Instrucció 4/2022, de 5 de maig, 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 dades personals

1. Els sistemes d'informació són elements bàsics per assolir els objectius fonamentals encomanats al Servei de Salut de les Illes Balears, per la qual cosa els usuaris han d'emprar aquests recursos de manera que es preservin sempre les dimensions de la seguretat sobre la informació manejada i els serveis prestats: disponibilitat, integritat, confidencialitat, autenticitat i traçabilitat.

2. L'ús de recursos tecnològics per tractar la informació té una finalitat doble per al Servei de Salut:

   a) Facilitar i agilitar l'assistència sanitària d'atenció primària, d'atenció hospitalària i d'urgència, i també tramitar els procediments administratius emprant eines informàtiques i aplicacions de gestió

   b) Proporcionar informació completa, homogènia, actualitzada i fiable als usuaris.

3. L'ús de l'equipament informàtic i de comunicacions és actualment una necessitat en qualsevol organització del sector públic. Aquests mitjans i recursos es posen a disposició dels usuaris com a instruments de treball per desenvolupar l'activitat professional, raó per la qual competeix al Servei de Salut determinar les normes, les condicions i les responsabilitats sota les quals s'han d'emprar aquests recursos tecnològics.

4. El Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril 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, determina que les dades han de ser tractades de tal manera que se'n garanteixi una seguretat adequada, inclosa la protecció contra el tractament no autoritzat o il·lícit i contra la pèrdua, la destrucció o el dany accidental, aplicant mesures tècniques o organitzatives apropiades. Els

C/ de la Reina Esclarmunda, 9
07003 Palma
Tel. 971 17 56 00
ibsalut.es

responsables de tractament s'han de responsabilitzar d'aplicar les mesures que garanteixin un nivell de seguretat adequat al risc.

5. La Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, estableix que els responsables de tractament han de determinar les mesures tècniques i organitzatives apropiades que cal aplicar per garantir i acreditar que es compleix el Reglament (UE) 2016/679, la mateixa Llei, les normes que la despleguen i la legislació sectorial aplicable.

6. Per la seva banda, el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica, té per objecte establir la política de seguretat en l'ús de mitjans electrònics en l'àmbit de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, i estableix els principis bàsics i els requisits mínims que garanteixin adequadament la seguretat de la informació tractada.

7. En l'àmbit de la seguretat de la informació cal tenir en compte el Reial decret 43/2021, de 26 de gener, que té per objecte desplegar el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació, pel que fa al marc estratègic i institucional de seguretat de les xarxes i dels sistemes d'informació, la supervisió del compliment de les obligacions de seguretat dels operadors de serveis essencials i dels proveïdors de serveis digitals, i la gestió dels incidents de seguretat.

8. Aquests requeriments es reforcen amb l'obligació de garantir una protecció adequada de les dades clíniques, derivada d'aplicar-hi la 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, que estableix diverses previsions amb la finalitat de protegir la confidencialitat i la intimitat relatives a la informació relacionada amb la salut de la ciutadania.

9. En l'àmbit autonòmic, la Llei 5/2003, de 4 d'abril, de salut de les Illes Balears, estableix els drets i els deures de la ciutadania en l'àmbit sanitari, entre els quals el dret a la intimitat i a la confidencialitat de les dades que facin referència a la salut.

10. El Decret 63/2019, de 2 d'agost, pel qual s'estableix l'estructura orgànica bàsica del Servei de Salut de les Illes Balears, determina les funcions de la Subdirecció de Tecnologia de la Informació —depenent de la Direcció de Gestió i Pressuposts—, entre les quals hi ha establir i promoure la política de seguretat i els estàndards mínims i comuns relatius a la seguretat de la

C/ de la Reina Esclarmunda, 9
07003 Palma
Tel. 971 17 56 00
ibsalut.es

informació d'acord amb la normativa vigent en matèria de protecció de dades personals.

11. Per mitjà del 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, aquest ens assumeix el manteniment dels nivells adequats de seguretat i protecció davant amenaces a la informació que gestiona a partir dels objectius establerts en l'article 5 del Decret.

12. Tota aquesta normativa fa necessari incorporar a l'ús de les tecnologies de la informació i de la comunicació les pràctiques que permetin garantir un entorn segur per al tractament adequat de la informació i que optimitzin l'ús dels recursos disponibles en la prestació dels serveis sanitaris.

13. En aquest sentit, amb l'objectiu de mantenir uns nivells adequats de protecció de la informació i dels recursos informàtics, el Servei de Salut ha desenvolupat les pautes necessàries per mantenir les mesures de seguretat que garanteixin que es compleix la normativa vigent i que s'empren de manera adequada i eficient els recursos en la prestació dels serveis sanitaris.

14. Per mitjà de la Circular 4/2009, de 28 d'abril, del director general del Servei de Salut, es va aprovar el primer Codi de bones pràctiques en l'ús dels sistemes d'informació i el tractament de les dades de caràcter personal del Servei de Salut.

15. D'acord amb el Reial decret 3/2010 i a causa de la necessària gestió dels recursos tecnològics de manera que proporcionin una protecció adequada de la informació i dels serveis, de la proliferació de l'ús dels dispositius personals per a finalitats professionals, i de l'aparició i l'evolució dels serveis d'emmagatzematge en el núvol, el director general del Servei de Salut va considerar oportú aprovar l'actualització del Codi de bones pràctiques per mitjà de la Circular 01/2014, de 3 de març, i deixar sense efecte la Circular 4/2009.

16. Després de l'aprovació de la política de seguretat del Servei de Salut per mitjà del Decret 2/2018, l'aplicació del Reglament General de Protecció de Dades el 25 de maig de 2018 i l'entrada en vigor de la Llei orgànica 3/2018, de Protecció de dades personals i garantia dels drets digitals es considera oportú actualitzar el Codi de bones pràctiques, deixant sense efectes l'esmentada Circular 1/2014.

17. Aquest Codi de bones pràctiques detalla les mesures —orientades als usuaris— que formen part de la política de seguretat del Servei de Salut, el

compliment de les quals es considera imprescindible. Mantenir els nivells adequats de seguretat de la informació depèn en gran manera del fet que tots els usuaris apliquin aquests criteris en acomplir les seves funcions i també del seu compromís, en primer lloc, de custodiar la informació (especialment les dades personals) contra l'accés, l'ús o la divulgació no autoritzats, la pèrdua o la destrucció, i, en segon lloc, de protegir els recursos informàtics utilitzats per al tractament d'aquestes dades de l'ús no autoritzat, de l'alteració, de la destrucció, del mal ús i del robatori.

Per tot el que s'ha exposat, d'acord amb l'article 21 de la Llei 3/2003, de 26 de març, de règim jurídic de l'Administració de la Comunitat Autònoma de les Illes Balears, dict la següent

Instrucció

1. Objecte

Aquesta instrucció té l'objecte d'establir les directrius i les recomanacions en l'ús dels sistemes d'informació a fi d'optimitzar l'ús dels recursos disponibles i mantenir la seguretat, la confidencialitat, la disponibilitat i la integritat de les dades personals, tot això sense perjudici de complir la normativa vigent.

2. Àmbit d'aplicació

2.1. Tots els usuaris —tant els empleats públics com els adscrits a empreses externes públiques o privades— que tenguin accés als sistemes d'informació del Servei de Salut i/o a les dades que figurin sota la titularitat d'aquest han de conèixer i aplicar els requisits i les instruccions d'aquest Codi de bones pràctiques.

2.2. El Codi és aplicable a tots els recursos —equipament físic, equipament lògic, serveis i informació— emprats pels usuaris per acomplir les seves funcions.

2.3. Cal garantir la seguretat de la informació al llarg de totes les fases del seu cicle de vida (generació, distribució, emmagatzemament, processament, transport, consulta i destrucció) i la dels sistemes que la suporten (anàlisi, disseny, desenvolupament, implantació, explotació, integració i manteniment).

