DOCUMENT DE SEGURETAT

FITXERS DE DADES DE CARÀCTER PERSONAL AMB NIVELL DE SEGURETAT BÀSIC i MIG

-NIVEL MIG-

FITXER DE RECURSOS HUMANS
FITXER DE CONSULTORS I TUTORS
FITXER DE GESTIÓ ACADÈMICA

-NIVELL BÀSIC-

FITXER DE ADMINISTRACIÓ
FITXER DE CAMPUS PER LA PAU
FITXER DE CAMPUS VIRTUAL
FITXER DE EMPRESES
FITXER DE INFORMACIÓ
FITXER DE SEGURETAT

Empresa:	Fundació per a la Universitat Oberta de Catalunya (FUOC)
Grup Operatiu:	Gabinet de Gerència
Data d'edició:	Dicembre de 2011
Versió:	3.0

ÍNDEX

ANNEXOS

1. OBJECTE DEL DOCUMENT

L'objecte del present document respon a l'obligació que conté el Real Decret 1720/2007, on es regulen les mesures de seguretat dels fitxers que continguin dades de caràcter personal, d'establir les mesures d'índole tècnica i organitzatives necessàries per a garantir la seguretat que han de reunir els fitxers automatitzats i no automatitzats, i de l'obligat compliment per a tots els usuaris amb accés a ells, així como als sistemes d'informació i documentació en suport paper que els continguin.

Els fitxers de dades personals relacionats en la primera pàgina d'aquest document: ***Fitxer de Recursos Humans / Fitxer de Consultors i Tutors / Fitxer de Gestió***

Acadèmica / Fitxer de administració / Fitxer de Campus per la Pau / Fitxer de Campus Virtual / Fitxer d'Empreses / Fitxer de Informació / Fitxer se Seguretat, degudament notificats davant l'Agència Catalana de Protecció de Dades, documents de inscripció que s'adjunten en l'Annex A, es troben oficialment classificats com:

a) **Nivell bàsic**: Fitxer de administració / Fitxer de Campus per la Pau / Fitxer de Campus Virtual / Fitxer d'Empreses / Fitxer de Informació / Fitxer se Seguretat, atenent les condicions descrites per als fitxers automatitzats a la Secció 1a (articles 89 a 94) del Capítol III del Reial Decret 1720/2007, i per als tractament no automatitzats a la Secció 1a (articles 105 a 109) del Capítol IV, sent per tant aplicables a ells totes les mesures de seguretat de nivell bàsic que s'estableixen al Reial Decret referenciat.

b) **Nivell Mig:** Fitxer de Recursos Humans / Fitxer de Consultors i Tutors / Fitxer de Gestió Acadèmica: Aquests fitxers impliquen el tractament i anàlisi de dades curriculars, que poden contenir dades personals que ofereixin una definició de les característiques o de la personalitat dels Candidats, Treballadors, Consultors i Tutors, i que permeti avaluar determinats aspectes de la personalitat o comportament dels mateixos, i en conseqüència, a més de les mesures de seguretat de nivell bàsic, s'adoptaran les mesures de nivell de seguretat mitjà|medi atenent les condicions descrites per als fitxers automatitzats a la Secció 2a (articles 95 a 100) del Capítol III del Reial Decret 1720/2007, i per als tractament no automatitzats a la Secció 2a (articles 109 i 110) del Capítol IV, sent per tant aplicables a ells totes les mesures de seguretat de nivell mig que s'estableixen en el Real Decret referenciat.

Tenint en compte la contínua evolució dels sistemes d'informació i de la pròpia organització, el document intentarà ser en el seu conjunt un marc estable, però al seu torn adaptable a les noves necessitats tant informàtiques com organitzatives que es vagin succeint, de manera que, es pretén donar a aquest document la versatilitat necessària per a no versi sotmès a constants actualitzacions. En aquest sentit, el present document es compon de dues parts, una on es descriuen les mesures tècniques i organitzatives que s'han d'adoptar, i altra on s'inclouen uns Annexos que contenen la política de seguretat establerta per FUOC.

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, les mesures de seguretat establertes en el present document, es fan extensives als fitxers de les empreses del grup, a les quals se'ls presten

diversos serveis com encarregats de tractament, sense perjudici dels corresponents documents de seguretat de cada una de les empreses.

El document de seguretat s'actualitzarà i revisarà quan es produeixin canvis rellevants en el sistema d'informació o organitzatius de l'empresa. Així mateix, el present document s'adaptarà en tot moment, a les disposicions vigents en matèria de seguretat de les dades de caràcter personal.

2. ÀMBIT D'APLICACIÓ I RECURSOS PROTEGITS

2.1. Àmbit jurídic

L'elaboració del present document de seguretat s'ha realitzat sota la responsabilitat de FUOC, que té el compromís i l'obligació d'implantar i actualitzar les normes que conté el Reglament de Mesures de Seguretat (1720/2007) i recollides en aquest document.

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 del grup, que comparteixen en diferent grau els recursos i els serveis del sistema informàtic, 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'altre.

- EDITORIAL UOC, S.L.
- EURECA MEDIA, S.L.
- EDUCACIONLINE, S.L.
- XARXA VIRTUAL DE CONSUM "LA VIRTUAL"

2.2. Àmbit personal

Totes les persones internes o externes amb accés a través de qualsevol mitjà a les dades personals que contenen els Fitxers o als sistemes d'informació que hi permeten l'accés, estan obligades legalment a complir l'estipulat en aquest document, i per tant, subjectes a les conseqüències legals del seu incompliment.

Les normes internes contingudes en el 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. 89.2 del Real Decret 1720/2007.

2.3. Recursos protegits

Totes les mesures de seguretat adoptades van encaminades a protegir els Fitxers, aplicacions i els seus mecanismes d'actualització, recursos del sistema operatiu, xarxes de telecomunicacions, suports i equips informàtics i arxiu i custòdia dels tractaments no automatitzats, ja siguin gestionats per FUOC o per empreses o personal expressament autoritzat, com per exemple, aquells que hagin subscrit un contracte de prestació de serveis, o bé, cessionaris legalment autoritzats.

En definitiva, les mesures de seguretat recollides en aquest document s'encaminen a protegir tots les dades de caràcter personal que són objecte de tractament, des de l'òptica de les aplicacions amb les quals es tracten, els equips informàtics que les suporten, els locals on es troben situats, així com dels mecanismes d'arxiu i custòdia de les dades tractades en suports no automatitzats. La protecció de les dades dels Fitxers enfront d'accessos no autoritzats s'haurà de realitzar mitjançant el control, al seu torn, de totes les vies per les quals es pugui tenir accés a aquesta informació:

1 . Locals i centres de tractament on se situïn els fitxers.
2 . Llocs on es guardin o emmagatzemin suports que continguin fitxers.
3 . Llocs de treball locals i remots des dels quals es pugui accedir als Fitxers.
4 . Servidors, entorn del sistema operatiu i de comunicacions.
5 . Sistemes operatius i aplicacions que donen accés a les dades

3. MESURES, NORMES, PROCEDIMENTS I REGLES DE SEGURETAT

A fi de complir degudament allò que s'estableix el Real Decret 1720/2007, la FUOC ha establert les normes de seguretat següents en relació a:

1 . Locals i centres de tractament de les dades
2 . Llocs de treball amb accés als Fitxers
3 . Sistema Operatiu i Entorn de Comunicacions
4 . Sistema informàtic, aplicacions o programes d'accés als Fitxers
5 . Contrasenyes personals: protecció i salvaguarda
6 . Gestió de suports informàtics
7. Copies de seguretat
8. Tractaments no automatitzats de dades personals

3.1. Locals i centres de tractament de les dades

Els locals on es troben instal·lats els equips informàtics que contenen els Fitxers y els mecanismes de custodia dels suport paper, són objecte de protecció per a garantir la

inaccessibilitat i confidencialitat de les dades protegides. Especial atenció es té amb els servidors amb accés a través de la xarxa que alberguin Fitxers.

a) En els locals on se situen els Fitxers s'han adaptat les mesures de seguretat necessàries per a evitar els riscos de indisponiblitat dels Fitxers que poguessin produir-se per incidències intencionades o fortuïtes. En l'Annex E s'especifiquen les mesures adoptades.

b) Es controlen les parts dels locals des d'on es pugui accedir als Fitxers amb la finalitat d'evitar els possibles intents d'accés a les dades protegides per persones no autoritzades.

