# Codi de bones pràctiques

## Versió reduïda


GOIB
CONSELLERIA
SALUT I CONSUM
SERVEI SALUT
ILLES BALEARS

## Justificació

### Per què és necessari el Codi de bones pràctiques?

- ✓ Els sistemes d'informació són bàsics per assolir els objectius de l'organització; per això els usuaris els han d'emprar preservant la seguretat.
- ✓ L'ús de sistemes d'informació per tractar la informació té una finalitat doble:
  - Facilitar i agilitar l'assistència sanitària i tramitar els procediments administratius.
  - Proporcionar informació completa, homogènia, actualitzada i fiable.
- ✓ L'ús d'equipament informàtic i de comunicacions és una necessitat, i per això es posa a la disposició dels usuaris com a instrument de treball. És competència del Servei de Salut determinar les normes, les condicions i les responsabilitats per emprar-lo.
- ✓ També és un instrument per complir la legislació vigent en matèria de protecció de dades, de seguretat de la informació i sobre drets i deures dels ciutadans.

### Què és un usuari?

Tot empleat públic que presti servei en el Servei de Salut i el personal d'empreses externes que acompleixi tasques de manera permanent o ocasional en qualsevol òrgan pertanyent o adscrit al Servei de Salut.

### Què és un sistema d'informació?

És un conjunt de dades que interactuen entre si amb una finalitat comuna.

## Objecte i abast

### Quin és l'objecte del Codi de bones pràctiques?

L'objectiu és establir les directrius i les recomanacions que han de tenir en compte tots els professionals que facin feina per al Servei de Salut sobre l'ús dels sistemes d'informació, a fi d'optimitzar els 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.

### A qui s'ha d'aplicar el Codi de bones pràctiques?

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 o a les dades que figurin sota la seva titularitat han de saber i aplicar els requisits i les instruccions d'aquest Codi.

### Sobre quins recursos s'ha d'aplicar el Codi de bones pràctiques?

És aplicable a tots els recursos —equipament físic, equipament lògic, serveis i informació— emprats pels usuaris per acomplir les funcions pròpies.

### Quan cal garantir la seguretat de la informació? I la dels sistemes que permeten el tractament de la informació?

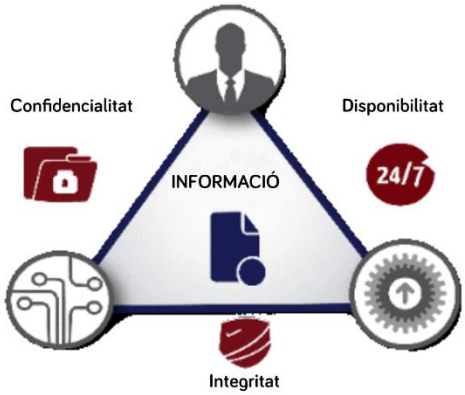
Cal garantir la seguretat de la informació al llarg de totes les fases del seu cicle de vida (generació, distribució, emmagatzematge, processament, transport, consulta i destrucció) i la dels sistemes en què es basa (anàlisi, disseny, desenvolupament, implantació, explotació, integració i manteniment).

### Què és la disponibilitat?

És la propietat o característica que consisteix a tenir accés a les dades o processos quan es requereixin.

### Què és la integritat?

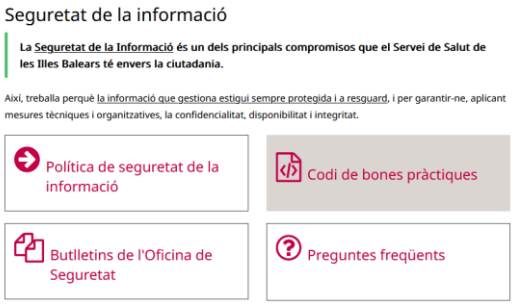
És la propietat o característica que consisteix en el fet que la informació no ha estat alterada de manera no autoritzada.




## Informació als usuaris

### On es pot trobar el Codi de bones pràctiques?

- ✓ És a la disposició de tots els usuaris en el web del Servei de Salut.
- ✓ Cal adjuntar-lo als manuals de benvinguda de les gerències territorials, a fi que els treballadors que s'hi incorporin el consultin abans d'emprar els recursos del Servei de Salut.




