Secció I. Disposicions generals

CONSELL DE GOVERN

2134 ***Decret 2/2018, de 23 de febrer, pel qual s'aprova la política de seguretat de la informació del Servei de Salut de les Illes Balears***

El Servei de Salut de les Illes Balears és un ens públic de caràcter autònom, adscrit a la Conselleria de Salut del Govern de les Illes Balears, dotat de personalitat jurídica i patrimoni propis, amb plena capacitat d'obrar per complir les seves finalitats, al qual es confia la gestió dels serveis públics sanitaris de caràcter assistencial. De conformitat amb la Llei 5/2003, de 4 d'abril, de salut de les Illes Balears, els objectius fonamentals del Servei de Salut consisteixen a participar en la definició de les prioritats de l'atenció sanitària a partir de les necessitats de salut de la població i donar efectivitat al catàleg de prestacions i serveis que es posa al servei de la població amb la finalitat de protegir la salut; distribuir de manera òptima els mitjans econòmics assignats al finançament dels serveis i de les prestacions sanitàries; garantir que les prestacions es gestionin de manera eficient; garantir, avaluar i millorar la qualitat del servei al ciutadà, tant en l'assistència com en el tracte; promoure la participació dels professionals en la gestió del sistema sanitari balear i fomentar la motivació professional, i promoure la formació, la docència i la recerca en l'àmbit de la salut.

S'ha de considerar que la informació que recull i gestiona el Servei de Salut en l'exercici de les seves competències constitueix un actiu essencial per complir adequadament els objectius ressenyats, i que el funcionament correcte dels sistemes d'informació que acullen i gestionen aquestes dades és imprescindible per a l'exercici adequat, eficaç i eficient de les obligacions atribuïdes en matèria d'assistència i de gestió sanitària. Per tant, assumeix la responsabilitat associada a la protecció d'aquestes dades davant les amenaces que puguin afectar-ne la seguretat.

Els beneficis de la implantació de les tecnologies de la informació en els entorns sanitaris són més que evidents, ja que faciliten la prestació de serveis sanitaris amb coherència i cohesió des dels diferents nivells assistencials, en especial en un àmbit geogràfic caracteritzat per la insularitat, la qual cosa no fa sinó potenciar encara més els beneficis d'aquestes tecnologies. No obstant això, en aquest entorn la seguretat de la informació és clarament un imperatiu, ja que la informació gestionada en aquest àmbit està sotmesa a uns requisits de seguretat molt exigents.

L'article 11 del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica, estableix que tots els òrgans superiors de les administracions públiques han de tenir una política de seguretat de la informació, aprovada pel titular de l'òrgan superior corresponent.

Per la seva banda, el Decret 97/2006, de 24 de novembre, regula les comissions per a la millora contínua de la seguretat de la informació en l'Administració de la Comunitat Autònoma de les Illes Balears. D'acord amb aquest Decret, la Comissió Directora de Seguretat de la Informació va emetre l'informe corresponent sobre el Decret present.

Atesa la matèria que es regula, que afecta la seguretat de la informació, moltes vegades referida a dades protegides especialment, és convenient que la regulació d'aquesta política de seguretat de la informació es faci per la via del decret, tenint en compte, a més, que encara no s'ha aprovat la política de seguretat de la informació per a la resta de l'Administració de la Comunitat Autònoma.

Aquest Decret té per objecte desplegar un aspecte específic de l'accés electrònic dels ciutadans als serveis públics, que és el de la seguretat.

D'acord amb el Decret 24/2015, de 7 d'agost, 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, la Vicepresidència i Conselleria d'Innovació, Investigació i Turisme —a través de la Direcció General de Desenvolupament Tecnològic— té competència en matèria de seguretat de la informació dels recursos tecnològics. D'altra banda, el Servei de Salut està adscrit a la Conselleria de Salut i ha d'organitzar la planificació de la seguretat de la informació en el seu àmbit. Aquesta Conselleria —mitjançant la Direcció General de Planificació, Avaluació i Farmàcia— s'encarrega de la planificació i l'ordenació de l'assistència sanitària, un dels aspectes de la qual és la seguretat de la informació que es maneja.

En conseqüència, a proposta de la consellera d'Innovació, Investigació i Turisme i de la consellera de Salut, oït el Consell Consultiu de les Illes Balears i havent-ho considerat prèviament el Consell de Govern en la sessió del 23 de febrer de 2018,

DECRET

Capítol I
Aspectes generals

Article 1
Objecte

Aquest Decret té per objecte definir la política de seguretat de la informació del Servei de Salut de les Illes Balears.

Article 2
Àmbit d'aplicació

1. La política de seguretat de la informació del Servei de Salut és aplicable amb caràcter obligatori a totes les unitats administratives i a tots els òrgans del Servei de Salut, i també als ens que —si n'hi ha— hi estiguin adscrits, per la qual cosa l'ha d'observar tot el personal que hi presti servei.

2. Així mateix, és aplicable als centres privats que estiguin incorporats al sistema sanitari públic de les Illes Balears per mitjà d'acords, convenis o altres fórmules de gestió integrada o compartida. Aquesta política de seguretat ha de ser observada pel seu personal.

