compliment de les obligacions en matèria de seguretat de la informació i analitzar els informes d'auditoria, elaborant les conclusions, que s'han de presentar al responsable del sistema per tal que adopti les mesures correctores adients.

    k) Elaborar informes periòdics de seguretat que incloguin els incidents més rellevants i elevar-los a la Comissió Tècnica de Seguretat de la Informació.

    l) Determinar la categoria del sistema d'informació segons el procediment descrit a l'Esquema Nacional de Seguretat i les mesures de seguretat que han d'aplicar-se.

    m) Realitzar els anàlisis de riscos i fer el seguiment del procés de gestió del risc.

    n) Aprovar la declaració d'aplicabilitat, que comprèn la relació de mesures de seguretat seleccionades per a un sistema d'informació.

    o) Elaborar els plans de millora de la seguretat i els plans de continuïtat, juntament amb el responsable del sistema.

p) Aprovar, amb caràcter previ a la implantació, els canvis que impliquin un risc de nivell alt en la seguretat del sistema.

q) Ordenar la suspensió del tractament de la informació o de la prestació del servei corresponent si s'aprecien deficiències greus de seguretat, i informar-ne els responsables de la informació, del servei i del sistema.

r) Exercir qualsevol altra funció prevista per la normativa de seguretat.

Article 11
Responsable del sistema

1. El responsable del sistema és l'encarregat de desenvolupar la forma concreta d'implementar la seguretat en el sistema i de supervisar-ne l'operació diària. Pot delegar aquesta darrera tasca en els administradors de seguretat.
2. El responsable de cada servei ha de nomenar un responsable de sistema. En el cas que la gestió de la seguretat d'un sistema d'informació l'assumeixi, per raó de competència, la Direcció General d'Estratègia Digital i Desenvolupament Tecnològic, el responsable del sistema serà el cap del Departament de Infraestructures Tecnològiques i Plataformes Corporatives, que podrà delegar en els caps de servei adscrits a aquest Departament. En el supòsit en què l'explotació i manteniment del sistema informàtic estigui externalitzat, el contracte ha de recollir l'obligació del compliment de les funcions pròpies del responsable del sistema.

3. Són funcions pròpies del responsable del sistema:

a) Operar i mantenir el sistema durant tot el seu cicle de vida i responsabilitzar-se de les seves especificacions, de la instal·lació i de la verificació del seu correcte funcionament.

b) Definir la tipologia i la política de gestió del sistema, i establir els criteris d'ús i els serveis de què disposa.

c) Comprovar que les mesures específiques de seguretat s'integren adequadament dins el marc general de seguretat.

d) Suspendre l'ús de la informació o de la prestació d'un determinat servei si l'informen de deficiències greus de seguretat que puguin afectar la satisfacció dels requisits que s'hagin establert, i informar-ne immediatament els responsables de la seguretat, del servei i de la informació.

e) Proposar les normes de tercer nivell, d'acord amb l'article 13.

f) Elaborar els plans de millora de la seguretat i els plans de continuïtat, juntament amb el responsable de la seguretat.

g) Mantenir la documentació de seguretat organitzada i actualitzada, i gestionar els mecanismes per accedir-hi, juntament amb el responsable de seguretat.

h) Qualsevol altra funció en l'àmbit de la seguretat de sistemes d'informació que li sigui encomanada a través de la normativa de seguretat.

Article 12
Administradors de la seguretat del sistema

1. Els administradors de la seguretat del sistema, designats pel responsable de seguretat o pel responsable del sistema, tenen les funcions següents dins del seu àmbit de responsabilitat:

a) Implementar, gestionar i mantenir les mesures de seguretat aplicables al sistema d'informació.

b) Gestionar, configurar i actualitzar el hardware i software en els quals es basen els mecanismes i serveis de seguretat del sistema d'informació.

c) Gestionar les autoritzacions concedides als usuaris del sistema i monitorar l'activitat desenvolupada en el sistema per comprovar que s'ajusta a allò autoritzat.

d) Aplicar els procediments de seguretat de la informació.

e) Assegurar que es compleixen estrictament els controls de seguretat establerts .

f) Assegurar que s'apliquen els procediments aprovats per manejar el sistema d'informació.

g) Supervisar les instal·lacions de hardware i software, així com les seves modificacions i millores, per tal d'assegurar que la seguretat no es troba compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.

h) Monitorar l'estat de la seguretat dels sistemes obtingut a través de les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica.

i) Informar als responsables de la seguretat i als responsables del sistema de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.

j) Col·laborar en la investigació i resolució d'incidents de seguretat, des de la seva detecció fins a la seva resolució.

k) Mantenir la documentació de seguretat organitzada i actualitzada, i gestionar els mecanismes per accedir-hi, juntament amb el responsable de seguretat.

l) Qualsevol altra funció que dins el seu àmbit d'actuació li encomani el responsable de seguretat o del sistema.