C/ de la Reina Esclarmunda, 9
07003 Palma
Tel. 971 17 56 00
ibsalut.es

3. Definicions

a) *Actiu*: component o funcionalitat d'un sistema d'informació susceptible de ser atacat deliberadament o accidentalment amb conseqüències per a l'organització. Inclou informació, dades, serveis, aplicacions (programari), equips (maquinari), comunicacions, recursos administratius, recursos físics i recursos humans.

b) *Autenticació*: procediment de comprovació de la identitat d'un usuari.

c) *Autenticitat*: propietat o característica consistent en el fet que una entitat és qui diu ser o bé que garanteix la font de la qual procedeixen les dades.

d) *Autoritat de control*: autoritat pública independent establerta per un estat membre de la Unió Europea.

e) *Caracterització del lloc de feina*: definició de les responsabilitats relacionades amb cada lloc de feina en matèria de seguretat i els requisits que han de complir els usuaris en termes de confidencialitat.

f) *Programa maliciós*: codi informàtic nociu que té l'objectiu d'infiltrar-se o danyar un equip informàtic o sistema d'informació sense el consentiment del seu propietari.

g) *Confidencialitat*: propietat o característica que consisteix a no posar informació a disposició de persones, entitats o processos no autoritzats ni revelar-los-ne.

h) *Consentiment de l'interessat*: tota manifestació de voluntat lliure, específica, informada i inequívoca per la qual l'interessat accepta, per mitjà d'una declaració o una clara acció afirmativa, el tractament de dades personals que el concerneixen.

i) *Correu brossa*: també conegut com a *spam*, és tot missatge de correu electrònic no volgut que s'envia aleatòriament en processos per lots, al qual està exposada la majoria dels usuaris. És una manera extremadament eficient i barata de comercialitzar qualsevol producte; de fet, les enquestes confirmen que més del 50 % dels missatges de correu electrònic són correu brossa. No és una amenaça directa, però la quantitat de missatges generats i el temps que necessiten les empreses i els usuaris particulars per detectar-lo i eliminar-lo suposa una gran molèstia.

j) *Dades personals*: tota informació sobre una persona física identificada o identificable («l'interessat»). Es considera *persona física identificable* tota persona la identitat de la qual es pugui determinar, directament o indirectament, en particular per mitjà d'un identificador: un nom, un número d'identificació, dades de localització, un identificador en línia o

un o alguns elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona.

k) *Dades relatives a la salut*: dades personals relatives a la salut física o mental d'una persona, inclosa la prestació de serveis d'atenció sanitària, que revelin informació sobre el seu estat de salut.

l) *Dades genètiques*: dades personals relatives a les característiques genètiques heretades o adquirides d'una persona que proporcionin una informació única sobre la fisiologia o la salut d'aquesta persona, particularment les obtingudes a partir de l'anàlisi d'una mostra biològica.

m) *Dades biomètriques*: dades personals obtingudes a partir d'un tractament tècnic específic i que són relatives a les característiques físiques, fisiològiques o conductuals d'una persona i permeten o confirmen la identificació única d'aquesta persona, com ara imatges facials o dades dactiloscòpiques.

n) *Dada anonimitzat*: dada que no permet identificar la persona afectada o interessada.

o) *Delegat de protecció de dades del Servei de Salut*: persona física, jurídica o òrgan que s'encarrega de garantir que en l'organització es compleixin les directrius del Reglament (UE) 2016/679.

p) *Destinatari*: persona física o jurídica, autoritat pública, servei o un altre organisme al qual es comuniquin dades personals, es tracti o no d'un tercer. No obstant això, no es consideren destinatàries les autoritats públiques que puguin rebre dades personals en el marc d'una investigació concreta de conformitat amb el dret de la Unió Europea o dels seus estats membres. El tractament d'aquestes dades per aquestes autoritats públiques ha de complir les normes en matèria de protecció de dades aplicables a les finalitats del tractament.

q) *Disponibilitat*: propietat o característica dels actius que consisteix en el fet que les entitats o els processos autoritzats hi tenen accés quan ho requereixen.

r) *Elaboració de perfils*: tot mode de tractament automatitzat de dades personals que consisteixi a utilitzar dades personals per avaluar determinats aspectes personals d'una persona física, en particular per analitzar o predir aspectes relatius al rendiment professional, a la situació econòmica, a la salut, a les preferències personals, als seus interessos, a la fiabilitat, al comportament, o a la ubicació o els moviments d'aquesta persona.

C/ de la Reina Esclarmunda, 9
07003 Palma
Tel. 971 17 56 00
ibsalut.es

s) *Empresa*: persona física o jurídica dedicada a una activitat econòmica, independentment de la forma jurídica, incloses les societats o associacions que desenvolupin regularment una activitat econòmica.

t) *Encarregat del tractament*: persona física o jurídica, autoritat pública, servei o un altre organisme que tracti dades personals per compte del responsable del tractament.

u) *Identificació*: procediment de reconeixement de la identitat d'un usuari.

v) *Incidència*: qualsevol anomalia que afecti o pugui afectar la seguretat de les dades.

w) *Integritat*: propietat o característica consistent en el fet que l'actiu d'informació no ha estat alterat de manera no autoritzada.

x) *Limitació del tractament*: marcatge de les dades personals conservades amb la finalitat de limitar-ne el tractament en el futur.

y) *Persona identificable*: tota persona la identitat de la qual es pugui determinar directament o indirectament per mitjà de qualsevol informació referida a la seva identitat física, fisiològica, psíquica, econòmica, cultural o social. Una persona física no es considera identificable si la identificació requereix terminis o activitats desproporcionats.

z) *Responsable de la seguretat*: responsable de determinar les decisions per complir els requisits de seguretat de la informació i dels serveis sobre la base de la declaració d'aplicabilitat del Servei de Salut. Actua com a punt de contacte amb les autoritats competents en matèria de ciberseguretat i de supervisió dels requisits de seguretat de les xarxes i els sistemes d'informació.

aa) *Pseudonimització*: tractament de dades personals de manera que ja no es puguin atribuir a un interessat sense utilitzar informació addicional, sempre que aquesta informació addicional figuri per separat i estigui subjecta a mesures tècniques i organitzatives destinades a garantir que les dades personals no s'atribueixin a una persona física identificada o identificable.

bb) *Responsable del tractament*: persona física o jurídica, autoritat pública, servei o un altre organisme que, tot sol o juntament amb d'altres, determini les finalitats i els mitjans del tractament. Si el dret de la Unió Europea o dels seus estats membres determina les finalitats i els mitjans del tractament, el responsable del tractament o els criteris específics per nomenar-lo pot establir-los el dret de la Unió Europea o dels seus estats membres.

cc) *Risc*: possibilitat de materialització d'una amenaça i conseqüències relatives a aquesta materialització.

C/ de la Reina Esclarmunda, 9
07003 Palma
Tel. 971 17 56 00
ibsalut.es

dd) *Centre d'Atenció a Usuaris (CAU)*: servei que presta suport informàtic i gestiona les incidències dels usuaris amb relació a les aplicacions i a les infraestructures informàtiques.

ee) *Sistema d'informació*: conjunt de dades que interactuen entre si amb una finalitat comuna.

ff) *Teletreball*: feina que es fa des d'un lloc fora de l'empresa utilitzant les xarxes de telecomunicació per complir les càrregues laborals assignades.

gg) *Tercer*: persona física o jurídica, autoritat pública, servei o organisme diferent de l'interessat, del responsable del tractament, de l'encarregat del tractament i de les persones autoritzades per tractar les dades personals sota l'autoritat directa del responsable o de l'encarregat.

hh) *Tractament de dades*: qualsevol operació o conjunt d'operacions sobre dades personals o conjunts de dades personals, ja sigui per procediments automatitzats o no: recollida, registre, organització, estructuració, conservació, adaptació o modificació, extracció, consulta, utilització, comunicació per transmissió, difusió o qualsevol altre mode d'habilitació d'accés, acarament o interconnexió, limitació, supressió o destrucció.

ii) *Traçabilitat*: propietat o característica que consisteix en el fet que les actuacions d'una entitat es poden imputar exclusivament a aquesta.

jj) *Usuaris*: tots els empleats públics que presten servei al Servei de Salut i el personal d'empreses externes que desenvolupi tasques de manera permanent o ocasional a qualsevol òrgan pertanyent o adscrit al Servei de Salut.

kk) *Violació de la seguretat de les dades personals*: tota violació de la seguretat que ocasioni la destrucció, la pèrdua o l'alteració accidentals o il·lícites de dades personals transmeses, conservades o tractades d'una altra manera, o bé la comunicació o l'accés no autoritzats a aquestes dades.

4. Informació als usuaris

4.1. Aquesta instrucció s'ha de posar a la disposició de tots els usuaris a la seu electrònica del Servei de Salut. De la mateixa manera, s'ha d'enviar a tots els usuaris un missatge de correu electrònic que ha de contenir els enllaços de consulta de la normativa.

4.2. En els manuals de benvinguda de les gerències territorials s'ha d'incorporar el Codi de bones pràctiques a fi que les persones que

s'hi incorporin el consultin abans d'emprar els recursos del Servei de Salut.