### Qui s'ha d'encarregar de difondre aquesta norma?

Els òrgans de direcció i de gestió del Servei de Salut —estructurats en Serveis Centrals i en gerències territorials— són els responsables de difondre aquesta norma a les empreses externes, a fi que els seus usuaris la coneguin i la compleixin, i també el Servei de Seguretat de la Informació.

### Què passar si no es compleix el Codi de bones pràctiques?

L'incompliment de qualsevol de les pautes de comportament establertes en el Codi pot donar lloc a la responsabilitat disciplinària corresponent, tot aplicant les normes reguladores del règim jurídic propi de l'usuari.

### Què passar si es detecta un ús inadequat dels sistemes o no es compleixen els requisits mínims de seguretat?

- ✓ Els sistemes poden ser bloquejats o suspesos temporalment.
- ✓ El servei es restablirà quan la causa de la inseguretat o de la degradació hagi desaparegut.

## Confidencialitat de la informació

### A què es refereix la confidencialitat?

És la propietat o característica que consisteix a no posar informació a la disposició de persones, entitats o processos no autoritzats ni revelar-los-la.


### Amb qui es pot compartir la informació a la qual hom té accés per raons de la feina?

- ✗ **Només amb el personal que tengui l'autorització deguda i explícita**. Com a mesura de protecció de la informació pròpia, confiada o tractada pel Servei de Salut, els usuaris s'han d'abstenir de comunicar-la, divulgar-la, distribuir-la o posar-la a l'abast d'altres persones (externes o internes no autoritzades) per mitjà de suports informàtics o per qualsevol altre mitjà que no s'hagi autoritzat prèviament.

### Quan acaba el compromís de confidencialitat amb el Servei de Salut?

- ✗ **Mai.** Tot el personal del Servei de Salut i el personal aliè que, per raó de l'activitat professional que desenvolupi, hagi tingut accés a informació gestionada pel Servei de Salut (dades personals, documents, metodologies, claus, anàlisis, programes, etc.) ha de mantenir una absoluta reserva durant temps indefinit, fins i tot després que hagi acabat la relació que tenia amb el Servei de Salut.

### A quina informació es pot accedir?

- ✓ Els usuaris només poden accedir a la informació per a la qual tenguin l'autorització deguda i explícita depenent de les funcions que acompleixin.
- ✓ 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.
- ✗ En cap cas poden tenir accés a informació que pertanyi a altres usuaris o grups d'usuaris per a la qual no tenguin autorització.

### En què consisteixen els principis de *mínim privilegi possible* i de *necessitat de conèixer*?

En virtut d'aquests principis, els usuaris només poden accedir a la informació i als sistemes d'informació per als quals tenguin l'autorització deguda i explícita depenent de les funcions que acompleixin.

### Què ha de fer un usuari quan acaba la relació que tenia amb el Servei de Salut?

- ✓ Deixa de tenir accés als sistemes d'informació del Servei de Salut i a les dades que contenen. Per això ha de tornar qualsevol suport que contengui dades a les quals hagi tingut accés durant la relació amb el Servei de Salut.
- ✓ També ha de cedir el control sobre qualsevol fitxer o document relatiu a la prestació professional. Si ha creat fitxers o documents de caràcter no professional, els ha d'eliminar.

## Protecció de dades de caràcter personal

### Què és una dada de caràcter personal?

És 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: nom, número d'identificació, dades de localització, identificador en línia o un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social.

### Què són les dades personals relatives a la salut?

Són dades personals relatives a la salut física o mental—inclosa la prestació de serveis d'atenció sanitària— que revelin informació sobre l'estat de salut.

### Què és el tractament de les dades?

És qualsevol operació o conjunt d'operacions sobre dades personals o conjunts de dades personals, per procediments automatitzats o no: recollida, registre, organització, estructuració, conservació, adaptació o modificació, extracció, consulta, utilització, comunicació per transmissió, difusió o qualsevol altra manera d'habilitació d'accés, acarament o interconnexió, limitació, supressió o destrucció.

### Quines mesures de seguretat cal tenir en compte per emprar els sistemes d'informació i en el tractament de dades de caràcter personal?

