OTIC Seguretat

Govern de les Illes Balears
Servei de Salut

versió reduïda

Codi de bones pràctiques

OFICINA DE SEGURETAT

Servei de Salut de les Illes Balears
Oficina de Tecnologies de la Informació i Comunicació

Codi de bones pràctiques

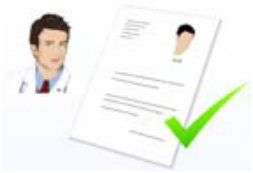
OBJECTE I ABAST

Quin és l'objecte del Codi de bones pràctiques?

- ✓ L'objecte del Codi de bones pràctiques és definir els requisits i les instruccions que han de tenir en compte tots els professionals que treballin per al Servei de Salut pel que fa a l'ús dels recursos informàtics i al tractament de dades de caràcter personal, a fi de mantenir-ne **la seguretat, la confidencialitat, la disponibilitat i la integritat**.

Qui ha d'aplicar el Codi de bones pràctiques?

- ✓ Tot el personal que tengui accés als sistemes d'informació del Servei de Salut està obligat a conèixer i aplicar els requisits establits en el Codi de bones pràctiques.



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

- ✓ Els requisits establits pel Codi de bones pràctiques es refereixen a l'ús de tots els recursos (sistemes d'informació, ordinadors personals, mitjans de transmissió, etc.).

Quan s'ha de garantir la seguretat de la informació? I la dels sistemes que permeten el tractament de la informació?

- ✓ S'ha de garantir durant la generació, la distribució, l'emmagatzemament, el processament, el transport, la consulta i la destrucció, a més de la dels sistemes que la permeten (anàlisi, disseny, desenvolupament, implantació, explotació, integració i manteniment).

On es pot trobar més informació sobre el Codi de bones pràctiques?

- ✓ La versió íntegra del Codi de bones pràctiques està publicada en el web del Servei de Salut de les Illes Balears (clicau en aquest enllaç): http://www.ibsalut.es/ibsalut/documentospdf/cat/cbp_cat.pdf.

- ✓ Així mateix, des del menú **Professionals > Seguretat de la informació** es pot accedir al curs interactiu sobre el Codi de bones pràctiques.

CONFIDENCIALITAT DE LA INFORMACIÓ

A què es refereix la *confidencialitat*?

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

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

- ✗ **Mai**. El personal que hagi tengut accés a dades de caràcter personal en acomplir la seva feina ha de servar estrictament el secret professional durant temps indefinit, fins i tot després que hagi acabat la relació amb el Servei de Salut.

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 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 infor-

mació que pertanyi a altres usuaris o grups d'usuaris si no tenen autorització.

PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

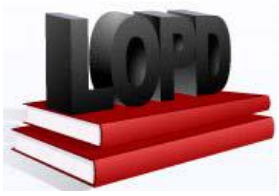
Què és una dada de caràcter personal?

Qualsevol informació numèrica, alfabètica, gràfica, fotografia, acústica o de qualsevol altre tipus relativa a les persones físiques identificades o identificables.

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.
- ✓ Conèixer els principis de la Llei orgànica de protecció de dades de caràcter personal.
- ✓ Garantir en qualsevol cas la confidencialitat de les dades a què tenguin accés.
- × No accedir a les dades per mitjans diferents als proporcionats pel Servei de Salut.



Quines mesures de seguretat cal aplicar per al tractament de la documentació impresa en paper que contengui dades de caràcter personal?

- ✓ Desar la documentació confidencial dins calaixos o armaris tancats amb clau.
- ✓ Destruir de manera segura la documentació confidencial.
- × Evitar generar documentació impresa.
- × Evitar que la documentació confidencial impresa en paper quedi a l'abast de persones no autoritzades (en impressores, faxos, llocs de treball...).
- × Evitar generar fitxers temporals.
- × Evitar deixar informació confidencial desatesa (memòria USB sense xifrar o sense desar, equips sense bloquejar...).

Què és una dada personal relativa a la salut?

En particular, es consideren dades relatives a la salut les referides al percentatge de discapacitat i a la informació genètica.

ÚS DELS RECURSOS

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 del personal d'acord amb les funcions assignades.