3. La política de seguretat de la informació també és aplicable i de compliment obligat per a les persones que, encara que no prestin servei directament en el Servei de Salut o en algun ens que hi estigui adscrit, tenguin accés a la informació o als sistemes que gestionen aquesta informació.

4. La política de seguretat de la informació inclou tots els sistemes d'informació que gestiona el Servei de Salut.

Article 3
Definicions

Als efectes de la política de seguretat de la informació del Servei de Salut, són aplicables les definicions que estableix el Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica. Així mateix, es defineixen els conceptes següents:

a) Responsable de la informació: persona que té la potestat d'establir els requisits d'una informació en matèria de seguretat.
b) Responsable de la seguretat de la informació: persona que determina les decisions per satisfer els requisits de seguretat de la informació i dels serveis.
c) Responsable del servei: persona que té la potestat d'establir els requisits d'un servei en matèria de seguretat.
d) Responsable del sistema: persona que s'encarrega de l'explotació del sistema d'informació.

Article 4
Missió

Als efectes d'aquest Decret, el Servei de Salut actua d'acord amb la Llei 5/2003, de 4 d'abril, de salut de les Illes Balears, i té per missió mantenir uns nivells adequats de seguretat i de protecció davant amenaces a la informació que gestiona, la qual cosa és l'actiu fonamental per complir els seus objectius.

Article 5
Objectius

El Servei de Salut assumeix els objectius següents en matèria de seguretat de la informació:

1) Establir les pautes necessàries per garantir sempre la seguretat de la informació a través de directrius per tal de preservar, protegir i consolidar la seguretat dels serveis i els actius d'informació amb l'objectiu de millorar la qualitat dels serveis que es presten als ciutadans.
2) Garantir la implantació de les mesures i dels mecanismes de seguretat apropiats per protegir els serveis prestats, els sistemes d'informació emprats per prestar-los i la informació processada, emmagatzemada o transmesa per aquests, de manera coherent amb els riscs afrontats.
3) Assegurar que es compleixi la normativa vigent en matèria de seguretat i protecció de dades a què el Servei de Salut s'hagi de sotmetre.
4) Garantir l'eficàcia de les mesures de seguretat implantades per mitjà d'avaluacions i auditories.

5) Establir una estructura organitzativa adequada per a la gestió de la seguretat de la informació definint els rols i els comitès necessaris, a més de les funcions i les responsabilitats respectives.
6) Garantir l'operació continuada i adequada dels serveis i dels sistemes i actuar per prevenir, detectar, reaccionar i operar de manera oportuna davant els incidents de seguretat que es produeixin, a més de vetlar per la implantació dels mecanismes necessaris que assegurin la continuïtat de les activitats crítiques permetent que es recuperin en un període de temps acceptable.
7) Impulsar i fomentar la formació, la conscienciació i el compliment de les obligacions en matèria de seguretat de la informació del personal al servei de l'organització, a fi de garantir el coneixement de les polítiques i les normatives aprovades i de les pràctiques recomanades, amb l'objectiu últim d'aconseguir que la seguretat de la informació es converteixi en un factor inherent al desenvolupament de les funcions i de les operatives quotidianes.
8) Promoure que les activitats destinades a aconseguir els nivells de seguretat requerits s'estructurin i es concebin com un procés de millora contínua, i no com a accions o esforços puntuals, sustentant-ho en l'anàlisi i la gestió sistematitzades dels riscs.

Article 6
Marc normatiu

1. El disseny, l'operació, l'ús i l'administració de la informació, dels sistemes d'informació i dels serveis del Servei de Salut han de complir les normes següents, les quals s'esmenten amb caràcter enunciatiu i no limitador:

a) Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.
b) Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
c) Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
d) Llei 3/2003, de 26 de març, de règim jurídic de l'Administració de la Comunitat Autònoma de les Illes Balears.
e) Llei 41/2002, de 14 de novembre, bàsica reguladora de l'autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica.
f) Llei 5/2003, de 4 d'abril, de salut de les Illes Balears.
g) Llei 59/2003, de 19 de desembre, de signatura electrònica.
h) Llei 4/2011, de 31 de març, de la bona administració i del bon govern de les Illes Balears.
i) Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica.
j) Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'administració electrònica.
k) Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999.
l) Decret 39/2006, de 21 d'abril, pel qual s'aproven els Estatuts de l'ens públic Servei de Salut de les Illes Balears.
m) 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.
n) 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.
o) Decret 113/2010, de 5 de novembre, d'accés electrònic als serveis públics de l'Administració de la Comunitat Autònoma de les Illes Balears.
p) Decret 126/2010, de 23 de desembre, pel qual es regulen la Comissió Superior de Sistemes d'Informació en Tecnologia i Comunicacions i l'adquisició, l'alienació, l'arrendament i el manteniment de béns i serveis dels sistemes d'informació.
q) Decret 24/2015, de 7 d'agost, 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.
r) Decret 81/2015, de 25 de setembre, pel qual s'estableix l'estructura orgànica bàsica del Servei de Salut de les Illes Balears.
s) 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 (Reglament general de protecció de dades).
t) Circular 1/2014, de 18 d'agost, del director general del Servei de Salut de les Illes Balears, per la qual s'aprova el Codi de bones pràctiques del Servei de Salut en l'ús dels sistemes d'informació i en el tractament de les dades de caràcter personal.

