DOCUMENT

DE

SEGURETAT

Empresa:	**Fundació per a la Universitat Oberta de Catalunya**
Grup Operatiu:	**Gabinet de Gerència**
Data d'edició:	**1 de desembre de 2000**
Versió:	**3.0**

R.D. 994/1999 Reglament de mesures de seguretat de fitxers automatitzats que continguin dades de caràcter personal

DOCUMENT DE SEGURETAT

R.D. 994/1999 Reglament de mesures de seguretat dels fitxers automatitzats que continguin dades de caràcter personal

0.- Introducció

Aquest document de seguretat ha estat elaborat per complir el Real Decret 994/1999, de 11 de juny pel qual s'aprova el Reglament de mesures de seguretat dels fitxers automatitzats que continguin dades de caràcter personal, i és de compliment obligatori per a tot el personal amb accés al sistema informàtic o els seus components, la informació que conté o que ha estat elaborada per ell; sigui personal propi de la FUOC o empreses del grup amb accés als recursos al sistema d'informació, sigui personal extern de tercers que desenvolupen la seva activitat en l'àmbit de domini del nostre sistema informàtic o amb caràcter d'encarregats del tractament de la informació de la qual la FUOC és titular.

Atès que el sistema informàtic dóna suport centralitzat a tots els usuaris de les empreses del grup i participades, i també els fitxers afectats pel Real Decret que es troben ubicats en els seus servidors centrals, el present document s'ha elaborat des de la perspectiva d'establir un Document de Seguretat global per a tot el sistema, dins del qual s'ubiquen els fitxers amb dades de caràcter personal.

Per les seves característiques, els fitxers o bases de dades inclosos en aquest document es troben catalogats dins del **nivell bàsic** de mesures de seguretat exigit pel Reglament.

1.- Àmbit d'aplicació d'aquest document

1.1 Àmbit jurídic: Aquest document s'aplicarà a la FUNDACIÓ PER A LA UNIVERSITAT OBERTA DE CATALUNYA, en endavant "la FUOC", i a totes les empreses agrupades o participades per ella, que comparteixen en diferent grau els recursos i els serveis del sistema informàtic.
A més, i per tal d'adequar a la normativa de seguretat vigent el nivell de qualitat dels serveis informàtics que la FUOC presta a terceres empreses, la normativa de seguretat continguda en aquest document serà d'aplicació en aquells casos en què la FUOC actuï com a responsable del tractament per compte d'altri.

FUNDACIÓ PER A LA UNIVERSITAT OBERTA DE CATALUNYA
- XARXA VIRTUAL DE CONSUM, SCC

- GRUP UOC
  - Editorial UOC
    - Eureca Media

- PLANETA UOC, S.L.
  - GMMD, S.L.

(*) En l'annex A-9 s'inclou una relació dels serveis oferts a cada empresa.

1.2 Àmbit personal: Aquest document de seguretat és de compliment obligatori per a tot el personal de la FUOC, d'empreses del grup i de proveïdors de serveis amb accés a les dades protegides o als sistemes d'informació que hi permeten l'accés. Tot el personal afectat es troba obligat per llei a complir allò que s'estableix en aquest document, i subjecte a les conseqüències que es podrien donar en cas d'incompliment. Les normes internes contingudes en el punt 3 del present document, en la mesura que afecten cada persona, se us han comunicat a fi i efecte d'acomplir degudament l'obligació continguda a l'art. 9.2 del Real Decret 994/1999, de 11 de juny.

1.3 Àmbit material: Las presents normes de seguretat són d'aplicació als recursos informàtics de la FUOC que es descriuen tot seguit:

- Centres de tractament i locals
- Xarxa corporativa
- Intranet
- Servidors centrals
- Terminals de treball (PC i similars)
- Servidor de pàgines WEB
- Sistemes operatius i aplicacions que donen accés a les dades

2.- Normes de seguretat

A fi de complir degudament allò que s'estableix a l'art. 8.2.b del Real Decret 994/1999, de 11 de juny, la FUOC ha establert les normes de seguretat següents, que hauran de ser conegudes, acceptades i respectades per tot el personal.

2.1.- Centres de Tractament i Locals

1. Els locals on s'ubiquin els servidors que contenen els fitxers han de ser objecte de protecció especial que garanteixi la disponibilitat i la confidencialitat de les dades protegides.

2. Els locals hauran de disposar de mesures de seguretat que evitin els riscs d'indisponibilitat o violabilitat dels fitxers que podrien produir-se com a conseqüència d'incidències fortuïtes o intencionades. La descripció d'aquestes mesures es troba al punt 4.4.

3. L'accés als locals on es trobi el fitxer haurà d'estar restringit exclusivament als administradors del sistema i al personal tècnic autoritzat que hagin de realitzar tasques de manteniment per a les quals sigui imprescindible accedir-hi físicament.

4. L'execució de tractament de dades de caràcter personal fora des locals de la ubicació del fitxer haurà de ser autoritzada expressament pel responsable del fitxer i, en qualsevol cas, s'haurà de garantir un nivell de seguretat corresponent al tipus de fitxer que es tracti.

5. Continuant amb el punt anterior, el responsable del fitxer comunicarà a les empreses proveïdores de serveis externs la implantació d'aquest Document de Seguretat i n'exigirà la presentació dels seus respectius Documents de Seguretat i la signatura d'un contracte/acord de "Confidencialitat i Tractament de Dades Personals", que garanteixi un nivell de seguretat en els seus locals, equips i personal, equiparable amb el d'aquest document.

2.2.- Llocs de Treball

1. Entenem per llocs o estacions de treball tots aquells dispositius a partir dels quals els usuaris tinguin accés al sistema per al desenvolupament de les seves funcions, com per exemple terminals o ordinadors personals.

2. Cada lloc de treball estarà sota la responsabilitat de l'usuari al qual està assignat, el qual garantirà que se li doni un ús adequat i en cap cas no serà utilitzat per persones alienes a la FUOC, o personal de la FUOC que utilitza la identitat de l'usuari.

3. En conseqüència, tant les pantalles com les impressores o altres tipus de dispositius perifèrics connectats amb lloc de treball hauran d'estar físicament ubicats en llocs que garanteixin la confidencialitat.

4. Quan l'usuari abandoni el seu lloc de treball, de manera temporal o en finalitzar la seva jornada laboral, haurà de deixar-lo apagat, o bé, bloquejat. Això últim es farà

mitjançant un protector de pantalla que obligui a identificar-se mitjançant una clau per tal de reprendre la feina.

5. En el cas de les impressores, caldrà estar segur que no quedin documents impresos en la safata de sortida que continguin dades protegides. Si les impressores es comparteixen amb altres usuaris no autoritzats a accedir a aquest tipus de dades, els responsables de cada lloc hauran de retirar els documents a mida que es vagin imprimint.

6. Els llocs de treball tindran una configuració fixa pel que fa als serveis de xarxa, recursos ofimàtics i aplicatius, en els seus respectius nivells de seguretat, que només es podrà canviar sota la supervisió d'un responsable autoritzat.

2.3.- Sistemes Operatius i Entorn de Comunicacions

1. Atès que en aquests nivells es dóna un risc més gran d'accessos per part de personal especialitzat amb coneixements i habilitats molt superiors als usuaris de *gestió*, els administradors de sistemes col·laboraran amb el responsable de seguretat per tal de garantir la seguretat en el nivell establert en aquest document.

2. Cada sistema operatiu (en els nivells de xarxa local, xarxa corporativa, CAMPUS i servidors de fitxers), i també el sistema de comunicacions, haurà de tenir almenys un responsable de la seva administració.

3. L'accés de personal tècnic (de la FUOC o extern) haurà d'estar perfilat de manera que només el personal autoritzat pugui accedir a serveis, utilitats i eines de sistema que proporcionin accessos als fitxers protegits i als aplicatius que els gestionen.

4. Tot usuari, el perfil del qual li proporcioni accés a fitxers protegits o als aplicatius i a les eines que els tracten, sigui de la FUOC o de proveïdors externs, serà identificat individualment, de manera que s'evitarà en tot moment l'ús de *logins* genèrics que dificultin el control esmentat.

5. En cap cas no és recomanable l'ús de *logins genèrics*. Tanmateix, es podran aplicar quan el volum d'accessos ho exigeixi, sempre que no autoritzin l'accés a fitxers protegits o a qualsevol recurs del sistema susceptible de manipular-los (aplicatius, eines ofimàtiques, serveis o comandaments de sistema).

6. Els sistemes operatius i qualsevol software especialitzat de control d'accessos seran configurats de manera que un usuari només pugui mantenir una connexió oberta al mateix temps; d'aquesta manera s'evita que un mateix login pugui estar actiu des de més d'un lloc simultàniament.

7. Els mitjans d'accés *en brut*, és a dir no editat o processat, als fitxers, com ara editors, debuggers, eines *query*, etc... estaran sota el control dels administradors i només seran accessibles a aquells usuaris que estiguin autoritzats.

8. Continuant amb el punt anterior, la definició de perfils d'accés des d'eines *query* es farà sempre limitant les dades a les *vistes* necessàries per a cada consulta. A més, s'evitarà incloure dades personals no imprescindibles a les consultes a fi de reduir l'interès de les dades seleccionades més enllà d'allò que és estrictament necessari per a cobrir la funció sol·licitada.

9. L'administrador o responsable de còpies de seguretat haurà de responsabilitzar-se de realitzar i de guardar en un lloc protegit les còpies de seguretat segons les condicions establertes en aquest document, de manera que cap persona no autoritzada no hi tingui accés.

10. Si existeixen unitats virtuals o fixes per a l'emmagatzematge de fitxers temporals derivats de l'activitat del sistema i dels aplicatius, l'administrador garantirà que les unitats esmentades es buidin regularment i que, mentre siguin utilitzades, no hi sigui possible l'accés per part d'usuaris no autoritzats.

11. El responsable o administrador del sistema de comunicacions, en col·laboració amb el responsable de seguretat i el responsable del fitxer, garantirà que els accessos al fitxers protegits mitjançant la xarxa presentin un nivell de seguretat equivalent a aquell establert per als accessos de manera local.

12. Quan, a causa d'avaries o de defectes operatius en els sistemes, als servidors hagi d'accedir personal que no pertanyi a la FUOC, els administradors s'ocuparan del seguiment de les operacions fins que es concloguin, garantint la inviolabilitat dels fitxers protegits.

13. Continuant amb el punt anterior, quan l'avaria aconselli la sortida dels equips dels locals de la FUOC, l'administrador es responsabilitzarà de l'execució de còpies de seguretat i d'esborrar tots el continguts protegits del sistema (llistes d'usuaris, aplicatius d'accés a dades protegides, fitxer protegits, etc...), en els casos en què sigui necessari lliurar un sistema mínimament operatiu.

14. De la mateixa manera, quan el problema afecti l'activitat dels discs del servidor i sigui impossible esborrar-los, s'exigirà l'autorització del responsable dels fitxers que hi estan continguts. A més, quan el problema afecti els discs pròpiament i siguin irrecuperables, quedaran en mans de la FUOC per tal de destruir-los immediatament.

2.4.- Desenvolupament i manteniment d'aplicatius

1. A partir de la implantació d'aquest document, els responsables del disseny, de l'anàlisi i del desenvolupament d'aplicatius propis actuaran en col·laboració amb el responsable de seguretat i el responsable del fitxer, per dotar els nous desenvolupaments de les mesures de seguretat requerides pel Reglament, segons les dades de caràcter personal que hagin d'emmagatzemar els fitxers.

2. Continuant amb el punt anterior, l'adquisició de software estàndard per a cobrir futures necessitats contemplarà també l'adaptació d'aquest software, segons les seves característiques, a les mesures establertes en aquest document i als requisits del Reglament en matèria de dades de caràcter personal.

3. Durant les fases de desenvolupament i proves s'utilitzaran fitxers en què no constin dades reals. Si per raons tècniques i de productivitat fos aconsellable utilitzar fitxers amb les dimensions i les característiques dels reals, el responsable del projecte juntament amb el responsable de seguretat dissenyaria un algorisme de desagregació per alterar les dades de manera que no poguessin ser regenerades als seus valors originals.

4. Si, per raons imperatives i inevitables, les proves d'un nou desenvolupament o les modificacions sobre un ja existent exigissin la utilització de dades reals, aquests

fitxers de proves haurien d'estar protegits en les mateixes condicions que les fitxers reals.

2.5.- Identificació i autenticació

1. El responsable del fitxer elaborarà una relació actualitzada d'usuaris que tinguin accés autoritzat al sistema d'informació. Aquesta relació s'integrarà en el document de seguretat com a ANNEX A-2.

2. El responsable de seguretat custodiarà i actualitzarà la relació de tots els usuaris de la xarxa que tenen accés autoritzat al sistema d'informació, garantint-ne la confidencialitat i la integritat. És competència del sistema de seguretat l'assignació automàtica de contrasenyes d'una manera segura.

3. Existirà un procediment d'identificació i d'autenticació dels usuaris que intentin accedir al sistema. Aquest sistema es descriu a l'apartat 4.5.1.

4. Existirà un procediment d'assignació, de distribució i d'emmagatzematge de contrasenyes que en garanteixi la confidencialitat i la integritat. Aquest procediment es descriu a l'apartat 4.5.1.3. i apartats següents.

5. Els números d'identificació i les claus d'accés assignades a cada usuari de la xarxa corporativa de la FUOC són personals i intransferibles, i l'usuari és l'únic responsable de les conseqüències que podrien derivar-se'n del mal ús, de la divulgació o de la pèrdua.

6. Les contrasenyes dels usuaris autoritzats tindran una longitud mínima de sis caràcters i màxima de vuit i seran modificades periòdicament. El sistema requerirà automàticament a cada usuari que modifiqui la contrasenya.

7. Les operacions susceptibles de seguiment que es realitzin en la xarxa corporativa o intranet de la FUOC quedaran enregistrades en els arxius LOG dels servidors. L'ús de l'identificador i de la clau assignats a cada usuari implicarà l'acceptació, com a document probatori de l'operació efectuada, dels registres generats en els arxius LOG esmentats i emmagatzemats en el sistema informàtic de la FUOC. Si no es demostra el contrari, es presumirà que els actes que es duguin a terme amb l'identificador i la clau assignats han estat realitzats en realitat per l'usuari que n'és titular.

2.6.- Control d'accés i confidencialitat de la informació

1. Tota la informació albergada en la xarxa corporativa de la FUOC, de forma estàtica o circulant en forma de missatges de correu electrònic, és propietat de la FUOC i té caràcter confidencial.

2. Els usuaris només tindran accés autoritzat a aquelles dades i aquells recursos que necessitin per a desenvolupar les seves funcions. El sistema utilitzat per a limitar l'accés d'acord amb el perfil de cada usuari es descriu a l'apartat 4.5.2.

3. Només el personal que hi està autoritzat en el document de seguretat podrà concedir, alterar o anul·lar l'accés autoritzat sobre les dades i els recursos, conforme als criteris establerts pel responsable del fitxer.

4. Tindran caràcter d'informació especialment reservada els secrets industrials o

comercials de la FUOC, en els quals s'inclouen, sense caràcter limitatiu, els procediments, les metodologies, el codi font, els algorismes, les bases de dades de clients, els plans de marketing, i qualsevol altre material que forma part de l'estratègia industrial o comercial de la FUOC.

2.7.- Còpies de Seguretat i Gestió de suports

1. Els suports informàtics que continguin dades de caràcter personal permetran d'identificar el tipus d'informació que contenen, ser inventariats i emmagatzemar-se en un lloc amb accés restringit al responsable del fitxer, al responsable de seguretat i al responsable de realitzar i d'administrar les còpies de seguretat.

2. El sistema d'identificació, d'inventari i de custòdia de suports es descriu a l'apartat 4.6.3.

3. Els responsables de fitxer juntament amb el responsable de seguretat establiran la freqüència i l'estratègia de còpies a aplicar sobre els fitxers i també els criteris i els procediments que s'hauran d'aplicar quan sigui necessari recuperar dades d'una còpia de seguretat.

4. Quan com a conseqüència d'una incidència detectada sigui aconsellable la recuperació de dades de les còpies, serà necessària l'autorització per escrit del responsable del fitxer. A més, haurà de deixar-se constància en el registre d'incidències del problema causant i de les manipulacions que s'hagin hagut de fer per completar la recuperació.

5. Atesa la complexitat i l'amplitud del sistema informàtic de la FUOC, l'administració de les còpies de seguretat i la seva realització serà automatitzada mitjançant l'aplicació d'un software especialitzat autoritzat únicament al personal d'explotació responsable de les còpies. Aquest software disposarà d'un registre d'activitat que coincideix amb la identificació dels suports utilitzats en cada còpia de seguretat.

6. Amb periodicitat setmanal, es farà un joc de còpies que es lliurarà a una empresa externa per tal que siguin emmagatzemades amb seguretat fora dels local de la FUOC. Aquestes còpies es lliuraran en un recipient tancat amb clau i amb clau de seguretat només conegudes pel responsable de les còpies i pel responsable de seguretat.

7. Continuant amb el punt anterior, la còpia externa inclourà també còpia dels procediments de recuperació i del software necessari per a la seva manipulació efectiva.

8. El responsable del fitxer serà l'única persona que podrà autoritzar la sortida de suports informàtics que continguin dades personals, fora dels locals en què estigui ubicat el fitxer.

9. Un cop retirats els suports de la seva activitat per obsolescència, error o per un altre motiu, seran físicament destruïts a fi de garantir que de cap manera els seus continguts no puguin ser recuperats.

