INFORME D'AUDITORIA DE PROTECCIÓ DE DADES PERSONALS

COL·LEGI OFICIAL D'INFERMERIA DE BARCELONA

FEBRER 2008 PROTOCOL NÚMERO 4706

Índex

1. Introducció 2
2. Objectius i contingut de l'auditoria 2
3. Dades de l'entitat auditada 3
4. Metodologia i fases del treball 5
5. Punts objecte de la revisió 6
6 Anàlisis de les diferents àrees de l'auditoria 11
7 Conclusions (salvetats) 30

1. Introducció

El present informe s'elabora dins del marc legal establert per la normativa en protecció de dades, que exigeix la revisió i adequació dels fitxers automatitzats que contenen dades de nivell mitjà i alt, conforme al que estableixen els articles 5 a 26 del RD 994/1999, que aprova el Reglament sobre Mesures de Seguretat.

2. Objectius i contingut de l'auditoria

De conformitat amb el que estableix la normativa sobre protecció de dades, totes les entitats que disposin de fitxers automatitzats que continguin dades de nivell mitjà i/o alt, hauran de sotmetre, de forma biennal, els seus sistemes d'informació i instal·lacions de tractament de dades a una auditoria.

Com a resultat de l'auditoria s'ha elaborat el present informe que dictamina quines deficiències té el sistema i quines són les propostes de millora.

En aquest sentit es pronuncia l'article 17 del Reglament de Mesures de Seguretat:

> *"Els sistemes d'informació i les instal·lacions de tractament de dades es sotmetran a una auditoria interna o externa, que verifiqui el compliment del present Reglament, dels procediments i instruccions vigents en matèria de seguretat de dades, com a mínim un cop cada dos anys.*
>
> *L'informe d'auditoria haurà de dictaminar sobre l'adequació de les mesures i controls al present Reglament, identificar les seves deficiències i proposar les mesures correctores o complementaries necessàries. Igualment haurà d'incloure les dades, fets i observacions en que es basin els dictàmens assolits i les recomanacions proposades.*
>
> *Els informes d'auditoria seran analitzats pel responsable de seguretat competent, que elevarà les conclusions al responsable del fitxer per tal que adopti les mesures correctores adequades i quedaran a disposició de l'Agència de Protecció de Dades"*

3. Dades de l'entitat auditada

Dades identificatives

Entitat	Col·legi Oficial d'Infermeria de Barcelona
NIF	Q0866003G
Domicili	Carrer Alcoi, 21 08022 Barcelona
Telèfon	93 2128108

Dies de realització de l'auditoria

Dies	27 i 28 de febrer de 2008

Persones entrevistades

Entrevista 1	Sra. Gabriel Bronchales	Auditor Intern
Entrevista 2	Sra. Rosa Rivas	Cap d'Administració Col·legial i Sec. Gral.
Entrevista 3	Sr. Oriol Roura	Responsable de l'Àrea Social
Entrevista 4	Sra. Manel Tomás	Responsable de Cooperació i Voluntariat
Entrevista 5	Sra. Isabel Quintana	Responsable de Prevenció Riscos Laborals
Entrevista 6	Sra. Sònia Navarro	Suport Administratiu, Àrea de Formació
Entrevista 7	Sra. Magda Tur	Suport Administratiu, Àrea d'Inscripcions
Entrevista 8	Sra. Carles Ureña	Responsable d'Informàtica (Softeng, SL)
Entrevista 9	Sr. David Rangel	Responsable d'Informàtica (Softeng, SL)

Entrevista 10	Sra. Maite Framis	Resp. Biblioteca, Documentació i Arxiu
Entrevista 11	Sr. Jordi Cardila	Arxiu documental
Entrevista 12	Sra. Gemma Bruna	Responsable de Comunicació
Entrevista 13	Sra. Laura Rausell	Suport Administratiu, Àrea de Recerca

A més a més, s'han realitzat comprovacions al servei d'informàtica (sala de servidors), arxius, comptabilitat, així com a diferents punts d'atenció al col·legiat.

4. Metodologia i fases del treball

Per portar a terme l'auditoria s'ha realitzat una revisió in situ de les instal·lacions de tractament de dades i sistemes d'informació del **Col·legi Oficial d'Infermeria de Barcelona (COIB)**, situat al Carrer Alcoi número 21 (08022) de Barcelona, així com també una revisió de la documentació lliurada als auditors.

Tant el treball d'auditoria com l'elaboració d'aquest informe han sigut desenvolupats per un equip de persones constituït per professionals qualificats en el camp de la protecció de dades de Faura-Casas, treballant de forma simultània els aspectes tècnics i organitzatius de la seguretat, així com també els legals.

Per portar a terme l'execució de l'encàrrec d'auditar l'entitat, s'han efectuat les següents actuacions:

→ Realització de l'auditoria a través d'entrevistes, qüestionaris, recopilació i supervisió de documents i anàlisi i revisió de les mesures, controls i procediments.

→ Elaboració del present informe d'auditoria.

El treball d'auditoria s'ha desenvolupat complint els terminis pactats, i s'ha dividit en les fases que s'indiquen a continuació:

- Identificació dels interlocutors.
- Recollida de la informació.
- Estudi i anàlisi de la informació.
- Aclariments.
- Lliurament de l'informe provisional.
- Correccions i aclariments sobre l'informe provisional.
- Lliurament de l'informe definitiu.

5. Punts objecte de la revisió

En el desenvolupament dels treballs s'han revisat els següents extrems:

5.1 Contingut mínim del document de seguretat

S'ha comprovat si el Document de Seguretat tenia el contingut mínim que la normativa estableix com obligatori. Aquest contingut mínim, en el cas dels fitxers de nivell mitjà és:

Contingut Document de Seguretat Fitxers de nivell mitja
Àmbit d'aplicació del document
Mesures, normes i procediments per a garantir la seguretat: - Relació d'usuaris autoritzats - Contrasenyes que garanteixen la confidencialitat i integritat - Control d'accés a usuaris no autoritzats - Inventari de suports informàtics en llocs d'accés per personal autoritzat - Còpies de seguretat setmanalment
Funcions i obligacions del personal
Estructura dels fitxers i descripció dels sistemes d'informació que s'utilitzen
Procediment de notificació, gestió i resposta de les incidències
Identitat del responsable de seguretat
Mesures, normes i procediments per garantir el nivell mínim de seguretat exigit: - Identitat dels usuaris que intenten accedir al sistema d'informació - Limitació i control d'accés físic als locals a on estiguin ubicats els sistemes de informació
Controls periòdics per verificar el compliment del document de seguretat (auditoria interna o externa cada dos anys)
Procediments d´ aplicació pels usuaris que ja no seran utilitzats
Registre de les incidències: - Procediments de recuperació de les dades - Persona que executa aquest procediment - Dades restaurades i dades gravades manualment.