Com a regla general, els professionals han de seguir les pautes següents:

- ✓ Servar estrictament el secret professional per temps indefinit, fins i tot després d'haver acabat la relació amb el Servei de Salut.
- ✓ Saber els principis del Reglament general d protecció de dades (Reglament (UE) 2016/679) i la Llei orgànica 3/2018, de 5 de

desembre, de protecció de dades de caràcter personal i garantia dels drets digitals.

- ✗ Garantir en qualsevol cas la confidencialitat de les dades a les quals tenguin accés (no enviar o compartir dades sense tenir garanties sobre la identitat del destinatari). No accedir a les dades per mitjans diferents als proporcionats pel Servei de Salut.

**Quines mesures de seguretat cal aplicar per tractar la documentació impresa que contengui dades de caràcter personal?**

- ✗ S'ha d'evitar imprimir en paper documentació que contengui dades personals, si no és necessari.
- ✗ S'ha d'evitar que la documentació confidencial impresa quedi a l'abast de persones no autoritzades (a impressores o fotocopiadores, al lloc de treball, etc.).
- ✓ Els documents s'han de desar dins calaixos o armaris tancats amb pany quan s'estigui absent del lloc de treball.
- ✓ Cal destruir de manera segura (en contenidors reciclatge segellats o amb màquines destructores de paper) els documents confidencials quan s'hagi complert la finalitat per a la qual es van generar.

**Quines mesures de seguretat cal aplicar si és necessari generar fitxers temporals?**

- ✗ S'ha d'evitar generar fitxers temporals, però si és estrictament necessari cal eliminar-los convenientment quan s'hagi complert la finalitat per a la qual es van generar.
- ✓ S'han d'allotjar dins les carpetes assignades per l'organització a fi de garantir els controls tècnics establerts.

**Quins són les diferències entre *interessat*, *responsable* del tractament i *encarregat del tractament*?**

L'*interessat* (pacient) és la persona física titular de les dades la identitat de la qual es pugui determinar, directament o indirectament, en particular per mitjà d'un identificador (nom, document d'identitat, dades de localització, identificador, etc.). El *responsable* del tractament és la persona física o jurídica, l'autoritat pública, el servei o un altre organisme que, tot sol o amb d'altres, determini les finalitats i els mitjans del tractament. L'*encarregat del tractament* és la persona física o jurídica, l'autoritat pública, el servei o un altre organisme que tracti dades personals per compte del responsable del tractament.

**Què és la figura de *delegat de protecció de dades* i quines funcions té?**

És la persona física o jurídica o l'òrgan designat pel Servei de Salut perquè s'encarregui de garantir que en l'organització es compleixin les directrius del Reglament general de protecció de dades.

**Què és una dada anonimitzada?**

És una dada que no permet identificar l'interessat.

**Què és la pseudonimització?**

És el tractament de dades personals de manera que ja no es puguin atribuir a un interessat sense utilitzar informació addicional, sempre que aquesta 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.

## Ús dels recursos informàtics

**Es poden utilitzar els recursos informàtics per a ús personal?**

- ✗ **Com a norma general, no.** Només s'han d'utilitzar per a les tasques pròpies dels usuaris d'acord amb les funcions assignades.

**Qui és el propietari dels recursos informàtics?**

Són propietat del Servei de Salut, de manera que li correspon determinar les condicions i les responsabilitats per protegir-los i emprar-los.

**Quines són les responsabilitats dels usuaris?**

Els usuaris són responsables de custodiar els recursos i de protegir-los de les possibles amenaces (accessos no autoritzats, ús indegut, errors o omissions, robatori, etc.).

**Quines són les pràctiques que cal evitar per no comprometre les mesures de seguretat establertes pel Servei de Salut?**

- ✗ No s'han d'emprar programes ni equips informàtics que no siguin els estàndards del Servei de Salut.
- ✗ No s'ha de modificar la configuració establerta.
- ✗ No s'han de treure equips dels locals, excepte quan estigui autoritzat prèviament.