2.8.- Ús del correu electrònic

1. El sistema informàtic, la xarxa corporativa i els terminals utilitzats per tot usuari són propietat de la FUOC.

2. En cas de conflicte, la FUOC es reserva el dret de revisar els missatges de correu electrònic dels usuaris de la xarxa corporativa i els arxius LOG del servidor, per tal de comprovar el compliment d'aquestes normes i de prevenir activitats que puguin afectar la FUOC com a responsable civil subsidiari.

   Aquesta revisió serà supervisada pel responsable de seguretat i es realitzarà sota el principi casuístic (cas a cas), sota el principi de bona fe (actuar amb preavís i en benefici del patrimoni empresarial) i sota el principi de garantia (respectant la dignitat del treballador).

3. Qualsevol fitxer introduït en la xarxa corporativa o en el terminal de l'usuari mitjançant missatges de correu electrònic que provinguin de xarxes externes haurà de complir els requisits establerts en aquestes normes i, especialment, aquelles que fan referència a la propietat intel·lectual i industrial i al control de virus.

2.9.- Accés a Internet

1. L'accés a debat en temps real (Chat / IRC) és especialment perillós, ja que facilita la instal·lació d'utilitats que permeten accessos no autoritzats al sistema, per la qual cosa el seu ús és estrictament prohibit.

2. En cas de conflicte, la FUOC es reserva el dret de monitoritzar i de comprovar, de forma aleatòria i sense avís previ, qualsevol sessió d'accés a Internet iniciada per un usuari de la xarxa corporativa.

3. Qualsevol fitxer introduït en la xarxa corporativa o en el terminal de l'usuari des de Internet haurà de complir els requisits establerts en aquestes normes i, especialment, aquelles que fan referència a la propietat intel·lectual i industrial i al control de virus.

2.10.- Propietat intel·lectual i industrial

1. És estrictament prohibit d'utilitzar programes informàtics sense la llicència corresponent, i també l'ús, la reproducció, la cessió, la transformació o la comunicació pública de qualsevol tipus d'obra o invenció protegida per la propietat intel·lectual o industrial.

3.- Funcions i obligacions del personal

A fi de complir degudament allò que s'estableix a l'art. 8.2.c del Real Decret 994/1999, de 11 de juny, la FUOC imposa al seu personal el compliment de les obligacions següents, que hauran de ser conegudes, acceptades i respectades per tot el personal amb accés al sistema informàtic de la FUOC, o qualsevol dels seus components, sobre la informació que conté o que ha estat elaborada per ell.

En endavant s'utilitzarà el terme usuari en el seu sentit ampli, que servirà per a identificar qualsevol persona amb accés al sistema informàtic de la FUOC, tant en qualitat de personal tècnic com de personal administratiu, docent i de gestió en les diferents àrees de la FUOC a les quals el sistema dóna suport.

Amb caràcter general, tots els usuaris estan obligats a complir les normes establertes a l'epígraf "Obligacions de caràcter general". Amb caràcter particular, aquestes normes seran ampliades i matisades per a usuaris que s'englobin en àrees d'actuació específiques, que exigeixin un major nivell de responsabilitat en l'aplicació d'aquest Document de Seguretat. És a dir:

- Usuaris (amb caràcter general tot el personal amb accés al sistema) [*]
- Responsables de fitxer
- Responsable de seguretat
- Cap de Personal o Director de RRHH
- Personal de l'Àrea de Sistemes d'Informació
  - Administradors (Xarxa, Sistemes, Bases de Dades, etc...)
  - Responsable de còpies de seguretat
  - Personal informàtic de desenvolupament i manteniment d'aplicatius
  - Personal informàtic de suport.

[*] Un cas especial d'usuari es dóna en els alumnes, els quals tenen un accés totalment restringit a les àrees que tenen autoritzades pel seu perfil d'estudiant. Les normes de seguretat per a aquest col·lectiu estan recollides en el document "Carta de Compromisos", en què s'estableixen els principis d'interacció de l'alumne amb el sistema informàtic.

3.1.- Obligacions de caràcter general

3.1.1.- Identificadors i claus d'accés

1. És prohibit de comunicar a una altra persona l'identificador d'usuari i la clau d'accés. Si l'usuari sospita que una altra persona coneix les seves dades d'identificació i d'accés haurà de comunicar-ho al responsable de seguretat, per tal que li assigni una nova clau. Davant una baixa o absència temporal de l'usuari, el responsable del departament podrà sol·licitar al responsable de seguretat la cessió de la clau o dades a la persona designada per ell.

2. L'usuari està obligat a utilitzar la xarxa corporativa i la intranet de la FUOC i les seves dades sense incórrer en activitats que puguin ser considerades il·lícites o il·legals, que infringeixin els drets de la FUOC o de tercers, o que puguin atemptar contra la moral o les normes d'etiqueta de les xarxes telemàtiques.

3. Estan **expressament prohibides** les activitats següents:

- Compartir o facilitar l'identificador d'usuari i la clau d'accés donats per la FUOC amb una altra persona física o jurídica, inclòs el personal de la pròpia empresa. En cas d'incompliment d'aquesta prohibició, l'usuari serà l'únic responsable dels actes realitzats per la persona física o jurídica que utilitzi de forma no autoritzada l'identificador de l'usuari.

- Intentar distorsionar o falsejar els registres LOG del sistema.

- Intentar desxifrar les claus, sistemes o algorismes de xifrat i qualsevol altre element de seguretat que intervingui en els processos telemàtics de la FUOC.

- Destruir, alterar, inutilitzar o de qualsevol forma danyar les dades, els programes o els documents electrònics de la FUOC o de tercers. (Aquests actes poden constituir un delicte de danys, previst a l'article 264.2 del Codi Penal).

- Intentar llegir, esborrar, copiar o modificar els missatges de correu electrònic o arxius d'altres usuaris. (Aquesta activitat pot constituir un delicte d'intercepció de les telecomunicacions, previst a l'article 197 del Codi Penal).

- Utilitzar el sistema per a intentar accedir a àrees restringides dels sistemes informàtics de la FUOC o de tercers.

- Instal·lar còpies il·legals de qualsevol programa, inclosos aquells que són estandarditzats.

- Esborrar qualsevol dels programes instal·lats legalment.

- Obstaculitzar voluntàriament l'accés d'altres usuaris a la xarxa mitjançant el consum massiu dels recursos informàtics i telemàtics de la FUOC, i també realitzar accions que perjudiquin, interrompin o generin errors en els sistemes esmentats.

- Enviar missatges de correu electrònic de forma massiva o amb fins comercials o publicitaris sense el consentiment del destinatari (Spam).

- Intentar augmentar el nivell de privilegis d'un usuari en el sistema.

- Introduir voluntàriament programes, virus, macros, applets, controls ActiveX o qualsevol altre dispositiu lògic o seqüència de caràcters que causin o siguin susceptibles de causar qualsevol tipus d'alteració en els sistemes informàtics de l'entitat o de tercers. L'usuari tindrà l'obligació d'utilitzar els programes antivirus i les seves actualitzacions per a prevenir l'entrada en el sistema informàtic de qualsevol element a destruir o a corrompre les dades informàtiques.

3.1.2.- Confidencialitat de la informació

1. És prohibit d'enviar informació confidencial de la FUOC a l'exterior, mitjançant suports materials o per qualsevol mitjà de comunicació, incloent-hi la simple visualització o accés.

2. Els usuaris dels sistemes d'informació corporatius hauran de guardar, per un temps indefinit, la màxima reserva i no divulgar ni utilitzar directament ni mitjançant terceres persones o empreses, les dades, els documents, les metodologies, les claus, les anàlisis, els programes i altra informació a la qual

tinguin accés durant la seva relació laboral amb la FUOC i amb empreses que pertanyen al grup, tant en suport material com electrònic. Aquesta obligació continuarà vigent un cop extingit el contracte laboral.

3. Cap col·laborador no podrà posseir, per a usos que no siguin propis de la seva responsabilitat, cap material o informació propietat de la FUOC, tant ara com en el futur.

4. En cas que, per motius directament relacionats amb el lloc de treball l'empleat prengui possessió d'informació confidencial sota qualsevol tipus de suport, s'entendrà aquesta possessió com estrictament temporal, amb obligació de secret, sense que aquest fet li concedeixi cap dret de possessió, o de titularitat o còpia sobre la informació esmentada. A més, el treballador haurà de tornar aquest materials a la FUOC, immediatament després de la fi de les tasques que n'han originat l'ús temporal i, en qualsevol cas, en acabar la relació laboral. La utilització continuada de la informació en qualsevol format o suport de manera diferent a aquella pactada i sense el coneixement de la FUOC no suposarà, en cap cas, una modificació d'aquesta clàusula.

5. L'incompliment d'aquesta obligació pot constituir un delicte de revelació de secrets, previst a l'article 197 i articles següents del Codi Penal i donarà el dret a la FUOC d'exigir a l'usuari una indemnització econòmica.

3.1.3.- Ús del correu electrònic

1. El sistema informàtic, la xarxa corporativa i els terminals utilitzats per tot usuari són propietat de la FUOC.

2. En cas de conflicte, la FUOC es reserva el dret de revisar els missatges de correu electrònic dels usuaris de la xarxa corporativa i els arxius LOG del servidor, per tal de comprovar el compliment d'aquestes normes i de prevenir activitats que puguin afectar la FUOC com a responsable civil subsidiari.

   Aquesta revisió serà supervisada pel responsable de seguretat i es realitzarà sota el principi casuístic (cas a cas), sota el principi de bona fe (actuar amb preavís i en benefici del patrimoni empresarial) i sota el principi de garantia (respectant la dignitat del treballador).

3. Qualsevol fitxer introduït en la xarxa corporativa o en el terminal de l'usuari mitjançant missatges de correu electrònic que provinguin de xarxes externes haurà de complir els requisits establerts en aquestes normes i, especialment, aquelles que fan referència a la propietat intel·lectual i industrial i al control de virus.

3.1.4.- Accés a Internet

1. L'accés debat en temps real (Chat / IRC) és especialment perillós, ja que facilita la instal·lació d'utilitats que permeten accessos no autoritzats al sistema, per la qual cosa el seu ús és estrictament prohibit.

2. En cas de conflicte, la FUOC es reserva el dret de monitoritzar i de comprovar, de forma aleatòria i sense avís previ, qualsevol sessió d'accés a Internet iniciada per un usuari de la xarxa corporativa

3. Qualsevol fitxer introduït en la xarxa corporativa o en el terminal de l'usuari des

d'Internet haurà de complir els requisits establerts en aquestes normes i, especialment, aquelles que fan referència a la propietat intel·lectual i industrial i al control de virus.

3.1.5.- Propietat intel·lectual i industrial

1. És estrictament prohibit d'utilitzar de programes informàtics sense la llicència corresponent, i també l'ús, la reproducció, la cessió, la transformació o la comunicació pública de qualsevol tipus d'obra o invenció protegida per la propietat intel·lectual o industrial.

3.1.6.- Incidències

1. Tot el personal de la FUOC té l'obligació de comunicar qualsevol incidència que es produeixi en els sistemes d'informació als quals tingui accés.

2. Entenem per incidència qualsevol anomalia que afecti o pugui afectar la seguretat de les dades i el seu correcte tractament, i també el correcte funcionament dels equips i dels programes per mitjà dels quals es realitza.

3. Aquesta comunicació s'haurà de realitzar immediatament, i sempre conforme al procediment de notificació d'incidències indicat a l'apartat 4.7.1., a menys que l'usuari estigui associat a un departament amb un procediment particular.

4. Els responsables de cada grup operatiu seran informats del procediment i dels punts de suport als quals ha de dirigir-se tot usuari per notificar les incidències detectades en el compliment de les seves funcions i s'encarregaran de notificar-ho de manera fefaent a cadascun dels usuaris del grup.

5. Qualsevol usuari que detecti una incidència és el responsable de comunicar-la pel procediment i al punt de suport que té assignat o, per defecte, al responsable de seguretat o al responsable del fitxer afectat, quan sigui el cas.

6. El coneixement i la no notificació d'una incidència per part d'un usuari serà considerat com una falta contra la seguretat del sistema i, donat el cas, del fitxer afectat, per part d'aquest usuari.

3.1.7.- Protecció de dades

És terminantment prohibit de:

1. Crear fitxers paral·lels o extreure parts dels fitxers de dades personals sense l'autorització del responsable del fitxer.

2. Creuar informació relativa a dades de diferents fitxers o serveis a fi i efecte d'establir perfils de personalitat, hàbits de consum o qualsevol altre tipus de preferències, sens l'autorització expressa del responsable del fitxer.

3. Qualsevol altra activitat expressament prohibida en aquest document o en les normes sobre protecció de dades i Instruccions de l'Agència de protecció de Dades.

Deure de secret:

4. De conformitat amb l'art. 10 de la Llei 15/1999, de 13 de desembre de 1999 de Protecció de Dades de Caràcter Personal: el responsable del fitxer i aquells que intervinguin en qualsevol fase del tractament de les dades de caràcter personal n'estan obligats al secret professional i al deure de guardar-los. Aquestes obligacions encara subsistiran després de finalitzar les seves relacions laborals amb el titular del fitxer, o, donat el cas, amb el seu responsable.

3.1.8.- Llocs de treball

1. Un lloc de treball és responsabilitat de l'usuari al qual està assignat. L'usuari garantirà que se'n fa un ús apropiat i que la informació que mostra no és visible per al personal no autoritzat.

2. Si per qualsevol motiu raonable un altre usuari ha de d'accedir al sistema des del lloc de l'usuari habitual, aquest segon usuari tancarà tots els recursos oberts i sortirà del sistema per forçar l'usuari ocasional a identificar-se amb el seu propi *login* d'accés i d'aquesta manera establir el seu perfil d'autoritzacions.

3. Si un usuari autoritat ha de compartir impressores o altres perifèrics de sortida de dades amb usuaris no autoritzats, procurarà recollir immediatament els llistats, els documents, els informes, etc... de la seva competència.

4. En qualsevol cas, l'usuari sol·licitant és el responsable de la destinació dels llistats, dels informes o de qualsevol altra informació de sortida sol·licitada. Per aquest motiu, no s'han de deixar documents sense recollir en les safates de sortida d'impressores o altres perifèrics.

5. Quan l'usuari abandoni el seu lloc de treball, temporalment o en acabar la seva jornada laboral, haurà de deixar-lo apagat o bé bloquejat. Això últim es farà preferentment sortint l'usuari del sistema de manera manual; per defecte, s'activarà automàticament un protector de pantalla que obligui a identificar-se mitjançant la clau per poder reprendre la feina.

6. Els llocs de treball tenen una configuració determinada (sistema operatiu, aplicatius, software ofimàtic, antivirus, etc....) que només podrà ser modificada a petició del responsable del grup operatiu, sota la supervisió del responsable de seguretat i pel personal de suport degudament autoritzat.

7. L'accés a fitxers protegits està configurat partint de les autoritzacions de l'usuari i controlat pels aplicatius i eines utilitzades. És prohibit de descarregar dades als discs locals del lloc de treball i és necessari mantenir qualsevol feina dins de les unitats de xarxa assignades, garantint-ne, d'aquesta manera, la seguretat i còpies dins dels procediments habituals del sistema.

8. Les mesures de seguretat descrites en aquest document i les funcions i les obligacions del personal seran d'igual aplicació quan l'accés es produeixi en la modalitat de teletreball i/o fora dels locals de l'organització.

3.2 Funcions del responsable de fitxer

El responsable de fitxer, en permanent i en fluida comunicació amb el titular dels fitxers i en coordinació amb el responsable de seguretat, s'encarregarà de:

1. Notificar a l'Agència de Protecció de Dades els fitxers amb dades personals existents a la FUOC, actualment i en el futur, com a conseqüència del desenvolupament de nous projectes o la implantació de nous serveis.

2. Vetllar pel compliment de tots els requisits establerts a la Llei de Protecció de Dades de Caràcter Personal i al Reglament de Mesures de Seguretat dels Fitxers Automatitzats que continguin Dades de Caràcter Personal.

3. Elaborar i implantar el Document de Seguretat i vetllar per la seva aplicació i el seu compliment.

4. Descriure l'estructura dels fitxers i dels sistemes d'informació que realitzen el tractament de les dades personals de la FUOC.

5. Definir els criteris que el responsable de seguretat ha de seguir per tal d'administrar les autoritzacions d'accés a les dades i als recursos.

6. Establir els mecanismes necessaris per a evitar que un usuari pugui accedir a dades o recursos amb drets diferents a aquells autoritzats.

7. Garantir la difusió d'aquest document entre tot el personal afectat.

8. Mantenir actualitzat aquest document, sempre que es produeixin canvis rellevants en el sistema d'informació o en la seva organització, d'acord amb els articles 8 i 9 del Reglament.

9. Vetllar per l'adequació en tot moment del document de seguretat a les disposicions vigents en matèria de seguretat de dades.

10. Definir, en col·laboració amb el responsable de seguretat, les mesures de seguretat que han de complir els responsables de l'àrea de Sistemes d'Informació en el disseny de nous projectes i en l'execució de modificacions sobre aquells que ja existeixen.

11. Establir les funcions i les obligacions d'àmbit intern del personal al seu càrrec.

12. Tramitar les sol·licituds d'accés als sistemes d'informació del seu personal, especificant els perfils d'usuari de cadascun partint de les seves funcions i la seva responsabilitat.