I en el cas dels fitxers de nivell alt, a més del contingut descrit, també s'ha comprovat que contingués els següents punts:

Contingut Document de Seguretat Fitxers de nivell alt
Establiment de registres d'entrada i sortida dels suports informàtics.
Prohibició de realitzar proves amb dades reals.
Mesures, normes i procediments per tal de garantir la seguretat exigida: - Mecanismes que garanteixin la seguretat durant el transport de suports - Ubicació física de les còpies en llocs diferents als d'ubicació dels equips - La transmissió de dades per mitjans telemàtics haurà de ser encriptada
Establiment d'un registre d'accessos: - Identitat de l'usuari que té accés, data i hora, fitxer accedit i tipus d'accés - Manteniment del registre com a mínim durant dos anys.

5.2 Accés a dades a través de xarxes de comunicacions.

S'ha comprovat si existia un accés a dades a través de xarxa de comunicacions, i en cas afirmatiu s'ha procedit a verificar si s'ha implantat un nivell de seguretat equivalent al dels accessos en mode local.

5.3 Règim de treball fora dels locals d'ubicació.

S'ha comprovat si s'ha donat algun cas de tractament de dades fora dels locals d'ubicació dels fitxers, i en cas afirmatiu si s'ha autoritzat tal tractament de forma expressa pel responsable del fitxer.

5.4 Fitxers temporals

S'ha comprovat si existeixen fitxers temporals, i en cas afirmatiu, s'ha procedit a inspeccionar i verificar que aquests fitxers compleixen amb les mesures de seguretat adequades, en funció del nivell de les dades que contenen.

També s'ha verificat si un cop deixen de ser necessaris, aquests fitxers s'esborren.

5.5 Funcions i obligacions del personal

S'ha comprovat si estan clarament definides les funcions i obligacions de cada una de les persones amb accés a les dades caràcter personal i als sistemes d'informació.

5.6 Registre d'incidències

S'ha comprovat si existeix un procediment de notificació i gestió d'incidències .

En cas afirmatiu s'ha procedit a l'estudi d'aquest procediment i a la verificació de si inclou els punts que la normativa considera imprescindibles com és la inclusió d'un registre d'incidències on queda constància del tipus d'incidència, el moment en que s'ha produït, la persona que realitza la notificació, a qui se li comunica i els efectes que s'han derivat de la mateixa.

També si existeix un procediment de recuperació de dades que inclogui l'autorització prèvia per escrit del responsable del fitxer, la descripció dels procediments realitzats de recuperació de dades, la indicació de la persona que va executar el procediment, la descripció de les dades restaurades i quan sigui el cas, la descripció de les dades que hagi estat necessari gravar manualment en el procediment de recuperació.

5.7 Identificació i autenticació dels usuaris

S'ha comprovat si existeix una relació actualitzada dels usuaris que poden accedir al sistema i dels procediments d'identificació i autenticació d'aquests accessos.

En cas afirmatiu, i sempre que el procediment d'autenticació s'hagi basat en contrasenyes, s'ha verificat si existeix un procediment d'assignació, distribució i emmagatzematge en garanteixi la integritat i confidencialitat. També s'ha comprovat si aquestes contrasenyes s'han canviat amb periodicitat.

I finalment, també s'ha verificat que les contrasenyes s'emmagatzemin de forma inintel·ligible i que existeixi un sistema que permeti identificar de forma inequívoca i personalitzada a tot aquell usuari que intenti accedir al sistema d'informació i la verificació de que està autoritzat.

5.8 Control d'accés lògic i físic

L'auditoria també ha verificat si l'accés per part dels usuaris queda limitat als recursos que necessiten pel desenvolupament de les seves funcions, i en cas afirmatiu, si existeixen mecanismes per evitar que un usuari pugui accedir a recursos diferents als autoritzats.

S'ha inspeccionat si la relació d'usuaris del sistema detalla a quins recursos hi tenen accés i si existeix un llistat del personal autoritzat de forma expressa per alterar l'accés autoritzat als recursos.

També s'ha comprovat si només el personal autoritzat en el Document de Seguretat té accés físic als locals on es troben ubicats els sistemes d'informació on es contenen les dades de caràcter personal .

I en cas que les mesures de seguretat corresponents siguin de nivell alt, s'ha comprovat si s'ha creat un registre d'accessos, on es guarda la identificació de l'usuari, la data i l'hora en que es va realitzar, el fitxer accedit, el tipus d'accés i si l'accés s'ha autoritzat o denegat. En el cas dels accessos autoritzats s'ha comprovat si es guarda la informació que permet identificar el registre accedit, durant un mínim de dos anys i si hi ha una revisió mensual de la informació de control registrada.

5.9 Gestió de suports

S'ha comprovat si els suports informàtics permeten identificar el tipus d'informació que contenen i ser inventariats, si s'emmagatzemen en un lloc amb accés restringit al personal que està autoritzat al document de seguretat i si es produeix la sortida de suports fora del local on està ubicat el fitxer.

En cas que existeixin sortides, s'ha verificat si aquestes sortides es troben expressament autoritzades pel Responsable del fitxer i si existeix un registre d'entrada i sortida dels suports que permeti conèixer el tipus de suport, la data i la hora, l'emissor, el número de suports, el tipus d'informació que conté, la forma d'enviament i la persona responsable del lliurament o recepció.

També s'ha verificat si es prenen les mesures necessàries per a garantir que sigui impossible recuperar la informació del suports reutilitzats.

Si el fitxer conté dades de nivell alt també s'haurà comprovat que la distribució de suports es realitza xifrant les dades o de qualsevol altra forma que els faci inintel·ligibles.

5.10 Còpies de recolzament i recuperació.

S'ha comprovat si existeix la descripció dels procediments de realització de còpies de recolzament i recuperació de forma que es garanteixi la reconstrucció de les dades en l'estat en que es trobaven al temps de produir-se la pèrdua o destrucció de les mateixos i si es realitzen còpies de seguretat amb una freqüència mínima setmanal.

I en el cas de ser fitxers que continguin dades de nivell alt, s'haurà verificat que es conserva una còpia de seguretat i dels procediments de recuperació de les dades en un lloc diferent on es troben ubicats els equips que tracten les dades.

5.11 Responsable de seguretat

S'ha comprovat que existeix la figura del Responsable de Seguretat i que desenvolupa totes les tasques que li pertoquen.

5.12 Proves amb dades reals

S'ha comprovat si es realitzen proves amb dades reals i, en cas afirmatiu, si es garanteix el nivell de seguretat corresponent al tipus de fitxer tractat.

5.13 Transmissió de dades a través de xarxes de telecomunicacions.

Finalment, i únicament pels fitxers de nivell alt, s'ha verificat si es transmeten dades a través de xarxes de telecomunicacions, i en cas afirmatiu si es transmeten xifrades o de qualsevol altra forma que faci que sigui inintel·ligible i no pugui ser manipulada per tercers.