c) L'accés físic al local o locals on es trobin situats els equips i sistemes informàtics on estan allotjats els Fitxers i els arxius de custodia de la documentació en paper, hauran d'estar restringits exclusivament al personal autoritzat, sempre que estiguin relacionades en l'Annex F, i als administradors del sistema i personal informàtic que hagin de realitzar labors de manteniment per a les quals sigui imprescindible l'accés físic a les mateixes.

d) Règim de treball fora dels locals d'ubicació dels Fitxers:

1. Per a tots els ordinadors portàtils o altres equips informàtics mòbils gestionats per FUOC que continguin Fitxers amb dades personals, s'estableix l'obligació d'habilitar una contrasenya d'arrencada. El responsable de l'ús de l'ordinador portàtil o equip informàtic mòbil s'encarregarà de configurar-la i quan sigui necessari modificar la contrasenya, segons les normes establertes per l'empresa a aquest efecte.
2. En el cas que l'ordinador o equip informàtic mòbil, a més de la contrasenya d'arrencada, disposi d'altre tipus de contrasenyes, aquestes estaran sota la custòdia i manteniment del Responsable dels Fitxers.
3. Per a la sortida d'ordinadors portàtils o equips informàtics mòbil que continguin dades personals fora dels locals d'ubicació dels Fitxers haurien de seguir-se els següents passos:
   - Tota sol·licitud i autorització haurà de realitzar-se per escrit.
   - La sol·licitud per part del peticionari haurà de contar amb el beneplàcit del Responsable dels Fitxers.
   - El Responsable dels Fitxers, revisarà i comprovarà la sol·licitud, autoritzant-la o denegant-la.

- La documentació original relativa a la sortida del local d'ordinadors portàtils o equips informàtics mòbils serà arxivada pel responsable dels Fitxers.

4. Per Així mateix, s'adoptaran les mesures de seguretat oportunes per custodiar la documentació en paper que contingui dades de caràcter personal, que s'extreguin dels locals de treball.
5. Per norma general, exclusivament el personal autoritzat al document de seguretat podrà tenir accés als llocs on es trobin instal·lats els equips físics de suport als sistemes d'informació.

3.2. Llocs de treball amb accés als Fitxers

Tenen la consideració de llocs de treball, tots aquells dispositius des d'on es pot tenir accés als Fitxers que contenen dades personals, com per exemple, terminals o ordinadors personals, terminals d'administració del sistema, quan des d'aquestes es pugui també accedir a les dades personals dels Fitxers, armaris, arxivadors, sales de arxiu, calaixos.

La FUOC es responsabilitza de cadascun dels llocs de treball, garantint a més, que la informació disponible sobre dades personals des de cadascun d'ells és inaccessible, i per tant, no pot ser vista per persones no autoritzades.

Els equips informàtics han de mantenir-se adequadament per a assegurar la disponibilitat i integritat continuades dels Sistemes d'Informació. En particular:

- Els equips han de mantenir-se d'acord a les recomanacions i especificacions dels subministradors del servei.
- Els equips només han de ser trets fora de les seves instal·lacions per a la seva reparació i servei per personal de manteniment degudament autoritzat.
- Abans de desfer-se d'equips propis, han d'esborrar-se les dades que contenen per a assegurar que totes les dades personals han estat eliminades.

Amb l'objectiu d'evitar aquests tractaments no autoritzats, s'han adoptat una sèrie de mesures d'obligat compliment per a tot el personal, encaminades a garantir la confidencialitat de les dades personals accessibles des dels llocs de treball. Totes aquestes mesures estan relacionades en l'Annex I "Funcions i Obligacions del Personal" del present document.

3.3. Sistema Operatiu i Entorn de Comunicacions

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 haurien d'establir els mecanismes necessaris per tal de garantir la seguretat en el nivell establert en aquest document.

Mitjançant la present normativa, es regula l'ús i accés de les parts al sistema operatiu, eines o programes d'utilitat, o de l'entorn de comunicacions, per a intentar evitar tractaments no autoritzats de les dades que contenen els Fitxers:

a) 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.

b) 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.

c) S'establiran els mecanismes necessaris perquè per tots els usuaris, 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, estiguin identificats per mig de logins d'accés.
d) 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.

e) 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.

f) 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. Cap usuari, quan es connecti als sistemes i aplicacions remotament, podrà accedir a dades als quals no tingués en manera local. Tots els procediments de tractament remot exigeixen la identificació i autenticació dels usuaris igual que accedint en manera local.

g) 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. Tots els procediments estaran supervisats pels administradors del sistema i seran monitoritzats.

h) 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.

i) Continuant amb el punt anterior, la FUOC ha establert sistemes periòdics d'esborrat automàtic dels fitxers temporals. Els fitxers que complerta la seva finalitat no siguin eliminats haurien de complir totes les exigències legals i les mesures de seguretat establertes per als Fitxers mestres.

3.4. Sistemes informàtics, aplicacions o programes d'accés als Fitxers

Són tots els sistemes informàtics per mitjà dels quals podem accedir a les dades personals que incorporen els Fitxers, i que són els quals generalment utilitzen tots els usuaris com mitjà de tractament de les dades.

Aquests sistemes poden consistir en programes o aplicacions creades a mesura, o poden ser aplicacions preprogramades d'ús generalitzat com programes i paquets estàndard disponibles en el mercat informàtic.

a) 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 del fitxer i de seguretat, 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.

b) 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.

c) La FUOC ha configurat un procediment d'identificació i d'autenticació dels usuaris per a impedir l'ús no autoritzat d'aquestes aplicacions.

d) El responsable del fitxer o tractament establirà un mecanisme que limiti la possibilitat d'intentar reiteradament a l'accés no autoritzat al sistema d'informació.

3.5. Contrasenyes personals: protecció i salvaguarda

Les contrasenyes personals constituïxen un dels components bàsics de la seguretat de les dades, i per tant, han d'estar especialment protegides. Com claus d'accés al sistema, les contrasenyes haurien de ser estrictament confidencials i personals, i qualsevol incidència que comprometi la seva confidencialitat haurà de ser immediatament comunicada a l'administrador del sistema o al Responsable de Seguretat, i resolta en el menor termini de temps possible.

a) Tots els usuaris autoritzats per a accedir als Fitxers de FUOC, tenen un codi d'usuari únic i associat a una contrasenya, aquesta, només serà coneguda pel propi usuari i pels Responsables dels Fitxers o els administradors del sistema designats.

b) 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 F. Només les persones expressament autoritzades i relacionades en l'Annex F poden tenir accés a les dades dels Fitxers.

c) Els usuaris només tindran accés autoritzat a aquelles dades i aquells recursos que necessitin per a desenvolupar les seves funcions.

d) El Responsable dels Fitxers establirà mecanismes per a evitar que un usuari pugui accedir a dades o recursos amb drets distints dels autoritzats.

e) 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.

f) Cada usuari serà responsable de la confidencialitat de la seva contrasenya i, en cas que la mateixa sigui coneguda fortuïta o fraudulentament per persones no autoritzades, haurà de registrar-lo com incidència i procedir immediatament al seu canvi.

g) Els arxius on s'emmagatzemin les contrasenyes haurien d'estar protegits i sota la responsabilitat del Responsable dels Fitxers o l'administrador del sistema.

h) 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.

i) S'estableixen en l'Annex G, amb la finalitat de garantir la seguretat i control dels accessos als Fitxers, les normes reguladores dels procediments de control d'accés,

privadesa, assignació, canvi de contrasenyes, distribució, emmagatzematge i seguretat en general dels sistemes d'accés als Fitxers.

3.6. Fitxers temporals

Tots els fitxers temporals que continguin dades personals generats per l'activitat de la FUOC, una vegada han complert la finalitat pel que van ser creats, són eliminats o incorporat a la següent execució del procés periòdic. Els fitxers temporals utilitzats com a entrada de noves cadenes, es conserven fins a completar l'execució de les mateixes.

Ocasionalment, en els casos de processos que consumin gran quantitat de temps de procés, es manté el resultat temporalment a tall de còpia seguretat. La cancel·lació dels fitxers es produeix quan el fitxer ha deixat de ser necessari o amb l'execució d'un nou procés en el supòsit que aquest sigui periòdic.

Els fitxers que complerta la seva finalitat no siguin eliminats hauran de complir totes les exigències legals i les mesures de seguretat establertes per als Fitxers mestres.

La generació de fitxers temporals per al lliurament a usuaris finals per al compliment d'alguna finalitat, es realitzarà sota la supervisió del Responsable dels Fitxers. L'usuari final serà l'encarregat de la cancel·lació dels fitxers una vegada complerta la seva finalitat.