2. A banda d'aquestes disposicions legals i, en qualsevol cas, el Servei de Salut —en matèria de política de seguretat de la informació— ha d'actuar amb compliment estricte de la legalitat vigent.

Article 7
Desenvolupament de la política de seguretat de la informació

1. Aquesta política de seguretat de la informació s'ha de desenvolupar en diversos àmbits:

a) Àmbit estratègic, en el qual s'inclouen les directrius emeses per la normativa vigent i per aquesta política de seguretat de la informació.
b) Àmbit tàctic, en el qual s'estableixen les normes que defineixen les pautes per a cada una de les àrees de coneixement i seguretat del Servei de Salut de conformitat amb els objectius establerts per la política de seguretat de la informació.
c) Àmbit operatiu, en el qual es desenvolupen els procediments i les instruccions tècniques que detallen les activitats que s'han de dur a terme per gestionar la seguretat de la informació definint els detalls concrets i els aspectes pràctics sobre la manera de fer-les per executar la tasca especificada i complir les responsabilitats assignades.

2. Els àmbits tàctic i operatiu es desenvolupen al voltant d'un marc documental que consisteix en instruccions o circulars internes proposades pel Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació als òrgans directius del Servei de Salut.

3. Aquest marc documental ha d'estar a disposició del personal que faci feina per al Servei de Salut i que necessiti conèixer-lo, en particular per a qui empri o administri els sistemes d'informació i les comunicacions.

4. En particular, tot el personal que estigui al servei del Servei de Salut ha de respectar i conèixer el Codi de bones pràctiques del Servei de Salut de les Illes Balears en l'ús dels sistemes d'informació i en el tractament de les dades de caràcter personal, aprovat per una circular del director general.

5. Pel que fa al tractament de les dades de caràcter personal, cal actuar segons el que disposen els documents corresponents de seguretat que exigeix el Reglament de desplegament de la Llei orgànica 15/1999.

Article 8
Revisió de la política de seguretat de la informació

El Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació que estableix l'article 10 d'aquest Decret ha de revisar i proposar les actualitzacions necessàries de la política de seguretat de la informació per assegurar que compleix la legalitat vigent. Per complir aquest objectiu pot proposar qualsevol modificació d'aquest Decret que consideri necessària.

Capítol II
Organització de la seguretat de la informació

Article 9
Estructura organitzativa i rols de seguretat

1. L'estructura organitzativa per gestionar la seguretat de la informació en el Servei de Salut està integrada pels actors següents:

a) El Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació.
b) El Comitè de Seguretat de la Informació dels Serveis Centrals i els comitès respectius de cada gerència territorial.

2. Es defineixen els rols següents per gestionar la seguretat de la informació en el Servei de Salut:

a) Els responsables de la informació.
b) Els responsables dels serveis.
c) El responsable de la seguretat de la informació dels Serveis Centrals del Servei de Salut.
d) El responsable de la seguretat de la informació de cada gerència territorial.
e) Els responsables dels sistemes.

3. Els rols de responsable de la informació i de responsable dels serveis poden coincidir en una mateixa persona quan la prestació del servei depengui de la unitat que és responsable de la informació o quan el servei no manegi informació de procedències diferents.

4. El rol de responsable dels serveis i el de responsable dels sistemes no poden recaure en una persona que exerceixi simultàniament el paper de responsable de la seguretat de la informació dels Serveis Centrals del Servei de Salut o de qualsevol de les gerències territorials.

Article 10
El Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació

1. El Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació és un òrgan col·legiat, dependent de la Direcció General del Servei de Salut de les Illes Balears, l'objectiu del qual és impulsar i promoure la seguretat de la informació del Servei de Salut i dels ens que hi estan adscrits.

2. Aquest Comitè està format per les persones següents:

a) El secretari general del Servei de Salut, que n'ocupa la Presidència.
b) Vocals:
1) El subdirector de Tecnologia i Sistemes d'Informació.
2) Un representant dels serveis jurídics del Servei de Salut.
3) Els responsables de la seguretat de la informació de cadascuna de les gerències territorials.

c) El responsable de la seguretat de la informació dels Serveis Centrals del Servei de Salut, que hi actua com a secretari, amb veu i vot.

3. El Comitè pot recollir del personal tècnic propi o extern la informació pertinent per prendre decisions i pot convidar aquest personal a les reunions, amb veu però sense vot. Tots aquests professionals han de servar el secret sobre els assumptes de què tenguin coneixement a les reunions.

4. El Comitè depèn del Consell de Direcció del Servei de Salut, al qual ha de comunicar qualsevol qüestió, activitat o necessitat relacionada amb la seguretat de la informació en el seu àmbit de responsabilitat.