Un cop inspeccionats tots els punts descrits a través de la revisió de documents, sistemes i entrevistes a usuaris, s'ha procedit a emetre el següent informe.

6 Anàlisis de les diferents àrees de l'auditoria

6.1 Accés a dades a través de xarxes de comunicacions

Article 5 RMS.- Les mesures de seguretat exigibles als accessos a dades de caràcter personal per mitjà de xarxes de comunicacions han de garantir un nivell de seguretat equivalent al corresponent als accessos de manera local.

Situació actual:

L'accés dels usuaris a les dades es produeix a través d'una xarxa LAN per a tots els equips informàtics. Anteriorment també es treballava amb una petita part inalàmbrica, però ja no està operativa.

La infraestructura informàtica és la següent: el COIB disposa de 33 ordinadors, més 5 que estan de reserva, i de 9 portàtils, a més el centre de Ronda Sant Pere treballa amb 10 ordinadors i 1 portàtil. Actualment hi ha 5 servidors operatius.

Tots els usuaris de l'entitat disposen de connexió a internet i correu electrònic. No hi ha filtres ni a l'ús d'internet ni per l'e-mail.

Hi ha instal·lat un antivirus xarxa Hard-Panda més *ETrust* (*Computer Associates*) a nivell de cada equip. Tot amb actualitzacions diàries. Hi ha un sistema d'alimentació ininterrompuda (SAIS), tant en servidor com en router i switchs.

Es treballa amb el programa *Ulisses* de gestió col·legial i amb el paquet *Office.* També s'utilitzen altres programes com per exemple el *Contaplus* per a comptabilitat o el *Inmagic* de llibres de biblioteques.

Àrees de millora

No detectada.

Es recomana que s'informi als usuaris de la necessitat d'emprar internet i el correu electrònic només per a tasques relacionades directament amb l'exercici de les seves funcions com a treballadors de l'entitat.

6.2 Règim de treball fora dels locals de la ubicació dels fitxers

Article 6 RMS.- L'execució de tractament de dades de caràcter personal fora dels locals de la ubicació del fitxer ha de ser autoritzada expressament pel responsable del fitxer i, en tot cas, s'ha de garantir el nivell de seguretat corresponent al tipus de fitxer tractat.

Situació actual:

Es realitzen tractaments de dades de caràcter personal fora dels locals en els que es troben ubicats els fitxers però en tot cas, aquests tractaments estan autoritzats pel responsable del fitxer.

El programa *Ulisses* permet treballar des de fora de l'entitat. Aquests tractaments sempre segueixen els mateixos processos de mesures de seguretat com si es treballés a mode local i l'accés d'aquests equips passa pel servidor de Terminal Server (*COIBAPP*), que permet en tot moment conèixer els diferents accessos i seguir-ne la traça.

A vegades s'ha fet alguna connexió remota per alguna sessió a la universitat, però en aquests casos sempre amb el suport de l'empresa *Softeng*. Des del centre que l'entitat té a Ronda Sant Pere de Barcelona, també hi ha una connexió diària i externa al COIB,

Els anomenats "assessors" que treballen per l'entitat com a externs, també tenen accés al programa *Ulisses*, tot i que aquest queda limitat a la part de les assessories exclusivament (els permisos són atorgats per COIB). Per últim, es pot donar un accés extern per part de l'empresa *Softeng* que fa el manteniment i suport informàtic, normalment es realitza dues o tres vegades a la setmana.

Àrees de millora

No detectada.

Recomanem que s'indiqui als documents de seguretat tot aquells accessos que no s'executen en mode local, fent menció que en tot cas els usuaris estan autoritzats i que les mesures de seguretat garantides són les mateixes que en mode local.

6.3 Fitxers temporals

Article 7 RMS.-

1. Els fitxers temporals han de complir el nivell de seguretat que els correspongui d'acord amb els criteris que estableix aquest Reglament.
2. Qualsevol fitxer temporal ha de ser esborrat quan deixa de ser necessari per a les finalitats que n'hagin motivat la creació.

Situació actual:

No és habitual que es treballi amb fitxers temporals paral·lels perquè el programa de gestió emprat per l'entitat en relació a l'activitat col·legial, el programa *Ulisses*, és molt complet i ja satisfà en gran mesura l'operativitat del COIB. A més a més, té la utilitat de ser exportable al programa *excel* per posar un exemple.

Des de la direcció de l'entitat i també pel responsable d'informàtica, a través d'una sessió realitzada a finals de l'any 2006 de bona *praxis* de les eines informàtiques, es va informar als usuaris del sistema de la necessitat de guardar la informació dins de la xarxa.

Àrees de millora

Tot i que no és habitual generar fitxers paral·lels perquè la base de dades del programa *Ulisses* ja satisfà totes les necessitats, som conscients que és inherent a qualsevol organització la generació de fitxers ofimàtics paral·lels, amb possibles dades de caràcter personal. No obstant, recomanem que des d'Informàtica hi hagi un control més estricte de l'existència i i perdurabilitat dels mateixos i que en tot cas, s'hauria de justificar en motiu d'una finalitat concreta i legítima.

Pels casos de documents que es puguin generar, el COIB disposa al servidor d'una estructura d'arxiu amb carpetes per usuaris o àrees de treball, a les quals es restringeixen els accessos. Únicament en tenen accés aquells que ho precisin per la seva feina. Aquesta dinàmica és possible de controlar a través del sistema de GPO's al servidor.

L'entitat hauria de conscienciar als usuaris, i concretament als àmbits més proclius a generar fitxers, de la transcendència d'eliminar els fitxers un cop ha finalitzat el seu ús. Per això i davant de la rotació del personal administratiu, seria convenient realitzar alguna altra sessió de bona *praxis* sobre mesures informàtiques com ja es va fer i penjar aquestes mesures en la intranet

corporativa de l'entitat. De la mateixa manera, també recomanem que a cada nou treballador se li doni un *Manual de Bones Pràctiques* en el que es recullin una sèrie de normes en base a les mesures de seguretat a tenir en compte pel que fa a dades personals i en el que s'incloguin les mesures a prendre respecte els fitxers temporals.

6.4 Document de seguretat

Article 8 RMS

1. El responsable del fitxer ha d'elaborar i implantar la normativa de seguretat mitjançant un document de compliment obligatori per al personal amb accés a les dades automatitzades de caràcter personal i als sistemes d'informació.
2. El document ha de contenir, com a mínim, els aspectes següents:

   a) Àmbit d'aplicació del document amb especificació detallada dels recursos protegits.

   b) Mesures, normes, procediments, regles i estàndards destinats a garantir el nivell de seguretat que exigeix aquest Reglament.

   c) Funcions i obligacions del personal.

   d) Estructura dels fitxers amb dades de caràcter personal i descripció dels sistemes d'informació que els tracten.

   e) Procediment de notificació, gestió i resposta davant les incidències.

   f) Els procediments de realització de còpies de seguretat i de recuperació de les dades.
3. El document s'ha de mantenir sempre actualitzat i ha de ser revisat quan es produeixin canvis rellevants en el sistema d'informació o en la seva organització.
4. El contingut del document s'ha d'adequar, en tot moment, a les disposicions vigents en matèria de seguretat de les dades de caràcter personal.