4.3. Els òrgans de direcció i de gestió del Servei de Salut, estructurats en Serveis Centrals i en gerències territorials, són els responsables de fer arribar aquesta norma a les empreses externes a fi que els seus usuaris la coneguin i la compleixin.

5. Confidencialitat de la informació

5.1. Com a mesura de protecció de la informació pròpia, confiada o tractada pel Servei de Salut, els usuaris s'han d'abstenir de comunicar aquesta informació, divulgar-la, distribuir-la o posar-la en coneixement o a l'abast de tercers (externs o interns no autoritzats) per mitjà de suports informàtics o per qualsevol altre mitjà que no hagi estat autoritzat prèviament.

5.2. Tot el personal del Servei de Salut i el personal aliè que, per raó de la seva activitat professional, hagi tingut accés a informació gestionada pel Servei de Salut (dades personals, documents, metodologies, claus, anàlisi, programes...) ha de mantenir una absoluta reserva sobre aquesta durant temps indefinit.

5.3. Si hom té accés en qualsevol tipus de suport a informació que no sigui de difusió lliure, s'ha d'entendre que l'accés és estrictament temporal, mentre duri la funció encomanada, que comporta l'obligació indefinida de secret o de reserva i que això no atorga cap dret de possessió, titularitat o còpia d'aquesta informació. Així mateix, és imprescindible tornar els suports d'informació emprats immediatament després que hagin acabat les tasques que n'hagin originat l'ús.

5.4. Els usuaris només poden accedir a la informació per a la qual tenguin l'autorització deguda i explícita depenent de les funcions que acompleixin, de tal manera que en cap cas no poden tenir accés a informació que pertanyi a altres usuaris o a grups d'usuaris per al qual no tenguin autorització.

5.5. Els drets d'accés a la informació i als sistemes d'informació que la tracten s'han d'atorgar sempre de conformitat amb els principis del mínim privilegi possible i de la necessitat de conèixer.

6. Protecció de dades personals

6.1. Els usuaris amb accés a les dades personals o als sistemes de tractament de dades estan obligats a complir totes les mesures de seguretat establertes i els requisits i les condicions aplicables d'acord amb les normes i els procediments vigents i els controls de seguretat establerts. Així mateix, han d'utilitzar la informació a la qual tenguin accés només per a les finalitats relacionades amb les seves competències i exclusivament per dur a terme la feina i acomplir les funcions assignades. Aquests usuaris podrien haver de respondre del fet d'incomplir aquestes obligacions de conformitat amb el règim jurídic aplicable.

6.2. A les Illes Balears, la protecció de les dades personals està regulada per la normativa següent:

- El Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril 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.
- La Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, per la qual es deroga la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

6.3. Basant-se en la normativa vigent, s'han desenvolupat els criteris següents sobre les responsabilitats que ha d'assumir el responsable de tractament —o, si escau, els representants— del Servei de Salut:

6.3.1. Ha de designar un delegat de protecció de dades per al Servei de Salut.

6.3.2. Sempre que un tercer s'hagi d'encarregar del tractament de les dades, ha de ser sota la relació jurídica d'encarregat del tractament.

6.3.3. Ha de mantenir el registre de les activitats de tractament duites a terme sota la seva responsabilitat i fer públic un inventari d'aquestes, accessible per mitjans electrònics.

6.3.4. Ha de prendre mesures organitzatives i tècniques per integrar en els tractaments garanties que permetin aplicar

de manera efectiva els principis bàsics del Reglament (UE) 2016/679 i de la Llei orgànica 3/2018.

6.3.5. S'ha d'assegurar que s'implantin correctament les mesures de seguretat establertes per l'Esquema Nacional de Seguretat en el tractament de dades personals per evitar-ne la pèrdua, l'alteració o l'accés no autoritzat, adaptant els criteris de determinació del risc en el tractament de les dades.

6.3.6. Ha d'adoptar mesures que garanteixin que només es tractaran les dades necessàries pel que fa a la quantitat de dades tractades, l'extensió del tractament, els períodes de conservació i l'accessibilitat a les dades.

6.3.7. Ha de facilitar als interessats l'exercici dels drets relatius a les dades personals, de manera que el procediment per exercir-los sigui visible, accessible i senzill.

6.3.8. Ha de notificar a l'autoritat de protecció de dades competent en un termini màxim de 72 hores quan es produeixi un incident de seguretat de les dades, llevat que sigui improbable que la violació suposi un risc per als drets i les llibertats dels interessats.

6.3.9. Les dades només poden ser comunicades fora de l'Espai Econòmic Europeu si es compleixen els supòsits que s'especifiquen en el procediment de transferències internacionals de dades.

6.3.10. Ha de garantir la formació necessària en matèria de protecció de dades personals a les persones autoritzades per tractar dades personals.

6.3.11. Ha de fer consultes a l'autoritat de control pertinent sobre els tractaments de dades amb la finalitat de garantir que es compleixi la normativa de protecció de dades vigent.

6.4. Sobre la base de la legislació establerta, s'han desenvolupat els criteris següents sobre les normes que han de complir tots els usuaris del Servei de Salut amb accés a dades personals:

6.4.1. És fonamental que els usuaris amb accés a dades personals servin un estricte secret professional durant temps indefinit

sobre qualsevol informació a la qual tenguin accés en acomplir la seva feina. Això implica que aquesta obligació continua vigent fins i tot després que s'hagi extingit la relació amb el Servei de Salut.

6.4.2. Els usuaris tenen el compromís de no tractar les dades personals a les quals tenguin accés, ni cedir-les, ni comunicar-les, ni utilitzar-les en benefici propi, ni revelar-les a tercers, i el compromís de respectar sempre la privacitat i la confidencialitat d'aquestes dades.

6.4.3. Els usuaris han de conèixer els principis bàsics del Reglament (UE) 2016/679 i la Llei orgànica 3/2018 relatius al tractament de dades personals requerides per acomplir les seves funcions. A continuació es detallen algunes consideracions essencials sobre aquests principis:

a) Tots els usuaris que tenguin accés a dades personals han de conèixer la finalitat d'emprar-les i les seves obligacions particulars relatives al tractament requerit en l'acompliment de la seva activitat professional.

b) Les dades personals han de ser exactes i, si és necessari, actualitzades; per això cal adoptar totes les mesures raonables perquè se suprimeixin o rectifiquin sense dilació les dades personals que siguin inexactes respecte de les finalitats per a les quals es tracten.

c) L'usuari que tengui accés a dades personals ha d'extremar les precaucions per evitar-ne la difusió o l'accés no autoritzat i per no tractar-les sense l'autorització prèvia del responsable de tractament. Les cessions de dades han de comptar amb habilitació legal i de conformitat amb les mesures de seguretat aplicables, tot i que és preferible —sempre que sigui possible— comunicar només dades pseudonimitzades o anònimes.

d) S'ha d'accedir a la informació que contengui dades personals només per mitjà dels procediments habilitats a l'efecte pel Servei de Salut.

e) Qualsevol requeriment nou per al tractament de dades personals que sigui identificat —fora de l'activitat prevista— ha de ser analitzat i autoritzat prèviament pel delegat de protecció de dades del Servei de Salut.

f) Tots els usuaris han de col·laborar per satisfer l'exercici de qualsevol dels drets d'accés, rectificació, supressió, oposició, portabilitat, limitació del tractament i no ser objecte d'elaboració de perfils, l'exercici dels quals es reconeix als interessats, atenent-los correctament i adequadament i informant-los sobre quin és el procediment que han de seguir.

g) Qualsevol iniciativa, projecte o desenvolupament que s'hagi d'iniciar dins el Servei de Salut ha de passar per una fase d'anàlisi de la privadesa des del disseny i per defecte.

6.4.4. Qui tengui necessitat de generar fitxers temporals s'ha d'assegurar dels aspectes següents:

a) Ha de garantir que el tractament compleix les finalitats autoritzades.

b) Ha de complir totes les mesures de seguretat establertes d'acord amb el nivell de risc identificat.

c) Ha d'allotjar les dades temporals a les unitats ofimàtiques (carpetes) assignades als usuaris per les unitats responsables en matèria de tecnologia de la informació a fi de garantir els controls tècnics preestablerts, i ha d'evitar allotjar-les en un ordinador personal, sempre que sigui possible.

d) Ha d'eliminar o destruir convenientment els fitxers quan deixin de ser necessaris per a la finalitat per a la qual hagin estat creats.