5. El Comitè té les funcions següents:

a) Coordinar els esforços de les diferents gerències, dels òrgans i els organismes que pertanyen al Servei de Salut o hi estan adscrits i, en general, de tots els grups interns amb responsabilitats sobre la seguretat de la informació, a fi d'assegurar que les iniciatives en aquesta matèria siguin homogènies i d'evitar duplicitats.
b) Assessorar els òrgans de direcció del Servei de Salut en qüestions, peticions o activitats relacionades amb la seguretat de la informació.
c) Revisar i proposar les actualitzacions necessàries que estableix aquest Decret de política de seguretat perquè el Consell de Govern les aprovi, i emetre un informe en els termes que indica l'article 7 d'aquest Decret.
d) Elaborar l'estratègia del Servei de Salut en matèria de seguretat de la informació establint les directrius i les responsabilitats principals en matèria de seguretat que garanteixin l'autenticitat, la confidencialitat, la integritat, la disponibilitat i la traçabilitat de la informació i dels serveis, i alinear les activitats de seguretat amb la missió i els objectius del Servei de Salut.
e) Aprovar les mesures necessàries per aplicar i complir les disposicions que estableix aquesta política de seguretat de la informació.
f) Fer el seguiment general de l'estat de la seguretat de la informació en el Servei de Salut.
g) Aprovar i coordinar tots els projectes de millora o canvi sobre la seguretat de la informació en aplicacions, sistemes, actius i recursos de l'organització, incloent-hi els plans de millora de la seguretat.
h) Fomentar la creació i l'ús de serveis horitzontals que redueixin duplicitats i donin suport a un funcionament homogeni de tots els sistemes d'informació.
i) Monitorar els principals riscs residuals assumits per les gerències i recomanar-hi possibles actuacions.
j) Revisar i prendre les decisions sobre les qüestions que els remetin els comitès de seguretat de la informació dels Serveis Centrals o de les gerències territorials.

6. S'han de convocar reunions ordinàries del Ple del Comitè amb una periodicitat mínima semestral. A més, qualssevol dels seus membres pot sol·licitar una convocatòria extraordinària si hi concorren causes que l'aconsellin. Els membres del Comitè tenen les funcions següents:

a) Proposar que s'incloguin en l'ordre del dia les qüestions que considerin oportunes amb relació a la seguretat de la informació.
b) Assistir a les reunions del Comitè, participar en els debats, formular precs i preguntes i exercir el dret a vot.

7. El Comitè pot acordar crear els grups de treball que consideri necessaris per preparar, estudiar i desenvolupar les qüestions sotmeses al seu coneixement. Aquests grups han d'exercir per raons d'urgència i operativitat les funcions que el Ple els delegui. El Comitè ha de conèixer en les sessions del Ple els resultats de les actuacions dels grups de treball.

8. De cada sessió s'ha d'estendre una acta, en la qual han de constar les circumstàncies de lloc i temps, les persones assistents, l'ordre del dia, un resum de les deliberacions, les decisions acordades i qualsevol altre tema que els membres del Comitè sol·licitin expressament que hi consti.

9. El funcionament del Comitè s'ha d'ajustar al que preveu la Llei 40/2015.

10. S'ha de procurar la participació equilibrada d'homes i dones en el si del Comitè.

Article 11
Els comitès de seguretat de la informació dels Serveis Centrals i de les gerències territorials

1. S'ha de definir un comitè de seguretat de la informació per als Serveis Centrals del Servei de Salut i per a cadascuna de les gerències territorials, dependents de la Direcció General del Servei de Salut de les Illes Balears. L'objectiu d'aquests comitès és fomentar la seguretat de la informació en el seu àmbit de responsabilitat i vetlar per aquesta seguretat.

2. L'àmbit de responsabilitat del Comitè de Seguretat de la Informació dels Serveis Centrals és el que defineix el capítol II del Decret 81/2015. De la mateixa manera, l'àmbit de responsabilitat dels comitès de seguretat de la informació de les gerències territorials que regula el capítol III del Decret 81/2015 és el corresponent a cada gerència.

3. Cada comitè de seguretat de la informació està format per les persones següents:

a) El director de cada gerència, que n'ocupa la presidència. En el cas del Comitè de Seguretat de la Informació dels Serveis Centrals, aquest càrrec recau en el secretari general del Servei de Salut.
b) Vocals:
1) Un representant de la Subdirecció de Tecnologia i Sistemes d'Informació; per al Comitè de Seguretat de la Informació dels Serveis Centrals ha de ser el seu subdirector.
2) Els responsables de les àrees que el president del comitè consideri.
c) El responsable de la seguretat de la informació de la gerència o el responsable de seguretat de la informació dels Serveis Centrals, respectivament per a cada comitè, que hi actuen com a secretaris, amb veu i vot.