Article 15 RMS.- El document de seguretat ha de contenir, a més del que disposa l'article 8 d'aquest Reglament, la identificació del responsable o els responsables de seguretat, els controls periòdics que s'hagin de fer per verificar el compliment del que disposa el mateix document i les mesures que calgui adoptar quan un suport hagi de ser rebutjat o reutilitzat.

Situació actual:

L'entitat disposa de 4 documents de seguretat (DS), corresponents als fitxers de: Personal, Prevenció de Riscos Laborals, Administració i Col·legiats; tots inscrits al Registre de l'*Agencia Española de Protección de Datos* (AEPD) excepte el de Col·legiats, inscrit al Registre de l'Agència Catalana de Protecció de Dades (APDCAT), per raó de la competència d'aquesta darrera en matèria de fitxers de titularitat pública.

Tots els documents es troben en la seva primera versió, aprovada en data 09/01/2006 per la Junta de Govern del COIB.

Els documents de seguretat no es troben actualitzats ja que no reflecteixen la pràctica en diversos tractaments de dades ni incorporen directrius que posteriorment es segueixen, com per exemple en allò referent a les còpies de seguretat o al programa que s'empra actualment per a la gestió comptable, el *Contaplus*.

De totes maneres, com ja es va comentar en l'informe de l'anterior auditoria, s'han incorporat referències a procediments de la ISO, com per exemple. punt 5.4 DS Col·legiats que remet al procediment PR11-S01, de Manteniment Informàtic, i les instruccions IT01-PR11-S01, de Seguretat Informàtica.

En essència, els documents de seguretat comprenen tots els apartats als que obliga el reglament, excepte el referent a les mesures que cal adoptar quan un suport hagi de ser rebutjat o reutilitzat, sempre i quan no sigui material informàtic ja que en aquest últim cas sí que es disposa d'un protocol destinat a tal efecte.

Àrees de millora

Caldria que s'afegís un apartat que detalli les mesures a adoptar quan un suport paper hagi de ser rebutjat o reutilitzat, i que el *Protocol de Destrucció de Material Informàtic* s'annexi al Document de Seguretat.

Tal i com s'indica al RD 994/1999, en concret arts. 8 i 15, el DS constitueix una normativa interna de compliment obligatori i aquesta cal que estigui en tot moment d'acord amb la situació real de l'entitat.

Tot i que els documents de seguretat disposen del contingut mínim establert en base a la normativa, seria recomanable que s'anessin actualitzant, millorant i ampliant, incorporant en forma d'annexos els protocols interns ja definits per

l’entitat, com per exemples les mesures d’arxiu i documentació. L'objectiu final seria compilar totes les pautes d’actuació i funcionament en un mateix document.

6.5 Funcions i obligacions del personal

Article 9 RMS

1. Les funcions i les obligacions de cada una de les persones amb accés a les dades de caràcter personal i als sistemes d’informació estaran clarament definides i documentades, d’acord amb el que preveu l’article 8.2.c).
2. El responsable del fitxer ha d’adoptar les mesures necessàries perquè el personal conegui les normes de seguretat que afecten l’exercici de les seves funcions, com també les conseqüències en què pugui incórrer en cas d’incompliment.

Situació actual:

Les funcions i obligacions del personal de l’entitat estan detallades en els documents de seguretat: el personal afecte al document de seguretat (punt 4), la relació d’usuaris autoritzats amb accés a les dades (punt 5.3.1. DS Col·legiats, PRL i Personal; i punt 5.2.1. DS d’Administració), i la descripció de les obligacions dels usuaris i tercers amb accés a les dades (punt 5.3.2. DS Personal, PRL i Col·legiats, i punt 5.2.2. DS d’Administració).

De totes maneres, les funcions i obligacions del personal amb accés als sistemes d’informació que tracten dades personals no estan definides ni per usuaris, ni tampoc per grups d’usuaris. Únicament, a nivell de control informàtic, es disposa d’una relació nominal que agrupa als usuaris per a cada secció, per exemple, vocalia de salut mental, vocalia de llevadores, etc. En aquest llistat s’identifica el treballador nominalment, el departament, el nom d’usuari, el correu electrònic, així com també si cal mantenir l’e-mail al servidor.

No obstant l’esmentat, aquest document no es troba annexat al corresponent DS, ni tampoc desenvolupa suficientment quines són les funcions i obligacions de les persones amb accés a les dades, tal i com requereix l’art.9 del reglament.

Àrees de millora

El responsable del fitxer hauria d'adoptar les mesures necessàries perquè els treballadors de l'entitat coneguin les normes de seguretat en relació a dades personals que afecten l'exercici de les seves funcions, com també les conseqüències que es puguin derivar en cas d'incompliment.

Per tal de millorar i perfeccionar el sistema de control d'accés a les dades, seria recomanable generar un catàleg de llocs de treball amb les funcions associades, que després seria útil per relacionar els privilegis d'accés a la informació (programari i paper).

L'entitat hauria de conscienciar als usuaris que efectuen tractament específics de dades de caràcter personal (suport administratiu, secretaries, tècnics de les diferents àrees, administració) de les normes de seguretat a prendre. Per això i com ja hem comentat anteriorment, seria convenient realitzar alguna altra sessió de bona *praxis* sobre mesures informàtiques i l'entrega d'un Manual de Bones Pràctiques.

6.6 Registre d'incidències

Article 10 RMS.- El procediment de notificació i gestió d'incidències ha de contenir necessàriament un registre en què es faci constar el tipus d'incidència, el moment en què s'ha produït, la persona que fa la notificació, a qui es comunica i els efectes que en derivin.

Article 21 RMS

1. En el registre que regula l'article 10 s'han de consignar, a més, els procediments efectuats de recuperació de les dades, i indicar la persona que hagi executat el procés, les dades restaurades i, si s'escau, quines dades s'han hagut de gravar manualment en el procés de recuperació.

2. Cal l'autorització per escrit del responsable del fitxer per a l'execució dels procediments de recuperació de les dades.

Situació actual:

El registre d'incidències es troba detallat a l'apartat 5.7.2 dels Documents de Seguretat de Col·legiats, 5.7.3. del DS de Personal, 5.8.3 del DS de PRL, i 5.4 del

DS d'Administració; junt amb els annexos 4 i 5. Aquests models s'adeqüen als requeriments legals.