6.4.5. Tot tractament que s'hagi de fer fora dels sistemes d'informació del Servei de Salut s'ha d'autoritzar prèviament i ha de complir les mesures necessàries per protegir la informació.

6.4.6. Quan s'enviïn per primera vegada dades personals —en format electrònic o impreses en paper—, cal validar el mètode de tramesa a fi de garantir que es compleixen les mesures de seguretat requerides pel tractament.

6.4.7. De conformitat amb l'article 24 del Reial decret 311/2022, els sistemes d'informació que gestionin categories especials de dades personals han de generar un registre d'accessos amb la finalitat exclusiva de registrar les activitats dels

usuaris retenint la informació necessària per monitorar, analitzar, investigar i documentar activitats indegudes o no autoritzades i permetre identificar en tot moment la persona que actua.

6.4.8. Els usuaris autoritzats per gestionar suports amb dades personals els han de desar en un lloc segur quan no els emprin, especialment fora de la jornada laboral. Addicionalment, han d'elaborar i mantenir un inventari dels suports que estiguin sota custòdia seva. En cas que es rebutgin o reutilitzin els suports, han d'impedir que es pugui recuperar posteriorment la informació emmagatzemada.

6.4.9. Per tractar documentació que contengui dades personals cal observar les directrius següents:

a) Llevat que sigui estrictament necessari, cal evitar imprimir en paper documentació que contengui dades personals.

b) Cal posar un esment especial a no deixar documents impresos amb dades personals o confidencials a la safata de sortida d'impressores ni als faxos, per evitar que estiguin a l'abast de persones no autoritzades. De la mateixa manera, cal evitar fer fotocòpies d'aquests documents; si se'n fan, cal controlar l'ús que se'ls dona i destruir-les oportunament.

c) Els documents s'han de desar dins calaixos o armaris amb pany i clau en els períodes d'absència del lloc de treball.

d) Les llistes impreses que contenguin dades amb informació personal no s'han de rebutjar dins els contenidors de paper per reciclar. Cada usuari ha de revisar periòdicament els documents que estiguin sota custòdia seva i destruir els que siguin obsolets. La documentació impresa o en suport òptic que contengui dades personals que s'hagi de rebutjar s'ha d'eliminar amb màquines destructores de paper o mecanismes similars, o d'alguna manera que eviti que les dades es puguin recuperar.

6.4.10. Qualsevol incidència o anomalia que pugui afectar la seguretat de les dades personals s'ha de comunicar al CAU

o al servei d'informàtica corresponent d'acord amb el procediment de comunicació i gestió d'incidències.

7. Ús dels recursos informàtics

7.1. Pautes generals

7.1.1. El Servei de Salut posa a disposició dels usuaris l'accés a determinats recursos informàtics i dispositius de comunicacions, tant fixos com mòbils, que faciliten l'acompliment de la seva feina. Aquests recursos són propietat del Servei de Salut; com a tals, s'han d'emprar per a les tasques pròpies dels usuaris d'acord amb les funcions assignades. Amb caràcter general, els recursos informàtics i dispositius de comunicacions s'han d'utilitzar per a finalitats institucionals i com a eina de suport en les competències professionals dels usuaris autoritzats.

7.1.2. El Servei de Salut és el responsable de determinar les normes, les condicions i les responsabilitats oportunes per protegir els recursos informàtics. Els usuaris amb accés a aquests són responsables de custodiar-los i de protegir-los davant de les possibles amenaces (accessos no autoritzats, ús indegut, errors o omissions, robatori, etc.).

7.1.3. Per tal de no comprometre les mesures de seguretat establides pel Servei de Salut, els usuaris han d'evitar les accions següents, llevat que disposin de l'autorització prèvia corresponent:

a) Emprar equips o aplicacions que no estiguin especificats directament com a part del suport lògic o del suport físic estàndard del Servei de Salut. En cap cas no es pot modificar la configuració establerta dels recursos ni intercanviar components o perifèrics (teclats, pantalles, ratolins, etc.) entre ordinadors.

b) Extreure equips dels locals o de les instal·lacions del Servei de Salut, llevat que estigui autoritzat prèviament.

c) Fer connexions a xarxes o a sistemes externs o a la xarxa corporativa per mitjans que no siguin els definits i administrats pel personal informàtic competent. En aquest sentit, cal evitar especialment establir connexions addicionals de manera independent. També cal evitar emprar xarxes sense fil alienes, perquè es

poden utilitzar per capturar informació sensible o comprometre la seguretat dels sistemes que s'hi connectin.

d) Extreure o utilitzar informació confidencial o dades personals en entorns que no estiguin protegits o configurats adequadament per evitar l'accés no autoritzat. Per exportar aquestes dades a altres entorns cal garantir el nivell de seguretat corresponent abans d'extreure-les.

e) Traslladar fora de les instal·lacions habituals de treball dades o informacions —en format digital, impreses en paper o en qualsevol altre suport— sense l'autorització prèvia corresponent.

f) Destruir, alterar, inutilitzar o fer malbé de qualsevol altra manera els recursos informàtics, els programes, les dades, els suports i els documents.

g) Intentar desxifrar les claus, els sistemes o els algorismes d'encriptació i qualsevol altre element de seguretat establert.

h) Modificar o desactivar els mecanismes de seguretat implantats per protegir els recursos informàtics i els sistemes d'informació.

i) Accedir a informació que no sigui necessària per acomplir les funcions de cada persona.

j) Deixar els recursos de tractament d'informació desatesos sense les mesures de bloqueig adequades o mantenir suports amb informació sensible a llocs poc segurs.

k) Tenir permisos d'administrador dels equips sense l'autorització prèvia corresponent.

7.1.4. L'ús de l'ordinador, del navegador i del correu electrònic o de qualsevol altre recurs per a alguna finalitat particular ha de ser autoritzat prèviament.

7.1.5. Està prohibit expressament utilitzar els recursos informàtics per a les finalitats següents:

a) Emmagatzemar informació amb continguts de caràcter racista, xenòfob, pornogràfic, sexual, d'apologia del terrorisme o que atempti contra els drets humans, o que

C/ de la Reina Esclarmunda, 9
07003 Palma
Tel. 971 17 56 00
ibsalut.es

actuï en perjudici dels drets a la intimitat, a l'honor i a la imatge pròpia o contra la dignitat de les persones.

b) Instal·lar i/o emprar programes o continguts que atemptin contra la legislació en matèria de protecció de la propietat intel·lectual.

7.2. Ús de dispositius mòbils

7.2.1. Els dispositius mòbils —ordinadors portàtils, tauletes i telèfons mòbils— proporcionats pel Servei de Salut han de disposar de les mesures de seguretat necessàries per garantir-ne la seguretat, les quals s'han de basar almenys en la instal·lació de sistemes de protecció contra programes maliciosos i en actualitzacions i sistemes de protecció d'instal·lació de programes maliciosos.

7.2.2. Els dispositius mòbils han d'estar protegits amb contrasenya i blocatge automàtic per inactivitat.

7.2.3. En cap cas és permès instal·lar aplicacions no autoritzades pel Servei de Salut o que puguin comprometre el funcionament dels dispositius mòbils.

7.2.4. Els dispositius mòbils del Servei de Salut han de tenir mecanismes d'encriptació per impedir l'accés indegut de tercers no autoritzats a la informació que emmagatzemin.

7.2.5. Els usuaris han de comunicar immediatament al CAU o al servei d'informàtica corresponent la pèrdua del seu dispositiu mòbil, a fi que el bloqui i n'esborri el contingut.

7.2.6. Per motius de seguretat, el Servei de Salut pot blocar els dispositius mòbils que presentin riscs per a la seguretat o posin en perill la confidencialitat de la informació.

7.3. Ús d'unitats ofimàtiques

7.3.1. Amb caràcter general, la informació emmagatzemada de manera local als ordinadors i equips informàtics dels usuaris no serà objecte de salvaguarda per mitjà de cap procediment corporatiu de còpia de seguretat. El Servei de Salut pot fer còpies de seguretat de tots els actius i sistemes d'informació emmagatzemats de manera local quan disposi

del conjunt d'eines, mitjans i recursos per a la generació d'aquestes còpies.