Quines són les pràctiques que cal evitar per no comprometre les mesures de seguretat establides 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 establida.
- 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 instal·lacions habituals de treball cap dada ni informació sense l'autorització 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'ha d'accedir a la informació que no sigui necessària per acomplir les funcions de cada treballador.

Es pot descarregar música, pel·lícules i jocs als equips del Servei de Salut?

- No. Les unitats ofimàtiques no s'han d'utilitzar per a finalitats privades, ja que constitueixen una eina de treball i tenen capacitat limitada.

Es poden instal·lar programes a l'equip?

- No, excepte amb l'autorització expressa del responsable del servei i del Servei d'Informàtica.

Què és un sistema d'informació?

És un conjunt de fitxers —automatitzats o no—, programes, suports i equips utilitzats per emmagatzemar i tractar les dades.

Es pot emmagatzemar tota mena d'informació en núvol?

- **No.** Amb caràcter general està prohibit transmetre-hi o allotjar-hi informació sensible, confidencial, dades de caràcter personal o informació protegida pròpia del Servei de Salut, llevat que prèviament es disposi de l'autorització 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.

- ✓ Abans d'utilitzar aquests recursos externs, la Subdirecció de l'OTIC ha d'establir les característiques del servei prestat i les responsabilitats de les parts.

Què és un codi maligne?

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

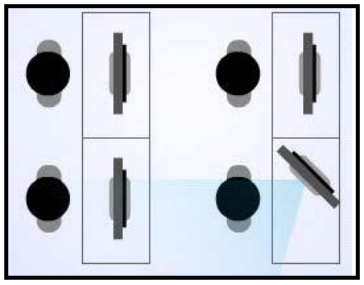
Quines mesures es poden prendre per evitar els virus i altres programes informàtics maliciosos?

- ✓ Davant de la sospita d'una infecció per virus, s'ha de comunicar la incidència d'acord amb el procediment corresponent. Cal adoptar totes les precaucions possibles en executar qualsevol programa, a més d'evitar executar fitxers adjunts rebuts per correu electrònic i visitar pàgines d'Internet amb contenguts de legalitat o moralitat dubtoses.

MESURES DE SEGURETAT

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

- ✓ Les pantalles —especialment les que estiguin a zones amb accés del públic— s'han d'orientar de tal manera que s'impedeixi al personal no autoritzat l'angle de visió tant com sigui possible.



- ✓ La informació que contengui dades de caràcter personal o sigui confidencial, independentment del format en què estigui (dispositius d'emmagatzematge, arxivadors, pantalles...), ha de ser custodiada sempre pel professional que la tengui a càrrec seu, per evitar que persones no autoritzades hi accedeixin.

- × **No s'ha de mantenir mai informació a la vista** d'altres persones sense que la persona que la té a càrrec seu ho controli degudament. Si s'absenta, cal prendre mesures per evitar que es pugui accedir a la informació: per exemple, bloquejar la sessió de l'ordinador, desar les històries clíniques amb pany i clau, recollir de les impressores els documents en el mateix moment en què s'imprimeixen...

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

- ✓ **Tant l'identificador d'usuari o les targetes criptogràfiques com la contrasenya corresponent són confidencials, personals i intransferibles**. Per tant, és responsabilitat del titular l'ús que en faci.

- × En cap cas no s'han de mantenir les contrasenyes en fitxers digitals, escrites en paper o en qualsevol altre tipus de suport llegible o accessible.

- ✗ **En cap circumstància no es pot utilitzar una sessió oberta sota cap altra identitat.**
- ✓ Si un usuari sospita que la seva contrasenya ha estat coneguda fortuïtament o fraudulentament per persones no autoritzades, l'ha de modificar i ha notificar immediatament la incidència al servei de suport corresponent.

- ✗ A l'hora de crear una contrasenya s'ha de procurar que altres persones no la puguin endevinar fàcilment.
- ✗ Cada usuari ha de canviar la seva contrasenya d'accés als sistemes almenys una vegada l'any i sempre que ho indiqui l'encarregat de la gestió dels usuaris.
- ✗ No s'ha de facilitar mai el nom d'usuari ni la contrasenya si es demanen per telèfon o correu electrònic. S'ha de comunicar aquesta incidència al Servei d'Atenció a l'Usuari**.**

- ✓ Quan un usuari acabi la seva relació o vinculació amb el Servei de Salut, la persona directament responsable d'aquest usuari ha de comunicar la nova situació a l'encarregat de la gestió dels usuaris perquè en doni de baixa els comptes i les autoritzacions.