3.7. Tractament no automatitzats de dades personals (Suport paper)

Addicionalment a ho disposat per als fitxers automatitzats en el present document de seguretat, per als tractaments de dades personals en suport paper, s'aplicaran les següents mesures de seguretat, recollides en el Capítol IV del Reial decret 1720/2007:

1. Per als fitxers de nivell Bàsic les recollides en la Secció 1ª (articles 105 a 108) del Capítol IV del RD1720/2007:
   a) Criteris d'arxiu: L'arxiu dels suports o documents es realitzarà d'acord amb els criteris previstos en la seva respectiva legislació. Aquests criteris haurien de garantir la correcta conservació dels documents, la localització i consulta de la informació i possibilitar l'exercici dels drets d'oposició al tractament, accés, rectificació i cancel·lació.

   b) En aquells casos en els quals no existeixi norma aplicable, el responsable del fitxer haurà d'establir els criteris i procediments d'actuació que hagin de seguir-se per a l'arxiu.

c) Dispositius d'emmagatzematge.: Els dispositius d'emmagatzematge dels documents que continguin dades de caràcter personal haurien de disposar de mecanismes que obstaculitzin la seva obertura. Quan les característiques físiques d'aquells no permetin adoptar aquesta mesura, el responsable del fitxer o tractament adoptarà mesures que impedeixin l'accés de persones no autoritzades.

d) Custòdia dels suports: Mentre la documentació amb dades de caràcter personal no es trobi arxivada en els dispositius d'emmagatzematge establerts en l'article anterior, per estar en procés de revisió o tramitació, ja sigui previ o posterior al seu arxiu, la persona que es trobi al càrrec de la mateixa haurà de custodiar-la i impedir en tot moment que pugui ser accedida per persona no autoritzada.

e) Els tractaments de dades no automatitzades fora de fora dels locals de tractament, haurien de ser autoritzats pel responsable dels fitxers, o persona que aquest designi, i s'haurien de prendre les mesures seguretat necessàries per a garantir la seva custòdia.

f) Per als fitxers de nivell mig, igual que per al seu tractament automatitzat es designarà un responsable de seguretat, i haurien de sotmetre's a una auditoria en idèntics termes que per als fitxers automatitzats.

g) Prestacions de serveis sense accés a dades personals: S'adoptaran les mesures necessàries per a limitar l'accés del personal a dades personals, als suports que continguin o als recursos del sistema d'informació, per a la realització de treballs que no impliquin el tractament de dades personals. Quan es tracti de personal aliè a l'organització, el contracte de prestació de serveis recollirà expressament la prohibició d'accedir a les dades personals i l'obligació de secret respecte a les dades que el personal hagués pogut conèixer amb motiu de la prestació del servei.

2. Per als fitxers de nivell Mig, s'aplicaran les mesures recollides en la Secció 2ª (articles 109) del RD1720/2007:

a) Igual que per al seu tractament automatitzat es designarà un responsable de seguretat, i haurien de sotmetre's a una auditoria en idèntics termes que per als fitxers automatitzats.

4. GESTIÓ DE SUPORTS INFORMÀTICS

Es consideren suports tots els sistemes que permetin l'enregistrament i recuperació de dades, i usats generalment per a realitzar còpies de seguretat o processos intermedis de les aplicacions que gestionen els Fitxers.

Tenint en compte que pràcticament la totalitat dels suports actualment utilitzats, com disquets, cintes, DVD's, CD-ROMs Pen Drives, discos durs externs…, són fàcilment transportables, reproduïbles i/o copiables, és evident la importància que per a la seguretat de les dades dels Fitxers té el control d'aquests mitjans

a) Els suports que continguin dades dels Fitxers, bé com a conseqüència d'operacions intermèdies pròpies de l'aplicació que els tracta, o bé com a conseqüència de processos periòdics de respatller o qualsevol altra operació esporàdica, haurien d'estar clarament identificats amb una etiqueta externa que indiqui el tipus d'informació que contenen (Fitxer), nombre d'ordre del suport.

b) En qualsevol cas, tots aquests suports haurien de ser degudament inventariats pel responsable dels Fitxers, que una vegada finalitzat el seu tractament, s'encarregarà de la seva custòdia i arxiu.

c) Aquells suports que siguin reutilitzables i que hagin contingut còpies de dades dels Fitxers, haurien de ser esborrats físicament abans del seu reutilització, de manera que les dades que contenien no siguin recuperables.

e) Els suports que continguin dades personals haurien de ser emmagatzemats en llocs als quals no tinguin accés persones no autoritzades per a l'ús dels Fitxers que no estiguin per tant relacionades en l'Annex F.

f) La sortida de suports informàtics que continguin dades personals fora dels locals on estan situats els Fitxers, haurà de ser expressament autoritzada pel responsable dels Fitxers, utilitzant per a això, l'annex F.

g) 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.

h) L'entrada i sortida de suports informàtics que continguin dades personals de fora dels locals on estan situats els Fitxers, haurà de ser expressament autoritzada pel responsable dels Fitxers, utilitzant per a això, el document adjunt en l'Annex F.

i) S'haurà de mantenir un sistema de registre d'entrades i sortides on es guardaran els formularis d'entrades i de sortides de suports descrits en el G, amb indicació de tipus

de suport, data i hora, emissor, nombre de suports, tipus d'informació que contenen, forma d'enviament, destinatari, o persona responsable de la recepció que haurà d'estar degudament autoritzada.

5. PROCEDIMENTS DE COPIES DE SEGURETAT I RECUPERACIÓ DE DADES

La protecció dels Fitxers que contenen dades de caràcter personal, no es redueix tan sols a protegir la confidencialitat dels mateixos, sinó que també, engloba altres aspectes com la integritat i la disponibilitat d'aquestes dades.

Com mesura de seguretat encaminada a garantir la integritat i disponibilitat de les dades, és fonamental l'existència d'uns procediments de còpies de seguretat i de recuperació que, en cas d'error o avaria del sistema informàtic, permetin recuperar i si escau reconstruir les dades dels Fitxers.

a) Els administradors del sistema o las persones designada, s'encarregaran de realitzar periòdicament una còpia de seguretat dels Fitxers, a l'efecte de respatller i possible recuperació dels mateixos en cas d'errors o avaries.

b) Les còpies de seguretat haurien d'executar-se amb una periodicitat mínima setmanal, excepte quan no s'hagi produït cap actualització de les dades.

c) Per als supòsits d'error o avaria que produeixin una pèrdua total o parcial de les dades personals que incorporen els Fitxers, existirà un procediment informàtic o manual que, partint de l'última còpia de seguretat i del registre de les operacions realitzades des del moment de la còpia, reconstrueixi les dades dels Fitxers a l'estat que es trobaven en el moment de l'error o avaria. Aquest procediment està descrit en l'Annex J.

d) El responsable dels fitxers, o la persona que aquest designi, s'encarregarà de verificar cada sis mesos la correcta definició, funcionament i aplicació dels procediments de realització de còpies de respatller i recuperació de dades.

e) Les proves anteriors a la implantació o modificació dels sistemes d'informació que tractin fitxers amb dades de caràcter personal no es realitzaran amb dades reals, tret que s'asseguri el nivell de seguretat corresponent al tractament realitzat i s'anoti la seva realització en el present document de seguretat.

f) En el cas que estigui previst la realització de proves amb dades reals, prèviament haurà d'haver-ne realitzat una còpia de seguretat.