4. Cada comitè té les funcions següents:

a) Resoldre les inquietuds i els problemes de les unitats del seu àmbit de responsabilitat en matèria de seguretat de la informació.
b) Fer el seguiment de l'estat de la seguretat dels sistemes d'informació en el seu àmbit de responsabilitat i revisar i analitzar els incidents, tant els esdevinguts de manera efectiva com els incidents potencials.
c) Aprovar iniciatives per elaborar normativa interna de seguretat de la informació en el seu àmbit de responsabilitat, sense perjudici de les normatives aplicables al Servei de Salut en conjunt.
d) Promoure la millora contínua en la gestió de la seguretat de la informació en el seu àmbit de responsabilitat i impulsar i gestionar la implantació d'un sistema de gestió amb aquest efecte.
e) Supervisar i controlar els riscs sobre els actius d'informació i els serveis, per a la qual cosa ha de determinar el risc assumible, monitorar-lo i fer un seguiment de les actuacions adequades.
f) Vetlar pel compliment de la normativa legal, regulatòria i sectorial aplicable.
g) Donar suport i prioritat a les iniciatives i a les accions de millora de la seguretat en els sistemes d'informació i promoure els projectes que es requereixin per implantar les mesures i les accions de seguretat d'acord amb el nivell de risc.
h) Determinar els nivells de seguretat dels serveis i de la informació en el cas que no els determinin els responsables dels serveis o els responsables de la informació.
i) Monitorar els processos de gestió d'incidents en la seguretat i recomanar les possibles actuacions; en particular, vetlar per la coordinació de les diferents àrees en la gestió dels incidents en la seguretat de la informació.
j) Promoure auditories periòdiques que permetin verificar si es compleixen les obligacions en matèria de seguretat de la informació.
k) Vetlar per tal que la seguretat de la informació es tengui en compte en tots els projectes, des de l'especificació inicial fins a la posada en operació.
l) Resoldre els conflictes de responsabilitat que puguin sorgir entre els diferents responsables i/o entre diferents àrees i elevar-los en cas que no tengui prou autoritat per decidir.
m) Impulsar accions de formació, conscienciació i compliment de les obligacions en matèria de seguretat de la informació.

5. Pel que fa a la gestió i el funcionament dels comitès, hi són aplicables les mateixes normes que les previstes per al Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació, concretament els apartats 7, 8 i 9 de l'article 10 d'aquest Decret.

6. El funcionament dels comitès s'ha d'ajustar al que preveu la Llei 40/2015.

7. Pel que fa a les iniciatives o actuacions que superin l'àmbit d'actuació de cada comitè, o quan hi hagi projectes horitzontals que afectin tot el Servei de Salut, cal atenir-se al que hagi decidit el Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació.

8. S'ha de procurar la participació equilibrada d'homes i dones en el si de cada comitè.

Article 12
Els responsables de la informació

1. Tota la informació gestionada pel Servei de Salut ha de tenir almenys un responsable.

2. Els responsables de la informació tenen la responsabilitat última de l'ús que es faci de la informació i de protegir-la.

3. El responsable de la informació, que ha de ser designat pel director general del Servei de Salut, té prou competència per decidir sobre la finalitat, el contingut i l'ús d'aquesta informació.

4. Si es tracta d'informació per a la qual hi hagi més d'un responsable, tots han d'assumir conjuntament el rol de responsable de la informació associada i exercir les funcions assignades. En cas de qualsevol discrepància per determinar els requisits de seguretat aplicables a la informació, cal aplicar-hi els més restrictius. Per a qualsevol altra discrepància cal aplicar el procediment de resolució de conflictes determinat en aquesta política de seguretat de la informació.

5. Els responsables de la informació tenen les funcions següents:

a) Establir els requisits de seguretat de la informació d'acord amb els criteris establerts per la política de seguretat de la informació.
b) Comunicar els requisits de seguretat de la informació als responsables de la seguretat de la informació competents.
c) Com a responsables últims de la informació, assumir la responsabilitat final d'implantar les mesures de protecció d'aquella.
d) Assumir la propietat dels riscs sobre la informació, monitorar-los i acceptar el risc residual.

Article 13
Els responsables dels serveis

1. En l'àmbit del Servei de Salut hi ha d'haver almenys un responsable per a cadascun dels serveis prestats per aquest ens.

2. Els responsables dels serveis tenen la responsabilitat última de l'ús que es faci d'un servei i de protegir-lo.

3. Els responsables dels serveis, que han de ser designats pel director general del Servei de Salut, tenen atribuïdes les competències relacionades amb la finalitat a què serveixen aquests serveis.

4. Els responsables dels serveis tenen les funcions següents:

a) Establir els requisits dels serveis en matèria de seguretat d'acord amb els criteris establerts en aquesta política de seguretat de la informació.
b) Comunicar els requisits dels serveis en matèria de seguretat als responsables de la seguretat de la informació competents.
c) Com a responsables últims dels serveis, assumir la responsabilitat final d'implantar-ne les mesures de protecció.
d) Assumir la propietat dels riscs sobre els serveis, monitorar-los i acceptar el risc residual.

Article 14
El responsable de la seguretat de la informació dels Serveis Centrals del Servei de Salut

1. El subdirector de Tecnologia i Sistemes d'Informació ha de designar el responsable de la seguretat de la informació del Servei de Salut tenint en compte les seves qualitats professionals, en particular els coneixements especialitzats en legislació i les pràctiques en matèria de seguretat de la informació i protecció de dades de caràcter personal.