Tot i el que estipulen els DS, el procediment d'incidències actual no és aquest, sinó que es segueix l'establert al procediment ISO. A nivell intern, *Softeng* fa una gestió de les incidències a través d'un sistema de tiquets que permet fer un seguiment. Respecte al programa *Ulisses* es treballa també d'aquesta manera però a través d'una eina concreta que genera un codi i permet fer un seguiment.

El COIB comunica la incidència a l'empresa informàtica via telèfon o per e-mail. En quant a les incidències que són de sistemes es va crear un full *excel* a través del qual s'intercanvien les dades entre l'entitat i *Softeng*. Aquestes incidències són molt variades i no necessàriament són incidències en quant a dades personals, ja que per exemple hi ha revisions de xarxa perquè determinat equips tenen desconnexions, necessitat d'instal·lar uns altaveus, etc. En aquest full *excel* el COIB prioritza les feines i imposa terminis òptims per a la seva resolució. Existeix un protocol específic sobre com notificar les incidències. Només hi ha dos persones del COIB que en són responsables.

A dia d'avui, encara no s'ha donat cap incidència que hagi provocat la restauració de dades considerades de nivell de seguretat mitjà o alt.

En tot cas, no es consta d'autorització per escrit del responsable del fitxer per executar els procediments de recuperació. Tot i així, s'entén que el responsable d'informàtica, que és la persona que executa aquests procediments, com a responsable de seguretat està autoritzat pel responsable del fitxer des del moment en que aquest ha signat i ha donat validesa al document de seguretat.

Àrees de millora

S'hauria de detallar als documents de seguretat els procediments emprats per a la gestió i notificació de les incidències en base a la pràctica que es segueix actualment i a les directrius ISO, verificant que no s'obvia cap dels extrems requerits per la normativa de protecció de dades. Com ja comentàvem en els informes de l'auditoria anterior, també hauria de quedar detallat el procediment per a la recuperació de dades i la persona que ha executat el procés, les dades que han estat restaurades i les dades que ha estat necessari gravar manualment.

Hem de recordar que no només s'hauria de mantenir un control de les incidències informàtiques, sinó de totes aquelles que es puguin produir en qualsevol altre tipus de suport, ja que això podria suposar una no disponibilitat de la informació i la pèrdua d'un expedient d'un treballador o d'un col·legiat.

6.7 Identificació i autenticació d'usuaris

Article 11 RMS

1. El responsable del fitxer s'encarrega que hi hagi una relació actualitzada d'usuaris que tinguin accés autoritzat al sistema d'informació i d'establir procediments d'identificació i autenticació per aquest accés.
2. Si el mecanisme d'autenticació es basa en l'existència de contrasenyes, hi ha d'haver un procediment d'assignació, distribució i emmagatzematge que en garanteixi la confidencialitat i la integritat.
3. Les contrasenyes s'han de canviar amb la periodicitat que determini el document de seguretat i mentre estiguin vigents s'han d'emmagatzemar de manera inintel·ligible.

Article 18 RMS

1. El responsable del fitxer estableix un mecanisme que permeti la identificació de manera inequívoca i personalitzada de tots els usuaris que intentin accedir al sistema d'informació i la verificació que està autoritzat.
2. Es limita la possibilitat d'intentar reiteradament l'accés no autoritzat al sistema d'informació.

Situació actual:

És possible extreure una relació actualitzada dels usuaris autoritzats per accedir al sistema.

Existeix un sistema d'identificació i autenticació d'usuaris a través de nom d'usuari i contrasenya, tant d'accés a *Windows* com al programa *Ulisses* i al programa *Contaplus*. El nom d'usuari, per defecte, coincideix amb el del propi sistema *Windows,* però es pot canviar. Per una altra banda, el sistema genera una primera contrasenya però que cal canviar obligatòriament, no hi ha cap norma en quant a l'extensió mínima tot i que es recomana que siguin 8 caràcters.

A la sessió de formació sobre mesures informàtiques realitzada a finals del 2006 es va insistir en tractar d'evitar contrasenyes típiques, com aquelles que coincideixen amb les dates de naixement.

Les contrasenyes s'assignen directament a cada nou usuari i aquest l'ha de canviar. No hi ha una periodicitat determinada per al canvi de les mateixes, depèn de cada usuari. Les contrasenyes s'emmagatzemen de forma inintel·ligible i encriptada a la base de dades del programa *Ulisses* mentre estan vigents.

El protector de pantalla per inactivitat no està instal·lat per defecte, sinó que depèn de cada usuari. La recomanació que fa l'empresa informàtica és bloquejar el sistema cada cop que l'usuari deixa el seu lloc de treball.

Es limita a 3 intents la possibilitat d'accessos no autoritzats al sistema. Al tercer intent erroni el sistema queda bloquejat. Pel compte de correu electrònic el desbloqueig es fa internament des del COIB.

En general, es pot considerar que existeix un mecanisme d'identificació inequívoca i personalitzada d'usuaris, no existeixen grups d'usuaris genèrics ni de grup, ni tampoc usuaris convidats o per defecte, de manera que es permet establir procediments d'identificació i autenticació.

Àrees de millora

Caldria destacar que en comparació amb l'anterior auditoria, hi ha algunes mesures informàtiques que s'han deixat de prendre a nivell corporatiu i que caldria reintroduir per tal d'evitar accessos no autoritzats, ja que ara mateix que s'introdueixin o no depèn exclusivament de cada usuari.

Actualment, a diferència del que passava abans, les contrasenyes no caduquen cada 3 mesos i no hi ha cap històric respecte les anteriors, i tampoc està instal·lat als equips el protector de pantalla per inactivitat transcorregut un temps determinat.

Malgrat que les contrasenyes són individuals, durant els treballs d'auditoria s'ha tornat a manifestar que aquestes en moltes ocasions són conegudes per part de la resta dels companys, la qual cosa cal evitar, doncs desvirtua el procediment d'identificació i autenticació d'usuaris de l'entitat. A tall d'exemple, insistir en que aquest fet constitueix una incidència en quant a l'accessibilitat dels usuaris a les dades.

6.8 Control d'accés lògic. Control d'accés físic.

Article 12 RMS

1. Els usuaris tenen accés autoritzat únicament a les dades i els recursos que requereixin per a l'exercici de les seves funcions.
2. El responsable del fitxer ha d'establir mecanismes per evitar que un usuari pugui accedir a dades o recursos amb drets diferents dels autoritzats.

3. La relació d'usuaris a què es refereix l'article 11.1 d'aquest Reglament ha de contenir l'accés autoritzat per a cadascun d'ells.
4. Exclusivament el personal autoritzat per fer-ho en el document de seguretat pot concedir, alterar o anul·lar l'accés autoritzat sobre les dades i els recursos, d'acord amb els criteris que estableixi el responsable del fitxer.

Article 19 RMS.- Exclusivament el personal autoritzat en el document de seguretat pot tenir accés als locals on es trobin ubicats els sistemes d'informació amb dades de caràcter personal.