13. Comunicar a les empreses proveïdores de serveis externs la implantació d'aquest Document de Seguretat i exigir-ne la presentació dels seus respectius Documents de Seguretat, quan sigui possible, i la signatura d'un contracte/acord de "Confidencialitat i Tractament de Dades Personals", que garanteixi un nivell de seguretat en els seus locals, equips i personal, equiparable amb el que s'estableix en aquest document.

3.3 Funcions del responsable de seguretat

El responsable de seguretat actuarà com a coordinador i garant de la correcta aplicació de les mesures de seguretat incloses en aquest document, establint un punt d'enllaç entre les especificacions dictades pel responsable del fitxer en compliment de les seves obligacions i la implantació efectiva portada a terme pels responsables de l'àrea de Sistemes d'Informació designats per a aplicar tecnològicament les solucions a aquestes especificacions. S'encarregarà de:

1. Vigilar el compliment de les normes de seguretat establertes en aquest document de seguretat.

2. Elaborar les mesures, les normes, els procediments, les regles i els estàndards de seguretat aplicats a la FUOC.

3. Definir l'àmbit d'aplicació del document de seguretat.

4. Decidir i documentar els recursos informàtics subjectes al document de seguretat.

5. Definir i verificar l'aplicació dels procediments de gestió d'incidències.

6. Definir i verificar l'aplicació dels procediments de còpies de seguretat i de recuperació de dades.

7. Elaborar i mantenir actualitzat el registre d'usuaris amb accés als sistemes d'informació.

8. Definir i verificar l'aplicació del procediment d'identificació i d'autenticació d'usuaris.

9. Definir i verificar l'aplicació del procediment d'assignació, de distribució i d'emmagatzematge de contrasenyes.

10. Definir i verificar l'aplicació del procediment de canvi periòdic de les contrasenyes dels usuaris.

11. Definir i verificar el mètode aplicat per a l'emmagatzematge encriptat de les contrasenyes.

12. Definir i verificar l'aplicació i l'efectivitat d'un sistema de control d'accessos que limiti l'accés dels usuaris únicament a aquelles dades i a aquells recursos que els siguin autoritzats per al desenvolupament de la seva activitat.

13. Administrar les autoritzacions d'accés segons els criteris establerts pel responsable del fitxer.

14. Definir i verificar la implantació d'un sistema de gestió de suports informàtics que contenen dades de caràcter general.

15. Confirmar la sortida de suports informàtics que continguin dades de caràcter personal, prèvia autorització del responsable del fitxer.

16. Verificar que es compleixen les normes de seguretat, informant el cap de personal de les infraccions comeses, per a l'aplicació de les sancions que se'n deriven.

17. Coordinar i controlar les mesures definides en el document de seguretat amb el responsable del fitxer i els responsables de l'àrea de Sistemes d'Informació encarregats de l'administració de sistemes, del desenvolupament i del manteniment

d'aplicatius, i de donar suport tècnic a la implantació efectiva de les mesures de seguretat descrites en aquest document.

18. Controlar i coordinar les mesures definides en el document de seguretat amb el responsable del fitxer i els responsables de les empreses proveïdores de serveis que actuen com a encarregats del tractament per compte de la FUOC, i com a empreses de suport tècnic i outsourcing.

3.4 Funciones del cap de personal

1. Col·laborar en la redacció de les normes internes per als usuaris

2. Publicar les normes internes

3. Revisar la signatura de les normes internes per part del personal de la FUOC

4. Vetllar pel compliment de les normes internes de la FUOC, establint les sancions corresponents en cas d'infracció.

3.5 Personal Informàtic

Dins d'aquest col·lectiu es troben catalogats els professionals amb coneixements i amb capacitat per a actuar en els nivells més baixos de les capes de seguretat del sistema informàtic. Per aquest motiu, la direcció de l'Àrea de Sistemes d'informació en col·laboració amb el responsable de seguretat garantirà el coneixement i la comprensió de les mesures de seguretat establertes en aquest document en els diferents nivells de responsabilitat dins del departament.

Tot i que no tot el personal informàtic estarà afectat pel mateix nivell de responsabilitat ni d'autorització en el seu accés al sistema informàtic, sí que ha d'existir una consciència clara dels aspectes legals recollits a les normes a les quals hem estat fent referència, i també de la necessitat que el sistema informàtic de la FUOC gaudeixi d'una seguretat efectiva derivada d'una correcta aplicació de les tecnologies utilitzades i de la feina responsable de cadascun dels empleats en l'execució de les seves funcions.

El director de l'Àrea de Sistemes d'Informació decidirà les persones que es responsabilitzaran en tot moment de les funcions de seguretat que es deriven de les normes establertes en aquest document i comunicarà les directrius que cal aplicar en l'execució de les seves funcions.

Es cataloguen en aquest grup:

- Director de l'Àrea de Sistemes d'Informació
- Administrador o Responsable de Comunicacions
- Administradors de Sistemes
- Administradors de Xarxes
- Administrador de CAMPUS
- Administrador de XARXA INTERNA
- Administrador de perfils (TREN)
- Administradors de Bases de Dades
- Administradors d'Explotació de Dades (DISCOVERY)
- Responsable de Còpies de Seguretat i Gestió de Suports
- Caps de Projecte (Producció i Manteniment d'Aplicatius)
- Responsable del Servei de Suport

- Servei de Suport i Gestió d'Incidències
- Servei(s) de Suport Intern
- Servei(s) de Suport Extern

3.6 Infraccions i Sancions

Aquest apartat es regirà per allò que estableix el capítol V (Art. 27 i 28) del R.D. 994/1999 de 11 de juny.

4.- Descripció del Sistema d'Informació

La Fundació Universitat Oberta de Catalunya neix amb l'objectiu fonamental de promoure la creació i el reconeixement d'una universitat de formulació jurídica privada amb la finalitat d'oferir ensenyaments universitaris no presencials.

La UOC és una institució pionera en el desenvolupament de metodologies d'ensenyament no presencial basades en l'aplicació telemàtica amb una modalitat d'estudis que supera les barreres de l'espai i del temps.

Mitjançant el Campus Virtual s'accedeix no només a les possibilitats de formació sinó també a tot tipus de serveis, acadèmics i no acadèmics, propis d'un campus universitari que, pel fet de ser virtual, no requereix l'existència física convencional dels recursos i, per tant, permet l'accés a tota la informació electrònica emmagatzemada en el sistema, delimitada per àrees i amb els nivells de seguretat d'acord amb cada necessitat, facilitant, d'aquesta manera, la interconnexió amb totes les xarxes externes d'informació com ara Internet i altres grans nodes.

El concepte universitari desenvolupat per la UOC relaciona els recursos del Campus Virtual i els pedagògics d'ensenyament no presencial: acció docent, materials didàctics, avaluació continuada, disseny formatiu, biblioteca virtual i el sistema d'informació.

En l'àmbit estrictament privat de gestió, d'administració i de suport a l'entorn, la FUOC disposa d'una àmplia infraestructura en telecomunicacions que interactua amb diferents xarxes locals i nodes servidors que donen entitat a una xarxa corporativa multidisciplinar, en què s'organitzen i s'administren els recursos i els serveis a disposició de la comunitat FUOC.

En l'eix central d'aquest entramat tan complex, es troben els recursos informàtics, de harware i de software, personal de gestió, administratiu, tècnic i de suport, que constitueixen el nucli vital per al funcionament adequat de tota la comunitat UOC.

4.1.- Descripció d'aplicatius

Els aplicatius que cobreixen les necessitats informàtiques de la FUOC i en els quals es gestionen els fitxers amb dades de caràcter personal són els següents:

Àrea	*Aplicatiu (*)*	*Descripció*	*Producció*	*Fitxers(*)*
Acadèmica	GAT	Gestió acadèmica i dels expedients dels alumnes	Pròpia	GAT
Sistemes d'Informació	CAMPUS VIRTUAL	Intranet educativa de la UOC	Pròpia	CAMPUS VIRTUAL
Recursos Humans	CURRO	Gestió del personal de la UOC	Pròpia i Standard	PERSONAL
Formació continuada	GAT FORMACIÓ	Informació dels alumnes de màster i postgrau	Pròpia	FORMACIÓ CONTINUADA
Marketing	PCRM	Dades de persones externes que han sol·licitat a la UOC informació	Pròpia i Standard	INFORMACIÓ
Economia	COFROS	Comptabilitat de la UOC	Standard	GESTIÓ COMPTABLE
Infrastructura	GAME	Distribució de material	Pròpia	TRAMESES
Comunicació	CLUB	Dades dels socis i gestió del Club UOC	Pròpia	CLUB
EVIU	EVIU	Gestió acadèmica dels alumnes del curs d'anglès	Pròpia	EVIU

(*) En la resta del document s'utilitzarà la nomenclatura indicada per a referir-nos als fitxers i als aplicatius relacionats.

4.1.1.- Aplicatius propietaris

Aplicatiu	*Responsable*
GAT	

Fitxer	*Descripció de l'aplicatiu*
GAT	Gestió de dades personals i expedients acadèmics dels estudiants de la UOC, i dades personals, acadèmiques i laborals de tutors i de consultores.
Ubicació	
Senegal.uoc.es	
Àmbit d'accessos	
Usuaris autoritzats de la xarxa corporativa. Grups operatius: - Acadèmica - Formació continuada - Serveis - Economia - Campus Virtual	

Aplicatiu	***Responsable***
CAMPUS VIRTUAL	

Fitxer	***Descripció de l'aplicatiu***
CAMPUS VIRTUAL	Intranet educativa de la UOC. Administració de connexions al Campus Virtual de la UOC d'estudiants, consultores, personal administratiu i de gestió, i altres persones i entitats externes relacionades amb la UOC.
Ubicació	
Cuba.uoc.es	
Àmbit d'accessos	
Usuaris autoritzats de la xarxa corporativa, i dels serveis oferts per la UOC als seus alumnes.	

Aplicatiu	***Responsable***
CURRO	

Fitxer	***Descripció de l'aplicatiu***
PERSONAL	Gestió del personal de la UOC. Dades per a la confecció de la nòmina del personal de la UOC i per al manteniment de l'historial professional dels treballadors.
Ubicació	
Ruanda.uoc.es	
Àmbit d'accessos	
Usuaris autoritzats de la xarxa corporativa. Grups operatius: - RRHH - Campus Virtual - GAT - Economia	

Aplicatiu	***Responsable***
GAT FORMACIÓ	

Fitxer	***Descripció de l'aplicatiu***
FORMACIÓ CONTINUADA	Informació dels alumnes de màster i postgrau. Gestió acadèmica i de cobraments de les persones matriculades en los cursos de postgrau i seminaris de la UOC.
Ubicació	
Brunei.uoc.es	
Àmbit d'accessos	
Usuaris autoritzats de la xarxa corporativa. Grups operatius: - Formació continuada - Campus Virtual	

Aplicatiu	***Responsable***
PCRM	

Fitxer	***Descripció de l'aplicatiu***
INFORMACIÓ	Dades de persones externes que han sol·licitat a la UOC informació sobre els seus serveis.
Ubicació	
Senegal.uoc.es	
Àmbit d'accessos	
Usuaris autoritzats de la xarxa corporativa. Grups operatius: - Marketing	

Aplicatiu	***Responsable***
COFROS	

Fitxer	***Descripció de l'aplicatiu***
GESTIÓ COMPTABLE	Comptabilitat de la UOC.
Ubicació	
Benin.uoc.es	
Àmbit d'accessos	
Usuaris autoritzats de la xarxa corporativa. Grups operatius: - GAT - Economia	

Aplicatiu	***Responsable***
GAME	

Fitxer	***Descripció de l'aplicatiu***
TRAMESES	Distribució de material.
Ubicació	
Senegal.uoc.es	
Àmbit d'accessos	
Usuaris autoritzats de la xarxa corporativa. Grups operatius: - Infrastructura	

Aplicatiu	***Responsable***
CLUB	

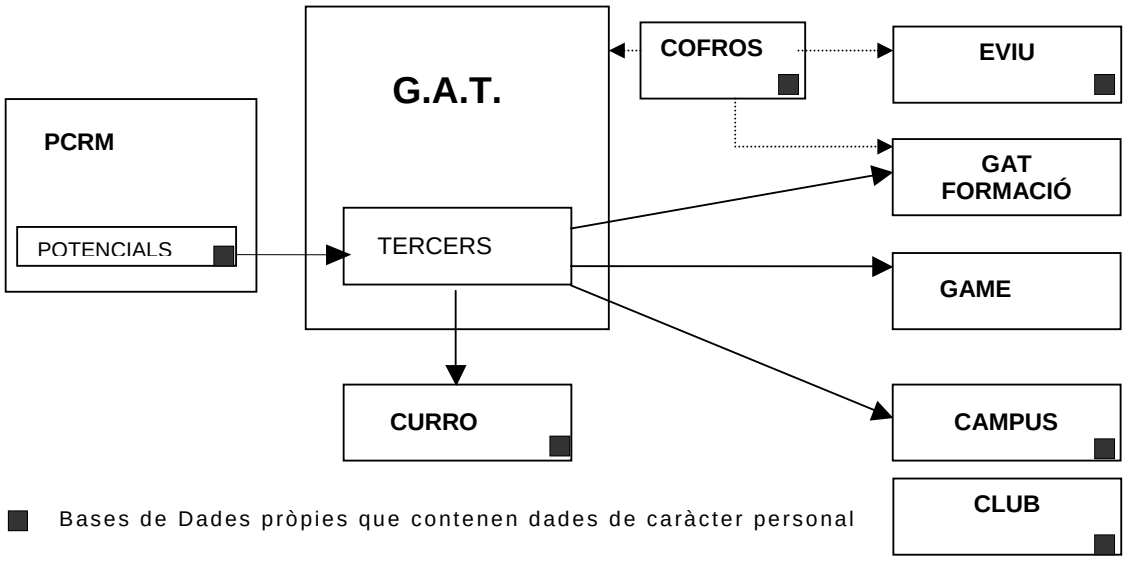
Fitxer	***Descripció de l'aplicatiu***
CLUB	Dades dels socis i gestió del Club UOC
Ubicació	
Brunei.uoc.es	
Àmbit d'accessos	
Usuaris autoritzats de la xarxa corporativa. Grups operatius: - Campus virtual - Club UOC - Economia	

Aplicatiu	***Responsable***
EVIU	

Fitxer	***Descripció de l'aplicatiu***
EVIU	Gestió acadèmica dels alumnes del curs d'anglès
Ubicació	
Brunei.uoc.es	
Àmbit d'accessos	
Usuaris autoritzats de la xarxa corporativa. Grups operatius: - Eviu	

4.1.2.- Compartició de dades entre Aplicatius

APL SERVIDOR	***APL CLIENT***	***DADES***
COFROS	GAT GAT FORMACIÓ	Formes de pagament
PCRM	GAT	Dades personals
GAT (*)	CAMPUS	Dades personals bàsiques
	CURRO	Identificador i dades personals bàsiques
	GAT FORMACIO	Identificador i dades personals bàsiques
	COFROS	Identificador i dades personals bàsiques + dades bancàries
	GAME	Identificador i dades personals bàsiques + dades enviaments
CURRO	CAMPUS	Dades personals bàsiques
GAT FORMACIÓ	CAMPUS	Dades personals bàsiques
	GAME	Identificador i dades personals bàsiques + DOM + dades enviament
(*) De fet, totes les dades personals bàsiques s'emmagatzemen en PERSONES, que formen part de l'aplicatiu GAT, actuant actualment com a BDD centralitzada. D'ella s'extreuen dades per alimentar altres aplicatius que assumeixen aquestes dades com a pròpies, mentre que la resta d'aplicatius comparteixen les dades personals en GAT. En tots els casos, cada aplicatiu gestiona i emmagatzema la seva pròpia base de dades amb la informació addicional relativa a persones físiques (dades personals) generada com a conseqüència de l'activitat quotidiana necessària per a la seva finalitat.		



4.2.- Estructura de los ficheros protegidos

4.2.1.- Base de Datos GAT

Responsable:		**Descripción del fichero**
Aplicativo:	GAT	Datos personales y expedientes académicos de los estudiantes de la UOC, y datos personales, académicos y laborales de tutores y consultores.
Fichero:	GAT	
Tipo:	Oracle	
Ubicación:	Senegal.uoc.es	

Datos especialmente protegidos
☐ IDEOLOGIA ☐ CREENCIAS ☐ RELIGION (*)¿Han sido recabados con consentimiento expreso y por escrito del afectado? SI π NO π
Otros datos especialmente protegidos
☐ ORIGEN RACIAL ☐ SALUD ☐ VIDA SEXUAL (*)¿Han sido recabados con consentimiento expreso y por escrito del afectado? SI π NO π
(*) En caso negativo, especifique la Ley que exime del consentimiento expreso por razones de interés general. Nº Ley ☐☐☐☐ Año ☐☐☐☐ **Indicar la Ley referida**

Datos de carácter identificativo	**Datos de características personales**
▣ DNI / NIF ▣ N SS/ MUTUALIDAD ▣ NOMBRE Y APELLIDOS ▣ DIRECCION ▣ TELEFONO ☐ FIRMA /HUELLA ▣ IMAGEN / VOZ ☐ MARCAS FISICAS ☐ OTROS (indicar) ……. Dirección de envío ..... …….	▣ DATOS DE ESTADO CIVIL ▣ DATOS DE FAMILIA ▣ FECHA / LUGAR DE NACIMIENTO ☐ CARACTERISTICAS FISICAS O ANTROPOMETRICAS ▣ SEXO ▣ NACIONALIDAD ☐ LENGUA MATERNA ☐ OTROS (indicar) ……. ……. …….
Datos de circunstancias sociales	
▣ CARACTERISTICAS DE NACIMIENTO, VIVIENDA ▣ SITUACION MILITAR ☐ PROPIEDADES, POSESIONES ☐ AFICIONES Y ESTILO DE VIDA ☐ PERTENENCIA A CLUBES, ASOCIACIONES... ☐ LICENCIAS, PERMISOS, AUTORIZACIONES ☐ OTROS (indicar) ……. ……. …….	