CAPÍTOL III

Cos normatiu de seguretat de la informació

Article 13
Estructura del cos normatiu

1. El cos normatiu de seguretat de la informació és d'obligat compliment i s'ha de basar en el principis fonamentals de l'article 4.

2. El cos normatiu de seguretat de la Informació ha d'estar a disposició de totes les persones que necessitin conèixer-lo, en particular d'aquelles que utilitzin, operin o administrin els sistemes d'informació i comunicacions.

3. El cos normatiu de seguretat de la informació s'estructura en els quatre nivells següents relacionats jeràrquicament, de manera que cada norma estigui fonamentada en les normes de nivell superior:

a) Primer nivell normatiu: està constituït per la PSI-CAIB i la normativa de caràcter general sobre la seguretat de la informació.

b) Segon nivell normatiu: està constituït principalment per les normes i directrius de seguretat generals que, d'acord amb la PSI-CAIB, determinen què es pot fer i què no des del punt de vista de la seguretat, sense entrar en detalls d'implementació ni tecnològics. En tot cas, els documents han de descriure, com a mínim, les mesures tècniques i organitzatives necessàries per a assegurar el control d'accés als sistemes d'informació, controlant i limitant les autoritzacions i l'accés a les seves funcions.

La documentació d'aquest segon nivell l'ha d'aprovar el director general d'Estratègia Digital i Desenvolupament Tecnològic, a proposta de la Comissió Tècnica de Seguretat de la Informació.

c) Tercer nivell normatiu: està constituït pels documents en què es formalitzen els procediments tècnics, incloent detalls d'implementació i tecnològics, i que expliquen com s'han de dur a terme determinades tasques amb respecte als principis de seguretat així com als processos interns que s'hi estableixin. En concret, els documents han de determinar com dur a terme les tasques habituals, qui ha de fer cada tasca, com identificar i reportar comportaments anòmals i la forma en què s'ha de tractar la informació en funció del nivell de seguretat que requereix.

La documentació d'aquest nivell l'han d'aprovar, segons l'àmbit de competència, els responsables de seguretat, o els responsables de la informació o dels serveis. Es poden aplicar a un àmbit organitzatiu específic o a un sistema d'informació determinat.

d) Quart nivell normatiu: està constituït per documentació de caràcter formatiu, com ara guies o recomanacions, amb la finalitat d'orientar als usuaris en l'aplicació correcta de les mesures de seguretat, en especial proporcionant raonaments on no existeixen procediments precisos.

La documentació d'aquest nivell l'han d'aprovar, segons l'àmbit de competència, els responsables de seguretat, o els responsables de la informació o dels serveis. Es poden aplicar a un àmbit organitzatiu específic o a un sistema d'informació determinat.

CAPÍTOL IV

Protecció de dades de caràcter personal

Article 14
Mesures de protecció de dades de caràcter personal

1. La seguretat de les dades personals, inclosa la protecció contra el tractament no autoritzat o il·lícit i contra la seva pèrdua, destrucció o mal accidental, constitueix un dels principis que han de regir el seu tractament.

2. Quan un sistema d'informació tracti dades de caràcter personal, també li serà d'aplicació la normativa en matèria de protecció de dades personals.

3. En aquests supòsits, el responsable o l'encarregat del tractament, amb l'assessorament del delegat de protecció de dades, ha de realitzar l'anàlisi de riscs o, si escau, l'avaluació de l'impacte relatiu a la protecció de dades, tal com estableixen els articles 24 i 35 del Reglament 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, i en la Llei orgànica 3/2018, de 5 de desembre.