- ✗ No s'han de fer connexions a xarxes o sistemes externs per altres mitjans que no siguin els definits i administrats pel personal competent.
- ✗ No s'han d'extreure o utilitzar informació confidencial ni dades de caràcter personal en entorns que no estiguin protegits o configurats adequadament.
- ✗ No s'han de traslladar fora de les installacions habituals de treball dades o informacions —impresos o en qualsevol altre suport, inclosos els digitals— sense l'autorització prèvia corresponent.
- ✗ No s'han de destruir, alterar o inutilitzar els recursos informàtics, els programes, les dades, els suports ni els documents.
- ✗ No s'ha d'intentar desxifrar les claus.
- ✗ No s'han de modificar o desactivar els mecanismes de seguretat implantats.
- ✗ No s'han de deixar els recursos de tractament d'informació desatesos sense les mesures de blocatge adequades o mantenir suports amb informació sensible a llocs poc segurs.
- ✗ No s'ha d'accedir a la informació que no sigui necessària per acomplir les funcions pròpies.

**Es poden descarregar música, pellícules i jocs als equips del Servei de Salut?**

No. Les unitats ofimàtiques no s'han d'utilitzar per a finalitats privades, perquè són una eina de treball amb capacitat limitada i, a més, es podria vulnerar la normativa en matèria de protecció de la propietat intellectual.

**Quin tipus d'informació es pot emmagatzemar a les unitats ofimàtiques?**

Està prohibit expressament emmagatzemar-hi informació amb 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, a l'honor i a la imatge pròpia o contra la dignitat de les persones.

**Es poden installar programes a l'equip?**

No, excepte amb l'autorització expressa del responsable del servei i del servei d'informàtica.

**Quines mesures de seguretat han de complir els dispositius 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 installació de sistemes de protecció contra programes maliciosos i en actualitzacions i sistemes de protecció d'installació de programes maliciosos.
- ✓ Han d'estar protegits amb contrasenya i blocatge automàtic per inactivitat.
- ✓ Han de tenir mecanismes d'encriptació per impedir que les persones no autoritzades accedeixin a la informació que emmagatzemen.

- ✗ En cap cas està permès instal·lar aplicacions no autoritzades pel Servei de Salut o que puguin comprometre el funcionament dels dispositius mòbils.
- ✓ 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 que contenguin.

### Com cal actuar en un incident de la seguretat amb un dispositiu mòbil?

- ✓ Si es perd un dispositiu mòbil, l'usuari ho ha de comunicar immediatament al Centre d'Atenció a Usuaris (CAU) o al servei d'informàtica corresponent perquè el bloqui i n'esborri el contingut.

### Es poden utilitzar dispositius personals per a la feina?

- ✓ Els dispositius personals emprats en l'àmbit del Servei de Salut que accedeixin a les xarxes i aplicacions corporatives poden ser sotmesos pel Servei de Salut a accions de prevenció i control, però es limitaran a les àrees, les aplicacions i els contenidors d'informació corporativa d'aquests dispositius personals.
- ✗ Si és necessari que un dispositiu personal es connecti a les xarxes i aplicacions corporatives, el nivell de seguretat del dispositiu ha de ser el mateix que el dels corporatius.
- ✗ 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.

### En què consisteix l'emmagatzematge en el nigul?

Consisteix en la disposició d'aplicacions, plataformes o infraestructures que, a càrrec d'un proveïdor o del mateix Servei de Salut, estan accessibles per mitjà d'internet, independentment d'on estiguin allotjats els sistemes d'informació, i de manera transparent per a l'usuari.

### Es pot emmagatzemar tot tipus d'informació en el nigul?

- ✗ 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'emmagatzematge en el nigul diferents de les corporatives, llevat que es disposi de l'autorització prèvia corresponent.
- ✓ Cal comprovar que no hi hagi traves legals per i verificar que s'hagi subscrit 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, l'acord de confidencialitat corresponent, i sempre havent analitzat els riscs associats.
- ✓ Abans d'emprar 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 el que es considera qualitat mínima del servei prestat i les conseqüències d'incomplir-lo.

### Què és un programa maliciós (*malware*)?

És un tipus de programari que té com a objectiu infiltrar-se en un equip informàtic o sistema d'informació sense el consentiment del seu propietari.

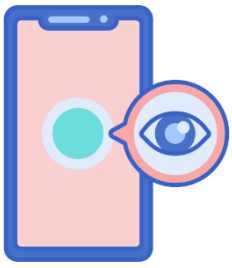
**Quines mesures es poden prendre per evitar els programes maliciosos?**

- ✓ Si se sospita que un equip ha estat infectat per un programa maliciós, cal comunicar la incidència seguint el procediment corresponent.
- ✓ Cal adoptar totes les precaucions possibles en executar qualsevol programa, fins i tot encara que procedeixi d'una font considerada de confiança, atès que pot haver estat suplantat per un programa maliciós.
- ✓ S'ha d'evitar executar fitxers adjunts rebuts per correu electrònic i visitar pàgines web amb continguts de legalitat o moralitat dubtoses, perquè habitualment són una font d'infeccions.