Datos académicos y profesionales	**Datos de detalle del empleo**
▣ FORMACION, TITULACIONES ▣ HISTORIAL DEL ESTUDIANTE ☐ EXPERIENCIA PROFESIONAL ☐ PERTENENCIA ASOCIACIONES PROFESIONALES ☐ OTROS (indicar) ……. ……. ……. …….	▣ PROFESION ☐ PUESTOS DE TRABAJO ☐ DATOS NO ECONOMICOS DE NOMINA ☐ HISTORIAL DEL TRABAJADOR ☐ OTROS (indicar) ……. ……. ……. …….
Datos de información comercial	**Datos económico – financieros**
☐ ACTIVIDADES Y NEGOCIOS ☐ LICENCIAS COMERCIALES ☐ SUSCRIPCIONES A PUBLICACIONES / MEDIOS DE COMUNICACIÓN ☐ CREACIONES ARTISTICAS, LITERARIAS, CIENTIFICAS O TECNICAS ☐ OTROS (indicar) ……. ……. ……. …….	☐ INGRESOS RENTAS ☐ INVERSIONES, BIENES PATRIMONIALES ▣ CREDITOS, PRESTAMOS, AVALES ▣ DATOS BANCARIOS (Cuentas…) ☐ PLANES DE PENSIONES, JUBILACION ▣ DATOS ECONOMICOS DE NOMINA ▣ SEGUROS ☐ HIPOTECAS ▣ SUBSIDIOS, BENEFICIOS ☐ HISTORIAL CREDITOS ▣ TARJETAS CREDITO ☐ OTROS (indicar) ……. ……. ……. …….
Datos de transacciones	
☐ BIENES Y SERVICIOS SUMINISTRADOS POR EL AFECTADO ▣ BIENES Y SERVICIOS RECIBIDOS POR EL AFECTADO ▣ TRANSACCIONES FINANCIERAS ☐ COMPENSACIONES / INDEMNIZACIONES ☐ OTROS (indicar) ……. ……. ……. …….	

4.2.2.- Base de Datos INFORMACIO

Responsable:		**Descripción del fichero**
Aplicativo:	PCRM	Datos de personas externas que han solicitado a la UOC información acerca de sus servicios.
Fichero:	INFORMACIO	
Tipo:	Oracle	
Ubicación:	Senegal.uoc.es	

Datos especialmente protegidos
☐ IDEOLOGIA ☐ CREENCIAS ☐ RELIGION (*)¿Han sido recabados con consentimiento expreso y por escrito del afectado? SI π NO π
Otros datos especialmente protegidos
☐ ORIGEN RACIAL ☐ SALUD ☐ VIDA SEXUAL (*)¿Han sido recabados con consentimiento expreso y por escrito del afectado? SI π NO π
(*) En caso negativo, especifique la Ley que exime del consentimiento expreso por razones de interés general. Nº Ley ☐☐☐☐ Año ☐☐☐☐ **Indicar la Ley referida**

Datos de carácter identificativo	**Datos de características personales**
▣ DNI / NIF ☐ N SS/ MUTUALIDAD ▣ NOMBRE Y APELLIDOS ▣ DIRECCION ▣ TELEFONO ☐ FIRMA /HUELLA ☐ IMAGEN / VOZ ☐ MARCAS FISICAS ▣ OTROS (indicar) ……. Dirección e-mail.....…….. ……. …….	▣ DATOS DE ESTADO CIVIL ☐ DATOS DE FAMILIA ▣ FECHA / LUGAR DE NACIMIENTO ☐ CARACTERISTICAS FISICAS O ANTROPOMETRICAS ▣ SEXO ☐ NACIONALIDAD ☐ LENGUA MATERNA ▣ OTROS (indicar) - Uso de ordenador.…… - Uso de Internet…….. - Medio de contacto con la UOC.…… …….
Datos de circunstancias sociales	
☐ CARACTERISTICAS DE NACIMIENTO, VIVIENDA ☐ SITUACION MILITAR ☐ PROPIEDADES, POSESIONES ☐ AFICIONES Y ESTILO DE VIDA ☐ PERTENENCIA A CLUBES, ASOCIACIONES... ☐ LICENCIAS, PERMISOS, AUTORIZACIONES ☐ OTROS (indicar) ……. ……. …….	

Datos académicos y profesionales	**Datos de detalle del empleo**
▣ FORMACION, TITULACIONES ☐ HISTORIAL DEL ESTUDIANTE ☐ EXPERIENCIA PROFESIONAL ☐ PERTENENCIA ASOCIACIONES PROFESIONALES ☐ OTROS (indicar) ……. ……. ……. …….	▣ PROFESION ☐ PUESTOS DE TRABAJO ☐ DATOS NO ECONOMICOS DE NOMINA ☐ HISTORIAL DEL TRABAJADOR ▣ OTROS (indicar) - Sector de actividad de la empresa... ……. ……. …….
Datos de información comercial	**Datos económico – financieros**
☐ ACTIVIDADES Y NEGOCIOS ☐ LICENCIAS COMERCIALES ☐ SUSCRIPCIONES A PUBLICACIONES / MEDIOS DE COMUNICACIÓN ☐ CREACIONES ARTISTICAS, LITERARIAS, CIENTIFICAS O TECNICAS ☐ OTROS (indicar) ……. ……. ……. …….	☐ INGRESOS RENTAS ☐ INVERSIONES, BIENES PATRIMONIALES ☐ CREDITOS, PRESTAMOS, AVALES ☐ DATOS BANCARIOS (Cuentas...) ☐ PLANES DE PENSIONES, JUBILACION ☐ DATOS ECONOMICOS DE NOMINA ☐ SEGUROS ☐ HIPOTECAS ☐ SUBSIDIOS, BENEFICIOS ☐ HISTORIAL CREDITOS ☐ TARJETAS CREDITO ☐ OTROS (indicar) ……. ……. ……. …….
Datos de transacciones	
☐ BIENES Y SERVICIOS SUMINISTRADOS POR EL AFECTADO ☐ BIENES Y SERVICIOS RECIBIDOS POR EL AFECTADO ☐ TRANSACCIONES FINANCIERAS ☐ COMPENSACIONES / INDEMNIZACIONES ☐ OTROS (indicar) ……. ……. ……. …….	

4.2.3.- Base de Datos FORMACIO CONTINUADA

Responsable:		**Descripción del fichero**
Aplicativo:	GAT FORMACIÓ	Información de los alumnos matriculados en los cursos de posgrado y seminarios de la UOC.
Fichero:	FORMACIO CONTINUADA	
Tipo:	Oracle	
Ubicación:	Brunei.uoc.es	

Datos especialmente protegidos

☐ IDEOLOGIA
☐ CREENCIAS
☐ RELIGION

(*)¿Han sido recabados con consentimiento expreso y por escrito del afectado?

SI π NO π

Otros datos especialmente protegidos

☐ ORIGEN RACIAL
☐ SALUD
☐ VIDA SEXUAL

(*)¿Han sido recabados con consentimiento expreso y por escrito del afectado?

SI π NO π

(*) En caso negativo, especifique la Ley que exime del consentimiento expreso por razones de interés general.

Nº Ley ☐ Año ☐☐☐☐

Indicar la Ley referida

Datos de carácter identificativo	**Datos de características personales**
▣ DNI / NIF	▣ DATOS DE ESTADO CIVIL
▣ N SS/ MUTUALIDAD	▣ DATOS DE FAMILIA
▣ NOMBRE Y APELLIDOS	☐ FECHA / LUGAR DE NACIMIENTO
▣ DIRECCION	☐ CARACTERISTICAS FISICAS O ANTROPOMETRICAS
▣ TELEFONO	▣ SEXO
▣ FIRMA /HUELLA	▣ NACIONALIDAD
▣ IMAGEN / VOZ	☐ LENGUA MATERNA
☐ MARCAS FISICAS	☐ OTROS (indicar)
▣ OTROS (indicar)	.....
.....	.....
- Dirección de envio.....	.....
.....	.....
.....	

Datos de circunstancias sociales	
▣ CARACTERISTICAS DE NACIMIENTO, VIVIENDA	
☐ SITUACION MILITAR	
☐ PROPIEDADES, POSESIONES	
☐ AFICIONES Y ESTILO DE VIDA	
☐ PERTENENCIA A CLUBES, ASOCIACIONES...	
☐ LICENCIAS, PERMISOS, AUTORIZACIONES	
☐ OTROS (indicar)	
.....	
.....	
.....	

Datos académicos y profesionales	**Datos de detalle del empleo**
▣ FORMACION, TITULACIONES ▣ HISTORIAL DEL ESTUDIANTE ▣ EXPERIENCIA PROFESIONAL ☐ PERTENENCIA ASOCIACIONES PROFESIONALES ☐ OTROS (indicar) …… …… …… ……	▣ PROFESION ▣ PUESTOS DE TRABAJO ☐ DATOS NO ECONOMICOS DE NOMINA ☐ HISTORIAL DEL TRABAJADOR ☐ OTROS (indicar) …… …… …… ……
Datos de información comercial	**Datos económico – financieros**
☐ ACTIVIDADES Y NEGOCIOS ☐ LICENCIAS COMERCIALES ☐ SUSCRIPCIONES A PUBLICACIONES / MEDIOS DE COMUNICACIÓN ☐ CREACIONES ARTISTICAS, LITERARIAS, CIENTIFICAS O TECNICAS ☐ OTROS (indicar) …… …… …… ……	☐ INGRESOS RENTAS ☐ INVERSIONES, BIENES PATRIMONIALES ▣ CREDITOS, PRESTAMOS, AVALES ▣ DATOS BANCARIOS (Cuentas...) ☐ PLANES DE PENSIONES, JUBILACION ☐ DATOS ECONOMICOS DE NOMINA ☐ SEGUROS ☐ HIPOTECAS ☐ SUBSIDIOS, BENEFICIOS ☐ HISTORIAL CREDITOS ☐ TARJETAS CREDITO ☐ OTROS (indicar) …… …… …… ……
Datos de transacciones	
☐ BIENES Y SERVICIOS SUMINISTRADOS POR EL AFECTADO ☐ BIENES Y SERVICIOS RECIBIDOS POR EL AFECTADO ☐ TRANSACCIONES FINANCIERAS ☐ COMPENSACIONES / INDEMNIZACIONES ☐ OTROS (indicar) …… …… …… ……	

4.2.4.- Base de Datos PERSONAL

Responsable:		**Descripción del fichero**
Aplicativo:	CURRO	Datos para la confección de la nómina del personal de la UOC y para el mantenimiento del historial profesional de los trabajadores.
Fichero:	PERSONAL	
Tipo:	Oracle	
Ubicación:	Ruanda.uoc.es	

Datos especialmente protegidos

☐ IDEOLOGIA
☐ CREENCIAS
☐ RELIGION

(*)¿Han sido recabados con consentimiento expreso y por escrito del afectado?

SI π NO π

Otros datos especialmente protegidos

☐ ORIGEN RACIAL
☐ SALUD
☐ VIDA SEXUAL

(*)¿Han sido recabados con consentimiento expreso y por escrito del afectado?

SI π NO π

(*) En caso negativo, especifique la Ley que exime del consentimiento expreso por razones de interés general.

Nº Ley ☐ Año ☐☐☐☐

Indicar la Ley referida

Datos de carácter identificativo	**Datos de características personales**
▣ DNI / NIF	▣ DATOS DE ESTADO CIVIL
▣ N SS/ MUTUALIDAD	▣ DATOS DE FAMILIA
▣ NOMBRE Y APELLIDOS	▣ FECHA / LUGAR DE NACIMIENTO
▣ DIRECCION	☐ CARACTERISTICAS FISICAS O ANTROPOMETRICAS
▣ TELEFONO	▣ SEXO
☐ FIRMA /HUELLA	☐ NACIONALIDAD
☐ IMAGEN / VOZ	☐ LENGUA MATERNA
☐ MARCAS FISICAS	☐ OTROS (indicar)
☐ OTROS (indicar)	.....
.....	.....
.....	.....
.....	.....
.....	

Datos de circunstancias sociales	
☐ CARACTERISTICAS DE NACIMIENTO, VIVIENDA	
☐ SITUACION MILITAR	
☐ PROPIEDADES, POSESIONES	
☐ AFICIONES Y ESTILO DE VIDA	
☐ PERTENENCIA A CLUBES, ASOCIACIONES...	
☐ LICENCIAS, PERMISOS, AUTORIZACIONES	
☐ OTROS (indicar)	
.....	
.....	
.....	
.....	

Datos académicos y profesionales	**Datos de detalle del empleo**
▣ FORMACION, TITULACIONES ☐ HISTORIAL DEL ESTUDIANTE ☐ EXPERIENCIA PROFESIONAL ☐ PERTENENCIA ASOCIACIONES PROFESIONALES ☐ OTROS (indicar) …… …… …… ……	▣ PROFESION ▣ PUESTOS DE TRABAJO ☐ DATOS NO ECONOMICOS DE NOMINA ▣ HISTORIAL DEL TRABAJADOR ☐ OTROS (indicar) …… …… …… ……
Datos de información comercial	**Datos económico – financieros**
☐ ACTIVIDADES Y NEGOCIOS ☐ LICENCIAS COMERCIALES ☐ SUSCRIPCIONES A PUBLICACIONES / MEDIOS DE COMUNICACIÓN ☐ CREACIONES ARTISTICAS, LITERARIAS, CIENTIFICAS O TECNICAS ☐ OTROS (indicar) …… …… …… ……	☐ INGRESOS RENTAS ☐ INVERSIONES, BIENES PATRIMONIALES ☐ CREDITOS, PRESTAMOS, AVALES ▣ DATOS BANCARIOS (Cuentas...) ☐ PLANES DE PENSIONES, JUBILACION ▣ DATOS ECONOMICOS DE NOMINA ☐ SEGUROS ☐ HIPOTECAS ☐ SUBSIDIOS, BENEFICIOS ☐ HISTORIAL CREDITOS ☐ TARJETAS CREDITO ☐ OTROS (indicar) …… …… …… ……
Datos de transacciones	
☐ BIENES Y SERVICIOS SUMINISTRADOS POR EL AFECTADO ☐ BIENES Y SERVICIOS RECIBIDOS POR EL AFECTADO ☐ TRANSACCIONES FINANCIERAS ☐ COMPENSACIONES / INDEMNIZACIONES ☐ OTROS (indicar) …… …… …… ……	

4.2.5.- Base de Datos GESTIO COMPTABLE

Responsable:		**Descripción del fichero**
Aplicativo:	COFROS	Contabilidad de la UOC
Fichero:	GESTIO COMPTABLE	
Tipo:	Oracle	
Ubicación:	Benin.uoc.es	

Datos especialmente protegidos

☐ IDEOLOGIA
☐ CREENCIAS
☐ RELIGION

(*)¿Han sido recabados con consentimiento expreso y por escrito del afectado?

SI π NO π

Otros datos especialmente protegidos

☐ ORIGEN RACIAL
☐ SALUD
☐ VIDA SEXUAL

(*)¿Han sido recabados con consentimiento expreso y por escrito del afectado?

SI π NO π

(*) En caso negativo, especifique la Ley que exime del consentimiento expreso por razones de interés general.

Nº Ley ☐ Año ☐☐☐☐

Indicar la Ley referida

Datos de carácter identificativo	**Datos de características personales**
▣ DNI / NIF	☐ DATOS DE ESTADO CIVIL
☐ N SS/ MUTUALIDAD	☐ DATOS DE FAMILIA
▣ NOMBRE Y APELLIDOS	☐ FECHA / LUGAR DE NACIMIENTO
▣ DIRECCION	☐ CARACTERISTICAS FISICAS O ANTROPOMETRICAS
☐ TELEFONO	☐ SEXO
☐ FIRMA /HUELLA	▣ NACIONALIDAD
☐ IMAGEN / VOZ	☐ LENGUA MATERNA
☐ MARCAS FISICAS	☐ OTROS (indicar)
☐ OTROS (indicar)	.....
.....	.....
.....	.....
.....	.....
.....	

Datos de circunstancias sociales	
☐ CARACTERISTICAS DE NACIMIENTO, VIVIENDA	
☐ SITUACION MILITAR	
☐ PROPIEDADES, POSESIONES	
☐ AFICIONES Y ESTILO DE VIDA	
☐ PERTENENCIA A CLUBES, ASOCIACIONES...	
☐ LICENCIAS, PERMISOS, AUTORIZACIONES	
☐ OTROS (indicar)	
.....	
.....	
.....	
.....	