6. FUNCIONS I OBLIGACIONS DEL PERSONAL

Aquesta normativa afecta a les següents categories de personal:

a) Responsable de fitxer. Com persona jurídica que, a través dels seus òrgans d'adreça, decideix sobre la finalitat, contingut, i ús del fitxer, es configura com Responsable del fitxer o Tractament. Així mateix, és el responsable jurídic de la seguretat dels Fitxers així com de la implantació de les mesures de seguretat corresponents.

b) Responsable de seguretat (fitxers nivell mig i alt). Serà l'encarregat de coordinar i controlar les mesures tècniques definides en el Document de Seguretat. Aquesta designació serà aplicable a la totalitat dels fitxers de la FUOC de nivell mig i alt, de manera que no suposa una delegació de responsabilitat per part del Responsable dels Fitxes, sinó l'obligació de controlar que el conjunt de les mesures tècniques de seguretat, previstes en el Reglament de mesures de seguretat i d'aplicació al tractament de dades personals es compleixen. El nomenament del Responsable de Seguretat es portarà a terme mitjançant el document que consta en l'Annex L - NOMENAMENTS.

c) Responsable protecció de dades. Serà l'encarregat de coordinar i controlar les mesures organitzatives definides en el Document de Seguretat, així com coordinar i controlar el compliment de les obligacions relatives al deure informació, consentiment, exercici de drets, deure secret i formació del personal. En qualsevol cas, complirà les indicacions del Responsable dels Fitxers, si les seves funcions han estat delegades. D'aquesta manera, tots aquells aspectes, prevists en la LOPD i desenvolupats pel RDLOPD haurien de ser supervisats per aquest. Aquesta delegació de funcions o nomenament no suposa una delegació de responsabilitat que correspon al Responsable dels Fitxers, i el seu nomenament serà aplicable a la totalitat dels fitxers inscrits titularitat de la FUOC. El nomenament del Responsable de Protecció de Dades es portarà a terme mitjançant el document que consta en l'Annex L - NOMENAMENTS.

d) Administradors del sistema o personal informàtic, la missió del qual és administrar i mantenir l'entorn operatiu dels Fitxers, tenint en compte que les funcions que realitzen i les eines que utilitzen, els pot permetre accedir a les dades protegides per altres vies distintes de les estipulades d'accés de les aplicacions. Haurien d'estar obligatòriament relacionats en l'Annex F.

e) Usuaris dels Fitxers, és a dir, tot el personal que habitualment utilitza el sistema informàtic d'accés als Fitxers. Estan explícitament relacionats en l'Annex F.*

f) El present document és d'obligat compliment per a tot el personal amb accés als Fitxers que continguin dades de caràcter personal. Les funcions i obligacions que els afecten es descriuen en l'Annex I. No obstant això, els administradors del sistema i personal informàtic, donada la seva peculiar posició, a més de les funcions i obligacions descrites en l'Annex I que afecten a tots els usuaris autoritzats, han de complir altres regles més completes i exigents.

La FUOC en compliment del article 89.2 del Reial Decret 1720/2007, que obliga a adoptar totes les mesures necessàries perquè el personal conegui de manera comprensible les normes de seguretat que afectin al desenvolupament de les seves funcions, així com les conseqüències que pogués incórrer en cas d'incompliment, ha habilitat l'annex I on s'inclouen els procediments d'informació als usuaris, on reconeixen i accepten les funcions i obligacions respecte al tractament de dades personals que recull el present Document de Seguretat.

* 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.

7. REGISTRE D'INCIDÈNCIES: PROCEDIMENTS DE NOTIFICACIÓ, GESTIÓ I RESPOSTA DAVANT LES INCIDÈNCIES

Una incidència és qualsevol situació que pugui produir-se ocasionalment i que pugui suposar un risc per a la seguretat dels Fitxers, des de l'òptica de la confidencialitat, integritat i disponibilitat de les dades.

El Reglament de mesures de seguretat obliga a mantenir un registre en el qual es faci constar les incidències que comprometin la seguretat dels Fitxers, ja que és una eina fonamental per a prevenir possibles atacs a la seguretat, així com per a la localització dels responsables dels mateixos.

La FUOC ha pres les següents mesures respecte al registre d'incidències:

a) Disposa de una eina informàtica (JIRA) de notificació, gestió i registre d'incidències que permet el seguiment d'aquestes i permet també crear un tipus d'incidència (problema, tasca, documentació, acta, incidència ...).

b) Qualsevol incidència que es produeixi, es registrarà al JIRA.

c) Qualsevol usuari que tingui coneixement d'una incidència que comporti risc per a la seguretat de les dades personals, és responsable de posar-lo en coneixement del seu Gestor de Demandes. El coneixement i la no notificació d'una incidència serà considerat com una falta contra la seguretat dels Fitxers per part d'aquest usuari.

d) El aplicatiu JIRA registra les següents dades: Codi de la incidencia, data d'alta de la incidencia, persona que crea la incidencia, persona a la que s'assigna la resolució de la incidencia, tipus d'incidència, prioritat, descripció de la incidencia, estat de la incidencia (Oberta / Tancada), resolució de la incidencia, i les activitats relacionades amb la incidència (Procediments per resoldre la incidència)

La FUOC, desitja tenir constància de quantes incidències de seguretat es produeixin sobre les dades dels Fitxers que tracta, i a aquest efecte , a continuació, descriu de forma merament exemplificativa i sense ànim de delimitar-les, una llista de les quals haurien de ser inexcusablement registrades, que podrà ser ampliada amb altre tipus d'incidències que poguessin haver quedat omeses:

- Incidències que afectin a la identificació i autenticació dels usuaris:
  - Pèrdua de confidencialitat de les contrasenyes
  - Períodes de desactivació de les eines de seguretat.
- Incidències que afectin als drets d'accés a les dades:
  - Revisió o coneixement d'intents fallits d'accessos i accessos fora d'hores d'oficina.
  - Comunicació dels usuaris de sospites que algú ha suplantat la seva personalitat.
  - Detecció de punts d'accés desatesos i sense protecció de pantalla activada.
  - Detecció de contrasenyes escrites en els llocs de treball.
- Incidències que afectin a la gestió de suports:
  - Comunicació de pèrdua de suports.
  - Comunicació de localització de suports en llocs inadequats.
  - Errors de contingut en suports rebuts.
- Incidències que afectin als procediments de còpies de salvaguarda i recuperació, com errors en els processos de realització de còpies de salvaguarda.

- Qualsevol altra incidència observada com a conseqüència del compliment dels controls i mesures de seguretat definits en el present document de seguretat.

8. ACCÉS A INTERNET i ÚS DEL CORREU ELECTRÒNIC

Internet s'ha consolidat com un dels mitjans més utilitzats i eficaços per a l'accés i transmissió de dades, ja sigui per mitjà de navegació per la xarxa, correu electrònic, o per sistemes de transferència de fitxers. Per tant, la visualització, i l'entrada i sortida de dades a través de la Xarxa, mereix un tractament específic donades les seves particularitats i els riscos que comporta, tenint en compte la seva especial vulnerabilitat.

8.1. Correu Electrònic

1. 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).
2. 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.

8.2. 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.

9. CONTROLS DE VERIFICACIÓ i AUDITORIES

Tenint en compte la importància de la veracitat de les mesures de seguretat contingudes en el present document, així com el compliment de les mateixes, la FUOC comprovarà el present document de seguretat, de manera que puguin detectar-se i resoldre's possibles anomalies.

1. Es comprovarà periòdicament, que la llista d'usuaris autoritzats de l'Annex F es correspon amb la llista dels usuaris realment autoritzats en l'aplicació d'accés als Fitxers. En cas de modificació es realitzarà la pertinent alta o baixa d'usuaris amb entrada autoritzada als Fitxers.

2. Es comprovarà també periòdicament, l'existència de còpies de respatller que permetin la recuperació de Fitxers segons l'estipulat en aquest document.

3. Es comprovarà qualsevol canvi que s'hagi realitzat en les dades tècniques dels annexos, com per exemple, canvis en els sistemes informàtics, base de dades o aplicacions d'accés als Fitxers, procedint igualment a l'actualització d'aquests annexos.

4. Es comprovarà i verificarà periòdicament, el compliment del previst en els apartats d'aquest document en relació amb les entrades i sortides de dades, siguin per la xarxa o mitjançant qualsevol tipus de suport.

5. S'analitzessin periòdicament les incidències registrades en el model corresponent, per a independentment de les mesures particulars que s'hagin adoptat en el moment que es van produir, adoptar les mesures correctores que limitin aquestes incidències en el futur.

6. Per als Fitxers de nivell mig, almenys cada dos anys, es realitzarà una auditoria externa o interna que dictamini el correcte compliment i adequació de les mesures recollides en el present document de seguretat, identificant les deficiències i proposant les mesures correctores necessàries.

7. De produir-se en qualsevol de les comprovacions algun canvi rellevant, s'anotarà en l'Annex corresponent.

ANNEX A - FITXERS NOTIFICATS EN EL REGISTRE GENERAL DE PROTECCIÓ DE DADES

S'adjunta una relació dels Fitxers inscrits en el Registre General de Protecció de Dades de la Agència Catalana de Protecció de dades amb els seus corresponents codis d'inscripció, al costat de les còpies dels documents remesos per l'Agència Catalana de Protecció de Dades, així com de les modificacions i supressions efectuades.