Article 24 RMS

1. De cada accés s'ha de guardar, com a mínim, la identificació de l'usuari, la data i l'hora en què s'hagi fet, el fitxer a què s'ha accedit, el tipus d'accés i si ha estat autoritzat o denegat.
2. En cas que l'accés hagi estat autoritzat, cal guardar la informació que permeti d'identificar el registre a què s'ha accedit.
3. Els mecanismes que permeten el registre de les dades detallades en els paràgrafs anteriors estan sota el control directe del responsable de seguretat competent sense que s'hagi de permetre, en cap cas, de desactivar-los.
4. El període mínim de conservació de les dades registrades és de dos anys.
5. El responsable de seguretat competent s'encarrega de revisar periòdicament la informació de control registrada i ha d'elaborar un informe de les revisions efectuades i dels problemes detectats una vegada cada mes com a mínim.

Situació actual:

La base de dades de caire informàtic està definida tècnicament. És la contrasenya personalitzada la que determina l'accés lògic al programari. Els usuaris només poden accedir a les dades i recursos estrictament necessaris per al desenvolupament de les seves funcions.

A través del Directori Actiu és possible conèixer en tot moment la relació dels usuaris actuals, lligat amb els accessos autoritzats al sistema d'informació.

En general, les altes es comuniquen via e-mail. La persona competent per a crear un nou accés o modificar-ne un d'existent és el responsable d'informàtica, d'acord amb els criteris que indiquen els responsables d'àrea corresponents. Normalment les baixes també es comuniquen.

Des del COIB s'informa a l'empresa informàtica sobre a quines carpetes pot accedir el nou usuari, segons el lloc de treballa que correspongui. A nivell del programa *Ulisses* és un procediment intern.

Existeix un registre dels accessos efectuats pels usuaris a les dades de caràcter personal. En aquest registre es recull: la identificació de l'usuari, la data i l'hora de l'accés, al fitxer al que s'ha accedit (concretament la taula específica) i el tipus d'accés. Aquest registre es manté a través d'un fitxer *log* i no queda mai desactivat.

La informació de control continguda en el registre d'accessos es conserva amb caràcter indefinit, no obstant es podria esborrar discrecionalment des del COIB. No es revisa periòdicament la informació de control registrada en el registre d'accessos, excepte per incidències.

En l'auditoria anterior es va manifestar que sí que es feien informes de revisió mensual del sistema, actualment no se'n fan. No obstant, des de *Softeng* s'envia amb periodicitat mensual un informe amb el detall de les tasques realitzades a efectes de facturació, tot i que no es pot entendre que aquesta relació sigui acceptable com a informe mensual requerit pel reglament.

La sala de servidors on resideixen les dades està ubicat a la planta del soterrani. El servidor està dins d'un espai tancat amb clau i amb condicions ambientals i de seguretat adequades. L'accés al servidor està limitat al personal degudament autoritzat (veure punt 5.4 DS Col·legiats). De l'accés al servidor n'ha de quedar constància al registre d'entrades i sortides situat al despatx de l'auditor intern del COIB.

Existeix un control d'accessos físics a través de claus, que estan guardades en una caixa, dins d'un armari del soterrani.

Àrees de millora

Informem que no cal que la informació de control continguda en el registre d'accessos es conservi indefinidament com es dóna actualment, ja que la reglamentació només exigeix que aquesta es guardi durant 2 anys.

Caldria assegurar que els mecanismes que permeten enregistrar la informació de control en el registre d'accessos no puguin quedar en cap cas desactivats.

S'hauria de recuperar la pràctica de fer informes de revisió mensual del sistema que en tot cas hauran de contemplar qualsevol dels àmbits que tracten informació amb dades de caràcter personal, és a dir, que a més a més de mencionar els de caire informàtic, també cal que es facin per altres tipus de suport, p. ex. paper.

6.9 Gestió de suports

Article 13 RMS

1. Els suports informàtics que continguin dades de caràcter personal han de permetre identificar el tipus d'informació que contenen, ser inventariats i emmagatzemar-se en un lloc amb accés restringit al personal autoritzat per fer-ho en el document de seguretat.
2. La sortida de suports informàtics que continguin dades de caràcter personal, fora dels locals en què estigui ubicat el fitxer, només pot ser autoritzada pel responsable del fitxer.

Article 20 RMS

1. S'ha d'establir un sistema de registre d'entrada de suports informàtics que permeti, directament o indirecta, de conèixer el tipus de suport, la data i l'hora, l'emissor, el nombre de suports, el tipus d'informació que contenen, la forma d'enviament i la persona responsable de la recepció que ha d'estar degudament autoritzada.
2. També s'ha de disposar d'un sistema de registre de sortida de suports informàtics que permeti, directament o indirecta, de conèixer el tipus de suport, la data i l'hora, el destinatari, el nombre de suports, el tipus d'informació que contenen, la forma d'enviament i la persona responsable del lliurament que ha d'estar degudament autoritzada.
3. Quan un suport hagi de ser rebutjat o reutilitzat, s'han d'adoptar les mesures necessàries per impedir qualsevol recuperació posterior de la informació emmagatzemada, abans de procedir a donar-lo de baixa en l'inventari.
4. Quan el suports hagin de sortir fora dels locals en què estiguin ubicats els fitxers com a conseqüència d'operacions de manteniment, s'han d'adoptar les mesures necessàries per impedir qualsevol recuperació indeguda de la informació emmagatzemada.

Article 23 RMS.- La distribució dels suports que continguin dades de caràcter personal s'ha de fer xifrant les dades esmentades o bé utilitzant qualsevol altre mecanisme que garanteixi que aquesta informació no sigui intel·ligible ni manipulada durant el transport.

Situació actual:

El COIB manté un inventari, degudament actualitzat, de tots els equips informàtics, ja siguin servidors, ordinadors, les impressores o portàtils. A més a més, hi ha documentació que detalla com està organitzada la infraestructura

(aquesta queda detallada al document de *Softeng* anomenat “Diagrama d’Infraestructura COIB”, que caldria annexar al Document de Seguretat).

Els portàtils i dispositius USB són els únics suports informàtics que podrien tenir dades personals i que surten fora de les instal·lacions del centre. No obstant, en ambdós casos són utilitzats, en general, pels membres de la Junta Directiva, per a presentacions en congressos per exemple, però en tot cas no contindrien dades de caràcter personal.

Fins ara, el portàtil només disposava d’un usuari genèric. L’entitat manifesta que a partir d’ara el que es farà serà crear 3 tipus d’usuaris: administrador (tots els privilegis), avançat i convidat (amb privilegis acotats segons correspongui). Depenent de l’usuari, el COIB donarà un permís o un altre.

El registre d’entrades i sortides està descrit a l’apartat 5.7.1. del DS Col·legiats i DS Personal, 5.8.1. DS PRL, junt amb l’annex 4.