Datos académicos y profesionales	**Datos de detalle del empleo**
☐ FORMACION, TITULACIONES ☐ HISTORIAL DEL ESTUDIANTE ☐ EXPERIENCIA PROFESIONAL ☐ PERTENENCIA ASOCIACIONES PROFESIONALES ☐ OTROS (indicar) ……. ……. ……. ……	☐ PROFESION ☐ PUESTOS DE TRABAJO ☐ DATOS NO ECONOMICOS DE NOMINA ☐ HISTORIAL DEL TRABAJADOR ☐ OTROS (indicar) ……. ……. ……. ……
Datos de información comercial	**Datos económico – financieros**
☐ ACTIVIDADES Y NEGOCIOS ☐ LICENCIAS COMERCIALES ☐ SUSCRIPCIONES A PUBLICACIONES / MEDIOS DE COMUNICACIÓN ☐ CREACIONES ARTISTICAS, LITERARIAS, CIENTIFICAS O TECNICAS ☐ OTROS (indicar) ……. ……. ……. ……	☐ INGRESOS RENTAS ☐ INVERSIONES, BIENES PATRIMONIALES ☐ CREDITOS, PRESTAMOS, AVALES ▣ DATOS BANCARIOS (Cuentas…) ☐ PLANES DE PENSIONES, JUBILACION ☐ DATOS ECONOMICOS DE NOMINA ☐ SEGUROS ☐ HIPOTECAS ☐ SUBSIDIOS, BENEFICIOS ☐ HISTORIAL CREDITOS ☐ TARJETAS CREDITO ☐ OTROS (indicar) ……. ……. ……. …….
Datos de transacciones	
☐ BIENES Y SERVICIOS SUMINISTRADOS POR EL AFECTADO ☐ BIENES Y SERVICIOS RECIBIDOS POR EL AFECTADO ▣ TRANSACCIONES FINANCIERAS ☐ COMPENSACIONES / INDEMNIZACIONES ▣ OTROS (indicar) - Facturas ……. - Recibos…… - Cobros/Pagos…… …….	

4.2.6.- Base de Datos TRAMESES

Responsable:		**Descripción del fichero**
Aplicativo:	GAME	Distribución de material didáctico
Fichero:	TRAMESES	
Tipo:	Oracle	
Ubicación:	Senegal.uoc.es	

Datos especialmente protegidos

☐ IDEOLOGIA
☐ CREENCIAS
☐ RELIGION

(*)¿Han sido recabados con consentimiento expreso y por escrito del afectado?

SI π NO π

Otros datos especialmente protegidos

☐ ORIGEN RACIAL
☐ SALUD
☐ VIDA SEXUAL

(*)¿Han sido recabados con consentimiento expreso y por escrito del afectado?

SI π NO π

(*) En caso negativo, especifique la Ley que exime del consentimiento expreso por razones de interés general.

Nº Ley ☐ Año ☐☐☐☐

Indicar la Ley referida

Datos de carácter identificativo	**Datos de características personales**
▣ DNI / NIF	☐ DATOS DE ESTADO CIVIL
☐ N SS/ MUTUALIDAD	☐ DATOS DE FAMILIA
▣ NOMBRE Y APELLIDOS	☐ FECHA / LUGAR DE NACIMIENTO
▣ DIRECCION	☐ CARACTERISTICAS FISICAS O ANTROPOMETRICAS
▣ TELEFONO	☐ SEXO
☐ FIRMA /HUELLA	☐ NACIONALIDAD
☐ IMAGEN / VOZ	☐ LENGUA MATERNA
☐ MARCAS FISICAS	☐ OTROS (indicar)
☐ OTROS (indicar)	.....
.....	.....
.....	.....
.....	.....
.....	.....

Datos de circunstancias sociales	
☐ CARACTERISTICAS DE NACIMIENTO, VIVIENDA	
☐ SITUACION MILITAR	
☐ PROPIEDADES, POSESIONES	
☐ AFICIONES Y ESTILO DE VIDA	
☐ PERTENENCIA A CLUBES, ASOCIACIONES...	
☐ LICENCIAS, PERMISOS, AUTORIZACIONES	
☐ OTROS (indicar)	
.....	
.....	
.....	
.....	

Datos académicos y profesionales	**Datos de detalle del empleo**
☐ FORMACION, TITULACIONES ☐ HISTORIAL DEL ESTUDIANTE ☐ EXPERIENCIA PROFESIONAL ☐ PERTENENCIA ASOCIACIONES PROFESIONALES ☐ OTROS (indicar) …… …… …… ……	☐ PROFESION ☐ PUESTOS DE TRABAJO ☐ DATOS NO ECONOMICOS DE NOMINA ☐ HISTORIAL DEL TRABAJADOR ☐ OTROS (indicar) …… …… …… ……
Datos de información comercial	**Datos económico – financieros**
☐ ACTIVIDADES Y NEGOCIOS ☐ LICENCIAS COMERCIALES ☐ SUSCRIPCIONES A PUBLICACIONES / MEDIOS DE COMUNICACIÓN ☐ CREACIONES ARTISTICAS, LITERARIAS, CIENTIFICAS O TECNICAS ☐ OTROS (indicar) …… …… …… ……	☐ INGRESOS RENTAS ☐ INVERSIONES, BIENES PATRIMONIALES ☐ CREDITOS, PRESTAMOS, AVALES ☐ DATOS BANCARIOS (Cuentas…) ☐ PLANES DE PENSIONES, JUBILACION ☐ DATOS ECONOMICOS DE NOMINA ☐ SEGUROS ☐ HIPOTECAS ☐ SUBSIDIOS, BENEFICIOS ☐ HISTORIAL CREDITOS ☐ TARJETAS CREDITO ☐ OTROS (indicar) …… …… …… ……
Datos de transacciones	
☐ BIENES Y SERVICIOS SUMINISTRADOS POR EL AFECTADO ☐ BIENES Y SERVICIOS RECIBIDOS POR EL AFECTADO ☐ TRANSACCIONES FINANCIERAS ☐ COMPENSACIONES / INDEMNIZACIONES ☐ OTROS (indicar) …… …… …… ……	

4.2.7.- Base de Datos CAMPUS VIRTUAL

Responsable:		**Descripción del fichero**
Aplicativo:	CAMPUS VIRTUAL	Administración de conexiones al Campus Virtual de la UOC.
Fichero:	CAMPUS VIRTUAL	
Tipo:	Oracle	
Ubicación:	Cuba.uoc.es	

Datos especialmente protegidos

☐ IDEOLOGIA
☐ CREENCIAS
☐ RELIGION

(*)¿Han sido recabados con consentimiento expreso y por escrito del afectado?

SI π NO π

Otros datos especialmente protegidos

☐ ORIGEN RACIAL
☐ SALUD
☐ VIDA SEXUAL

(*)¿Han sido recabados con consentimiento expreso y por escrito del afectado?

SI π NO π

(*) En caso negativo, especifique la Ley que exime del consentimiento expreso por razones de interés general.

Nº Ley ☐ Año ☐☐☐☐

Indicar la Ley referida

Datos de carácter identificativo	**Datos de características personales**
▣ DNI / NIF	☐ DATOS DE ESTADO CIVIL
☐ N SS/ MUTUALIDAD	☐ DATOS DE FAMILIA
▣ NOMBRE Y APELLIDOS	▣ FECHA / LUGAR DE NACIMIENTO
▣ DIRECCION	☐ CARACTERISTICAS FISICAS O ANTROPOMETRICAS
☐ TELEFONO	▣ SEXO
☐ FIRMA /HUELLA	☐ NACIONALIDAD
▣ IMAGEN / VOZ	☐ LENGUA MATERNA
☐ MARCAS FISICAS	☐ OTROS (indicar)
☐ OTROS (indicar)	.....
.....	.....
.....	.....
.....	.....
.....	.....

Datos de circunstancias sociales	
☐ CARACTERISTICAS DE NACIMIENTO, VIVIENDA	
☐ SITUACION MILITAR	
☐ PROPIEDADES, POSESIONES	
☐ AFICIONES Y ESTILO DE VIDA	
☐ PERTENENCIA A CLUBES, ASOCIACIONES...	
☐ LICENCIAS, PERMISOS, AUTORIZACIONES	
☐ OTROS (indicar)	
.....	
.....	
.....	
.....	

Datos académicos y profesionales	**Datos de detalle del empleo**
☐ FORMACION, TITULACIONES ☐ HISTORIAL DEL ESTUDIANTE ☐ EXPERIENCIA PROFESIONAL ☐ PERTENENCIA ASOCIACIONES PROFESIONALES ▣ OTROS (indicar) …… - Curriculum personal …… …… ……	☐ PROFESION ☐ PUESTOS DE TRABAJO ☐ DATOS NO ECONOMICOS DE NOMINA ☐ HISTORIAL DEL TRABAJADOR ☐ OTROS (indicar) …… …… …… ……
Datos de información comercial	**Datos económico – financieros**
☐ ACTIVIDADES Y NEGOCIOS ☐ LICENCIAS COMERCIALES ☐ SUSCRIPCIONES A PUBLICACIONES / MEDIOS DE COMUNICACIÓN ☐ CREACIONES ARTISTICAS, LITERARIAS, CIENTIFICAS O TECNICAS ☐ OTROS (indicar) …… …… …… ……	☐ INGRESOS RENTAS ☐ INVERSIONES, BIENES PATRIMONIALES ☐ CREDITOS, PRESTAMOS, AVALES ☐ DATOS BANCARIOS (Cuentas…) ☐ PLANES DE PENSIONES, JUBILACION ☐ DATOS ECONOMICOS DE NOMINA ☐ SEGUROS ☐ HIPOTECAS ☐ SUBSIDIOS, BENEFICIOS ☐ HISTORIAL CREDITOS ☐ TARJETAS CREDITO ☐ OTROS (indicar) …… …… …… ……
Datos de transacciones	
☐ BIENES Y SERVICIOS SUMINISTRADOS POR EL AFECTADO ☐ BIENES Y SERVICIOS RECIBIDOS POR EL AFECTADO ☐ TRANSACCIONES FINANCIERAS ☐ COMPENSACIONES / INDEMNIZACIONES ☐ OTROS (indicar) …… …… …… ……	

4.2.8.- Base de Datos CLUB

Responsable:		**Descripción del fichero**
Aplicativo:	CLUB	Dades personals dels socis
Fichero:	CLUB	
Tipo:	ORACLE	
Ubicación:	Brunei.uoc.es	

Datos especialmente protegidos
☐ IDEOLOGIA ☐ CREENCIAS ☐ RELIGION (*)¿Han sido recabados con consentimiento expreso y por escrito del afectado? SI π NO π
Otros datos especialmente protegidos
☐ ORIGEN RACIAL ☐ SALUD ☐ VIDA SEXUAL (*)¿Han sido recabados con consentimiento expreso y por escrito del afectado? SI π NO π
(*) En caso negativo, especifique la Ley que exime del consentimiento expreso por razones de interés general. Nº Ley ☐☐☐☐☐ Año ☐☐☐☐ **Indicar la Ley referida**

Datos de carácter identificativo	**Datos de características personales**
■ DNI / NIF ☐ N SS/ MUTUALIDAD ■ NOMBRE Y APELLIDOS ■ DIRECCION ■ TELEFONO ☐ FIRMA /HUELLA ☐ IMAGEN / VOZ ☐ MARCAS FISICAS ☐ OTROS (indicar) …… …… …… ……	☐ DATOS DE ESTADO CIVIL ☐ DATOS DE FAMILIA ■ FECHA / LUGAR DE NACIMIENTO ☐ CARACTERISTICAS FISICAS O ANTROPOMETRICAS ■ SEXO ■ NACIONALIDAD ☐ LENGUA MATERNA ☐ OTROS (indicar) …… …… …… ……
Datos de circunstancias sociales	
☐ CARACTERISTICAS DE NACIMIENTO, VIVIENDA ☐ SITUACION MILITAR ☐ PROPIEDADES, POSESIONES ☐ AFICIONES Y ESTILO DE VIDA ☐ PERTENENCIA A CLUBES, ASOCIACIONES... ☐ LICENCIAS, PERMISOS, AUTORIZACIONES ☐ OTROS (indicar) …… …… …… ……	

Datos académicos y profesionales	**Datos de detalle del empleo**
☐ FORMACION, TITULACIONES ☐ HISTORIAL DEL ESTUDIANTE ☐ EXPERIENCIA PROFESIONAL ☐ PERTENENCIA ASOCIACIONES PROFESIONALES ☐ OTROS (indicar) ……. ……. ……. ……	☐ PROFESION ☐ PUESTOS DE TRABAJO ☐ DATOS NO ECONOMICOS DE NOMINA ☐ HISTORIAL DEL TRABAJADOR ☐ OTROS (indicar) ……. ……. ……. ……
Datos de información comercial	**Datos económico – financieros**
☐ ACTIVIDADES Y NEGOCIOS ☐ LICENCIAS COMERCIALES ☐ SUSCRIPCIONES A PUBLICACIONES / MEDIOS DE COMUNICACIÓN ☐ CREACIONES ARTISTICAS, LITERARIAS, CIENTIFICAS O TECNICAS ☐ OTROS (indicar) ……. ……. ……. ……	☐ INGRESOS RENTAS ☐ INVERSIONES, BIENES PATRIMONIALES ☐ CREDITOS, PRESTAMOS, AVALES ☐ DATOS BANCARIOS (Cuentas…) ☐ PLANES DE PENSIONES, JUBILACION ☐ DATOS ECONOMICOS DE NOMINA ☐ SEGUROS ☐ HIPOTECAS ☐ SUBSIDIOS, BENEFICIOS ☐ HISTORIAL CREDITOS ☐ TARJETAS CREDITO ☐ OTROS (indicar) ……. ……. ……. …….
Datos de transacciones	
☐ BIENES Y SERVICIOS SUMINISTRADOS POR EL AFECTADO ☐ BIENES Y SERVICIOS RECIBIDOS POR EL AFECTADO ☐ TRANSACCIONES FINANCIERAS ☐ COMPENSACIONES / INDEMNIZACIONES ☐ OTROS (indicar) ……. ……. ……. …….	

4.2.9.- Base de Datos EVIU

Responsable:		**Descripción del fichero**
Aplicativo:	EVIU	Dades personals dels alumnes
Fichero:	EVIU	
Tipo:	ORACLE	
Ubicación:	Brunei.uoc.es	

Datos especialmente protegidos
☐ IDEOLOGIA ☐ CREENCIAS ☐ RELIGION (*)¿Han sido recabados con consentimiento expreso y por escrito del afectado? SI π NO π
Otros datos especialmente protegidos

☐ ORIGEN RACIAL
☐ SALUD
☐ VIDA SEXUAL

(*)¿Han sido recabados con consentimiento expreso y por escrito del afectado?

SI π NO π

(*) En caso negativo, especifique la Ley que exime del consentimiento expreso por razones de interés general.

Nº Ley ☐☐☐☐ Año ☐☐☐☐

Indicar la Ley referida

Datos de carácter identificativo	**Datos de características personales**
■ DNI / NIF	☐ DATOS DE ESTADO CIVIL
☐ N SS/ MUTUALIDAD	☐ DATOS DE FAMILIA
■ NOMBRE Y APELLIDOS	■ FECHA / LUGAR DE NACIMIENTO
■ DIRECCION	☐ CARACTERISTICAS FISICAS O ANTROPOMETRICAS
■ TELEFONO	■ SEXO
☐ FIRMA /HUELLA	■ NACIONALIDAD
☐ IMAGEN / VOZ	☐ LENGUA MATERNA
☐ MARCAS FISICAS	☐ OTROS (indicar)
☐ OTROS (indicar)	.....
.....	.....
.....	.....
.....	.....
.....	.....
Datos de circunstancias sociales	
☐ CARACTERISTICAS DE NACIMIENTO, VIVIENDA	
☐ SITUACION MILITAR	
☐ PROPIEDADES, POSESIONES	
☐ AFICIONES Y ESTILO DE VIDA	
☐ PERTENENCIA A CLUBES, ASOCIACIONES...	
☐ LICENCIAS, PERMISOS, AUTORIZACIONES	
☐ OTROS (indicar)	
.....	
.....	
.....	
.....	
Datos académicos y profesionales	**Datos de detalle del empleo**
■ FORMACION, TITULACIONES	☐ PROFESION
☐ HISTORIAL DEL ESTUDIANTE	☐ PUESTOS DE TRABAJO
☐ EXPERIENCIA PROFESIONAL	☐ DATOS NO ECONOMICOS DE NOMINA
☐ PERTENENCIA ASOCIACIONES PROFESIONALES	☐ HISTORIAL DEL TRABAJADOR
OTROS (indicar)	☐ OTROS (indicar)
.....	.....
-	.....
.....	.....
.....	.....
Datos de información comercial	**Datos económico – financieros**

☐ ACTIVIDADES Y NEGOCIOS ☐ LICENCIAS COMERCIALES ☐ SUSCRIPCIONES A PUBLICACIONES / MEDIOS DE COMUNICACIÓN ☐ CREACIONES ARTISTICAS, LITERARIAS, CIENTIFICAS O TECNICAS ☐ OTROS (indicar) ……. ……. ……. …….	☐ INGRESOS RENTAS ☐ INVERSIONES, BIENES PATRIMONIALES ☐ CREDITOS, PRESTAMOS, AVALES ■ DATOS BANCARIOS (Cuentas...) ☐ PLANES DE PENSIONES, JUBILACION ☐ DATOS ECONOMICOS DE NOMINA ☐ SEGUROS ☐ HIPOTECAS ☐ SUBSIDIOS, BENEFICIOS ☐ HISTORIAL CREDITOS ☐ TARJETAS CREDITO ☐ OTROS (indicar) ……. ……. ……. …….
Datos de transacciones	
☐ BIENES Y SERVICIOS SUMINISTRADOS POR EL AFECTADO ☐ BIENES Y SERVICIOS RECIBIDOS POR EL AFECTADO ☐ TRANSACCIONES FINANCIERAS ☐ COMPENSACIONES / INDEMNIZACIONES ☐ OTROS (indicar) ……. ……. ……. …….	