FITXERS INSCRITS

FITXERS
FITXER DE RECURSOS HUMANS
FITXER DE CONSULTORS I TUTORS
FITXER DE GESTIÓ ACADÈMICA
FITXER DE CAMPUS PER LA PAU
FITXER DE EMPRESES
FITXER DE ADMINISTRACIÓ
FITXER DE EMPRESES
FITXER DE CAMPUS VIRTUAL

FITXER DE INFORMACIÓ
FITXER DE SEGURETAT

ANNEX B – ENCARREGATS DE TRACTAMENT

En el present annex es descriuen totes les prestacions de serveis que impliquen l'accés als fitxers per part de tercers en els següents supòsits:

a) **La FUOC com encarregada de tractament en relació a les empreses que componen el GRUP UOC (Editorial UOC, S.L. / Eureca Media, S.L. / EducaciOnline, S.L. / Xarxa Virtual de Consum "La Virtual").**

b) **Proveïdors de la FUOC, que actuen com encarregats de tractament per la prestació de diversos serveis.**

Tots aquests tractaments es realitzen complint les exigències de l'article, 12 de la LOPD i en el Capítol III (art. 20, 21 i 22) del Reial decret 1720/2007.

a) **Relació de serveis prestats per la FUOC a les empreses del Grup UOC:**

1. Serveis estratègics i d'organització empresarial
2. Gestió i control laboral i gestió de nòmines
3. Outsourcing laboral (cessió de treballadors)
4. Recursos humans
5. Assessoria administrativa, econòmica, fiscal i comptable.
6. Facturació de serveis prestats
7. Serveis jurídics
8. Assessorament de processos de gestió de qualitat
9. Prevenció de riscos laborals
10. Formació
11. Central de compres i lloguer d'instal·lacions
12. Gestió Comercial i publicitària.
13. Serveis informàtics
14. Allotjament bases de dades, web i correu electrònic.

Editorial UOC, S.L.

Fitxers	Dades Accedides	Serveis	Contracte
Recursos Humans	Treballadors, Candidats	1,7,11,13,14	01/01/2008
Clients	Clients	1,7,11,13,14	01/01/2008
Comercial	Potencials Clients	1,11,13,14	01/01/2008
Administració	Treballadors, Clients, Proveïdors	1, 11,13,14	01/01/2008
Distribuïdors	Distribuïdors	1, 11,13,14	01/01/2008
Autors	Autors	1, 11,13,14	01/01/2008

Eureca Media, S.L.

Fitxers	Dades Accedides	Serveis	Contracte
Recursos Humans	Treballadors, Candidats	1,7,11,13,14	01/01/2008
Clients	Clients	1,7,11,13,14	01/01/2008
Comercial	Potencials Clients	1,11,13,14	01/01/2008
Administració	Treballadors, Clients, Proveïdors	1, 11,13,14	01/01/2008

EduaciOnline, S.L.

Fitxers	Dades Accedides	Serveis	Contracte
Personal	Treballadors, Candidats	13,14	01/01/2008
General	Alumnes, antics alumnes, potencials alumnes	13,14	01/01/2008
Proveïdors	Proveïdors	13,14	01/01/2008

Xarxa Virtual de Consum "La Virtual"

Fitxers	Dades Accedides	Serveis	Contracte
Recursos Humans	Treballadors, Candidats	1,2,3,4,7,8,9,10,11,13,14	01/01/2008
Administració	Treballadors, Clients, Proveïdors	1,,5,6,7,8,11,13,14	01/01/2008
Socis	Socis cooperativa	1,5,6,7,8,12,13,14	01/01/2008

b) Proveïdors de la FUOC, que actuen com encarregats de tractament per la prestació de diversos serveis. (Veure Fulla Excel "Llistat Proveïdors adjunta)

Denominació	Serveis Prestas	Acces a Fitxers

Tots els accessos descrits s'han plasmat en els corresponents contractes o clàusules de confidencialitat, a tenor de l'estipulat en l'article. 12 de la LOPD. S'adjunten al present document de seguretat, còpies de cadascun dels contractes, on es recullen les condicions, dates d'inici dels accessos i les identitats dels encarregats de tractament.

ANNEX C - DESCRIPCIÓ, FINALITAT I ESTRUCTURA DELS SISTEMES INFORMÀTICS D'ACCÉS ALS FITXERS

1. Ubicació del Fitxers

Els Fitxers referenciats en l'Annex A, es troben allotjats en els sistemes informàtics situats en el Centre de Processament de Dades (CPD) situat a Castelldefels (principalment) i en les oficines centrals d'Av. Tibidabo 39-43 de Barcelona.

La FUOC presta serveis informàtics com encarregat de tractament a la resta d'empreses del grup (EDITORIAL UOC, S.L., EURECA MEDIA, S.L., EDUCACIONLINE, S.L., i XARXA VIRTUAL DE CONSUM "LA VIRTUAL"), tant el des de l'òptica dels sistemes i equips informàtiques, sinó també dels procediments (còpies de seguretat, contrasenyes, polítiques de seguretat...).

2. Descripció del 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 hardware 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.

Així mateix, 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.

Tota transmissió de dades per mitjà de les línies de comunicacions entre les oficines centrals i altres centres de treball viatgen encriptades.

Els fitxers són tractats des de les terminals informàtiques convencionals (PC i Portàtils), totes connectades a la xarxa local i corporativa de l'empresa.

Per regla general, no s'utilitzen els discos durs locals de les terminals, excepte en casos excepcionals i per a processos temporals i amb dades que provenen dels fitxers mestres. En manual de funcions i obligacions dels usuaris, prohibeix la seva utilització, excepte en els casos especificats.

3. Sistemes d'organització i tractament de les dades

Tots els usuaris disposen d'un nom d'usuari i una contrasenya individual amb perfils d'accés en funció de la feina desenvolupada.

Les terminals informàtiques tenen una ubicació individualitzada per usuari, i el seu accés està controlat per un responsable, i només els usuaris autoritzats en l'annex F tenen accés.

Els accessos a les aplicacions estan restringits en funció de perfils d'accés segons el lloc ocupat en l'empresa i la tasca desenvolupada. La informació no continguda en aplicacions específiques (ofimàtica), es poden guardar en carpetes comuns per departaments, individuals per usuari, i també es disposa d'una carpeta Windows per a arxius generals comuns, totes ubicades en els servidors de dades.

Exclusivament el personal del departament informàtic i els encarregats dels fitxers tenen accés a tots els sistemes informàtics.

4. Procediment de control d'accés i de seguretat a l'equipament informàtic

4.1 En el centres de procés de dades estan instal·lats tots els servidors centrals de xarxa, els equips de xarxa i comunicacions centrals i les consoles d'operació que formen part de l'equipament informàtic de la companyia que assegura la continuïtat del negoci.

4.2 El centre de procés de dades, està situat en una dependència aïllada separada de la resta de llocs de treball, i no és accessible per cap persona no autoritzada en l'Annex F (administradors del sistema i personal informàtic).

4.3 FUOC s'ha establert una política de seguretat física, en la qual es permet l'accés exclusivament al personal informàtic i administradors del sistema. El centre de procés de dades està protegit amb diversos sistemes de seguretat.

5. Descripció, finalitats i estructura de les aplicacions d'accés als Fitxers

5.1.- 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	RRHH
Académica	GAT-Formac	Informació dels alumnes de màster i postgrau	Pròpia	GAT
Marketing	PCRM	Persones que han sol·licitat a la UOC informació	Pròpia i Standard	INFORMACI.
Economia	COFROS	Comptabilitat de la UOC	Standard	GESTIÓ COMPTABLE
Infrastructura	GAME	Distribució de material	Pròpia	GAT
Académica	EVIU	Gestió acadèmica dels alumnes del curs d'anglès	Pròpia	GAT

5.1.1.- 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	***Àmbit d'accessos***
Senegal.uoc.es	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	***Àmbit d'accessos***

Cuba.uoc.es	Usuaris autoritzats de la xarxa corporativa, i dels serveis oferts per la UOC als seus alumnes.