7.3.2. El Servei de Salut pot posar a la disposició dels usuaris unitats ofimàtiques —que consisteixen en espai de disc en xarxa assignat a cada usuari pel personal tècnic del Servei de Salut— per contenir les salvaguardes periòdiques de les seves unitats locals. Aquestes unitats corporatives no s'han d'utilitzar per a finalitats privades, perquè són una eina de treball, tenen una capacitat limitada i són compartides per tots els usuaris, per la qual cosa només s'hi ha de salvaguardar la informació que es consideri estrictament necessària. En particular, cal evitar emmagatzemar en aquestes unitats —fins i tot amb caràcter provisional o temporal— continguts de mida grossa, com ara fitxers multimèdia (àudio, vídeo, imatges...).

7.4. Ús i manteniment de programes informàtics

7.4.1. Cal evitar emprar, instal·lar o distribuir programes fora de les recomanacions i dels estàndards aprovats pel Servei de Salut, perquè poden comprometre la seguretat dels sistemes d'informació.

7.4.2. Si és necessari instal·lar programes aliens a l'estàndard establert, cal demanar autorització a la persona responsable del servei, però és necessària la valoració prèvia del servei d'informàtica corresponent.

7.4.3. La instal·lació de programes informàtics ha de ser sempre a càrrec del servei d'informàtica corresponent o ha de ser monitorada per aquest a fi d'assegurar que es compleixen les mesures de seguretat requerides i que es disposa de les garanties de suport oportunes. En cap cas no es poden eliminar o deshabilitar les aplicacions informàtiques instal·lades pel servei d'informàtica, especialment les relacionades amb la seguretat.

7.4.4. La instal·lació i l'ús de programes s'ha de fer d'acord amb les llicències d'ús adquirides i controlades pel Servei de Salut, per la qual cosa està prohibit instal·lar programes sense la llicència corresponent. Es prohibeixen la reproducció, la modificació, la transformació, la cessió, la comunicació i l'ús fora de l'àmbit del Servei de Salut de les

aplicacions i dels programes informàtics instal·lats en els equips que pertanyen a l'organització. Tampoc no és permès fer còpies dels programes instal·lats en els ordinadors.

7.4.5. Els usuaris han de facilitar al CAU i al servei d'informàtica corresponent l'accés al seu equip per a tasques de reparació, instal·lació o manteniment. Aquest accés es limitarà únicament a les accions necessàries per al manteniment o la resolució de problemes que es puguin trobar en l'ús dels recursos informàtics i de comunicacions, i acabarà una vegada que s'hagi completat el manteniment o s'hagin resolt els problemes.

7.4.6. Si el personal de suport tècnic detecta qualsevol anomalia que indiqui que els recursos s'utilitzen de manera contrària a allò que estableix aquest Codi, n'informarà la Subdirecció de Tecnologia de la Informació, que prendrà les mesures correctores oportunes.

7.4.7. Els equips informàtics de l'organització han de mantenir actualitzats els pegats de seguretat de tots els programes que tenguin instal·lats. Cal para atenció especialment a l'actualització, la configuració i el funcionament correctes dels programes antivirus i tallafocs.

7.5. Connexió de dispositius personals

7.5.1. No es pot connectar a la xarxa informàtica de comunicacions corporativa (xarxa interna) cap dispositiu diferent dels configurats, habilitats i admesos pel Servei de Salut, llevat que es disposi de l'autorització prèvia corresponent

7.5.2. Els dispositius personals emprats en l'àmbit del Servei de Salut que accedeixin a les xarxes i aplicacions corporatives poden ser sotmesos a activitats de prevenció i control pel Servei de Salut, però es limitaran a les àrees, les aplicacions i els contenidors d'informació corporativa dels dispositius personals en qüestió.

7.5.3. En cas de necessitar connectar-se, el nivell de seguretat dels dispositius personals ha de ser el mateix que el dels dispositius mòbils corporatius emprats.

7.6. Sistemes d'emmagatzematge d'informació en el núvol

7.6.1. L'emmagatzemament en el núvol consisteix en la disposició d'aplicacions, plataformes o infraestructura que, a càrrec d'un proveïdor o del mateix Servei de Salut, són accessibles per mitjà d'internet, independentment d'on estiguin allotjats els sistemes d'informació, i de manera transparent per a l'usuari final.

7.6.2. Amb caràcter previ a l'ús d'aquests recursos externs, la Subdirecció de Tecnologia de la Informació ha d'establir les característiques del servei prestat i les responsabilitats de les parts, detallant allò que es considera qualitat mínima del servei prestat i les conseqüències d'incomplir-lo.

7.6.3. No és permès transmetre o allotjar informació sensible, confidencial, dades personals o informació protegida pròpia del Servei de Salut en servidors externs o solucions d'emmagatzemament en el núvol diferent de les solucions corporatives, llevat que es disposi de l'autorització prèvia corresponent. Cal comprovar que no hi hagi traves legals per fer-ho i verificar la subscripció d'un contracte exprés entre el Servei de Salut i l'empresa responsable de la prestació del servei, inclosos els acords de nivell de servei que siguin procedents, el corresponent acord de confidencialitat, i sempre havent analitzat prèviament els riscs associats.

7.7. Control de programes maliciosos

7.7.1. Un programa maliciós és un tipus de programari que té com a objectiu infiltrar-se en un equip informàtic o sistema d'informació o danyar-lo sense el consentiment del seu propietari. La introducció d'un programa maliciós en els sistemes d'informació del Servei de Salut es pot originar en visitar pàgines web infectades, en obrir missatges de correu electrònic o en executar un programa contaminat o un fitxer infectat (procedent d'un disc dur extern, una memòria USB, un CD, un sistema d'emmagatzematge en el núvol, un dispositiu mòbil, etc.). L'usuari ha de ser conscient de les amenaces que això provoca; per tant, és imprescindible que faci un ús responsable dels equips per reduir aquest risc.

7.7.2. Tots els llocs de treball i dispositius mòbils del Servei de Salut han de tenir instal·lats i activats els mecanismes adequats per prevenir i detectar infeccions de programes maliciosos. En cap circumstància s'han de desactivar aquests mecanismes; no obstant això, cal tenir en compte que no garanteixen la protecció contra les amenaces, per la qual cosa de manera general cal actuar amb cautela i sentit comú:

a) Si se sospita d'una infecció amb un programa maliciós, virus, cucs, etc., cal comunicar la incidència d'acord amb el procediment de comunicació i gestió d'incidències corresponent.

b) Cal adoptar totes les precaucions possibles en executar qualsevol programa, fins i tot els procedents de fonts considerades de confiança, perquè poden haver estat suplantats.

c) Cal evitar executar fitxers adjunts rebuts per correu electrònic i visitar pàgines web amb continguts de legalitat o moralitat dubtoses, perquè són una font habitual d'infeccions.

8. Mesures de seguretat

8.1. Mesures de seguretat d'accés físic

8.1.1. La informació confidencial o amb dades personals —en CD, en dispositius d'emmagatzematge, en fitxers visibles directament a la pantalla de l'ordinador— s'ha de custodiar per evitar accessos no autoritzats.

8.1.2. No s'ha de mantenir la informació en llocs a la vista sense el control del responsable en aquell moment. En cas d'absència, cal establir mecanismes que impedeixin l'accés de persones no autoritzades a aquesta informació, d'acord amb les característiques del lloc de feina i del suport en què estigui la informació.

8.1.3. Addicionalment, les pantalles s'han d'orientar de tal manera que s'elimini tant com sigui possible l'angle de visió a les persones no autoritzades.

8.2. Mesures de seguretat d'accés lògic

8.2.1. El control d'accés als sistemes d'informació està basat en l'ús de certificats electrònics qualificats o identificadors d'usuari i contrasenyes lligades als perfils d'accés. Depenent del nivell de seguretat dels sistemes, es pot requerir un segon factor d'autenticació temporal. Aquests perfils han estat establerts d'acord amb les funcions que acompleix cada usuari i la criticitat dels sistemes.

8.2.2. L'identificador d'usuari i la contrasenya corresponent que s'assignen al personal que els requereixi són confidencials, personals i intransferibles. Per tant, és responsabilitat del titular l'ús que en faci.

8.2.3. Cada usuari ha de vetlar per la confidencialitat de la seva contrasenya; en cap cas no l'ha de guardar en fitxers digitals ni escrita en paper o en qualsevol altre tipus de suport de manera llegible o accessible. Tampoc pot comunicar a cap altra persona el seu identificador d'usuari ni la contrasenya, ni ha d'emprar una sessió oberta sota una altra identitat.

8.2.4. Si un usuari sospita que la seva contrasenya ha estat coneguda de manera fortuïta o fraudulenta per persones no autoritzades, l'ha de modificar i ha de notificar immediatament la incidència al servei de suport corresponent.