4.3.- Topologia del sistema d'informació

4.3.1.- Distribució dels recursos

Per tal de donar suport a les necessitats informàtiques de les diferents àrees de la FUOC en els àmbits informatius i promocional, acadèmic, docent, gestió administrativa i suport tècnic als serveis interns de la FUOC i aquells oferts a tercers, el sistema informàtic s'estructura mitjançant diferents xarxes locals interconnectades als servidors centrals de gestió i de serveis.

En l'àrea pública la FUOC disposa d'un portal Web en què es presenta a la comunitat internacional informació sobre la institució, les activitats i els continguts de la formació impartida en els seus programes. Des del portal i amb els nivells adequats de seguretat exigits en aquest entorn, només les persones autoritzades com a usuaris de la comunitat UOC poden accedir mitjançant la seva identificació amb login i password a les àrees privades, establint aleshores els controls de seguretat propis de l'àrea privada.

En l'àrea privada, diferents subxarxes organitzen els recursos disponibles i gestionen els serveis oferts als usuaris, sempre sota les polítiques d'autoritzacions i de privilegis definides en aquest document i aplicades pels responsables d'administració de sistemes.

En un primer nivell de seguretat de l'àrea privada, es dóna accés al CAMPUS VIRTUAL, que ofereix un conjunt de serveis comuns a tots els membres autoritzats de la comunitat UOC. En un segon nivell de seguretat es troben totes les subxarxes

internes pròpies de la FUOC a les quals només té accés el personal administratiu, docent, de gestió i tècnic.

Tant l'accés a l'àrea privada com el posterior trànsit intern entre les diferents subxarxes està controlat per un sistema de FIREWALL radial que garanteix la seguretat d'accés i el diàleg entre els nodes a nivell físic.

En el nivell lògic, el sistema de control d'accessos TREN garanteix la implantació efectiva dels perfils d'usuari, gestionant les autoritzacions d'accés i els privilegis amb els quals es realitzen, molt especialment als recursos de gestió des dels quals es pot accedir als fitxers protegits i als aplicatius que els tracten.

De manera exclusiva el servei de suport extern (Bull) pot connectar-se a través d'un node RDSI, amb filtratge del número de trucada i login d'accés, per a la realització de les seves funcions.

Subxarxes:

- CAMPUS VIRTUAL
- XARXA INTERNA
- GESTIÓ
- ALTRES
- DESENVOLUPAMENT

Bàsicament el gros dels recursos que donen suport al sistema informàtic es troben ubicats en els locals de la seu central (UOC), excepte tres servidors de Xarxa Interna que es troben instal·lats en els locals de Diputació, Drassanes i Castelldefels.

LOCAL	***DOMICILI***
UOC	FUNDACIÓ PER A LA UNIVERSITAT OBERTA DE CATALUNYA Àrea de Sistemes d'Informació Av. del Tibidabo, 39-43 08035 Barcelona
Diputació	UOC-Diputació C/ Diputació, 219 08011 Barcelona
Drassanes	Centre Suport Barcelonès Av. Drassanes, 3-5 08001 Barcelona
Castelldefels	Planeta UOC Av. Canal Olímpic, s/n Parc Mediterrani de la Tecnologia 08860 Castelldefels

4.3.2.- Ubicació de servidors i de fitxers protegits

Tots els servidors on s'emmagatzemen els fitxers protegits, que contenen dades de caràcter personal, es troben ubicats en els locals de la seu central de la FUOC i corresponen a la distribució següent:

LOCAL	***ÀREA***	***SERVIDOR***	***S.O.***	***FITXERS***
UOC	Sistemes d'Informació	Senegal.uoc.es	Unix	- GAT - INFORMACIÓ

		Liberia.uoc.es	Unix	- PERSONAL - TRAMESES
		Cuba.uoc.es	Unix	- CAMPUS VIRTUAL
		Brunei.uoc.es	Unix	- FORMACIÓ CONTINUADA
		Uoc-escarola.uoc.es	Win-NT	- GESTIÓ COMPTABLE

4.4.- Seguretat física

Els locals en què es troben ubicats els servidors centrals que donen suport a la xarxa corporativa estan protegits per les mesures de seguretat següents:

FUNDACIÓ PER A LA UNIVERSITAT OBERTA DE CATALUNYA
Àrea de Sistemes d'Informació
Av. Tibidabo, 39-43
08035 Barcelona

Accés a l'edifici

L'accés a l'edifici està vigilat les 24 hores per personal de la FUOC en horari diürn i per un vigilant d'una empresa de seguretat la resta de les hores.

Sala d'ordinadors

Accés

L'accés a la sala d'ordinadors, on s'ubiquen tots els servidors de fitxers, és prohibit a tot el personal aliè a l'àrea esmentada. El personal autoritzat disposa de claus per a activar els tancaments amb clau numèrica en les dues portes d'accés a la sala.

Sistema contra incendis

Dispositius d'alarma i sistemes contra incendis basat en:

- 2 bombones de 80 Kg de gas FE-13
- 2 bombones de 40 Kg de gas FE-13
- 8 detectors de fum iònics repartits en sostre i fals terra
- 10 difusors de 360º
- 3 avisadors acústics
- 1 central d'alarmes multizona

Sistema de detecció d'humitat

- 1 central d'alarmes multizona
- 6 detectors d'humitat

4.5.- Seguretat lògica

4.5.1.- Sistema d'autenticació

4.5.1.1. Identificació

1. Tots els usuaris del sistema informàtic de la FUOC són identificats en el moment de cursar-ne l'alta com a treballadors, mitjançant fotocòpia del DNI, passaport o targeta de residència.

2. Tots els usuaris no empleats de la FUOC que per diferents motius han de tenir accés al sistema informàtic seran identificats en el moment de sol·licitar-ne l'alta per mitjà d'un document acreditatiu (DNI, passaport, etc....) que doni fe inequívoca de la seva identitat.

3. Els responsables de grup operatiu, o personal autoritzat per ells, seran responsables de la identificació de les persones per a les quals es sol·licita l'alta com a usuari del sistema i, de la mateixa manera, seran ells els únics autoritzats per a tramitar la sol·licitud.

4. Abans de cursar la sol·licitud de l'alta com a usuari del sistema, es comprova que el document utilitzat per a la identificació estigui en vigor i sense senyals de manipulació.

5. Per al personal de la FUOC, i sempre que no sigui possible per a la resta d'usuaris, es sol·licita una fotografia de l'usuari a fi i efecte que, un cop digitalitzada, figuri en la base de dades del personal de la FUOC.

6. La sol·licitud es cursarà via e-mail als administradors de CAMPUS i XARXA INTERNA, depenent de les necessitats de l'usuari a crear. A l'e-mail s'indicarà la referència documental d'identificació de l'usuari (DNI, passaport, etc...), l'àrea o grup operatiu i el responsable sol·licitant.

7. Els administradors mantindran un registre de les sol·licituds presentades, i en cap cas no gestionaran peticions sense la deguda referència documental o que procedeixin d'un responsable no autoritzat.

8. Sempre que circumstancialment s'hagin d'aplicar procediments de generació massiva d'identificadors potencials (prematriculació), el responsable del fitxer i el responsable del grup operatiu implicat dissenyaran, en col·laboració amb el responsable de seguretat i el director de l'Àrea de Sistemes d'Informació, els mecanismes de control que hagin d'aplicar-se per tal de garantir la seguretat del procés.

4.5.1.2. Autenticació

1. A cada usuari del sistema se li assigna un identificador i una clau en el nivell de CAMPUS.

2. Si és necessari i es tramita la sol·licitud corresponent, després de l'alta en CAMPUS, es procedeix a donar d'alta l'usuari en XARXA INTERNA, utilitzant el

mateix identificador d'usuari però amb una clau diferent.

3. Les claus utilitzades tenen una longitud mínima de sis caràcters i màxima de vuit.

4.5.1.3. Assignació de contrasenyes

1. És competència dels administradors d'usuari de CAMPUS i XARXA INTERNA, i dels grups operatius autoritzats, que l'atribució i la assignació de contrasenyes es realitzi de forma que es garanteixi la seva confidencialitat i integritat.

2. L'assignació de contrasenyes es realitzarà de manera automàtica. L'usuari estarà obligat a modificar la seva contrasenya en el primer accés al sistema i haurà de modificar-la periòdicament quan el sistema li ho sol·liciti.

3. En cap cas l'administrador no està capacitat per a conèixer la contrasenya d'un usuari. En cas de pèrdua o d'oblit de la contrasenya, la contrasenya anterior quedarà anul·lada amb caràcter general i es subministrarà una nova contrasenya a l'usuari.

4. Excepcionalment, s'executarà un procediment d'assignació automàtica d'identificadors i de claus per a usuaris potencials dins de l'àrea acadèmica per a cobrir els processos de matriculació. Aquests identificadors no seran efectius mentre l'àrea acadèmica no trameti la matriculació de l'estudiant, eliminant tots els identificadors no utilitzats. El grup operatiu d'Atenció a l' Estudiant serà el dipositari i el responsable de l'administració i de la custòdia de la informació esmentada.

5. Continuant amb el punt anterior, l'assignació de contrasenyes es realitzarà de forma automàtica pel sistema per a la primera donada a un usuari. L'usuari serà responsable de modificar immediatament la seva contrasenya en el primer accés al sistema, i cada cop que se li sol·liciti en els processos de renovació de contrasenyes automàtics.

6. Ocasionalment per als alumnes d'Iberoamèrica, el propi usuari genera el seu identificador i password inicial. En aquest cas, l'usuari tindrà un accés mínim al sistema, que es normalitzarà quan l'alumne formalitzi la seva matrícula i entri en el procés general de matriculació.

4.5.1.4. Distribució de contrasenyes

1. La distribució de contrasenyes del personal intern i del personal extern (i invitats) al qual circumstancialment s'hagi de donar accés al sistema, es realitzarà via e-mail al responsable de la sol·licitud per un mitjà segur, o bé comunicant-la directament a l'interessat.

2. La distribució de contrasenyes a l'alumnat es realitzarà en mà juntament amb la documentació de matriculació que es lliura a l'interessat.

3. En el seu primer accés al sistema, l'usuari estarà obligat a modificar la seva contrasenya. A partir d'aquest moment, l'usuari és l'únic responsable de l'ús i de la confidencialitat de la seva contrasenya, i haurà de modificar-la a petició del sistema periòdicament.

4.5.1.5. Emmagatzematge de contrasenyes

1. Els *login* i les claus d'accés assignades a cada usuari de la xarxa corporativa de la FUOC són personals i intransferibles, essent l'usuari l'únic responsable de les conseqüències que puguin derivar-se'n del mal ús, de la divulgació o de la pèrdua.

2. Durant el temps de vigència, les contrasenyes s'emmagatzemaran de forma inintel·ligible i seran salvaguardades en els processos de còpia de seguretat del sistema.

3. Ningú no està autoritzat a desxifrar la clau d'un usuari, ni tan sols el personal tècnic de suport. En cas de pèrdua o d'oblit per part de l'usuari, se li generarà una nova clau d'accés sotmesa als mateixos requisits que una clau inicial.

4.5.2.- Sistema de control d'accessos

4.5.2.1.- Perfils d'usuari

Els perfils d'usuari determinen el conjunt d'opcions de procés a les quals pot accedir un usuari determinat des del moment en què s'identifica com a usuari del sistema mitjançant la introducció del seu *login* o identificador.

El sistema de control d'accessos es basa en un conjunt de relacions establertes a a nivell dels aplicatius CAMPUS VIRTUAL i TREN. L'aplicatiu TREN recull les sol·licituds d'accés i, un cop verificat el perfil assignat a l'usuari, estableix la configuració del seu lloc de treball.

Per tal de configurar el perfil d'un usuari (accessos accessibles i privilegis amb els quals s'accedeix), el sistema de control d'accessos aplica les regles següents:

- Cada persona s'identifica individualment com a USUARI.
- Cada USUARI té un TIPUS D'USUARI primari.
- Cada USUARI pot tenir un o més TIPUS D'USUARI secundari.
- Cada USUARI està subscrit a una o més LLISTES DE ROL.

- Cada aplicació s'identifica individualment (APL).
- Cada aplicació té associats **n** ROLS.
- Cada aplicació té associats **n** MÒDULS.
- Cada mòdul té associats **n** ACCESSOS.

- Un ACCÉS pot definir els privilegis d'un USUARI individual.
- Un ACCÉS pot definir els privilegis d'un TIPUS (diferents usuaris).
- Un ACCÉS pot definir els privilegis d'un ROL (diferents usuaris).

De manera que l'accés a un mòdul està controlat pel filtre següent:

(1) Si l'USUARI té ACCÉS al MÒDUL, accedeix segons parametrització personalitzada.
(2) Si el TIPUS de l'usuari té ACCÉS al MÒDUL, l'usuari accedeix segons parametrització del TIPUS.
(3) Si el ROL al que està subscrit l'usuari té ACCÉS al MÒDUL, l'usuari accedeix segons parametrització del ROL.
(4) En qualsevol altre cas, es denega l'accés a l'usuari.

A l'ANNEX A-3 es presenta el format dels diferents llistats a disposició de l'administrador per a controlar els perfils per tipus d'usuari i rol actius en el sistema.

A l'ANNEXO A-2 es presenta el format dels diferents llistats a disposició de l'administrador per a obtenir la llista de tots els usuaris amb accés al sistema, indicant el perfil al qual està associat en aquest moment.

4.5.2.2.- Administració d'usuaris

1. Per a donar d'alta un usuari en el sistema de control d'accessos (TREN), serà imprescindible que ja estigui donat d'alta com a usuari del sistema en la base de dades de CAMPUS.

2. Tant l'operació d'alta com qualsevol altra operació posterior de manteniment (excepte aquelles que responguin a actuacions tècniques per incidències) necessitaran la confirmació corresponent del responsable de l'aplicatiu al qual estigui subscrit l'usuari.

3. En donar d'alta un usuari, assumirà les autoritzacions i els privilegis que es derivin del perfil sol·licitat pel responsable d'aplicatiu que ha cursat la sol·licitud.

4. Un usuari sense perfil definit no tindrà accés al sistema.

5. La baixa d'un usuari suposarà la seva eliminació total del nivell de XARXA INTERNA, i la redefinició del seu perfil al nivell mínim en CAMPUS, on continuarà subscrit al Club UOC. En els aplicatius es donarà de baixa quan el responsable cursi una petició de baixa definitiva.

6. A petició del responsable del grup operatiu, la baixa pot suspendre's durant un període de reserva fins que l'usuari deixi efectivament de prestar els seus serveis a la FUOC. A partir d'aquest termini la baixa serà física.

7. La informació relacionada amb la feina de l'usuari passarà a còpies de seguretat, dins del procés de còpies del dia, on s'emmagatzemarà fins que caduqui el període de vigència històrica de la còpia esmentada.

8. El sistema evitarà que una identificació d'usuari pugui tornar a ser utilitzada.

4.5.2.3.- Administració de perfils

1. L'administrador de perfils crea el perfil d'un nou usuari a petició del responsable de l'aplicatiu al qual està subscrit l'empleat el perfil del qual es crearà.

2. Les peticions d'alta, de modificació o de baixa seran cursades per e-mail a l'administrador de perfils des dels responsables d'aplicatius o personal autoritzat amb aquesta finalitat. Només es cursaran aquelles sol·licituds que arribin correctament autoritzades.

3. Només l'administrador de perfils té privilegis per a validar qualsevol de les operacions a les quals pot sotmetre's un perfil d'usuari.

4. L'administrador de perfils tractarà la informació dins del nivell d'administració. Un cop realitzades les modificacions, ho notificarà al responsable de l'aplicatiu al qual el perfil estigui subjecte per a la seva validació i notificació a l'usuari interessat.

4.5.2.4.- Control d'accessos al sistema

1. En encendre un ordinador d'usuari, el sistema operatiu s'engegarà i es sol·licitarà l'identificador d'usuari i la clau d'accés a la xarxa (XARXA INTERNA), des d'on es realitzarà la configuració de serveis i de recursos disponibles en el PC local de l'usuari.

2. Tot seguit s'inicia el programa de control d'accessos (TREN) que configurarà les opcions d'aplicatius als quals té accés l'usuari segons el seu perfil.

3. Cada identificador tindrà un perfil associat, segons el càrrec i les funcions de l'usuari que sol·licita l'accés.

4. La introducció d'una clau diferent d'aquella autoritzada impedirà l'accés, oferint la possibilitat d'introduir novament la clau, a fi i efecte de corregir errors de digitació.

4.5.2.5.- Control d'accés al programa que gestiona la base de dades

1. El control d'accessos als fitxers que continguin dades de caràcter personal es realitzarà sempre per mitjà de l'aplicatiu específic que les gestiona, i de la forma i amb els privilegis que estableix l'accés de l'usuari sobre cadascun del mòduls autoritzats segons el seu perfil.

2. Quan l'usuari seleccioni un aplicatiu des del seu PC, el sistema de control d'accessos (TREN) validarà els permisos de l'usuari i perfilarà la configuració d'opcions disponibles segons el perfil.

3. Quan l'usuari opti per una opció determinada de programa, el sistema de control d'accessos (TREN) validarà la forma i els privilegis amb els quals aquest usuari concret accedeix al mòdul seleccionat.

4.6.- Còpies de Seguretat i Gestió de Suports

A fi de complir allò que s'estableix en l'article 8.2.f del Real Decret 994/1999, de 11 de juny, la FUOC disposa d'un procediment de realització de còpies de seguretat i de recuperació de dades que en garanteix la reconstrucció en l'estat en què es trobaran en el moment de produir-se la pèrdua o la destrucció.