## Mesures de seguretat

**Quines són les mesures de seguretat principals d'accés físic?**

- ✓ Els monitors d'ordinador—especialment els que siguin a zones amb accés del públic—s'han d'orientar de tal manera que s'elimini tant com sigui possible l'angle de visió a les persones no autoritzades.



- ✓ Cal custodiar la informació confidencial o amb dades personals que figuri en qualsevol suport digital o que sigui visible directament en el monitor de l'ordinador, a fi d'evitar que s'hi accedeixi sense autorització.
- ✗ **No s'ha de mantenir informació a la vista** sense el control del responsable en aquell moment. Si està absent, cal establir els mecanismes oportuns segons les característiques del lloc de treball i del suport en el qual estigui la informació per impedir que persones no autoritzades hi puguin accedir.

**Quines són les principals mesures de seguretat d'accés lògic?**

- ✓ **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 se'n faci.

- ✗ **Cada usuari ha de vetlar per la confidencialitat de la seva contrasenya;** en cap cas l'ha de desar en fitxers digitals ni l'ha d'escriure en paper o en qualsevol altre suport que sigui llegible o accessible. Tampoc pot comunicar a una altra persona el seu identificador d'usuari ni la contrasenya.
- ✗ En cap circumstància es pot utilitzar una sessió oberta amb una altra identitat.
- ✓ Si un usuari sospita que la seva contrasenya ha estat coneguda de manera fortuïta o fraudulenta per una persona no autoritzada, l'ha de modificar i ha de notificar immediatament la incidència al CAU o al servei d'informàtica corresponent.

- ✗ A l'hora de crear una contrasenya cal procurar que altres persones no la puguin endevinar fàcilment.

- ✗ Tot usuari ha de canviar la contrasenya d'accés als sistemes cada 45 dies i sempre que ho indiqui l'encarregat de la gestió dels usuaris.
- ✗ Mai s'ha de facilitar el nom d'usuari ni la contrasenya si es demanen per telèfon o correu electrònic. A més, s'ha de comunicar immediatament la incidència al CAU o al servei d'informàtica corresponent.
- ✓ Quan un usuari acabi la relació o vinculació amb el Servei de Salut, el seu responsable directe ha de comunicar la nova situació a l'encarregat de la gestió dels usuaris perquè doni de baixa els comptes i les autoritzacions que tengui.

### Es poden utilitzar altres mecanismes d'identificació i autenticació?

- ✓ Sí, a més del sistema basat en l'ús d'identificadors d'usuari i contrasenya es poden utilitzar algorismes criptogràfics i certificats digitals, amb els quals s'estableixen garanties equivalents respecte de l'autenticació de la identitat, la confidencialitat, la integritat i el no rebuig de la informació tractada.
- ✓ Es requereix que l'usuari empri un certificat electrònic, l'autenticitat i la integritat del qual estan garantides per un tercer de confiança.


## El lloc de treball

### Com s'ha de mantenir el lloc de treball?

Amb caràcter general, el lloc de treball s'ha de mantenir adesat, sense cap més material damunt la taula que el que calgui per desenvolupar l'activitat de cada moment.

### Què cal fer quan s'abandona el lloc de treball?

- ✓ Cal desar tota la informació que s'estigui tractant, de manera que no quedin desatesos memòries USB o suports externs d'informació, llistes o informació visible en el monitor de l'ordinador o documentació damunt la taula. Aquest material s'ha de desar dins un calaix o un armari tancat amb pany o en una estança separada, igualment tancada, almenys fora de l'horari de feina.
- ✓ Es pot establir un procediment per revisar que es compleix aquesta mesura fent regularment una inspecció després del tancament, notificant els incompliments detectats i retirant el material oblidat dins un lloc tancat.
- ✓ És imprescindible blocar els terminals i els dispositius mòbils amb accés a la informació quan no s'hi estigui treballant, tant momentàniament com al final de la jornada laboral.