Aplicatiu	***Responsable***
CURRO	
Fitxer	***Descripció de l'aplicatiu***
RECURSOS HUMANS	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 i entitats externes relacionades amb la UOC.
Ubicació	***Àmbit d'accessos***
Ruanda.uoc.es	Usuaris autoritzats de la xarxa corporativa. Grups operatius: a) RRHH, b) Campus Virtual, c) GAT, d) Economia

Aplicatiu	***Responsable***
GAT FORMACIÓ	
Fitxer	***Descripció de l'aplicatiu***
GAT	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	***Àmbit d'accessos***
Brunei.uoc.es	Usuaris autoritzats de la xarxa corporativa. Grups operatius: a) Formació continuada, b)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	***Àmbit d'accessos***
Senegal.uoc.es	Usuaris autoritzats de la xarxa corporativa. Grups operatius: Marketing

Aplicatiu	***Responsable***
COFROS	
Fitxer	***Descripció de l'aplicatiu***
ADMINISTRACIÓ	Comptabilitat de la UOC.
Ubicació	***Àmbit d'accessos***

Benin.uoc.es	Usuaris autoritzats de la xarxa corporativa. Grups operatius: a) GAT, b) Economia

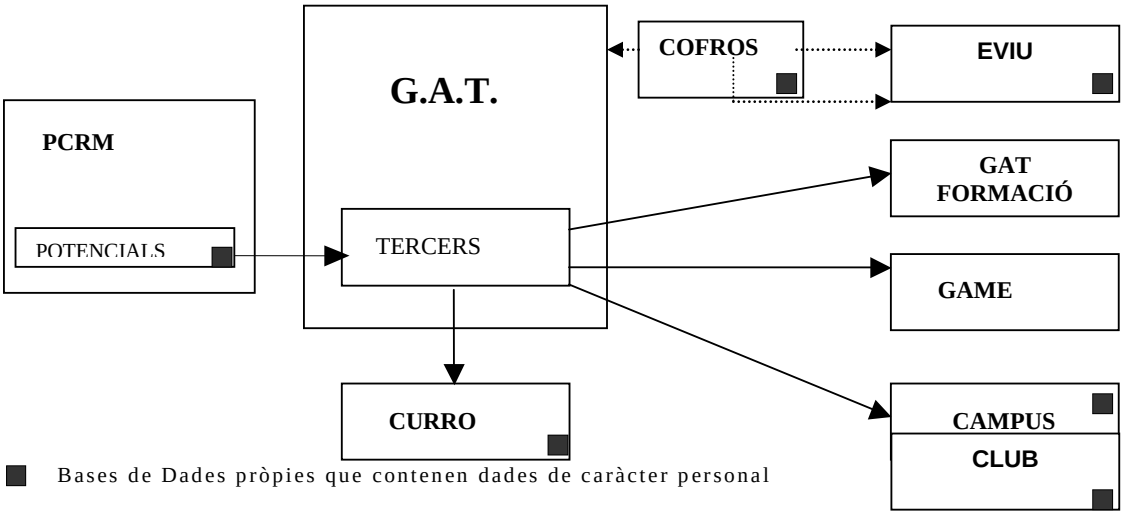
Aplicatiu	***Responsable***
GAME	
Fitxer	***Descripció de l'aplicatiu***
GAT	Comptabilitat de la UOC.
Ubicació	***Àmbit d'accessos***
Senegal.uoc.es	Usuaris autoritzats de la xarxa corporativa. Grups operatius: Infrastructura

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

5.1.2.- 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.



5.2.- Estructura del fitxers protegits

5.2.1.- Base de Dades 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	
☐ SALUD	
Datos de carácter identificativo	**Datos de características personales**
▣ DNI / NIF ▣ N SS/ MUTUALIDAD ▣ NOMBRE Y APELLIDOS ▣ DIRECCION ▣ TELEFONO ▣ FIRMA /HUELLA ▣ IMAGEN / VOZ	▣ DATOS DE ESTADO CIVIL ▣ DATOS DE FAMILIA ▣ FECHA / LUGAR DE NACIMIENTO ▣ SEXO ▣ NACIONALIDAD
Datos de circunstancias sociales	**Datos de información comercial**
Datos académicos y profesionales	**Datos de detalle del empleo**
▣ FORMACION, TITULACIONES ▣ HISTORIAL DEL ESTUDIANTE	▣ PROFESION
Datos de transacciones	**Datos económico – financieros**
▣ BIENES Y SERVICIOS RECIBIDOS POR EL AFECTADO ▣ TRANSACCIONES FINANCIERAS	▣ CREDITOS, PRESTAMOS, AVALES ▣ DATOS BANCARIOS (Cuentas...) ▣ DATOS ECONOMICOS DE NOMINA ▣ SEGUROS ▣ SUBSIDIOS, BENEFICIOS ▣ TARJETAS CREDITO

5.2.2.- Base de Datos INFORMACIÓ

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

Datos de carácter identificativo	Datos de características personales
▣ DNI / NIF ▣ NOMBRE Y APELLIDOS ▣ DIRECCION ▣ TELEFONO ▣ FIRMA /HUELLA	▣ DATOS DE ESTADO CIVIL ▣ FECHA / LUGAR DE NACIMIENTO ▣ SEXO ▣ OTROS (indicar) - Uso de ordenador…… - Uso de Internet…… - Medio de contacto con la UOC……
Datos de circunstancias sociales	**Datos de información comercial**
Datos académicos y profesionales	**Datos de detalle del empleo**
▣ FORMACION, TITULACIONES	▣ PROFESION ▣ OTROS (indicar) - Sector de actividad de la empresa...
Datos de información comercial	**Datos económico – financieros**
Datos de transacciones	

5.2.3.- 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 de carácter identificativo	Datos de características personales
▣ DNI / NIF ▣ N SS/ MUTUALIDAD ▣ NOMBRE Y APELLIDOS ▣ DIRECCION ▣ TELEFONO ▣ FIRMA /HUELLA ▣ IMAGEN / VOZ ▣ OTROS: Dirección de envio.	▣ DATOS DE ESTADO CIVIL ▣ DATOS DE FAMILIA ▣ SEXO ▣ NACIONALIDAD
Datos de circunstancias sociales	**Datos de información comercial**
Datos académicos y profesionales	**Datos de detalle del empleo**
▣ FORMACION, TITULACIONES ▣ HISTORIAL DEL ESTUDIANTE ▣ EXPERIENCIA PROFESIONAL	▣ PROFESION ▣ PUESTOS DE TRABAJO
Datos de transacciones	**Datos económico – financieros**

	▣ CREDITOS, PRESTAMOS, AVALES ▣ DATOS BANCARIOS (Cuentas...)

5.2.4.- 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 de carácter identificativo	Datos de características personales
▣ DNI / NIF ▣ N SS/ MUTUALIDAD ▣ NOMBRE Y APELLIDOS ▣ DIRECCION ▣ TELEFONO ▣ FIRMA /HUELLA	▣ DATOS DE ESTADO CIVIL ▣ DATOS DE FAMILIA ▣ FECHA / LUGAR DE NACIMIENTO ▣ SEXO
Datos de circunstancias sociales	**Datos de información comercial**
Datos académicos y profesionales	**Datos de detalle del empleo**
▣ FORMACION, TITULACIONES	▣ PROFESION ▣ PUESTOS DE TRABAJO ▣ HISTORIAL DEL TRABAJADOR
Datos de transacciones	**Datos económico – financieros**
	▣ DATOS BANCARIOS (Cuentas...) ▣ DATOS ECONOMICOS DE NOMINA

5.2.5.- Base de Datos GESTIÓ COMPTABLE

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

Datos de carácter identificativo	Datos de características personales

▣ DNI / NIF ▣ NOMBRE Y APELLIDOS ▣ DIRECCION	▣ NACIONALIDAD
Datos de circunstancias sociales	**Datos de información comercial**
Datos académicos y profesionales	**Datos de detalle del empleo**
Datos de transacciones	**Datos económico – financieros**
▣ TRANSACCIONES FINANCIERAS ▣ OTROS (indicar) - Facturas , Cobros/Pagos	▣ DATOS BANCARIOS (Cuentas...)

5.2.6.- Base de Datos TRAMESES

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

Datos de carácter identificativo	**Datos de características personales**
▣ DNI / NIF ▣ NOMBRE Y APELLIDOS ▣ DIRECCION ▣ TELEFONO	
Datos de circunstancias sociales	**Datos de transacciones**
Datos académicos y profesionales	**Datos de detalle del empleo**
Datos de información comercial	**Datos económico – financieros**

5.2.7.- 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 de carácter identificativo	Datos de características personales
▣ DNI / NIF ▣ NOMBRE Y APELLIDOS ▣ DIRECCION ▣ IMAGEN / VOZ	▣ FECHA / LUGAR DE NACIMIENTO ▣ SEXO
Datos de circunstancias sociales	**Datos de transacciones**
Datos académicos y profesionales	**Datos de detalle del empleo**
▣ OTROS: Curriculum personal	
Datos de información comercial	**Datos económico – financieros**

5.2.8.- Base de Datos CLUB

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

Datos de carácter identificativo	Datos de características personales
■ DNI / NIF ■ NOMBRE Y APELLIDOS ■ DIRECCION ■ TELEFONO	■ FECHA / LUGAR DE NACIMIENTO ■ SEXO ■ NACIONALIDAD .....
Datos de circunstancias sociales	**Datos de transacciones**
Datos académicos y profesionales	**Datos de detalle del empleo**
Datos de información comercial	**Datos económico – financieros**

5.2.9.- Base de Datos EVIU

Responsable:		**Descripción del fichero**
Aplicativo:	EVIU	Dades personals dels alumnes
Fichero:	EVIU	
Tipo:	ORACLE	

Ubicación:	Brunei.uoc.es	

Datos de carácter identificativo	Datos de características personales
■ DNI / NIF ■ NOMBRE Y APELLIDOS ■ DIRECCION ■ TELEFONO	■ FECHA / LUGAR DE NACIMIENTO ■ SEXO ■ NACIONALIDAD
Datos de circunstancias sociales	**Datos de transacciones**
Datos académicos y profesionales	**Datos de detalle del empleo**
Datos de información comercial	**Datos económico – financieros**
	■ DATOS BANCARIOS (Cuentas...)