4. En el cas que l'anàlisi de riscos o de l'impacte a què es refereix l'apartat anterior determini mesures de seguretat agreujades respecte de les que preveu l'Esquema Nacional de Seguretat, aquelles seran les que s'han d'implementar amb caràcter prevalent en la protecció de dades de caràcter personal.

CAPÍTOL V

Gestió de la seguretat

Article 15
Gestió de riscos

1. La gestió de riscos s'ha de realitzar de manera contínua sobre els sistemes d'informació, d'acord amb els principis de gestió de la seguretat basada en els riscos, de vigilància contínua i reavaluació periòdica que defineix l'article 4.

2. El procés de gestió de riscos comprèn les fases de categorització dels sistemes, anàlisi de riscos i selecció de mesures de seguretat a aplicar, que han de ser proporcionals als riscos i han d'estar justificades.

3. Les fases de la gestió de riscos esmentades en l'apartat anterior s'han de realitzar d'acord amb els als annexos I i II de l'Esquema Nacional de Seguretat.

4. Els responsables del servei o els responsables de la informació són els encarregats de sol·licitar l'anàlisi de riscos preceptiu.

5. Els responsables de seguretat, una vegada que els responsables de la informació i del servei hagin qualificat la informació i hagin determinat el nivell de seguretat del sistema, han de realitzar els anàlisis de riscos amb la col·laboració d'aquests responsables, i elaboraran la declaració d'aplicabilitat i el conjunt de mesures per garantir la confidencialitat, la integritat, la disponibilitat, l'autenticitat i la traçabilitat de la informació i del servei respectiu. L'anàlisi dels riscos ha d'identificar els riscos residuals, amb base en els quals determinaran el tractament adequat i el comunicaran als responsables de la informació i del servei.

6. Els anàlisis de riscos, així com el seu tractament, s'han de realitzar també quan es detectin incidents de seguretat o s'identifiquin canvis organitzatius, metodològics, legals o tecnològics que puguin suposar un increment del risc a què es troben exposats els sistemes d'informació.

7. Quan de l'anàlisi de riscos realitzat resulti probable que el tractament suposi un risc significatiu per als drets i les llibertats de les persones, conforme a l'article 35 del Reglament (UE) 2016/679 els responsables del tractament, amb l'assessorament del delegat de protecció de dades, han de realitzar prèviament una avaluació d'impacte de les operacions de tractament en la protecció de les dades personals.

Article 16
Gestió d'incidents

1. La Direcció General d'Estratègia Digital i Desenvolupament Tecnològic ha d'implantar els mecanismes apropiats per identificar correctament, registrar i resoldre els incidents de seguretat dels sistemes d'informació de l'Administració de la Comunitat Autònoma.

2. Aquesta Direcció General ha de notificar els incidents de seguretat al Centre Criptològic Nacional (CCN-CERT) a través de l'eina desenvolupada per a aquesta finalitat.

3. Tots els responsables de seguretat dels sistemes d'informació inclosos en l'àmbit d'aplicació de la PSI-CAIB han de notificar de forma immediata els incidents de seguretat a la Direcció General d'Estratègia Digital i Desenvolupament Tecnològic amb una proposta de categorització de l'incident segons les guies CCN-CERT de gestió d'incidents de la seguretat. La Direcció General esmentada, amb caràcter urgent, ha de convocar el comitè de crisis pertinent d'acord amb l'article 17.

Article 17
Comitès de crisi

1. Els comitès de crisi són els òrgans encarregats de gestionar, prendre decisions, i coordinar les accions necessàries per fer front als incidents de seguretat en els sistemes d'informació que s'hagin qualificat com a crisi.

2. Els comitès han de determinar si s'està davant una crisi o no, el seu nivell, les mesures que s'han de prendre i el repartiment de responsabilitats. Així mateix, han de dur a terme la gestió adequada dels grups d'interès i la gestió de la comunicació tant durant les crisis com posteriorment, durant la recuperació.

3. El Comitè Operatiu de Crisi està format pels membres de la Comissió Tècnica de la Seguretat de la Informació. El Comitè Superior de Crisi estarà format pels membres de la Comissió Directora de Seguretat de la Informació.

4. El Comitè Operatiu ha d'actuar davant els incidents de seguretat qualificats amb un impacte baix, mitjà i alt. En aquests casos no és necessària la declaració de crisi.