## Accés per mitjà de xarxes externes

### Quan i com està permès connectar-se a les xarxes corporatives des de l'exterior?

- ✓ En accedir a les xarxes corporatives des de l'exterior del Servei de Salut, els usuaris han de complir les normes de seguretat establertes.
- ✓ Cal accedir-hi exclusivament pels mitjans implantats corporativament, de manera que no és permès utilitzar qualsevol altre mitjà sense l'autorització prèvia.

### Cal autorització per habilitar connexions remotes?

- ✓ Per emprar les xarxes corporatives cal tenir les credencials d'accés (generalment un identificador, una contrasenya i, si de cas, un segon factor d'autenticació), que s'assignen només als usuaris autoritzats.
- ✓ 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 del responsable corresponent i la validació de la Subdirecció de Tecnologia de la Informació a fi de garantir els nivells de seguretat requerits.

## Ús d'internet

### Quan és permès connectar-se a internet?

- ✓ Internet ha de ser accessible exclusivament als usuaris que ho necessitin per acomplir les funcions assignades.
- ✓ En l'ús d'internet, tot usuari ha de ser conscient que en acomplir les 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 treballadors adscrits al Servei de Salut.

### Es poden enviar dades personals per internet?

- ✗ **No, s'hauria d'evitar.** En qualsevol cas, només es poden enviar emprant els mecanismes que garanteixin la ininteligibilitat i la integritat de les dades, i amb l'autorització prèvia corresponent.

### Com es pot assegurar la confidencialitat de la informació que es transmetrà per internet?

Cal comprovar en la barra d'adreces que s'està utilitzant el protocol HTTPS (protocol segur de transferència d'hipertext) en lloc del protocol estàndard HTTP. En aquesta barra 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.


### A qui s'han de notificar les anomalies detectades en l'accés a internet?

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

### Quines accions es consideren com a ús incorrecte d'internet?

- ✗ L'accés a llocs d'internet i la distribució de missatges amb continguts en què s'inciti o es promogui la pornografia i la segregació racial, sexual o religiosa, o amb continguts de violència.
- ✗ La descàrrega i la transmissió indiscriminada d'imatges o de fitxers d'àudio o vídeo.
- ✗ La distribució de virus o troians i qualsevol activitat encaminada a accedir il·lícitament a altres sistemes d'informació.
- ✗ 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.
- ✗ Fer un ús inadequat de qualsevol material multimèdia amb drets de la propietat intel·lectual.
- ✗ Utilitzar l'accés a internet per emprar serveis de missatgeria instantània no autoritzats pel Servei de Salut.
- ✗ Emmagatzemar informació que contengui dades personals o confidencials del Servei de Salut en sistemes d'emmagatzematge, en dispositius o en el nigul que no disposin de la validació de seguretat de la Subdirecció de Tecnologia de la Informació.
- ✗ Transferir fitxers no relatius a les activitats professionals de l'usuari (jocs, fitxers d'àudio, d'imatge, de vídeo, etc.).
- ✗ La publicació a internet d'informació relacionada amb el Servei de Salut, llevat que es disposi de l'autorització prèvia corresponent.
- ✗ Dur a terme qualsevol activitat de promoció d'interessos personals.

### Es pot limitar l'ús d'internet?

- ✓ El sistema que proporciona el servei de navegació pot disposar de filtres que bloquin l'accés a pàgines web amb continguts inadequats, programes lúdics de descàrrega massiva, serveis de xarxes socials, servei d'emmagatzematge en el nigul, serveis de missatgeria instantània, serveis de videoconferència no autoritzats i pàgines potencialment insegures o que continguin virus o programes maliciosos.

- ✓ 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.

**Què és la traçabilitat?**

És la propietat o característica que consisteix en el fet que les actuacions d'una entitat es poden imputar exclusivament a aquesta.

## Eines de missatgeria instantània i sistemes de videoconferència

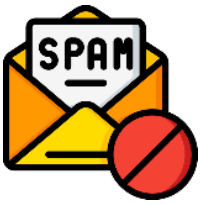
**Es poden emprar eines de missatgeria instantània i sistemes de videoconferència?**

Sí. El Servei de Salut dotarà el personal d'eines de missatgeria instantània i sistemes de videoconferències que compleixin els requeriments legals vigents, però només els autoritzats pel Servei de Salut.