Aquest procediment consisteix en la realització, amb periodicitat diària, d'una còpia de seguretat de la informació de la FUOC. Setmanalment, un còpia és dipositada en una empresa externa, contractada amb aquesta finalitat, que custodia les còpies de seguretat esmentades.

En cas de produir-se una incidència que generi destrucció d'informació, s'aplicarà el procediment de notificació, de tractament i de registre d'incidències previst a l'apartat 4.7. d'aquest document de seguretat, i es procedirà a la recuperació de la informació destruïda. Si aquesta recuperació fos impossible, es procedirà a sol·licitar la còpia de seguretat més recent i a restaurar la informació destruïda.

4.6.1.- Normes sobre còpies de seguretat i gestió de suports

Qualsevol actuació o procediment en matèria de còpies de seguretat i de gestió de suports haurà d'ajustar-se exactament a les normes establertes al punt 2.7 d'aquest document.

4.6.2.- Procediments de còpia de seguretat i de recuperació de dades

D'acord amb les mesures de seguretat en matèria de còpia i de recuperació de dades establertes en aquest document i les especificacions manifestades pel responsable de fitxer i pel responsable del seu tractament, l'administrador de còpies mantindrà actualitzada la documentació sobre els procediments de còpia i de recuperació de dades per a cadascun dels servidors afectats i els fitxers que conté.

Aquests documents tècnics s'incorporen als manuals d'explotació del grup operatiu d'Infrastructura Tecnològica amb les denominacions "Manuals de Còpia" i només seran accessibles pels responsables del fitxer i de seguretat, l'administrador de còpies i el personal d'explotació autoritzat.

El sistema de còpies actualment en funcionament es divideix en dos grups:

Còpies UNIX: Conté els fitxers, els aplicatius i els sistemes dels servidors UNIX, en els quals resideixen els fitxers protegits.
Software de còpia: Networker (Legato)
Freqüència ……: Diària incremental i còpia total setmanal
Vigència……..: Les còpies es mantenen durant 2 mesos
Històric……..: Còpia mensual

Còpies NT : Contenen els fitxers, els aplicatius i els sistemes dels servidors de la xarxa corporativa, serveis ofimàtics, etc...
Software de còpia: Backup Exec (Veritas)
Freqüència ……: Diària incremental i còpia total setmanal
Vigència……..: Les còpies es mantenen durant 2 mesos
Històric……..: Totes les còpies

Regularment, amb freqüència setmanal, un joc de còpia és lliurat a l'empresa ESABE SEGURIDAD INFORMÁTICA en un maletí tancat i amb clau de seguretat, per emmagatzemar-lo fora del locals de la FUOC. En aquesta còpia, a més dels fitxers, dels aplicatius i dels sistemes dels servidors, es guarden també els procediments de recuperació i una còpia del software de backup utilitzat, de manera que davant una situació de màxima emergència es garanteix l'autonomia total per a realitzar una recuperació integral dels sistemes.

Sempre que, en cas d'incidència es requereixi la recuperació de part o de la totalitat de les dades, sobretot pel que fa a fitxers protegits, s'aplicaran els procediments de recuperació preestablerts, quan la incidència sigui previsible, i els procediments que aconselli el Comitè de Crisi, quan la incidència obeeixi a una situació excepcional. En qualsevol cas, si es posen en perill fitxers protegits, serà necessària la conformitat per escrit del responsable de fitxer. Aquestes incidències quedaran enregistrades en el registre d'incidències.

4.6.3.- Tractament i administració de suports

A causa del gran volum de suports utilitzats en el sistema de còpies, les eines de backup utilitzades per a automatitzar les tasques del responsable de còpies aporten la base informativa per mantenir actualitzat el registre diari de còpies i els seus continguts.

4.6.3.1.- Identificació

1. Els suports utilitzats en les còpies s'etiquetaran fent constar la referència de la còpia d'acord amb el registre generat per les eines de backup utilitzades amb aquesta finalitat.

2. Els suports que continguin dades personals seran etiquetats de forma diferenciada, a fi de distingir-los de la resta de suports.

3. L'etiqueta serà de color vermell o altra marca identificativa, i contindrà una advertència clara sobre el contingut del suport i sobre la prohibició d'accés al personal no autoritzat.

4.6.3.2.- Inventari

1. El responsable de seguretat portarà una relació detallada dels suports, amb indicació d'aquells que continguin fitxers protegits.

2. A la relació s'especificarà la situació de cada suport.

3. La relació esmentada s'actualitzarà un cop mes, mitjançant l'inventari corresponent, coincidint amb la realització de les còpies històriques mensuals.

4. L'inventari també recollirà els suports que han produït una baixa en el sistema de còpies, els quals seran efectivament inutilitzats per tal d'evitar la possible recuperació dels seus continguts. La inutilització consistirà en l'alteració física del suport i el seu emmagatzematge separat per possibilitar l'evidència de la seva localització.

5. Periòdicament, el responsable de seguretat s'encarregarà de la destrucció física dels suports inutilitzats a fi d'optimitzar l'inventari i de garantir la destinació certa dels suports retirats.

4.6.3.3.- Emmagatzematge

1. Els únics suports homologats per a contenir dades de caràcter personal a la FUOC són els següents:

    - Discs del servidor en el qual s'ubica el fitxer mestre
    - Memòria RAM del sistema i dels llocs de treball (Suport temporal)
    - Discs virtuals i de suport per a fitxers temporals
    - Suports homologats per a realitzar còpies de seguretat
    - Suports homologats per a realitzar cessions temporals a empreses de serveis o a administracions públiques
    - Suports homologats per a realitzar cessions permanents a altres empreses del grup o terceres.

2. És prohibit d'utilitzar suports no homologats per a emmagatzemar fitxers que continguin dades de caràcter personal.

3. Els suports utilitzats per a còpies de seguretat s'emmagatzemaran en armaris tancats amb clau, i un cop per setmana es lliurarà una copia de seguretat a l'empresa de seguretat ESABE.

4.7.- Gestió d'Incidències

A fi de complir degudament allò que s'estableix a l'art. 8.2.e del Real Decret 994/1999, de 11 de juny, la FUOC disposa d'un procediment de notificació, de gestió i de resposta de les incidències, entenent per "incidència" qualsevol anomalia que afecti o pugui afectar la seguretat de les dades o dels sistemes i dels recursos utilitzats per al seu tractament adequat.

Depenent directament del responsable de seguretat, la direcció de l'Àrea de Sistemes d'Informació designarà els mitjans tècnics i humans per organitzar, en tots els nivells adequats per a donar cobertura a tot el sistema informàtic, el sistema de gestió d'incidències.

Davant la diversitat d'usuaris enquadrats en els diferents grups operatius de la FUOC, el sistema de gestió d'incidències centralitzarà i coordinarà les accions de suport que afectin el nivell de seguretat del sistema. En aquest sentit, els serveis d'atenció a l'usuari existents anteriors a aquest document, és a dir:

- Ajuda informàtica
- Atenció a l'estudiant
- Atenció al docent

actuaran com a primer nivell de suport de les incidències detectades pels usuaris en la seva activitat habitual amb el sistema per a aquells grups d'usuaris. Quan la incidència suposi una amenaça per a la seguretat del sistema o dels seus fitxers, aquests serveis encaminaran les seves sol·licituds al sistema de gestió d'incidències.

Per a tots els empleats, tant personal administratiu i de gestió com personal tècnic, el nivell de suport s'establirà directament amb el servei de suport d'incidències.

4.7.1.- Procediments de notificació d'incidències

Qualsevol persona que formi part de la plantilla de la FUOC o hi presti temporalment servei, o bé com a personal extern d'empreses de serveis, haurà de notificar immediatament al personal de suport del servei de gestió d'incidències qualsevol anomalia que detecti i que afecti o pugui afectar la seguretat de les dades o del sistema informàtic.

En vista dels greus perjudicis que es poden ocasionar, la FUOC actuarà disciplinàriament en cas de no actuar amb la màxima diligència davant una irregularitat en el funcionament habitual del sistema informàtic.

El procediment de notificació es realitzarà a través de l'F6 "entrada d'incidències" al servei de suport assignat a cada grup operatiu i que ha estat notificat pel responsable a tots els usuaris afectats. Per defecte, i llevat que s'estableixin procediments especials autoritzats pel responsable de seguretat, el servei de suport d'incidències es podrà contactar pels mitjans següents:

- Servei de Suport d'Incidències

  - Comunicació telefònica: 93.2532318
  - E-mail : xinterna@campus.uoc.es

4.7.2.- Procediments de gestió d'incidències

D'acord amb les mesures adoptades per la direcció de l'Àrea de Sistemes d'Informació per organitzar el servei de suport d'incidències, de les directrius del responsable de seguretat, i de l'experiència acumulada en la casuística d'actuacions de l'equip de suport, es mantindrà actualitzada la documentació sobre els procediments de gestió d'incidències susceptibles de normalització.

Aquests documents tècnics s'incorporen als manuals d'explotació del grup operatiu d'Infraestructura Tecnològica amb la denominació "Manual de Gestió d'Incidències" i només seran accessibles pels responsables del fitxer i de seguretat, i al equip de suport a les incidències.

4.7.2.1.- Gestió

El responsable de suport rebrà les notificacions d'incidències i procedirà a la seva obertura en el registre, a l'avaluació preliminar i a la comunicació als tècnics de suport, interns o externs, encarregats de la resolució, quan no existeixi un procediment aplicable que es derivi de la casuística documentada.

Quan existeixi la evidència o, fins i tot, la sospita que la incidència ha afectat o pot haver afectat un fitxer protegit, el responsable de suport ho comunicarà al responsable del fitxer per realitzar-ne el seguiment.

4.7.2.2.- Resposta

El responsable de suport s'assegurarà que els tècnics donin resposta immediata a la incidència i supervisarà la feina de reparació de l'anomalia detectada.

Un cop resolta l'anomalia, omplirà en el registre d'incidències la fitxa d'incidència oberta, i comunicarà el resultat a l'usuari sol·licitant.

Quan del tractament aconsellat per a la resolució es derivin riscs certs o potencials per a la seguretat i la integritat dels fitxers protegits, o dels recursos (software i hardware) que els tracten, el responsable de suport comunicarà al responsable de seguretat i al responsable del fitxer la situació, per al seu seguiment i l'avaluació en conjunt.

Un cop resolta l'anomalia, enviarà un informe al responsable del fitxer, amb totes les dades requerides per al registre de la incidència.

4.7.2.3.- Registre

El responsable del fitxer, d'acord amb l'Art. 10 del Real Decret 994/1999, ha creat un registre informatitzat en què es fa constar la informació següent relativa a les incidències:

- Tipus d'incidència
- Moment en el qual s'ha produït la incidència
- Persona que realitza la notificació i problema manifestat
- Procediment aplicat per a la seva resolució
- Tècnic que s'ocupa de la incidència

- Moment en el qual es considera solucionada la incidència
- Indicació de fitxers afectats
- Validació del responsable de seguretat i del fitxer.

És obligació del responsable de suport mantenir actualitzat el registre d'incidències, i també notificar al responsable de seguretat i al responsable del fitxer qualsevol incidència en què es vegin afectades o es posin en perill les dades dels fitxers expressament protegides en aquest document.

A més, és obligació del responsable gestionar les incidències que podrien produir-se, en el mínim temps possible, garantint, en qualsevol cas, que la seguretat de les dades de caràcter personal no es vegi alterada en cap moment.

A l'(ANNEX A-6) s'estableix el registre d'incidències per a recollir l'evidència d'aquests fets i la seva resolució.

4.8.- Cessió de dades

Atesa l'àmplia varietat de tractaments aplicats a la informació en mans de la FUOC, com a conseqüència de la diversificació de serveis i de recursos a disposició de les persones que conformen la comunitat universitària en totes les seves facetes i àrees d'actuació, per a determinats conceptes és necessària la participació de tercers en la realització dels objectius perseguits a diferents nivells.

Aquests "tercers" poden catalogar-se bàsicament en dos grans grups: empreses que realitzen serveis per compte de la FUOC, per la qual cosa necessiten conèixer dades i actuar com a encarregats del tractament, i organismes que depenen de les Administracions Públiques a les quals es notifiquen certes informacions en compliment de les disposicions i de les normatives vigents.

D'altra banda, depenent de les condicions de la comunicació de dades i de la finalitat perseguida, existeix una clara diferència entre la comunicació de dades a tercers que actuen com a proveïdors de serveis per al titular dels fitxers i aquells casos en què la comunicació de dades es deu a altres finalitats.

En qualsevol cas, en el moment actual i en el futur i sense detriment de l'observança estricta de les disposicions legals vigents, la FUOC establirà un procediment de sol·licitud de cessions de dades i un registre dels moviments d'aquesta naturalesa, independentment de la consideració o no consideració estricta de cessió.

En última instància, aquest registre permetrà de conèixer, en tot moment, les destinacions de les dades subministrades des de les instal·lacions de la FUOC, les característiques de la cessió i la finalitat perseguida, les condicions del tractament aplicat i el responsable de la seva autorització.

De manera general, les comunicacions de dades obeiran a la catalogació següent segons la durada i la finalitat:

- **Cessions permanents**: Es tracta de comunicacions de dades a empreses que realitzen tractaments per compte de la FUOC i que s'actualitzen periòdicament amb la freqüència establerta.

- **Cessions temporals**: Es tracta de comunicacions que obeeixen a una necessitat circumstancial i que seran anul·lades o cancel·lades un cop acabi la necessitat que les origina.

La forma dels formularis utilitzats i el registre de cessions es presenta a l'Annex A-7.

4.8.1.- Normes per a la cessió de dades

Qualsevol sol·licitud per a la cessió o comunicació de dades de caràcter personal s'ajustarà a allò que s'estableix a la Llei de Protecció de Dades de Caràcter Personal, articles 11 i 12, en què es regula la Comunicació de Dades i l'Accés a les Dades per compte de tercers.

D'acord amb les seves funcions, el responsable del fitxer i el responsable de seguretat seran els encarregats d'avaluar la necessitat, la finalitat i el contingut de la sol·licitud de cessió de dades per determinar la seva autorització o denegació, requisits legals que s'hagin de complir, notificacions a l'APD, etcètera, d'acord amb les disposicions vigents en matèria de seguretat de dades.

4.8.2.- Procediments de sol·licitud

Qualsevol petició de dades haurà de ser tramitada al responsable del fitxer o dels fitxers afectats, els quals de comú acord amb el responsable de seguretat, i partint del coneixement de les disposicions legals i de la normativa de seguretat de la institució, procediran a avaluar les característiques de la sol·licitud, la necessitat de comunicar les dades sol·licitades, la finalitat perseguida i els requisits legals que s'hagin d'observar per fer-la efectiva i viable, o bé que determinin la seva denegació.

El formulari de sol·licitud es descriu a l'Annex A-7, i passaran a formar part de l'expedient de cessió o de comunicació de dades del fitxer juntament amb la resolució.

4.8.3.- Procediments de preparació i de lliurament

Un cop autoritzada la sol·licitud de cessió o comunicació de dades, els responsables del fitxer i de seguretat gestionaran amb l'Àrea de Sistemes d'Informació les característiques i les condicions en què s'hagi de realitzar la cessió.

Un cop validada la viabilitat tècnica per donar suport a la sol·licitud presentada, es cursarà la corresponent petició al responsable o al equip tècnic designat per a la seva realització en les condicions establertes.

Un cop preparats els elements tècnics necessaris per a realitzar la cessió, el responsable tècnic designat ho comunicarà al sol·licitant i al responsable del fitxer per omplir l'autorització de sortida i subministrar-la al destinatari.

4.8.4.- Registre de cessions

El registre de cessions pròpiament dit es portarà com un ANNEX (A-7).
Es mantindrà un registre en què quedi constància de les cessions, permanents o temporals, que es fan a tercers, amb el detall següent:

- Data de sol·licitud
- Persona i departament sol·licitant, motiu de la sol·licitud; autorització
- Tipus de cessió: permanent o temporal
- Data de vigència (si és temporal)
- Freqüència d'actualització (si és permanent)
- Descripció de l'estructura de dades dels fitxers resultants
- Persona i departament destinatari; aprovació
- Sol·licitud al departament d'informàtica, adjuntant la informació i l'autorització necessària
- Destinatari (empresa, departament, persona, etc...) i data de lliurament
- Contracte, condicions d'ús, o document similar signat pel destinatari
- Informació per a la seva notificació a l'A.P.D. (quan tingui lloc).

El registre estarà sota la custòdia del responsable de seguretat i adjunt a aquest document de seguretat. El responsable de seguretat actuarà com a coordinador en les diferents fases de tramitació, des que es presenta la sol·licitud fins a la confecció final de l'expedient i el seu registre.

5.- Legalització de fitxers en l'A.P.D.

Tot seguit es detallen les còpies dels formularis originals de sol·licitud d'inscripció dels fitxers protegits a l'Agència de Protecció de Dades, acompanyats de la notificació de registre cursada per l'Agència.

ANNEXOS

A-1) Descripció tècnica de fitxers

Amb caràcter general, la informació continguda en aquest document relativa als fitxers protegits (fitxers que contenen dades de caràcter personal), la seva estructura i els aplicatius que els tracten s'han recollit de les especificacions tècniques i funcionals desenvolupades en els documents següents:

Aplicatiu CAMPUS VIRTUAL:

Responsable: .....