2. El responsable de la seguretat de la informació del Servei de Salut té les funcions següents:

a) Actuar com a secretari del Comitè de Seguretat de la Informació dels Serveis Centrals i del Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació.
b) Representar el Servei de Salut en fòrums sectorials o davant agents externs en assumptes relacionats amb la seguretat de la informació.
c) Reportar informació resumida de les actuacions en matèria de seguretat i dels incidents, tant al Comitè de Seguretat de la Informació dels Serveis Centrals com al Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació.
d) Informar sobre els resultats de les avaluacions dels riscs —en particular del risc residual— tant el Comitè de Seguretat de la Informació dels Serveis Centrals com el Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació.
e) Coordinar l'execució de les decisions del Comitè de Seguretat de la Informació dels Serveis Centrals i —juntament amb els responsables de la seguretat de la informació de les gerències territorials— de les decisions del Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació.
f) Determinar la categoria dels sistemes a partir dels requisits de seguretat dels serveis als quals donen suport i de la informació que manegen.
g) Mantenir la seguretat de la informació manejada i dels serveis prestats pels sistemes d'informació gestionats per la Subdirecció de Tecnologia i Sistemes d'Informació, i instar a implantar les mesures de seguretat que hi pertoquin.
h) Promoure i coordinar les accions de formació, conscienciació i compliment de les obligacions en matèria de seguretat de la

informació en l'àmbit dels Serveis Centrals del Servei de Salut.
i) Elaborar les anàlisis de riscs sobre els actius dels Serveis Centrals del Servei de Salut i els sistemes gestionats per la Subdirecció de Tecnologia i Sistemes d'Informació, i monitorar que no se superin els marges tolerables de risc.
j) Identificar mancances i debilitats en els sistemes i informar-ne els responsables de la informació, dels serveis i del sistema.
k) Elaborar la declaració d'aplicabilitat dels sistemes, incloent-hi possibles mesures de seguretat addicionals requerides depenent de l'anàlisi dels riscs.
l) Promoure el desplegament del marc normatiu en matèria de seguretat.
m) Elaborar els plans de millora de la seguretat juntament amb els responsables dels sistemes.
n) Validar els plans de continuïtat.
o) Fomentar i supervisar la investigació dels incidents de seguretat des que es notifiquin fins que es resolguin.
p) Analitzar els incidents de seguretat i proposar salvaguardes que evitin que es repeteixin.
q) Verificar que les mesures de seguretat establertes són adequades per a la protecció de la informació manejada i els serveis prestats.
r) Analitzar els informes de les auditories. En el cas de les auditories en matèria de protecció de dades, elevar els resultats al responsable del fitxer.
s) Monitorar l'estat de seguretat del sistema proporcionat per les eines de gestió d'esdeveniments de la seguretat i pels mecanismes d'auditoria implementats en el sistema.
t) Assumir el rol de responsable de la seguretat dels tractaments de dades de caràcter personal aplicats en els Serveis Centrals i en l'àmbit de la Subdirecció de Tecnologia i Sistemes d'Informació, i en general sobre els tractaments aplicats als fitxers que són responsabilitat del Servei de Salut o d'òrgans, ens o unitats dels Serveis Centrals, i assumir així mateix les funcions que estableix la normativa aplicable, particularment les que defineix l'article 95 del Reglament de desplegament de la Llei orgànica 15/1999.

3. El responsable de la seguretat de la informació del Servei de Salut pot designar responsables de seguretat delegats en les situacions, en els àmbits o en els sistemes per als quals —per raó de la naturalesa, la complexitat, la distribució, la separació física dels seus elements, el nombre d'usuaris o per qualsevol altre motiu— el nomenament resulti aconsellable a fi d'exercir les funcions que té assignades. Els responsables de la seguretat delegats han de tenir coneixements especialitzats en legislació i pràctiques en matèria de seguretat de la informació i protecció de dades de caràcter personal. Depenen funcionalment del responsable de la seguretat de la informació del Servei de Salut i li han de retre comptes.

Article 15
Els responsables de la seguretat de la informació de les gerències territorials

1. Hi ha d'haver un responsable de la seguretat de la informació en cadascuna de les gerències territorials.

2. El director de cada gerència ha de designar el responsable de la seguretat de la informació respectiu tenint en compte les seves qualitats professionals, en particular els coneixements especialitzats de la legislació i les pràctiques en matèria de seguretat de la informació i protecció de dades de caràcter personal.

3. El responsable de la seguretat de la informació de cada gerència ha d'assumir les funcions establertes per al responsable de la seguretat de la informació del Servei de Salut —descrites en l'article 13.1 d'aquest Decret—, però amb les precisions següents:

a) Les funcions esmentades s'han d'entendre aplicades a l'àmbit d'actuació de cada gerència.
b) Les funcions relatives al Comitè de Seguretat de la Informació dels Serveis Centrals s'han d'entendre aplicables al comitè de seguretat de la informació de la gerència corresponent.
c) Pel que fa al Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació, els responsables de la seguretat de la informació de les gerències hi han de participar.

4. Els responsables de la seguretat de la informació de les gerències han d'assegurar una coordinació i un alineament adequats amb el responsable de la seguretat de la informació dels Serveis Centrals del Servei de Salut, de tal manera que la seva relació ha d'estar guiada pel principi de la voluntat de col·laboració mútua.

5. Els responsables de la seguretat de la informació de les gerències poden designar responsables de seguretat delegats en les situacions, en els àmbits o en els sistemes per als quals —per raó de la naturalesa, la complexitat, la distribució, la separació física dels seus elements, el nombre d'usuaris o per qualsevol altre motiu— el nomenament resulti aconsellable a fi d'exercir les funcions que té assignades. Els responsables de la seguretat delegats depenen funcionalment del responsable de la seguretat de la informació de la gerència corresponent i li han de retre comptes.