## Correu electrònic i agendes corporatives

**Què és el correu brossa?**

És tot missatge de correu electrònic no volgut que s'envia aleatòriament en processos per lots, al qual estan exposats la majoria dels usuaris.




**Què s'entén per *correu electrònic professional*?**

El correu electrònic és una eina que proporciona el Servei de Salut destinat a l'ús professional; per tant, és una eina de treball que necessita una autorització prèvia per a qualsevol ús particular, atès que és un recurs compartit per tots els usuaris de l'organització, de manera que l'ús indegut repercuteix directament en el servei ofert a tots.

**Quines accions es consideren com un ús inadequat del correu electrònic?**

- ✗ Utilitzar l'adreça de correu per registrar-se en pàgines web no institucionals i amb finalitats particulars.
- ✗ Utilitzar el correu per a activitats comercials particulars o amb ànim de lucre.
- ✗ Utilitzar el correu per difondre missatges inadequats o ofensius.
- ✗ És un mitjà de comunicació interpersonal, no un mitjà de difusió massiva i indiscriminada d'informació. Per això cal evitar tota pràctica que pugui posar en risc el funcionament i el bon ús del sistema.
- ✗ 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.
- ✗ 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.
- ✗ Divulgar missatges comercials o propagandístics sense l'autorització prèvia corresponent.
- ✗ Fer circular cartes encadenades i participar en esquemes piramidals o en activitats similars.
- ✗ Utilitzar el servei amb l'objectiu de degradar el Servei de Salut.
- ✗ Enviar massivament missatges o informació que consumeixin injustificadament recursos tecnològics.
- ✗ Installar o emprar servidors o serveis de correu que no tenguin l'autorització prèvia corresponent.

**Es poden enviar dades de caràcter personal per correu electrònic?**

Amb caràcter general, cal evitar enviar per correu electrònic informació de caràcter personal amb dades de salut. Si és necessari enviar-la, les dades han d'estar encriptades.

**Es pot accedir als missatges adreçats a altres usuaris?**

- ✗ **Està expressament prohibit** llegir, esborrar, copiar o modificar missatges de correu electrònic o fitxers adreçats a altres usuaris, i revelar a altres persones el contingut de qualsevol dada reservada o confidencial que sigui propietat del Servei de Salut o de tercers, llevat que calgui complir finalitats estrictament professionals, amb el consentiment previ de les persones afectades.

**Quines precaucions cal tenir per emprar correctament el correu electrònic?**

- ✓ Només s'ha d'emprar pels mitjans i les eines tecnològiques autoritzats degudament pel servei d'informàtica corresponent.
- ✓ Eliminar els missatges que no sigui necessari mantenir emmagatzemats, perquè la capacitat d'emmagatzematge és limitada.
- ✓ Quan es reenviïn missatges de correu electrònic que hagin estat adreçats a diversos destinataris, convé no difondre les adreces dels destinataris del missatge original esborrant aquesta informació abans de reenviar-lo, llevat que calgui conservar-les.
- ✓ Abans d'obrir un missatge de correu electrònic, s'ha d'intentar esbrinar si es tracta d'un missatge de procedència dubtosa o desconeguda. En cas de dubte, cal esborrar-lo sense obrir-lo o consultar el CAU o el servei d'informàtica corresponent.
- ✓ 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 de correu electrònic desconeguts o no sol·licitats no s'han de contestar, perquè en fer-ho es confirma l'adreça.
- ✗ Durant les tasques professionals, en cap cas s'han d'enviar missatges des de comptes de correu electrònic personals.
- ✗ Tampoc és permès en cap cas redirigir a comptes particulars missatges de correu electrònic de caràcter professional rebuts en el compte corporatiu del Servei de Salut.

**El sistema de correu electrònic pots de manera automatitzada rebutjar, blocar o eliminar part del contingut dels missatges enviats o rebuts?**

- ✓ **Sí,** en els casos en què s'hi detecti algun problema de seguretat o d'incompliment del Codi de bones pràctiques.
- ✓ Addicionalment 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.

**Com s'ha d'emprar la informació de les agendes corporatives?**

- ✓ L'ús de les agendes ha de ser exclusivament el corresponent als contactes requerits amb l'interessat i únicament per a les finalitats sol·licitades per aquest.
- ✗ En cap cas s'han d'utilitzar les adreces incloses en l'agenda corporativa amb finalitats particulars.