8.2.5. Cada usuari ha de canviar la seva contrasenya d'accés als sistemes almenys una vegada cada 45 dies i sempre que li ho indiqui l'encarregat de la gestió d'usuaris.

8.2.6. Si, en un moment donat, un usuari rep una trucada o un missatge electrònic en què se li sol·licita el nom d'usuari i/o la contrasenya, mai no ha de facilitar aquestes dades i ha de comunicar immediatament la incidència al CAU o al servei d'informàtica corresponent.

8.2.7. Quan un usuari acabi la relació o vinculació amb el Servei de Salut, la persona directament responsable de l'usuari ha de comunicar aquesta nova situació a l'encarregat de la gestió d'usuaris perquè doni de baixa els comptes i les autoritzacions que tengui.

C/ de la Reina Esclarmunda, 9
07003 Palma
Tel. 971 17 56 00
ibsalut.es

8.2.8. Correlativament, quan els mitjans informàtics o de comunicacions proporcionats pel Servei de Salut estiguin associats a l'acompliment d'un determinat lloc o funció, la persona que els tengui assignats els ha de tornar immediatament a la unitat responsable quan acabi la vinculació amb aquest lloc o funció.

8.3. Ús de certificats electrònics com a mecanisme de signatura, identificació i autenticació

8.3.1. Tots els accessos als sistemes que contenguin informació han de disposar d'un mecanisme d'identificació i autenticació que garanteixi la seguretat d'accés al sistema. Aquest mecanisme està basat normalment en l'ús d'identificadors d'usuari i contrasenyes, però en altres casos es pot basar en altres mecanismes que proporcionin un grau més alt de seguretat sobre la base de la informació que tractin els sistemes d'informació.

8.3.2. L'avenç en l'aplicació dels algorismes criptogràfics i en la certificació digital permet aplicar informàticament procediments que tradicionalment s'han aplicat manualment, amb la qual cosa s'estableixen garanties equivalents respecte a l'autenticació de la identitat dels actors i a la confidencialitat, la integritat i la falta de rebuig de la informació tractada.

8.3.3. L'ús d'aquests algorismes requereix que l'usuari empri un certificat electrònic, l'autenticitat i la integritat del qual estan garantides per un tercer de confiança. En aquest cas, l'usuari ha d'observar les pautes següents:

a) En l'ús del servei, l'usuari ha d'aplicar les pràctiques establertes pel Servei de Salut i per l'entitat prestadora de serveis de certificació que siguin necessàries per garantir la validesa de les transmissions electròniques emeses i rebudes.

b) L'usuari ha de comunicar qualsevol variació de les dades aportades per obtenir el certificat a l'entitat prestadora de serveis de certificació i/o registre.

c) L'usuari és el responsable de l'ús que es faci del seu certificat electrònic.

d) L'usuari ha de salvaguardar l'accés al seu certificat electrònic aplicant les mesures de seguretat descrites en l'apartat 8.2 i ha de protegir qualsevol element (targeta o dispositiu criptogràfic, fitxer informàtic, programa, PIN, contrasenya, etc.) que sigui necessari per accedir a aquestes claus. En cap cas els dispositius criptogràfics que emmagatzemin els certificats electrònics han de quedar inserits en els lectors en absència del titular.

e) L'usuari ha de comunicar immediatament qualsevol incidència que afecti la seguretat del seu certificat electrònic o dels elements i/o els codis utilitzats per accedir-hi. Aquesta comunicació s'ha de fer d'acord amb els procediments establerts pel Servei de Seguretat de la Informació.

8.4. Lloc de treball adesat

8.4.1. Amb caràcter general, els llocs de treball han d'estar adesats, sense cap més material damunt la taula que el que es requereixi per a l'activitat que s'estigui fent en cada moment.

8.4.2. En particular, quan un usuari del Servei de Salut amb accés als sistemes d'informació abandoni el lloc de treball ha de desar tota la informació que estigui tractant, de manera que no quedin desatesos memòries USB o suports externs d'informació, llistes o informació visible a la pantalla de l'ordinador personal o documentació sobre el lloc de treball propi. El material de treball s'ha de desar en un lloc tancat (en un calaix o un armari amb pany i clau) o en una habitació separada tancat amb clau, almenys fora de l'horari de feina.

8.4.3. Es pot establir un procediment per revisar que es compleix aquesta mesura fent una inspecció regularment després del tancament, notificant els incompliments detectats i retirant el material oblidat dins un lloc tancat.

8.5. Blocatge del lloc de treball

8.5.1. Tots els terminals, ordinadors personals i dispositius mòbils emprats pels usuaris del Servei de Salut amb accés a la informació en l'acompliment de les seves funcions han de

ser bloquejats convenientment per l'usuari abans d'abandonar el lloc de treball, tant momentàniament com al final de la jornada laboral.

8.5.2. Així mateix, ha de bloquejar el lloc de treball al cap d'un temps d'inactivitat, establert per la política de seguretat, que és part de la configuració de l'equip i no pot ser alterat per l'usuari.

9. Accés per mitjà de xarxes

9.1. En l'accés i l'ús de les xarxes implantades en els diferents centres del Servei de Salut, tot usuari ha de complir les normes de seguretat establertes.

9.2. L'accés a les xarxes internes s'ha de dur a terme exclusivament pels mitjans implantats corporativament, per la qual cosa no està permès utilitzar qualsevol altre mitjà de connexió amb xarxes externes sense l'autorització prèvia corresponent.

9.3. Per emprar la xarxa són necessàries les credencials d'accés (generalment un identificador, una contrasenya i, si escau, un segon factor d'autenticació), que s'assignen només als usuaris autoritzats. La custòdia d'aquestes credencials és responsabilitat de l'usuari autoritzat, per la qual cosa ha d'observar el que disposen els apartats 8.2 i 8.3.

9.4. Qualsevol connexió remota que s'hagi d'habilitar —a petició d'un usuari intern o d'un proveïdor extern— ha de tenir l'autorització prèvia de la persona responsable corresponent i la validació de la Subdirecció de Tecnologia de la Informació a fi de garantir els nivells de seguretat requerits.

10. Ús d'internet

10.1. Internet ha de ser accessible exclusivament als usuaris que el necessitin per acomplir les seves funcions, als quals es proveirà de permisos d'accés.

10.2. En l'ús d'internet, l'usuari ha de ser conscient que en acomplir les seves funcions laborals està representant el Servei de Salut; conseqüentment, es compromet a reflectir en la seva conducta l'ètica, la professionalitat, la cortesia i la responsabilitat que s'espera dels usuaris que estan adscrits a aquest organisme.

10.3. A causa de la necessitat d'optimitzar els recursos disponibles, l'accés a internet ha de respondre a finalitats professionals. El Servei de Salut vetlarà pel bon ús de l'accés a internet, tant des del punt de vista de l'eficiència i de la productivitat dels usuaris com des del punt de vista dels riscs de seguretat associats a l'ús d'internet.

10.4. Sense perjudici del que preveu l'apartat 6.4.2 amb relació a les cessions, cal evitar enviar dades personals per mitjà d'internet. En qualsevol cas, la transferència només es pot efectuar emprant els mecanismes que garanteixin la ininteligibilitat i la integritat de les dades, i amb l'autorització prèvia corresponent.

10.5. És important assegurar l'encriptació en la transmissió d'informació sensible, confidencial o protegida. Una manera d'assegurar la confidencialitat és comprovar que s'utilitza protocol HTTPS en la comunicació en lloc del protocol estàndard HTTP observant la barra d'adreces, en la qual també hi hauria d'aparèixer la icona d'un pany, clicant en el qual s'obté informació sobre el certificat digital d'identitat de la pàgina web visitada.

10.6. No s'han d'emprar navegadors ni programes de correu electrònic —ni versions d'aquests— que no estiguin prevists pels estàndards en vigor. Tampoc no es pot modificar la configuració d'aquests programes en els aspectes relacionats amb la seguretat.

10.7. Cal notificar al CAU o al servei d'informàtica corresponent qualsevol anomalia detectada en l'accés a internet i tota sospita de problemes o incidents de seguretat relacionats amb aquest accés.

10.8. Es consideren com a ús incorrecte del servei els casos següents:

10.8.1. Accedir a llocs d'internet o distribuir missatges amb continguts en els quals s'inciti o es promogui la pornografia o la segregació racial, sexual o religiosa, o amb continguts de violència.