Article 16
Els responsables dels sistemes

1. En l'àmbit del Servei de Salut, tot sistema d'informació ha de tenir un responsable, que ha de ser el titular de la unitat competent en la

gestió i l'operació del sistema.

2. El responsable dels sistemes en l'àmbit de les gerències territorials ha de ser designat pel gerent corresponent. Per la seva part, en l'àmbit dels Serveis Centrals i en el cas dels sistemes gestionats i operats de manera centralitzada, el rol de responsable del sistema l'ha d'assumir el subdirector de Tecnologia i Sistemes d'Informació.

3. Els responsables dels sistemes tenen les funcions següents:

a) Desenvolupar, fer funcionar i mantenir els sistemes d'informació durant tot el seu cicle de vida, ocupar-se'n de les especificacions i de la instal·lació i verificar que funcionen correctament.
b) Definir la tipologia i els mitjans de gestió dels sistemes d'informació i establir els criteris d'ús i els serveis disponibles.
c) Assegurar que les mesures específiques de seguretat s'integrin adequadament en el marc general de seguretat.
d) En cas necessari, acordar la suspensió del maneig d'una determinada informació o de la prestació d'un determinat servei si s'assabenta de deficiències greus en la seguretat que puguin afectar la satisfacció dels requisits establerts. Abans d'executar aquesta decisió, l'ha d'acordar amb els responsables de la informació i dels serveis afectats, amb el responsable de la seguretat de la informació del Servei de Salut i amb el responsable de la seguretat de la informació de la gerència corresponent, si hi escau.
e) Elaborar els plans de millora de la seguretat juntament amb els responsables de la seguretat de la informació.
f) Planificar la implantació de salvaguardes en els sistemes.
g) Executar els plans de seguretat aprovats.

Article 17
Resolució de conflictes

1. En cas de conflicte entre els diferents responsables que integren l'estructura organitzativa definida per a la gestió de la seguretat de la informació, l'ha de resoldre el seu superior jeràrquic; en absència d'aquest, hi preval la decisió del Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació.

2. En cas de conflicte entre els responsables que conformen l'estructura organitzativa per a la gestió de la seguretat de la informació i els definits en la normativa de protecció de dades de caràcter personal, hi preval la decisió que impliqui el nivell més alt de protecció.

Article 18
Coordinació amb terceres parts

1. Quan el Servei de Salut presti servei a un altre organisme o manegi informació d'un altre organisme, l'ha de fer partícip d'aquesta política de seguretat de la informació. S'han d'establir canals per al report i la coordinació dels comitès de seguretat de la informació i procediments d'actuació respectius per reaccionar davant incidents en la seguretat.

2. Quan el Servei de Salut utilitzi serveis d'una tercera part o li cedeixi informació, li ha de traslladar aquesta política de seguretat de la informació i la normativa de seguretat que sigui aplicable a aquests serveis. Aquesta tercera part queda subjecta a les obligacions que estableix aquesta normativa i pot desenvolupar els seus propis procediments operatius per complir-la.

3. No obstant això, quan aquesta tercera part sigui una administració pública o un organisme del sector públic, ha d'aplicar les seves pròpies normes de seguretat de la informació una vegada que li hagin cedit la informació.

4. Cal establir procediments específics de report i resolució d'incidències. Així mateix, cal garantir que el personal de qualsevol tercera part està format i compleix adequadament les obligacions en matèria de seguretat, almenys al mateix nivell que el que estableix aquesta política de seguretat de la informació.

5. Si una tercera part no pot complir algun aspecte de la política de seguretat de la informació segons el que es requereix en els paràgrafs anteriors, és necessari obtenir un informe del responsable de seguretat competent que precisi els riscs en què s'incorre i la manera de tractar-los. Abans de continuar endavant, també és necessari que els responsables de la informació i els responsables dels serveis afectats aprovin aquest informe.

Capítol III
Valoració dels requisits de seguretat de la informació

Article 19
Aspectes generals

1. L'aplicació de mesures de seguretat en els sistemes d'informació s'ha de fer tenint en compte la valoració dels requisits de seguretat dels serveis prestats i de la informació gestionada per cadascun d'aquests.

2. Els sistemes han d'assumir els requisits més exigents entre els indicats per a la informació que tracta i els serveis que presta.

3. Els requisits de seguretat identificats per als serveis i la informació s'han de tenir en compte així mateix en les anàlisis de riscs fetes sobre els sistemes d'informació.

Article 20
Procediment i nivells de valoració

1. En l'àmbit del Servei de Salut, la valoració dels requisits de seguretat de la informació i dels serveis s'ha de fer de conformitat amb l'Esquema Nacional de Seguretat, aprovat pel Reial decret 3/2010, en particular amb l'annex I.

2. Qui assumeixi els rols amb les funcions corresponents segons el que s'ha definit en el capítol II d'aquest Decret s'ha d'encarregar de valorar els requisits de seguretat existents sobre la informació i els serveis.