5.2.10.- Altres aplicacions:

1 Correu electrònic: Per a l'enviament i recepció de missatges, així com la per a conservació en la llibreta d'adreces dels diferents e-mails de remitents i destinataris, s'utilitza el gestor de correu electrònic Microsoft Outlook i la seva agenda de contactes.

2 Agendes de contactes electròniques de PDA's, exclusivament autoritzades per a l'equip directiu.

3 Microsoft Office: Com aplicacions de suport per a processos administratius i temporals, especialment, documents de Word, fulls de càlcul Excel i Power Point.

4 Aplicacions on-line d'entitats bancàries: Pagaments de nòmines i a proveïdors a través d'aplicacions on line d'entitats bancàries, protegides per contrasenya i solament coneguda pels usuaris expressament autoritzats.

6. Descripció del equipament informàtic principal

6.1. Servidors

Conjunt de servidors, del que destaquen els següents:

- Servidors principals: Fitxers, Dades.
- Servidors de red.
- Servidors de copies de seguretat.

6.2 Estacions de treball

Parc de d'ordinadors de sobretaula, format torre i portàtils.

6.3 Impressores

Conjunt d'impressores de xarxa, la major part compartides i distribuïdes per les àrees de treball.

6.4. Fax:

Equipament de faxs compartits, distribuïts per zones accessibles per les distintes àrees de treball

6.5 Escáner

Es disposa de diversos equips d'escaneo de documentació.

6.6 Fotocopiadores:

Equipament de fotocopiadores compartides, distribuïts per zones accessibles per les distintes àrees de treball

7. Tractament i gestió de dades personals en suport paper

7.1. Tota documentació en paper que contingui dades personals responsabilitat de la FUOC serà objecte d'arxiu amb les mesures que garanteixin la seguretat de la informació continguda o bé, serà objecte de destrucció per les màquines de destrucció de paper destinades a aquest efecte, seguint el procediment corresponent.

7.2. En aquelles ubicacions en les quals no es disposi de destructores de paper, es prendran les mesures oportunes per a impedir la seva posterior visualització, i es dipositarà el paper en els llocs habilitats per a la seva deixalla.

7.3. El suport en paper no podrà ser reutilitzat, tret que es garanteixi que no conté informació confidencial o de caràcter personal.

7.4. Els usuaris haurien d'assegurar-se que no queden documents impresos que continguin dades protegides en la safata de sortida de les impressores i fotocopiadores

7.5. La FUOC haurà de facilitar els mitjans necessaris per a evitar que persones no autoritzades tinguin accés a aquells documents impresos dels centres de la FUOC que continguin dades especialment sensibles.

7.6. Les impressores, faxos o altres dispositius que imprimeixin dades personales haurien d'estar físicament situats en llocs que garanteixin aquesta confidencialitat.

ANNEX D – TOPOLOGIA DEL SISTEMA D'INFORMACIÓ

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 Castelldefels i secundàriament a las seu central (UOC), excepte tres servidors de Xarxa Interna que es troben instal·lats en els locals de Diputació, i Drassanes.

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

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 Castelldefels 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

ANNEX E - CONTROL D'ACCÉS ALS LOCALS I LLOCS DE TREBALL

La FUOC desenvolupa la seva activitat principal en diferents centres de treball entre els quals destaquen els següents:

- Seu Social: Avinguda Tibidabo, nº 39-43, Barcelona.
- Base d'operacions: Rambla del Poble Nou, nº 156, Barcelona.
- Centre de Processament de Dades: Edifici UOC-IN3 de Castelldefels.

Així mateix, disposa d'altres centres de treball de menor entitat i de centres de suport que en la seva majoria són gestionades per organismes col·laboradors, que actuen com encarregats de tractament.

En tots els centres, independentment del seu grau d'importància, estan obligats a complir la normativa descrita a continuació:

1. Control d'accés físic

S'implantaran controls d'accés físic, de manera que exclusivament el personal autoritzat expressament pugui tenir accés a:

- Els centres de treball. El personal extern haurà de ser identificat i registrat pel personal de recepció.
- Les sales o despatxos on es trobin situats informes d'usuaris i personal de l'organització.
- Las sales on es troben els servidors.
- Les dependències on estiguin instal·lats ordinadors personals que continguin fitxers amb dades de caràcter personal.

Aquest accés autoritzat es podrà realitzar sota les següents condicions:

- Tenen accés als diferents locals que disposa la FUOC per a l'exercici de la seva activitat exclusivament el personal intern de l'empresa. Aquesta autorització d'accés físic és atorgada a cada treballador en el moment de la signatura del contracte laboral, i és revocada i per tant anul·lada quan deixa de pertànyer a la plantilla de treballadors de l'empresa, no podent accedir més a les instal·lacions, tret que ho faci en règim de visita i amb la pertinent autorització del responsable dels Fitxers.

- Les terceres persones que en qualitat de visitant o de personal de serveis externs accedeixin a qualsevol dels locals on la FUOC desenvolupa les seves activitats, han de contar amb el beneplàcit del corresponent responsable, i en cap cas tindran accés específic als llocs on es trobin els sistemes d'informació dels Fitxers. Aquests accessos físics sempre es realitzaran en presència de personal autoritzat de l'empresa.
- El personal que observi la presència de personal estrany a l'àrea haurà de notificar-lo immediatament.
- Els drets d'accés han de revocar-se immediatament al personal que deixi l'ocupació.
- Els locals haurien de contar amb els mitjans mínims de seguretat que evitin els riscos de indisponibilitat de la informació que poguessin produir-se com a conseqüència d'incidències fortuïtes o intencionades.
- Les pantalles de visualització de dades estan orientades en posicions que no permeten veure amb facilitat a tercers aliens a l'empresa el contingut d'aquestes.
- Cap armari o prestatgeria és accessible per persones alienes a l'empresa.
- Els terminals informàtiques tenen una ubicació individualitzada per usuari, i el seu accés està controlat per un responsable, i només els usuaris autoritzats en l'annex F tenen accés.

2. Sistemes de seguretat física

FUOC disposa de les mesures de seguretat necessàries per a impedir l'accessibilitat als seus locals per persones no autoritzades durant i fora dels horaris laborals.

2.1. Accés als edificis:

- Controls d'accessos mitjançant cameres de videovigilancia instal·lades en les entrades dels edificis principals de la FUOC. S'han instal·lat els corresponents cartells identificatius en compliment de la instrucció 1/2006 en relació a la LOPD.
- Control d'accés presencial portat a terme pel personal de recepció d'us diferents centres de treball, on se sol·licita al visitant: nom i cognoms, nº de document nacional d'identitat, persona a la qual pretén visitar, i quan sigui preceptiu, l'empresa a la qual pertany.

2.2. Accés als Centres de Processament de dades:

- L'accés a la sala d'ordinadors, on situïn tots els servidors de fitxers, és prohibit a tot el personal aliè a l'àrea esmentada.
- Les portes d'accés estan controlades per mitjà de sistemes de seguretat biomètrics (empremta digital) configurades per a l'accés exclusiu al personal autoritzat.