- Base de Dades: CAMPUS
- Tipus: ORACLE
- Administrador: Àrea de Sistemes d'Informació
- Servidor: UNIX (cuba.uoc.es)
- Documentació: Responsable del fitxer
  Àrea de Sistemes d'Informació
  Anàlisi funcional i Model de Dades

Aplicatiu GAT:

Responsable: .....

- Base de Dades: GAT
- Tipus: ORACLE
- Administrador: Àrea de Sistemes d'Informació
- Servidor: UNIX (senegal.uoc.es)
- Documentació: Responsable del fitxer
  Àrea de Sistemes d'Informació
  Anàlisi funcional i Model de Dades

Aplicatiu PERSONAL:

Responsable: .....

- Base de Dades: PERSONAL
- Tipus: ORACLE
- Administrador: Àrea de Sistemes d'Informació
- Servidor: UNIX (liberia.uoc.es)
- Documentació: Responsable del fitxer
  Àrea de Sistemes d'Informació
  Anàlisi funcional i Model de Dades

Aplicatiu FORMACIÓ CONTINUADA:

Responsable: .....

- Base de Dades: FORMACIÓ CONTINUADA
- Tipus: ORACLE
- Administrador: Àrea de Sistemes d'Informació
- Servidor: UNIX (brunei.uoc.es)

- Documentació: Responsable del fitxer
  Àrea de Sistemes d'Informació
  Anàlisi funcional i Model de Dades

Aplicatiu INFORMACIÓ:

Responsable: .....

- Base de Dades: INFORMACIÓ
- Tipus: ORACLE
- Administrador: Àrea de Sistemes d'Informació
- Servidor: UNIX (senegal.uoc.es)
- Documentació: Responsable del fitxer
  Àrea de Sistemes d'Informació
  Anàlisi funcional i Model de Dades

Aplicatiu GESTIÓ COMPTABLE:

Responsable: .....

- Base de Dades: GESTIÓ COMPTABLE
- Tipus: ORACLE
- Administrador: Àrea de Sistemes d'Informació
- Servidor: UNIX (uoc-escarola.uoc.es)
- Documentació: Responsable del fitxer
  Informació del fabricant
  Manual d'usuari

Aplicatiu TRAMESES:

Responsable: .....

- Base de Dades: TRAMESES
- Tipus: ORACLE
- Administrador: Àrea de Sistemes d'Informació
- Servidor: UNIX (liberia.uoc.es)
- Documentació: Responsable del fitxer
  Àrea de Sistemes d'Informació
  Anàlisi funcional i Model de Dades

A-2) Registre d'Usuaris

Atès el volum d'accessos i les dimensions del sistema informàtic de la FUOC, s'habilitaran els procediments tècnics per mantenir i elaborar les llistes d'usuaris i perfils per mitjans informatitzats amb les mesures de seguretat adequades. Aquests procediments només seran accessibles per al responsable de seguretat, i si ho delega, per als administradors d'usuaris i perfils.

Tot seguit, en aquest annex i el següent, es presenta un detall de continguts dels formats de llistat disponibles:

(a) Llistat simple (Llista)

Àrea	Nom	Login	Alta	Vigència	Altres	D.P.
Xxxxx	Xxxxxxxxxxxxxxxxxxxx	Xxxxxxxx	xx-xx-xx	xx-xx-xx		x

(b) Llistat d'usuaris i perfils (Resum)

Àrea	Nom Login – Alta - Vigència	Tipus principal Altres tipus	D P	Aplicatiu / Rol(s)	D P	Mòduls personalitzats	D P
Xxxxx	Xxxxxxxxxxxxxxxxxxxx Xxxxxx xx-xx-xx xx-xx-xx	Xxxxxxxxxxxxxxx Xxxxxxxxxxxxxx Xxxxxxxxxxxxxx	X X	Xxxxx xxxxxxxxxxxxxx Xxxxxxxxxxxxxx Xxxxx xxxxxxxxxxxxxx Xxxxxxxxxxxxxx Xxxxxxxxxxxxxx	X X X	Aplicatiu XXXX Aplicatiu XXXX Aplicatiu XXXX	X X

(c) Listat d'usuaris i perfils (Detall)

Àrea	Nom Login – Alta - Vigència	Tipus principal Altres tipus	D P	Aplicatiu / Rol(s)	D P	Mòduls personalitzats	D P
Xxxxx	Xxxxxxxxxxxxxxxxxxxx Xxxxxx xx-xx-xx xx-xx-xx	Xxxxxxxxxxxxxxx Xxxxxxxxxxxxxx Xxxxxxxxxxxxxx	X X	Xxxxx xxxxxxxxxxxxxx Xxxxxxxxxxxxxx Xxxxx xxxxxxxxxxxxxx Xxxxxxxxxxxxxx Xxxxxxxxxxxxxx	X X X	APL MÒDUL APL MÒDUL APL MÒDUL APL MÒDUL APL MÒDUL	X X

A-3) Registre de Perfils d'Usuari

Vegeu introducció en Annex A-2.

LLISTAT DE TIPUS D'USUARI – LLISTAT DE ROLS

(d) Llistat de Tipus d'Usuari (Resum – Detall)

Tipus d'usuari	Aplicatiu	Mòduls	D.P.
Xxxxxxxxxxxxxxxxx	Xxxxxxx	Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
	Xxxxxxx	Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
	Xxxxxxx	Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
Xxxxxxxxxxxxxxxxx	Xxxxxxx	Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
	Xxxxxxx	Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
Etc…	Etc…	Etc…	Etc

(e) Llistat de Rols (Resum – Detall)

Aplicatiu	Rol	Mòduls	D.P.
Xxxxxxxx	Xxxxxxxxxxxxxxxxx	Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
	Xxxxxxxxxxxxxxxxx	Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
	Xxxxxxxxxxxxxxxxx	Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
Xxxxxxxx	Xxxxxxxxxxxxxxxxx	Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
	Xxxxxxxxxxxxxxxxx	Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
		Xxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx	X
Etc…	Etc…	Etc…	Etc

A-4) Procediments de Còpia i de Recuperació

Tot seguit es detalla una llista de tots els documents tècnics en què es recullen les especificacions i els procediments per a l'aplicació correcta dels processos de còpia de seguretat i de recuperació de dades. Els documents esmentats es troben sota la custòdia de l'Administrador de Còpies, el qual, juntament amb el Responsable de Seguretat, té accés exclusiu a aquesta informació.

Referència	Descripció	Fitxer
NT-BK-UX1	• Procediment de còpia global de sistema UNIX • Procediment de restauració completa de sistema UNIX a partir de discs formatats (buits)	BKSYSALL.DOC

A-5) Registre de Còpies i E/S de Suports

Tot seguit es presenta el format de les etiquetes homologades per a identificar els suports utilitzats en les còpies de seguretat. La **referència** relaciona el suport amb la informació de continguts enregistrada en el software de backup utilitzat, o en casos especials, amb l'expedient de cessió de dades autoritzat. Les etiquetes que identifiquen a suports que contenen dades de caràcter personal són de color vermell, i a la seva llegenda s'inclou l'advertència (*) sobre el caràcter restringit d'accés als seus continguts.

Referència de la còpia	
UNIX_SCO_1	**(*) Aquest suport conté fitxers amb dades de carácter personal. En compliment del R.D. 994/1999, es totalment prohibit de manipular i d'utilitzar aquest suport al personal no autoritzat.**

Amb periodicitat mensual, coincidint amb la còpia, el responsable de còpies elaborarà un inventari de suports que adjuntarà al registre d'inventaris, en què detallarà la ubicació de cada suport, el seu contingut, la data d'alta en el circuit de còpies, la data de còpia i la data de baixa o de cancel·lació de vigència del suport esmentat. Quan es compleixi la data de baixa, s'indicarà la destinació que es dóna al suport (reutilització o destrucció) i el mètode aplicat. En el Document de Seguretat quedarà sempre l'últim inventari actualitzat.

INVENTARI DE SUPORTS en data: __/__/____								
Nº Sèrie	**Data alta**	**Contingut (Referència)**	**Ubicació**	**Data còpia**	**Data baixa**	**Baixes**		
						Reut.	**Dest.**	**Mètode**

A-6) Registre d'Incidències

Ateses les dimensions del sistema i l'índex d'activitat quotidià, la FUOC decideix informatitzar el registre d'incidències sobre una Base de Dades ACCESS d'accés restringit al responsable de suport. Tot seguit es presenta el disseny de la finestra de registre en què quedarà constància de qualsevol incidència detectada.

A més de les corresponents funcions per a l'administració del registre d'incidències, el sistema, a petició del responsable de seguretat, del responsable de fitxer o del responsable de suport, està capacitat per a subministrar un llistat de fitxes del registre per diferents criteris.

- Totes les fitxes d'incidència.
- Incidències que han afectat a un fitxer o aplicatiu.
- Incidències entre un marge de dates.
- Incidències per situació.
- Etc...

Aquest és un exemple que caldrà substituir per la versió definitiva:

Ref.	Data	Hora	Usuari	Lloc	Departament	Aplicatiu
2000/003	15-03-2000	16:44	U7772340	PC-W95-003	Formació	ACADÈMIA

Descripció de la incidència:

En intentar emetre un llistat d'alumnes per assignatura dóna un error "Registre fora d'interval" i el procés avorta, tornant novament al menú.

	RECURSOS AFECTATS			
Tècnic	**Aplicatiu**	**Fitxer**	**Servidor**	**Xarxa**
Felix Nadie Nadie (E5559098)	ACADEMIA	BDD_FORM	SERVIDOR-1	Estudios.net

Solució de la incidència:

S'ha verificat la integritat de la BDD i s'han detectat problemes d'índex a les taules:
BDD_FORM.ALUMNES
BDD_FORM.AULES
BDD_FORM.PLANS
BDD_FORM.ASSIGNATERS
En intentar reindexar les taules s'ha detectat un problema d'integritat en el sistema de fitxers.
Es procedeix a verificar físicament i lògica el volum VOL-2 del SERVIDOR-1.
Un cop regenerat es comprova la pèrdua de l'índex BDD_FORM.AULAS.INX.
Es procedeix a la seva recuperació pel procediment RECOVER_BDD_FORM_DIARIA seleccionant només l'índex afectat. Regeneració de la BDD sense problemes.

Sota la supervisió del responsable del fitxer es verifica que no hi ha hagut pèrdua de dades.

Signatura: TÈCNIC	**Signatura: Cap Seguretat**	**Signatura: Responsable Fitxer**	**Situació**	TANCADA
			Data	15-03-2000
			Hora	19:30

Si s'ha afectat les dades personals d'un fitxer, ha d'habilitar-se una segona finestra o pantalla on es documenta com s'ha afectat, quin procediment s'ha seguit per a la recuperació i si s'han hagut de recuperar les dades manualment o per mitjà d'altres procediments.

A-7) Registre de Cessions de Fitxers

Sol·licitud d'autorització per a una cessió de dades:

SOL·LICITUD DE CESSIÓ DE DADES	**Expedient núm.**	

a) SOL·LICITANT

Grup Operatiu/Àrea/Departament:	
Responsable (Cognoms i Nom):	**Càrrec:**
	DNI:

b) DADES SOL·LICITADES

	Format:	**Suport**: _ disquet _ cinta _ etiquetes _ llistat Altres:

b1) Criteris de selecció	**b2) Finalitat o Ús que se'n farà**

En signar aquest document el sol·licitant es compromet a utilitzar les dades cedides únicament per a la finalitat expressada.	**Signatura del sol·licitant:**

c) RESOLUCIÓ

D'acord amb allò que disposa la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de dades de Caràcter Personal (BOE 298 de 14/12/99), i d'acord amb les polítiques de seguretat de la FUOC, i vista la sol·licitud que inicia aquest expedient, aquesta Gerència resol:

_ Accedir a la sol·licitud, advertir el sol·licitant de la seva obligació de dedicar les dades cedides exclusivament a la finalitat per a la qual les va sol·licitar, i remetre una copia d'aquest expedient al Director d'Informàtica per tal que proporcioni les dades al sol·licitant.

_ No accedir a la sol·licitud, per no ajustar-se als objectius per als quals es sol·liciten les dades a les quals permetrien la seva cessió segons l'article 11 de la Llei Orgànica 15/1999 esmentada. Contra aquesta resolució es podà interposar recurs d'alçada davant el rector en el termini d'un mes.

El Responsable de Seguretat	**El Responsable del Fitxer**	**EL GERENT**
		Barcelona, __ de _____ de ____

Registre de cessions: S'habilitarà un registre de cessions únic sota la custòdia del responsable de seguretat, i adjunt al document de seguretat.

REGISTRE DE CESSIÓ DE DADES	**Expedient núm.**	
** Vàlida únicament si porta adjunta la sol·licitud autoritzada.*	**Referència**	

DESTINATARI

Grup Operatiu/Àrea/Departament/Proveïdor de Serveis:		**NIF:**
Responsable (Cognoms i noms):	**Càrrec:**	**DNI:**
Domicili:		

Mode d'enviament	**Suport**

Tipus de cessió:	(Indiqueu el tipus de cessió, la data del primer lliurament i la freqüència d' actualització o la data de caducitat)		
_ Permanent	***Data lliurament***	***Actualització cada:***	***Vigent fins (data/motiu):***
_ Temporal			

Procediment	***(descrigueu el procediment de generació i el departament i el responsable)***

Notificació a l'A.P.D.:	_SÍ _NO	**Codi d'inscripció:**	
(Per omplir si la cessió exigeix notificació a l'Agència de Protecció de Dades)			

Documentació adjunta:

_ Descripció tècnica de l'estructura i format de les dades de sortida
_ Descripció de les fonts originals de les dades obtingudes
_ Descripció dels criteris de selecció aplicats
_ Descripció del procediment de generació (comandaments SQL, aplicatiu, utilitats,...)
_ Descripció del software de tractament (quan la sortida no sigui llegible des d'un software estàndard)
_ Eina o algorisme d'encriptació aplicat (si hi té lloc)
_ Formulari de notificació a l'Agència de Protecció de Dades
_ Contracte del servei o Carta de Compromisos amb el destinatari
_ Referència a la documentació tècnica de l'Àrea d'Informàtica

El Responsable de Seguretat	**El Responsable del Fitxer**	**El Director de l'Àrea d'Informàtica**
		Barcelona, __ de _____ de ____

Qualsevol entrada o sortida de suports als/dels locals on es troba ubicat el fitxer haurà de ser autoritzada pel responsable del fitxer d'acord amb el document que s'adjunta.

Es mantindrà un registre de moviment de suports els assentaments dels quals seran els documents d'autorització d'entrada/sortida degudament emplenats.

REGISTRE D'ENTRADA/SORTIDA DE SUPORTS

☐ **Entrada**	**Data:**		**Referència:**	
☐ **Sortida**	**Hora:**			

	DESCRIPCIÓ DEL SUPORT
Tipus de suport:	
Identificació:	
Descripció del contingut:	
Fitxers d'Origen: **Destinació:**	
Data de creació:	

	FINALITAT I DESTINACIÓ
Finalitat:	
Destinació:	
Destinatari:	

	MODE D'ENVIAMENT
Mitjà:	
Remitent:	
Mesures de seguretat:	

	AUTORITZACIÓ	
Responsable del lliurament/recepció:		
Autoritzat per:	**DNI:** **Àrea:** **Càrrec:**	
Observacions:		Signatura:

A-8) Llista de Responsables

En aquest annex s'inclourà un detall de les persones (o unitats operatives, però preferiblement persones) que s'identifiquen com a responsables en els diferents nivells que estimi oportuns el responsable del fitxer com a conseqüència de la implantació efectiva del document de seguretat i la identificació i la assignació de funcions (la llista pot variar). Per a cada apartat s'inclourà una petita taula amb el format següent:

Responsable de Seguretat		
Nom i Cognoms	**Data Alta**	**Data Baixa**

Responsable de fitxer
Responsables d'Àrea o Grup Operatiu
    Personal autoritzat per a sol·licitar operacions sobre usuaris
Responsable de Seguretat
Director de l'Àrea de Sistemes d'Informació
Administrador o Responsable de Comunicacions
Administradors de Sistemes
Administradors de Xarxes
Administrador de CAMPUS
Administrador de XARXA INTERNA
Administrador de perfils (TREN)
Administradors de Bases de Dades
Administradors d'Explotació de Dades (DISCOVERY)
Responsable de Còpies de Seguretat i Gestió de Suports
Caps de Projecte (Producció i Manteniment d'Aplicatius)
Responsable del Servei de Suport
    - Servei de Suport i Gestió d'Incidències
    - Servei (s) de Suport Intern
    - Servei(s) de Suport Extern

A-9) Relació d'empreses del grup i serveis oferts

	Serveis oferts per la UOC	Qui tracta les dades
GMMD, SL	Supracampus	Ambdues parts
	Aplicacions de gestió	Ambdues parts
	Connexió als servidors UOC a través d'Infovia, Internet i UOCnet	UOC
	Backup de dades	Ambdues parts
	Hosting	GMMD, SL
	Disponibilitat de serveis	GMMD, SL
Xarxa Virtual de Consum, SCC	Supracampus	Ambdues parts
	Aplicacions de gestió	Ambdues parts
	Backup de dades	Ambdues parts
	Hosting	XVC
	Disponibilitat de serveis	XVC
EDIUOC	Servei de traducció automàtica	Ambdues parts
Planeta UOC, SL	Supracampus	Ambdues parts
	Aplicacions de gestió	Ambdues parts
	Connexió als servidors UOC a través d'Infovia, Internet i UOCnet	UOC
	Backup de dades	Ambdues parts
	Hosting	Planeta UOC
	Disponibilitat de serveis	Planeta UOC