Actualment, l’entitat disposa d’un registre d’entrades i sortides de documents del programa *Ulisses.* Aquest registre recull els següents camps (d’esquerra a dreta): tipus de suport, data i hora, receptor o emissor, número de suports, contingut, forma de recepció o enviament, responsable de la recepció o enviament i motius.

També es realitza un control de les entrades i sortides d’equips informàtics.

Els suports que s’han d’eliminar es sotmeten als següents processos: s’elimina tota la informació de l’equip obsolet i es guarda al servidor. Es formata i es trenca el disc.

Actualment, les mesures que s’adopten quan un suport informàtic s’hagi de destruir no estan descrites al document de seguretat, sinó que és un protocol de funcionament de l’entitat, anomenat *Destrucción de Material Informático*.

Àrees de millora

Seria convenient definir els processos d’esborrat o destrucció de suports no informàtics per escrit i annexar-los als documents de seguretat. De la mateixa manera s’hauria d’annexar als DS el protocol de destrucció de material informàtic que ja té implantat l’entitat.

De la mateixa manera que l’entitat està adoptant mesures en quant als equips portàtils, també cal que es donin indicacions als usuaris pels moviments d’informació que es puguin realitzar amb dispositius USB o altres.

6.10 Còpies de seguretat

Article 14 RMS

1. El responsable de fitxer s'encarrega de verificar la definició i l'aplicació correcta dels procediments de realització de còpies de seguretat i de recuperació de les dades.
2. Els procediments establerts per fer còpies de seguretat i per recuperar les dades han de garantir-ne la reconstrucció en l'estat en què estaven en el moment de produir-se la pèrdua o la destrucció.
3. S'han de fer còpies de seguretat com a mínim setmanalment, llevat que en aquest període no s'hagi produït cap actualització de les dades.

Article 25 RMS.- S'ha de conservar una còpia de seguretat i dels procediments de recuperació de les dades en un lloc diferent d'aquell en què es trobin els equips informàtics que els tracten i complir, en tot cas, les mesures de seguretat que exigeix aquest Reglament.

Situació actual:

El sistema de còpies s'estableix el punt 5.3.3. dels DS Col·legiats, PRL i Personal, i punt 5.2.3 DS Administració.

Es realitzen còpies de seguretat dels fitxers que contenen dades personals. Aquestes còpies estan programades automàticament, es fan en diferents suports, en cinta i en disc dur, i tenen una periodicitat diària. També es fan diàriament còpies completes de les imatges en format V2i.

De la mateixa manera es realitzen còpies completes, en cinta format DAT, amb periodicitat setmanal i mensual que es conserven en un lloc diferent, concretament una es porta al Banc Sabadell i una altra es guarda en una caixa forta del COIB.

Al tractar-se d'un sistema automàtic, s'envia un e-mail informant sobre si el procediment ha estat correcte o si pel contrari hi ha hagut algun error. El registre de les còpies queda dins del servidor, a més, a nivell intern, es controlen els moviments de cintes al Banc Sabadell en el registre d'entrades i sortides.

Es realitzen processos de recuperació de dades per algun fitxer que s'hagi pogut perdre puntualment i en tot cas, es garanteix la reconstrucció de les dades en el mateix estat anterior i queda tot reflectit en el registre d'incidències. Periòdicament, també a mode de prova, es verifica el correcte funcionament del sistema.

El personal autoritzat per a dur a terme les recuperacions de dades és el de l'empresa de manteniment informàtic *Softeng*, el COIB no pot encarregar-se d'aquesta activitat.

Àrees de millora

Tal i com ja vàrem reflectir en l'informe de l'anterior auditoria, realitzada al gener del 2006, caldria actualitzar els documents de seguretat per tal de referenciar tots els canvis que s'han produït en el sistema de còpies de seguretat. Per exemple, als DS no es reflecteix la possibilitat de guardar les imatges en format V2i.

A continuació reproduïm el contingut als documents de seguretat sobre la realització de còpies de seguretat que, com ja hem comentat, resulta del tot insuficient en base a la realitat actual:

Segons l'establert, les còpies es realitzen en suport cinta DAT, amb periodicitat diària, setmanal i mensual. La persona responsable de l'execució és una treballadora del COIB de suport administratiu. Les còpies es verifiquen diàriament i en cas d'error es notifica com a incidència.

Les còpies es troben ubicades a la sala del servidor, d'accés restringit a personal autoritzat. A més a més, mensualment les còpies es dipositen en una ubicació externa, en una caixa forta del Banc Sabadell, agència 0200.

6.11 Responsable de seguretat

Article 16 RMS .- El responsable del fitxer ha de designar un o diversos responsables de seguretat encarregats de coordinar i controlar les mesures definides en el document de seguretat. En cap cas aquesta designació suposa una delegació de la responsabilitat que correspon al responsable del fitxer d'acord amb aquest Reglament.

Situació actual:

A cada document de seguretat de nivell mitjà i alt hi està determinada la figura del responsable de seguretat. Concretament, el punt 5.2 del DS de Col·legiats estableix al responsable d'informàtica com a responsable de seguretat per aquelles mesures tecnològiques i a la responsable d'administració per a la resta de mesures; el punt 5.2.1. del DS de Prevenció de Riscos Laborals estableix com

a responsable de seguretat a la persona responsable de PRL, juntament amb Gerència; i el punt 5.2.1. del DS de Personal estableix com a responsable de seguretat al gerent.

Segons les directrius reglamentàries, el responsable de seguretat ha estat designat pel responsable del fitxer a través de l'aprovació del document de seguretat, amb la corresponent signatura.

En els propis documents de seguretat queden reflectides les funcions pròpies del responsable de seguretat.

Àrees de millora

No detectada.

6.12 Proves amb dades reals

Article 22 RMS .- Les proves anteriors a la implantació o modificació dels sistemes d'informació que tractin fitxers amb dades de caràcter personal no s'han de fer amb dades reals, llevat que s'asseguri el nivell de seguretat corresponent al tipus de fitxer tractat.

Situació actual:

No s'efectuen proves amb dades reals que suposin canvis en els sistemes d'informació. Sempre que l'entitat efectua proves no es fan mai amb dades reals, en tot cas sempre són fictícies. Aquestes proves són realitzades per l'empresa de manteniment informàtic, sempre previ avís a l'entitat.

De la mateixa manera, sempre que és necessari actualitzar una versió d'algun programa o aplicació, tampoc es realitza amb dades de producció.

Àrees de millora

No detectada.

Es recomana afegir un apartat al Document de Seguretat en el que s'expliqui el funcionament establert a l'entitat en quant a les proves amb dades reals.