Es poden emprar altres mecanismes d'identificació i autentificació?

- ✓ **Sí,** a més del sistema basat en l'ús d'identificadors d'usuari i contrasenya es poden emprar algorismes criptogràfics i certificats digitals, amb els quals s'estableixen garanties equivalents respecte de l'autenticació de la identitat dels actors, la confidencialitat, la integritat i el no-repudi de la informació tractada.

- ✓ Es requereix que l'usuari empri un certificat digital, l'autenticitat i la integritat del qual estan garantides per un tercer de confiança.

Què és el Servei d'Atenció a l'Usuari?

És el servei que dóna suport informàtic als usuaris i gestiona les incidències que pateixin amb relació a les aplicacions i a la infraestructura de les aplicacions.

EL LLOC DE TREBALL

Com ha d'estar el lloc de treball?

Amb caràcter general, el lloc de treball ha d'estar adesat, sense cap més material damunt la taula que el que sigui necessari per a l'activitat de cada moment**.**

Què s'ha de fer quan s'abandona el lloc de treball?

- ✓ S'ha de desar tota la informació que s'estigui tractant en un lloc tancat (dins un calaix o un armari amb pany i clau) o en una habitació separada i tancada amb pany, almenys fora de l'horari de feina.

- ✓ 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 en un lloc tancat.

S'han de bloquejar els terminals, els ordinadors personals i els dispositius mòbils amb accés a la informació abans d'abandonar el lloc de treball?

- ✓ **Sí,** tant momentàniament com al final de la jornada laboral. Així mateix, s'ha de bloquejar el lloc de treball al cap d'un temps d'inactivitat.

Què és la caracterització del lloc de treball?

És la definició de les responsabilitats relacionades amb cada lloc de treball en matèria de seguretat i els requisits que han de complir els usuaris en termes de confidencialitat.

ÚS D'INTERNET I DEL CORREU ELECTRÒNIC

Està permès connectar-se amb xarxes externes al Servei de Salut?

× **No està permès** utilitzar altres mitjans de connexió amb xarxes externes sense l'autorització corresponent.

És necessària l'autorització per habilitar connexions remotes?

✓ Qualsevol connexió remota que s'hagi d'habilitar —a sol·licitud d'un usuari intern o d'un proveïdor extern— ha de tenir l'autorització prèvia del responsable corresponent.

Es pot emprar qualsevol navegador o programa de correu electrònic?

× **No,** només es poden emprar els que estan prevists en els estàndards. 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.** Com qualsevol altre recurs, el navegador o el correu electrònic es poden emprar per a ús personal només si l'usuari hi està autoritzat.

Com es pot assegurar la confidencialitat de la informació que s'hagi de transmetre per Internet?

✓ Emprant el protocol HTTPS ("HTTP segur"); hauria d'aparèixer a la barra d'adreces del navegador.

✓ També hauria d'aparèixer-hi una icona en forma de pany, que informa sobre el certificat digital d'identitat del web visitat.

Què és el correu brossa?

Es tracta de missatges no sol·licitats, habitualment de tipus publicitari, enviats en grans quantitats i que perjudiquen d'alguna manera el receptor.

Què s'entén per *correu electrònic professional*?

El correu electrònic professional és un mitjà de comunicació interpersonal, **no un mitjà de difusió massiva** i indiscriminada d'informació.

Es poden enviar dades de caràcter personal per correu electrònic?

× Tot usuari **ha d'evitar enviar dades de caràcter personal per correu electrònic**. En qualsevol cas, només es poden transmetre emprant mecanismes que garanteixin la integritat de les dades i amb l'autorització corresponent.

Es pot accedir al correu adreçat a un altre usuari?

× **Està expressament prohibit** llegir, esborrar, copiar o modificar missatges de correu electrònic o fitxers adreçats a altres usuaris.

Es pot limitar l'ús d'Internet?

✓ El sistema que proporciona el servei de navegació pot disposar de filtres que bloquegin l'accés a pàgines web amb continguts inadequats, programes lúdics de descàrrega massiva o que contenguin virus o codis malignes.

✓ 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.