10.8.2. Descarregar i transmetre indiscriminadament imatges, àudios i vídeos, perquè la mida dels fitxers satura l'ample de banda i disminueix la velocitat de transmissió, cosa que perjudica els altres usuaris. Es prohibeix expressament emprar utilitats d'intercanvi d'informació a internet, com ara les xarxes d'igual a igual (P2P, per *peer-to-peer*).

10.8.3. Distribuir virus o troians o dur a terme qualsevol activitat a fi d'accedir il·lícitament a altres sistemes d'informació amb l'objectiu d'interceptar, fer malbé o manipular la informació per obtenir un benefici personal, per diversió o per beneficiar o perjudicar altres persones.

10.8.4. Dur a terme per mitjà d'internet qualsevol activitat il·legal o maliciosa que ocasioni molèsties o danys a altres persones dins o fora del Servei de Salut.

10.8.5. Fer un ús inadequat de qualsevol material multimèdia amb drets de la propietat intel·lectual.

10.8.6. Utilitzar l'accés a internet per a l'ús de serveis de missatgeria instantània no autoritzats pel Servei de Salut.

10.8.7. Emmagatzemar informació que contengui dades personals o confidencials del Servei de Salut en sistemes d'emmagatzematge, en dispositius o en el núvol que no disposin de la validació de seguretat de la Subdirecció de Tecnologia de la Informació.

10.8.8. Transferir fitxers no relatius a les activitats professionals de l'usuari (jocs, fitxers d'àudio, d'imatge, de vídeo...).

10.8.9. Publicar a internet informació relacionada amb el Servei de Salut, llevat que es disposi de l'autorització prèvia corresponent. En aquest sentit, els usuaris es comprometen a garantir la privacitat de les dades i de les contrasenyes d'accés i evitar difondre-les.

10.8.10. Dur a terme qualsevol activitat de promoció d'interessos personals.

10.9. Per motius de seguretat i de rendiment de la xarxa del Servei de Salut, el servei d'informàtica pot monitorar i limitar l'ús d'internet. El sistema que proporciona el servei de navegació pot disposar de filtres d'accés que bloquegin l'accés a pàgines web amb continguts inadequats, programes lúdics de descàrrega massiva, serveis de xarxes socials, servei d'emmagatzematge en el núvol, serveis de missatgeria instantània, serveis de videoconferència no autoritzats, o pàgines potencialment insegures o que contenguin virus o programes maliciosos. Igualment, el sistema pot registrar i deixar traça de les pàgines a les quals s'hagi accedit i del temps d'accés i del

volum i la mida dels fitxers descarregats. El sistema permet establir controls que possibilitin detectar i notificar usos prolongats i indeguts del servei.

11. Ús d'eines de missatgeria instantània i sistemes de videoconferència

11.1. El Servei de Salut dotarà el personal amb eines de missatgeria instantània i sistemes de videoconferències que compleixin els requeriments legals vigents.

11.2. En cap cas es poden utilitzar serveis de missatgeria instantània o sistemes de videoconferència no autoritzats pel Servei de Salut per comunicar-se.

12. Ús del correu electrònic i de l'agenda

12.1. El correu electrònic i l'agenda proporcionats pel Servei de Salut estan destinats a l'ús professional, perquè són eines de treball. Cal tenir l'autorització prèvia corresponent per a qualsevol ús particular, que ha de ser puntual i limitat en freqüència i durada. Atès que és un recurs compartit per tots els usuaris de l'organització, un ús indegut repercuteix de manera directa en el servei ofert a tots.

12.2. No es pot emprar l'adreça de correu electrònic del Servei de Salut per registrar-se en pàgines web no institucionals i amb finalitats particulars.

12.3. En cap cas l'ús autoritzat per a finalitats personals no pot constituir una activitat comercial o amb ànim de lucre ni pot ser inapropiat o ofensiu. S'aconsella evitar també les activitats que exigeixin o aconsellin una privacitat especial, ateses les obligacions del Servei de Salut pel que fa al monitoratge —segons es desprèn de l'apartat 16—, sense perjudici del respecte estricte al dret a la intimitat i al secret de les comunicacions.

12.4. El servei de correu electrònic corporatiu només s'ha d'emprar pels mitjans i les eines tecnològiques autoritzats degudament pel servei d'informàtica corresponent.

12.5. Tot usuari autoritzat per emprar el correu electrònic i l'agenda és responsable de l'ús que en faci. Cal dir que disposa d'una capacitat d'emmagatzemament limitada, per la qual cosa ha d'eliminar els missatges que no faci falta mantenir emmagatzemats.

12.6. El correu electrònic és un mitjà de comunicació interpersonal, no un mitjà de difusió massiva i indiscriminada d'informació. Cal evitar tota pràctica que pugui posar en risc el funcionament i el bon ús del sistema.

12.7. Està expressament prohibit llegir, esborrar, copiar o modificar missatges de correu electrònic o fitxers adreçats a altres usuaris, i revelar a tercers el contingut de qualsevol dada reservada o confidencial que sigui propietat del Servei de Salut o de terceres persones, llevat que aquesta actuació es faci per complir finalitats estrictament professionals, amb el consentiment previ dels afectats.

12.8. Durant les tasques professionals, en cap cas s'han d'enviar comunicacions des de comptes de correu electrònic personals oferts per proveïdors d'internet. Tampoc no és permès en cap cas redirigir a comptes particulars missatges de correu electrònic de caràcter professional rebuts en el compte proporcionat pel Servei de Salut.

12.9. Quan es reenviïn missatges electrònics que hagin estat adreçats a diversos destinataris, cal evitar difondre les adreces electròniques dels destinataris del missatge original esborrant aquesta informació del missatge reenviat, si cal.

12.10. Amb caràcter general, cal evitar enviar informació personals amb dades de salut per mitjà del correu electrònic. Si és necessari fer una tramesa d'aquest tipus, les dades han d'estar xifrades.

12.11. Abans d'obrir un missatge de correu electrònic, cal intentar detectar si es tracta d'un missatge de procedència dubtosa o desconeguda analitzant-ne la capçalera. En cas de dubte, cal esborrar els missatges sospitosos sense obrir-los o bé consultar el suport tècnic.

12.12. Per evitar el correu massiu no sol·licitat (correu brossa), com a regla general només s'ha de facilitar l'adreça electrònica a persones conegudes. Quan es rebin missatges electrònics desconeguts o no sol·licitats no s'han de contestar, perquè en fer-ho es confirma l'adreça.

12.13. Addicionalment, es consideren com a ús inadequat del servei de correu electrònic els casos següents:

12.13.1. Propagar contingut de caràcter racista, xenòfob, pornogràfic, sexual, d'apologia del terrorisme o que atempti contra els drets humans, o que actuï en perjudici

dels drets a la intimitat, l'honor i la imatge pròpia o contra la dignitat de les persones.

12.13.2. Difondre missatges de correu electrònic sense identificar plenament el remitent. Si el compte de correu és emprat per grups d'usuaris, cal identificar-ne l'autor.

12.13.3. Divulgar missatges comercials o propagandístics sense l'autorització prèvia corresponent.

12.13.4. Fer circular cartes encadenades i participar en esquemes piramidals o en activitats similars.

12.13.5. Utilitzar el servei amb l'objectiu de degradar el Servei de Salut.

12.13.6. Enviar massivament missatges o informació que consumeixin injustificadament recursos tecnològics.

12.13.7. Manipular la capçalera dels missatges per intentar falsejar o ocultar la identitat del remitent.

12.13.8. Instal·lar o emprar servidors o serveis de correu que no tenguin l'autorització prèvia corresponent.

12.13.9. El sistema que proporciona el servei de correu electrònic pot rebutjar, de manera automatitzada, blocar o eliminar part del contingut dels missatges enviats o rebuts en els quals es detecti algun problema de seguretat o d'incompliment del Codi de bones pràctiques. Es pot inserir contingut addicional en els missatges enviats per advertir els receptors sobre els requisits legals i de seguretat que han de complir amb relació a aquests missatges.

12.13.10. L'ús d'agendes telefòniques com a eina de treball està subjecte al contingut i als criteris d'ús següents, perquè contenen informació de caràcter personal:

a) Els continguts de les agendes corporatives només han d'incloure la informació següent: nom i llinatges, funció o lloc de feina, adreça postal o electrònica professional, telèfon i número de fax professionals.

b) L'ús de les agendes ha de ser exclusivament el corresponent als contactes requerits amb l'interessat i només per a les finalitats sol·licitades per aquest.