3. Els serveis i la informació s'han de valorar en cinc dimensions de seguretat: autenticitat, confidencialitat, integritat, disponibilitat i traçabilitat.

4. Per a cada dimensió de seguretat cal indicar un nivell de valoració entre les quatre possibilitats següents: *alt*, *mitjà*, *baix* i *sense valorar*.

Article 21
Criteris de valoració

1. Els valors corresponents als requisits de seguretat de cada servei i cada actiu d'informació s'han d'assignar segons les conseqüències que pugui tenir un possible incident de seguretat que afecti cada una de les dimensions de seguretat considerades sobre les funcions de l'organització i la seva capacitat per complir les seves finalitats, sobre els seus actius o sobre les persones afectades.

2. En cas que, per a un servei o actiu d'informació en una determinada dimensió de seguretat, es consideri que un incident tindria conseqüències qualificables com a perjudici molt greu, cal assignar-hi el nivell alt; si els efectes d'aquest incident es poden descriure com a perjudici greu, cal assignar-hi el nivell mitjà; si els efectes es poden descriure com a perjudici limitat, aleshores es tracta del nivell baix, i si, al contrari, es considera que no suposa cap perjudici, el valor adequat és «sense valorar».

3. El Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació ha d'elaborar uns criteris de valoració adaptats a la casuística i a les particularitats del Servei de Salut, a fi de facilitar als responsables corresponents l'especificació dels requisits de seguretat.

Capítol IV
Gestió dels riscs en la seguretat de la informació

Article 22
Anàlisi dels riscs

1. Tots els sistemes d'informació del Servei de Salut han de ser objecte d'una anàlisi dels riscs a càrrec dels responsables de seguretat de la informació, que s'ha de repetir amb una periodicitat mínima anual.

2. Les anàlisis dels riscs, a més, s'han d'actualitzar en qualsevol d'aquests casos:

a) Si s'identifiquen nous actius d'informació o si canvien els existents o els requisits de seguretat.
b) Si s'identifiquen canvis amb relació als serveis prestats.
c) Si s'esdevé un incident greu en la seguretat o s'identifiquen o reporten vulnerabilitats greus en la seguretat dels sistemes existents.

Article 23
Gestió dels riscs

1. Les decisions sobre les mesures, els projectes i les iniciatives de seguretat que s'hagin de prendre en l'àmbit del Servei de Salut han de preveure els resultats de l'avaluació dels riscs existents en relació amb la seguretat de la informació sobre els sistemes utilitzats.

2. El responsable de la seguretat de la informació ha d'elevar al comitè corresponent els resultats de les anàlisis dels riscs.

Capítol V
El personal del Servei de Salut

Article 24
Formació, conscienciació i compliment de les obligacions

1. El Servei de Salut ha de garantir la definició i l'execució de les accions necessàries per conscienciar i fomentar el compliment de les obligacions per part del personal amb relació als riscs i a les amenaces relatius a la seguretat de la informació.

2. Les persones que duguin a terme activitats especialment relacionades amb la seguretat de la informació —en particular el personal tècnic a càrrec de la gestió, l'operació i l'administració dels sistemes d'informació— han de rebre les accions formatives necessàries en matèria de seguretat.

Article 25
Obligació d'acatar la política de seguretat de la informació

1. Tot el personal que presti servei en l'àmbit del Servei de Salut ha de conèixer i respectar el contingut d'aquesta política de seguretat de la informació i el marc normatiu que la desplega.

2. La gestió i la preservació de la seguretat de la informació i el compliment dels objectius esmentats en l'article 4 d'aquest Decret han de ser la finalitat comuna de totes les persones que prestin servei directament o indirectament en el Servei de Salut, de manera que són responsables de l'ús correcte dels actius de tecnologies de la informació i de les comunicacions posats a disposició seva.

Article 26
Incompliment

L'incompliment d'aquesta política de seguretat de la informació pot suposar l'inici de les mesures disciplinàries procedents, sense perjudici de les responsabilitats legals corresponents.

Disposició addicional primera

No increment de la despesa pública

L'aplicació d'aquest Decret no suposa cap increment de la despesa pública; per això, el que estableix s'ha d'atendre amb els recursos humans i materials de què disposi el Servei de Salut.

Disposició addicional segona

Publicitat de la política de seguretat de la informació

A més de publicar-se en el *Butlletí Oficial de les Illes Balears*, aquest Decret també s'ha de fer públic en les respectives seus electròniques de l'Administració de la Comunitat Autònoma i del Servei de Salut.

Disposició addicional tercera

Denominacions

Totes les denominacions d'òrgans, càrrecs i col·lectius de persones que apareixen en aquest Decret en gènere masculí s'han d'entendre referides indistintament al gènere masculí i al femení.

Disposició final primera
Aplicació i desenvolupament de la política de seguretat de la informació

S'autoritza el Consell de Direcció del Servei de Salut per dictar les mesures necessàries per aplicar i complir les disposicions que estableix aquest Decret.

Disposició final segona

Entrada en vigor

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

Palma, 23 de febrer de 2018

La presidenta
Francesca Lluch Armengol i Socias

La consellera d'Innovació, Investigació i Turisme
Isabel M. Busquets i Hidalgo

La consellera de Salut
Patricia Gómez Picard