6.13 Auditoria

Article 17 RMS

1. Els sistemes d'informació i les instal·lacions de tractament de dades s'han de sotmetre a una auditoria interna o externa que verifiqui el compliment d'aquest Reglament, dels procediments i les instruccions vigents en matèria de seguretat de dades, com a mínim, cada dos anys.
2. L'informe d'auditoria ha d'emetre dictamen sobre l'adequació de les mesures i els controls a aquest Reglament, identificar-ne les deficiències i proposar les mesures correctores o complementàries necessàries. També ha d'incloure les dades, els fets i les observacions en què es basin els dictàmens fets i les recomanacions proposades.
3. Els informes d'auditories han de ser analitzats pel responsable de seguretat competent, que ha d'elevar les conclusions al responsable del fitxer perquè adopti les mesures correctores adequades, i queden a disposició de l'Agència de Protecció de Dades.

Situació actual:

Aquesta és la segona auditoria que es realitza, la primera data del gener del 2006. Malgrat que es va fer una reunió informativa de resultats, no existeix cap evidència per la que s'acrediti que els Informes d'Auditoria han estat analitzats pel responsable de seguretat i que s'han elevat les conclusions al responsable del fitxer.

Es compleix amb el règim de biennalitat que determina el Reglament de Mesures de Seguretat.

Àrees de millora

Quan s'hagi rebut l'Informe d'Auditoria, els responsables de seguretat competents hauran d'elevar les conclusions al responsable del fitxer, a efectes d'adoptar les mesures corresponents.

6.14 Transmissió de dades a través de xarxes de telecomunicacions

Article 26 RMS.- La transmissió de dades de caràcter personal per mitjà de xarxes de telecomunicacions s'ha de fer xifrant les dades esmentades o bé utilitzant qualsevol altre mecanisme que garanteixi que la informació no sigui intel·ligible ni manipulada per tercers.

Situació actual:

La transmissió de dades personal s'acostuma a realitza a través de missatgeria o correu certificat. Puntualment es pot enviar informació per fax.

En canvi, pel que fa a la gestió del personal, la transmissió de la informació cap a l'empresa amb la que hi ha externalitzat el servei acostuma a produir-se mitjançant el correu electrònic, sense cap mecanisme d'encriptació.

També s'envia mensualment al *Consell de Col·legis de Catalunya* i a la *Organización Colegial de Enfermería* de l'Estat el llistat dels col·legiats al COIB. Aquest enviament es fa per correu electrònic.

Àrees de millora

S'hauria de continuar amb la tendència de reduir al màxim l'ús del fax o l'email sense mecanisme d'encriptació com a mitjà de transmissió de la informació amb dades de nivell alt, o amb informació especialment sensible d'atemptar contra la intimitat personal.

Per tant, caldria procedir a emprar mecanismes més reforçats per a les transmissions de correus electrònics entre el COIB i la gestoria, sempre que el contingut tingui dades sensibles. Per contra, això no resulta requerit per aquelles comunicacions que contenen dades bàsiques, merament identificatives.

7 Conclusions (salvetats)

Inspeccionats tots els punts determinats pel Reglament de Mesures de Seguretat, havent-se dut a terme les actuacions a les diferents dependències de l'entitat, realitzades les entrevistes amb els corresponents responsables d'àrea, havent-se valorat la documentació aportada, avaluats els sistemes de tractament de la informació, l'equip auditor detecta que els incompliments del **Col·legi Oficial d'Infermeria de Barcelona (COIB)**, de conformitat amb l'establert al RMS, són:

a) *Existència de fitxers temporals* (veure apartat 6.3)

Tot i que esdevé difícil el control d'aquests fitxers, l'entitat ha de conscienciar (a més de facilitar els mitjans) als àmbits més proclius a generar fitxers, de la transcendència d'eliminar-los un cop ha finalitzat el seu ús, i que aquesta a més en garanteixi la seva total destrucció.

També recomanem que a cada nou treballador se li doni un *Manual de Bones Pràctiques* en el que posi de manifest quines són les mesures de seguretat a prendre en relació al tractament de dades de caràcter personal i en concret, com s'ha d'articular la creació de fitxers temporals.

b) *Document de seguretat incomplet* (veure apartat 6.4)

L'entitat disposa de tots els DS corresponents als fitxers notificats, i aquests estan degudament aprovats per la Presidenta a la Junta de Govern. Tot i que els documents disposen de tots els procediments indicats al RMS, no estan degudament actualitzats i no descriuen la realitat actual. Manca incorporar en forma d'annexos els protocols interns de l'entitat, com per exemple els protocols d'arxiu i documentació.

c) Funcions i obligacions del personal (veure apartat 6.5)

El responsable del fitxer hauria d'adoptar les mesures necessàries perquè els treballadors de l'entitat coneguin les normes de seguretat en relació a dades personals que afecten l'exercici de les seves funcions, per això seria seria convenient realitzar alguna altra sessió de bona *praxis* sobre mesures informàtiques.

d) *Registre d'Incidències Incomplet* (veure apartat 6.6)

S'hauria de detallar als documents de seguretat els procediments emprats per a la gestió i notificació de les incidències. També hauria de quedar detallat el procediment per a la recuperació de dades i la persona que ha executat el procés, les dades que han estat restaurades i les dades que ha estat necessari gravar manualment.

A més a més, recordar no només s'hauria de mantenir un control de les incidències informàtiques, sinó de totes aquelles que es puguin produir en qualsevol altre tipus de suport.

e) *Identificació i autenticació d'usuaris* (veure apartat 6.7)

En comparació amb l'anterior auditoria, hi ha algunes mesures informàtiques que s'han deixat de prendre a nivell corporatiu i que caldria reintroduir per tal d'evitar accessos no autoritzats, ja que ara mateix que s'introdueixin o no depèn exclusivament de cada usuari.

f) *Control d'accés lògic. Control d'accés físic* (veure apartat 6.8)

Els mecanismes que permeten enregistrar la informació de control en el registre d'accessos no haurien de quedar en cap cas desactivats.

S'haurien de fer els informes de revisió mensual del sistema que en tot cas hauran de contemplar qualsevol dels àmbits que tracten informació amb dades de caràcter personal, ja sigui en suport informàtic com en altre tipus de suport.

g) *Gestió de suports* (veure apartat 6.9)

S'haurien de definir els processos d'esborrat o destrucció de suports no informàtics per escrit i annexar-los als documents de seguretat, al igual que el protocol de destrucció de material informàtic de l'entitat. També s'haurien de donar indicacions als usuaris pels moviments d'informació que es puguin realitzar amb dispositius USB o altres.

h) *Transmissió de dades a través de xarxes de telecomunicacions* (veure apartat 6.14)

S'hauria reduir al màxim l'ús del fax o l'email sense mecanisme d'encriptació com a mitjà de transmissió de la informació amb dades de nivell alt, o amb informació especialment sensible d'atemptar contra la intimitat personal. Es podrien emprar mecanismes més reforçats per a les transmissions de correus electrònics entre el COIB i la gestoria, sempre que el contingut tingui dades sensibles.

Barcelona, febrer de 2008

Pere Ruiz Espinós