Quines accions es consideren com un ús incorrecte d'Internet?

- L'accés a llocs d'Internet i la distribució de missatges amb contenguts en què s'inciti o es promogui la pornografia i la segregació racial, sexual o religiosa, o amb contenguts de violència.
- La descàrrega i la transmissió indiscriminada d'imatges o de fitxers so o de vídeo.
- La distribució de virus o troians i qualsevol activitat encaminada a accedir il·lícitament a altres sistemes d'informació.
- La pirateria de qualsevol material multimèdia amb dret de la propietat intel·lectual.
- L'accés a xats i a jocs en línia.
- La publicació a Internet d'informació relacionada amb el Servei de Salut, llevat que es tengui l'autorització expressa per fer-ho.

El sistema que proporciona el servei de correu electrònic pot de manera automatitzada rebutjar, bloquejar o eliminar part del contengut dels missatges enviats o rebuts?

- ✓ **Sí**, en els casos en què es detecti algun problema de seguretat o d'incompliment del Codi de bones pràctiques.
- ✓ Així mateix, es pot inserir contengut addicional en els missatges per advertir els receptors sobre els requisits legals i de seguretat que han de complir amb relació als correus.

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 no s'han d'utilitzar les adreces incloses en l'agenda corporativa amb finalitats particulars.

INCIDÈNCIES EN LA SEGURETAT

Què és una incidència?

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

En quines circumstàncies s'han de comunicar les incidències en la seguretat?

- ✓ Segons el criteri de cada usuari, qualsevol incident que pugui tenir impacte en la seguretat i tots els detalls observats que l'hagin induït a sospitar. Per exemple, si observa que a l'ordinador es produeixen accions estranyes: augment de la mida dels fitxers, aparició d'avisos de Windows no habituals, recepció de correus de persones desconegudes o en idiomes no habituals, pèrdues de dades o de programes...

A qui s'han de notificar les incidències en la seguretat?

- ✓ Al servei de suport corresponent, al qual s'ha de prestar la col·laboració necessària per resoldre la incidència.
- ✗ L'omissió o el retard en la notificació d'un incident en la seguretat poden arribar a constituir una falta i, per tant, donar lloc a la responsabilitat disciplinària que hi correspongui.

Què és un actiu?

És un component o una funcionalitat d'un sistema d'informació susceptible de ser atacats 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.

Què s'ha de fer si es detecta una deficiència en una aplicació?

- ✓ A causa de la naturalesa dinàmica i canviant dels requisits que han de satisfer, les aplicacions informàtiques s'han de mantenir sempre actualitzades. Per fer-ho és imprescindible la col·laboració de tots els usuaris i per això els animam a comunicar qualsevol deficiència que detectin o les millores que considerin adequades.

ACABAMENT DE LA VINCULACIÓ O RELACIÓ AMB EL SERVEI DE SALUT

Què ha de fer un usuari quan acaba la seva relació amb el Servei de Salut?

- ✓ Tornar qualsevol suport que contengui dades a les quals hagi tengut accés en el marc de la seva vinculació o relació amb el Servei de Salut.
- ✓ Cedir el control sobre qualsevol fitxer o document relatiu a la seva prestació professional.

MONITORATGE I APLICACIÓ DEL CODI

Quines accions durà a terme el Servei de Salut?

Per motius legals, de seguretat i de qualitat del servei, el Servei de Salut durà a terme les accions següents:

- ✓ Revisarà periòdicament l'estat dels equips, de les aplicacions instal·lades, dels dispositius i de les xarxes.
- ✓ Monitorarà els accessos a la informació contenguda en els sistemes.
- ✓ Auditarà la seguretat de les credencials i de les aplicacions.
- ✓ Monitorarà els serveis d'Internet i de correu electrònic i altres eines de col·laboració.

Aquesta activitat es durà a terme sense emprar sistemes o programes que puguin atemptar contra els drets constitucionals dels usuaris.

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

- ✓ Es poden bloquejar o suspendre temporalment els sistemes.
- ✓ El servei es restablirà quan desaparegui la causa de la inseguretat o de la degradació.

Qui vetlarà perquè es compleixi el Codi de bones pràctiques?

La Subdirecció de l'OTIC, amb la col·laboració de la resta de les unitats del Servei de Salut.