5. El Comitè Superior ha d'actuar davant els incidents de seguretat qualificats amb un impacte crític i molt alt, amb coordinació permanent amb el Comitè Operatiu, i ha de declarar la crisi. El president del Comitè Superior informarà permanentment la Presidència del Govern de les Illes Balears sobre l'estat de l'incident i la seva evolució.

6. La coordinació entre els dos comitès es realitza a través del cap del Departament de Ciberseguretat i Telecomunicacions i el cap del Servei de Ciberseguretat.

Article 18
Resolució de conflictes

1. En cas de conflicte entre els diferents responsables que componen l'estructura organitzativa definida per a la gestió de la seguretat de la informació, s'han d'atendre les regles següents:

a) Si els responsables en conflicte tenen un superior jeràrquic comú de nivell directiu, aquest ha de resoldre el conflicte. En el cas que no existeixi un superior jeràrquic comú o aquest

sigui el director general d'Estratègia Digital i Desenvolupament Tecnològic, ha de resoldre la Comissió Tècnica de la Seguretat de la Informació.

b) En els casos en què la Comissió Tècnica de la Seguretat de la Informació resolgui el conflicte, qualsevol de les parts en conflicte, a través del seu òrgan directiu, podrà apel·lar a la Comissió Directora de la Seguretat de la Informació perquè resolgui el conflicte en última instància.

2. En qualsevol cas, mentre no es pugui aplicar el mecanisme de resolució de conflictes descrit, prevaldrà la decisió del responsable de seguretat que garanteixi un nivell de protecció de la informació i dels serveis més alt.

Article 19
Obligacions de compliment de la política de seguretat

1. La PSI-CAIB i els cos normatiu de desplegament és d'obligat compliment per a tot els òrgans superiors, òrgans directius i el personal de l'Administració de la Comunitat Autònoma de les Illes Balears; així com per al personal d'altres organismes o entitats que hagin estat autoritzats per a accedir als sistemes d'informació de l'Administració autonòmica, amb independència del destí, adscripció o relació.

2. Totes les persones a qui els sigui d'aplicació la PSI-CAIB tenen el deure d'informar el responsable de seguretat corresponent de qualsevol risc significatiu per a la seguretat dels sistemes d'informació protegits i de les violacions de seguretat de les quals tenguin coneixement, d'acord amb els procediments establerts.

3. L'incompliment de la normativa de seguretat pot comportar l'exigència de les responsabilitats administratives i legals corresponents.

Article 20
Terceres parts

1. Quan l'Administració de la Comunitat Autònoma utilitzi serveis o tracti informació d'altres entitats, se les ha de fer partícips de la PSI-CAIB i s'han d'establir mecanismes d'informació i coordinació dels respectius responsables de seguretat.

2. Quant l'Administració de la Comunitat Autònoma presti serveis o cedeixi informació a tercers, se'ls farà partícips de la PSI-CAIB i de la Normativa de Seguretat que afecta a aquests serveis i informació. En aquests cas, els tercers queden subjectes a les obligacions establertes en aquesta normativa, sense perjudici de poder desenvolupar els seus propis procediments operatius per a satisfer-la.

Article 21
Revisió de la Política de Seguretat de la Informació

La Comissió Tècnica de Seguretat de la Informació de la Comunitat Autònoma de les Illes Balears ha de revisar la PSI-CAIB a intervals planificats o sempre que es produeixin canvis significatius, a fi d'assegurar que mantingui la seva idoneïtat, adequació i eficàcia.

Disposició addicional primera
Dotació pressupostària

L'aplicació de les previsions contingudes en aquest Decret no suposa cap increment de la despesa pública, atès que s'atendrà amb els mitjans materials i humans personals de què disposa l'Administració autonòmica, per la qual cosa no requereix cap dotació pressupostària.

Disposició addicional segona
Adaptació de polítiques de seguretat existents

Els ens del sector públic instrumental de l'Administració de la Comunitat Autònoma de les Illes Balears que disposin d'una política de seguretat de la informació pròpia a l'entrada en vigor d'aquest Decret, hauran de revisar-la i adaptar-la, si escau, per mantenir la coherència amb la Política de Seguretat de la Informació de l'Administració autonòmica i el respecte als principis que s'hi recullen.