**Es pot emprar qualsevol navegador o programa de correu electrònic?**

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

### Es pot emprar el navegador o el correu electrònic per a ús personal?

✗ **No.** Atesa la necessitat d'optimitzar els recursos, 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.

## Incidències de seguretat

### Què és una incidència?

És qualsevol anomalia que afecti o pugui afectar la seguretat de les dades.

### A qui s'han de notificar les incidències de seguretat?

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, a parer seu, 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 important per garantir que es compleixin les directrius en matèria de protecció de dades, seguretat de la informació, ciberseguretat i infraestructures crítiques.

### Què és el CAU?

És el servei que dona suport informàtic i gestiona les incidències dels usuaris amb relació a les aplicacions i les infraestructures informàtiques.

### Què és un actiu?

És un component o una funcionalitat d'un sistema d'informació susceptible de ser atacat de manera deliberada o accidental amb conseqüències per a l'organització. Inclou informació, dades, serveis, aplicacions (programari), equips (maquinari), comunicacions, recursos administratius, recursos físics i recursos humans.

### Què cal fer si es detecta una deficiència en una aplicació?

Atesa la naturalesa dinàmica i canviant dels requisits que han de satisfer, els usuaris han de col·laborar per mantenir actualitzades les aplicacions; per tant, és imprescindible que cooperin en l'adaptació dels sistemes als requisits de cada moment. Per això han de comunicar per la via oportuna qualsevol deficiència que observin o qualsevol millora que considerin adequada.

## Teletreball

### Què s'entén per *teletreball*?

És la feina que es du a terme des d'un lloc fora de l'empresa emprant les xarxes de telecomunicació.

### Quines mesures cal aplicar en la modalitat de teletreball?

✓ L'usuari ha d'aplicar totes les mesures aconsellades en el Codi de bones pràctiques, com si s'estigués fent feina des de les instal·lacions corporatives.

✓ Durant el teletreball, tot usuari ha de seguir les normes, els procediments i les recomanacions internes vigents.

**Es pot utilitzar un equip personal per al teletreball?**

Preferiblement s'han d'emprar equips facilitats pel Servei de Salut. Però si només es pot utilitzar un equip personal, cal complir aquestes mesures de seguretat:

- ✓ Cal crear contrasenyes robustes i emprar el doble factor d'autenticació sempre que sigui possible.
- ✓ Han d'estar actualitzats el sistema operatiu i els programes instal·lats, tant els d'ús corporatiu com els de nivell d'usuari.
- ✓ Si es descarreguen altres programes, cal assegurar-se que provenen de fonts oficials i que estan autoritzats.
- ✓ Cal disposar d'un sistema antivirus actualitzat periòdicament.
- ✓ Cal encriptar els suports d'informació a fi de protegir-ne el contingut d'accessos malintencionats.
- ✓ Cal fer còpies de seguretat periòdicament.

**Es pot utilitzar un equip públic per al teletreball?**

- ✗ **No.** En cap cas es pot utilitzar un equip públic que no sigui el propi (p. ex., d'un cibercafè, un hotel, un aeroport, etc.).

**A quines xarxes és possible connectar-se per al teletreball?**

- ✗ Cal evitar les xarxes wi-fi públiques.
- ✓ Sempre que sigui possible s'ha d'emprar la xarxa domèstica.
- ✓ Si no és possible emprar la xarxa domèstica o, com a alternativa, qualsevol altra xarxa que es consideri segura, es recomana utilitzar la xarxa de dades mòbils pròpia.

**Com s'ha de connectar amb la xarxa corporativa i altres parts del Servei de Salut?**

- ✓ Per accedir a la xarxa interna i als sistemes d'informació del Servei de Salut cal emprar els mecanismes corporatius habilitats, com ara les xarxes privades virtuals (VPN) o els serveis d'accés remot segur (Citrix, per exemple).
- ✓ Per participar en reunions virtuals o fer videotelefonades, és aconsellable emprar exclusivament les eines corporatives habilitades per a aquesta necessitat.

**El Servei de Salut pot restringir l'accés a les seves xarxes i als serveis publicats a internet?**

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