13. Comunicació d'incidències de seguretat

13.1. L'ús adequat dels recursos informàtics evita que es produeixin incidents que puguin anar en detriment de la seguretat de la informació, alhora que garanteix un rendiment òptim. Per això, quan es detectin incidents que puguin afectar la seguretat de la informació, és responsabilitat del Servei de Salut dur a terme les actuacions que es considerin convenients i proporcionals per prevenir i/o corregir els riscs identificats, per mitjà del monitoratge i l'anàlisi dels recursos afectats per assegurar que s'empren de la manera apropiada i per preservar la seguretat dels sistemes del Servei de Salut.

13.2. Tot usuari que detecti un incident que pugui tenir un impacte significatiu en la informació manejada i en els serveis prestats ho ha de comunicar immediatament al CAU, al servei d'informàtica corresponent o al Servei de Seguretat de la Informació a fi de garantir que el Servei de Salut pugui complir les obligacions en matèria de protecció de dades, seguretat de la informació i infraestructures crítiques.

13.3. Tot usuari ha d'informar immediatament el CAU, el servei d'informàtica corresponent o el Servei de Seguretat de la Informació sobre els incidents que, al seu entendre, puguin afectar la seguretat dels actius del Servei de Salut. En la notificació, l'usuari ha d'indicar tots els detalls observats que l'hagin fet sospitar i ha de prestar la col·laboració necessària per resoldre la incidència. L'obligació d'informar és imprescindible per garantir que es compleixin les obligacions en matèria de protecció de dades, seguretat de la informació, ciberseguretat i infraestructures crítiques.

13.4. Així mateix, els usuaris han de col·laborar per mantenir actualitzades les aplicacions, perquè és imprescindible que cooperin en l'adaptació dels sistemes als requisits de cada moment. Per això els usuaris han de comunicar per la via oportuna qualsevol deficiència que observin o qualsevol millora que considerin escaient.

13.5. Quan una incidència i/o deficiència pugui causar un impacte greu en el funcionament del servei sanitari, l'usuari —d'acord sempre amb el servei de suport corresponent— ha d'adoptar les mesures d'urgència

oportunes. Ha d'informar en detall sobre els fets esdevinguts i les mesures adoptades perquè es registrin i s'avaluïn amb la finalitat d'aplicar les accions necessàries.

14. Teletreball

14.1. En la modalitat de teletreball, l'usuari ha d'aplicar totes les mesures aconsellades descrites en els punts precedents i les que es descriuen en els següents.

14.2. Preferiblement cal emprar els equips de treball facilitats pel Servei de Salut, que estan equipats amb les mesures de seguretat corporatives. Si l'usuari només pot emprar el seu equip personal, s'aconsella que segueixi les pautes i recomanacions de seguretat següents a fi de protegir adequadament la informació i les comunicacions:

14.2.1. Ha de crear contrasenyes robustes i emprar el doble factor d'autenticació sempre que sigui possible.

14.2.2. Ha de mantenir actualitzats el sistema operatiu i els programes instal·lats, tant els d'ús corporatiu com els de nivell d'usuari. Si es descarrega altres programes, s'ha d'assegurar que provenen de fonts oficials i que estan autoritzats.

14.2.3. Ha de disposar d'un sistema antivirus actualitzat periòdicament.

14.2.4. Ha d'encriptar els suports d'informació a fi de protegir-ne el contingut de possibles accessos malintencionats i, d'aquesta manera, garantir-ne la confidencialitat i la integritat.

14.2.5. Ha de fer còpies de seguretat periòdicament.

14.3. En cap cas l'usuari pot fer feina amb un equip públic que no sigui el propi (p. ex. , d'un cibercafè, un hotel, un aeroport...).

14.4. Sempre que sigui possible ha d'emprar la xarxa domèstica i evitar les xarxes wifi públiques. Si no és possible emprar la xarxa domèstica o, com a alternativa, qualsevol altra xarxa que es consideri segura, es recomana que empri la xarxa de dades mòbils pròpia.

14.5. Ha d'accedir a la xarxa interna i als sistemes d'informació del Servei de Salut emprant exclusivament els mecanismes corporatius habilitats, com ara les xarxes privades virtuals (VPN) o els serveis d'accés remot segur (Citrix, per exemple).

14.6. Si ha de participar en reunions virtuals o fer videotelefonades, és aconsellable que empri exclusivament les eines corporatives habilitades per a aquest efecte.

14.7. Durant l'activitat professional fora de les instal·lacions del Servei de Salut l'usuari ha de seguir les normes, els procediments i les recomanacions internes vigents.

14.8. El Servei de Salut pot en qualsevol moment limitar l'accés a les seves xarxes i als seus serveis publicats a internet als equips dels usuaris que no compleixin els requisits mínims de seguretat establerts.

15. Acabament de la vinculació o relació amb el Servei de Salut

15.1. Quan un usuari acaba la relació o vinculació amb el Servei de Salut deixa de tenir accés als sistemes d'informació del Servei de Salut i a les dades que contenen. Així mateix, ha de tornar qualsevol suport que tengui i que contengui dades a les quals hagi tingut accés en el marc de la vinculació o relació amb el Servei de Salut.

15.2. També ha de cedir el control sobre qualsevol fitxer o document relatiu a la prestació professional; en cas que hagi creat fitxers o documents de caràcter no professional, els ha d'eliminar.

16. Monitoratge i aplicació del Codi

16.1. Per motius legals, de seguretat i de qualitat del servei, i a fi de complir en tot moment els requisits que estableix la legislació vigent, el Servei de Salut ha de dur a terme les accions següents:

16.1.1. Revisar periòdicament l'estat dels equips, els programes instal·lats, els dispositius i les xarxes de comunicacions que siguin responsabilitat seva.

16.1.2. Monitorar els accessos a la informació que contenguin els seus sistemes.

16.1.3. Auditar la seguretat de les credencials i dels programes.

16.1.4. Monitorar els serveis d'internet i de correu electrònic i altres eines de col·laboració.

16.2. El Servei de Salut ha de dur a terme aquesta activitat de monitoratge sense utilitzar sistemes o programes que puguin atemptar contra els drets constitucionals dels usuaris excepte en els supòsits en què sigui estrictament necessari amb motiu d'un requeriment legal o una sol·licitud de col·laboració d'investigació.

16.3. Els sistemes en els quals es detecti un ús inadequat o que no compleixin els requisits mínims de seguretat poden ser blocats o suspesos temporalment. El servei es restablirà quan la causa de la inseguretat o de la degradació hagi desaparegut. La Subdirecció de Tecnologia de la Informació —amb la col·laboració de les altres unitats del Servei de Salut— vetlarà perquè es compleixi el Codi de bones pràctiques i informarà sobre els incompliments o les deficiències de seguretat observats, a fi que es prenguin les mesures oportunes.

17. Compliment del Codi

17.1. Tots els usuaris del Servei de Salut han de complir el Codi de bones pràctiques.

17.2. Addicionalment, els requisits i les previsions descrits en el Codi es complementen amb la resta de la normativa vigent i amb qualsevol disposició legal d'àmbit estatal o comunitari aplicable.

17.3. L'incompliment de qualsevol de les pautes de comportament establides en el Codi pot donar lloc a la responsabilitat disciplinària corresponent per tal d'aplicar les normes reguladores del règim jurídic propi de l'usuari.

17.4. L'ús dels recursos informàtics que el Servei de Salut posa a disposició dels usuaris implica el coneixement i l'acceptació plena de les normes d'ús, de les condicions i de les advertències legals que s'especifiquen en el Codi.

17.5. La Subdirecció de Tecnologia de la Informació ha de vetlar per què es compleixi el Codi de bones pràctiques.

18. Difusió i publicació

18.1. Aquesta instrucció s'ha de publicar a la seu electrònica del Servei de Salut de les Illes Balears i als altres mitjans que aquest òrgan de direcció consideri oportuns.

18.2. El Servei de Seguretat de la Informació és l'encarregat de difondre aquesta instrucció.

19. Vigència

Aquesta instrucció entra en vigor a partir de la publicació a la seu electrònica del Servei de Salut i deixa sense efecte la Circular del director general del Servei de Salut de les Illes Balears 1/2014, de 3 de març, per la qual s'aprova el Codi de bones pràctiques en l'ús dels sistemes d'informació i el tractament de les dades personals del Servei de Salut de les Illes Balears.

El director general del Servei de Salut

Julio Miguel Fuster Culebras

C/ de la Reina Esclarmunda, 9
07003 Palma
Tel. 971 17 56 00
ibsalut.es