Disposició addicional tercera
Referències als càrrecs

1. En aquest Decret s'utilitza la forma no marcada quant al gènere, que coincideix formalment amb la masculina, en totes les referències a òrgans, càrrecs i funcions, de manera que s'han d'entendre referides al masculí o al femení segons la identitat de gènere de la persona titular de qui es tracti.

2. Les referències contingudes en aquest Decret als càrrecs que s'esmenten a continuació s'han d'interpretar de la manera següent:

a) Les referències al director general d'Estratègia Digital i Desenvolupament Tecnològic es fan com a òrgan competent sobre els sistemes d'informació, recursos tecnològics i serveis informàtics i telemàtics de l'Administració de la Comunitat Autònoma; amb funcions d'encàrrec del tractament de les dades personals en relació amb aquests sistemes, recursos i serveis, i competent sobre la seguretat de la informació dels recursos tecnològics.
En el moment que l'Agència Balear de Digitalització, Ciberseguretat i Telecomunicacions assumeixi les competències esmentades en el paràgraf anterior les referències al director general d'Estratègia Digital i Desenvolupament Tecnològic s'han d'entendre realitzades al gerent de l'Agència.
b) Les referències al director general de Funció Pública es fan com a òrgan competent en matèria d'ordenació i gestió del personal al servei de l'Administració de la Comunitat Autònoma de les Illes Balears.
c) Les referències al director general d'Emergències i Interior es fan com a òrgan competent en matèria d'emergències, seguretat de les seus de l'Administració autonòmica i coordinació de policies locals.
d) Les referències al director general d'Innovació i Transformació Digital, s'entenen com a òrgan competent en la promoció de la cultura de la ciberseguretat a la societat de les Illes Balears, incloent-hi ciutadans, administracions i empreses.
e) Les referències al secretari general de la Conselleria de Presidència, Coordinació de l'Acció

de Govern i Cooperació Local s'entenen com a conselleria competent en matèria de coordinació interdepartamental entre els òrgans de conselleries diverses i de coordinació de les matèries de caràcter transversal.
f) Les referències al conseller d'Economia, Hisenda i Innovació s'entenen com a titular de la Conselleria d'adscripció de la Direcció General d'Estratègia Digital i Desenvolupament Tecnològic.

Disposició addicional quarta
Constitució de la Comissió Directora de la Seguretat de Informació i de la Comissió Tècnica de Seguretat de la Informació

La sessió constitutiva de la Comissió Directora de la Seguretat de la Informació i de la Comissió Tècnica de la Seguretat de la Informació s'ha de dur a terme en el termini de quatre mesos des de l'entrada en vigor d'aquest Decret.

Disposició addicional cinquena
Definicions

Els termes o expressions utilitzades en el Decret tenen el significat indicat en el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.

Disposició derogatòria única
Normes que es deroguen

Queden derogades totes les disposicions de rang igual o inferior que s'oposin a aquest Decret, el contradiguin o siguin incompatibles amb el que disposa aquest Decret i, en particular:

El Decret 97/2006, de 24 de novembre, pel qual es creen i regulen les comissions per a la millora contínua de la seguretat de la informació en l'Administració de la Comunitat Autònoma de les Illes Balears.

Disposició final primera
Modificació del Decret 24/2022, d'11 de juliol, de la Comissió Superior de Sistemes d'Informació en Tecnologies i Comunicacions

L'apartat 2 de l'article 6 del Decret 24/2022, d'11 de juliol, de la Comissió Superior de Sistemes d'Informació en Tecnologies i Comunicacions queda modificat de la manera següent:

«2. Correspon a la Comissió Superior de Sistemes d'Informació en Tecnologia i Comunicacions emetre l'informe previ i preceptiu sobre els plecs de prescripcions tècniques per als contractes en matèria de sistemes d'informació de quantia superior a cinc-cents mil euros i, al director general d'Estratègia Digital i Desenvolupament Tecnològic, quan no se superi aquest import, en ambdós casos, amb la consulta prèvia als caps de departament adscrits a aquesta Direcció General.»

Disposició final segona

Desenvolupament

Es faculta el conseller d'Economia, Hisenda i Innovació per dictar les disposicions necessàries per desplegar aquest Decret.

Disposició final tercera
Entrada en vigor

El Decret entrarà en vigor l'endemà d'haver-se publicat en el *Butlletí Oficial de les Illes Balears*.