2.3. Mesuris de Seguretat:

a) Generals:

- Respecte a l'equipament necessari per a la prevenció d'incendis, es disposa de l'organització: mitjans i instal·lacions necessàries exigides per la Llei i, si escau, per les Ordenances Municipals vigents com, segons el local, sistemes de detecció i alarma i extintors adequats en nombre i tipus d'agent extintor; de la mateixa manera, els materials de revestiment s'adeqüen a la normativa legal vigent i es troba al dia, conforme a les inspeccions administratives de seguretat.
- Sistemes de continuïtat: compte en totes les seves instal·lacions amb enllumenat d'emergència per a permetre l'evacuació fàcil i segura del públic i empleats cap a l'exterior i enllumenat de senyalització que permet la perfecta localització i d'una manera permanent la situació de portes, passadissos i sortides de locals, ambdós alimentats d'acord amb la normativa legal vigent.
- Els edificis disposen d'alarmes connectades a la central d'alarmes de l'empresa de seguretat subministradora de la mateixa.

b) Equips informàtics:

- Generador elèctric propi capaç de subministrar energia autònomament a l'equipament informàtic, per a supòsits d'interrupcions perllongades del subministrament elèctric, i que garanteix la continuïtat del negoci.
- Per a casos d'interrupcions del subministrament elèctric, es conta amb Sistemes d'Alimentació Ininterrompuda (SAI) que garanteixen l'energia pròpia durant una hora i protegeixen els sistemes informàtics i les seves dades contra les interrupcions del corrent.
- Les còpies de seguretat i qualsevol suport que reculli dades de caràcter personal, es custodien en caixes fortes ignífugas situades en l'interior dels centres de processament de dades. El seu accés és exclusiu al Responsable dels Fitxers o persona que aquest designi.
- Els Centres de Processament de Dades estan dotats de Dispositius d'alarma i sistemes contra incendis basat en bombons de gas, detectors de fum iònics repartits en sostre i fals terra, difusors de 360º, avisadors acústics, i central d'alarmes multizona.

- Així mateix, els Centres de Processament de Dades disposen de Sistemes de refrigeració, i Sistema de detecció d'humitat.

ANNEX F - AUTORITZACIONS D'ACCÉS ALS FITXERS I ZONES RESTRINGIDES

(Veure FULLA EXCEL "AUTORITZACIONS/DEPARTAMENTS")

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:

ADMINISTRADORS DELS FITXERS

Nom i cognoms	Àrea	Accessos	Restriccions

ADMINISTRADORS DEL SISTEMA O PERSONAL INFORMÀTIC

Nom i cognoms	Àrea	Accessos	Restriccions

PERSONAL AUTORITZAT PER A ACCEDIR AL CENTRE DE PROCÉS DE DADES

Nom i cognoms	Àrea	Accessos	Restriccions

PERSONAL AUTORITZAT PER A LA SORTIDA DE SUPORTS INFORMÀTICS

Nom i cognoms	Àrea	Accessos	Restriccions

USUARIS DEL FITXER

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:

Nom i Cognoms	*Centre de Treball*	*Lloc de Treball/ Accessos*	*Restriccions*

Nom i Cognoms	Centre de Treball	Lloc de Treball/ Accessos	Restriccions

ANNEX G - PROCEDIMENTS DE SEGURETAT: SEGURETAT LÒGICA

1.- Sistema d'autenticació

1.1. Identificació

1. FUOC ha establert un sistema d'identificació i autenticació inequívoc i personalitzat per als seus usuaris, com mesura de seguretat per a evitar accessos no autoritzats als sistemes informàtics que allotgen els Fitxers, i que contenen dades de caràcter personal.

2. Tot el personal de FUOC amb accés autoritzat al sistema informàtic que conté els Fitxers, posseeix un nom d'usuari i una contrasenya com mesura d'identificació i autenticació.

3. 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.

4. 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.

5. Els administradors mantindran un registre de les sol·licituds presentades. Les altes del personal intern de la FUOC, les gestiona el departament de recursos humans.

6. 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.

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.

1.3. Assignació de contrasenyes

1. És competència del departament de recursos humans la assignació de les contrasenyes del personal intern de la FUOC, la resta de assignacions, depenen dels administradors del sistema.

2. 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.

3. 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.

4. 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.

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. L'usuari no té l'obligació de modificar la primera contrasenya assignada, no obstant això, assumeix tota la responsabilitat respecte a la mateixa.

3. La distribució de contrasenyes es realitza de forma inintel·ligible.

4. Les gran majoria d'aplicacions, servidors de dades i web , disposen de Logs de contrasenyes.

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.

1.6. Característiques de les contrasenyes

Les contrasenyes d'accés són exclusivament conegudes per l'usuari propietari de les mateixes i pel responsable dels Fitxers o si escau l'administrador del sistema o cap del departament de recursos humans.

Els usuaris tenen l'obligació de tractar-les com informació confidencial, personal i intransferible.

Cadascun els usuaris de la FUOC es responsabilitza d'assegurar la confidencialitat i custòdia de la seva contrasenya.

La FUOC ha establert certes consideracions a l'hora de triar les contrasenyes:

Longitud mínima	6-8 caràcters
Canvi de contrasenyes	Automàtic cada 90 dies. Prohibició als usuaris de repetir l'última contrasenyes
Responsable canvi	Administradors del sistema
Control d'introducció de contrasenyes errònies	Umbral de bloqueig: 5 intents.
Obligacions i Prohibicions	- S'evitaran noms comuns, nombres de matrícules, telèfons, noms de familiars, amics, etc., i derivats del nom de l'usuari com permutacions o canvi d'ordre de les lletres, transposicions, repeticions d'un únic caràcter, etc… - Els usuaris seran responsables també de la seva salvaguarda i custòdia.

La FUOC ha adoptat sistemes o aplicacions comuns, que realitzen l'autenticació de l'usuari, permetent de forma general:

a) La introducció de la contrasenya, i la seva representació en pantalla en el moment de la identificació es realitzarà en un format inintel·ligible.

b) El sistema informàtic o si escau les aplicacions que requereixen control d'usuaris, emmagatzemen les contrasenyes en un format inintel·ligible.

c) La FUOC disposa la deguda assistència per a evitar supòsits que algun usuari oblidi o tingui qualsevol dificultat que li impedeixi l'accés per mitjà de la seva contrasenya.

d) En els sistemes o aplicacions que continguin dades de nivell mig, es controlaran els intents d'accés fraudulent al Fitxer, limitant el nombre màxim d'intents fallits..

2.- Sistema de control d'accessos

2.1.- Perfils d'usuari

1. La FUOC aplica com política d'accés la del mínim privilegi, en el sentit de permetre exclusivament l'ús dels Fitxers que contenen dades de caràcter personal als treballadors que ho requereixin per a l'exercici de les seves funcions i exclusivament als recursos que per als quals estiguin autoritzats.

2. 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.

3. El sistema de control d'accessos es basa en un conjunt de relacions establertes 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.

4. El Responsable dels Fitxers, és l'únic amb autoritat per a realitzar altes, baixes, modificacions i revocacions d'identificadors d'usuaris en qualsevol nivell d'accés d'informació: sistema operatiu, aplicacions, gestors de bases de dades, xarxes de comunicacions.

5. Per al compliment de tots els procediments esmentats, el Responsable dels Fitxers podrà delegar totes les seves funcions en un Administrador del sistema o en la persona que designi expressament, sempre que consti en l'Annex F.

2.2.- 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.

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.

ANNEX H - CÒPIES DE SEGURETAT i RECUPERACIÓ 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.

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 4 d'aquest document.

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 en el 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.

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.

Els procediments de còpia de seguretat i de recuperació de dades s'aplicaran tant en els sistemes informàtics del centre de processament de dades de Castelldefels, com de les oficines centrals d'Av. Tibidabo.

2.1. Sistema, Freqüència, Vigència i Històric de les còpies

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.

Suport de les còpies	Cintes LTO i LTO2
Sistema de còpies	Sistema de Còpies UNIX que conté els fitxers, els aplicatius i els sistemes dels servidors UNIX, en els quals resideixen els fitxers protegits.
Tipus de còpia	Automàtica
Numero de suports	Variable en funció de les activitat El nº exacte està reflectit en l'inventari i històric de cintes..
Vigència / Històric	2 mesos / Mensual
Freqüència copia	Diària incremental i còpia total setmanal
Responsable còpia	Administradors del sistema

2.2- 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.

2.2.1.- 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 (Codis de Barres i etiquetes).

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, així com la data de creació de la còpia.

2.2.2.- Inventari

1. El inventari de suports es realitza informàticament. El programaris de Backus identifiquen les cintes amb al codi de barres.

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

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

4. La relació esmentada s'actualitzarà periòdicament, mitjançant l'inventari corresponent, coincidint amb la realització de les còpies històriques mensuals.

5. 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.

6. 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.

2.2.3.- 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.

2.2.4.- Procediment de gestió de suports

1. Els suports que contenen les còpies de seguretat són emmagatzemats sota clau en 2 Caixes fortes ignífugas en CPD de Castelldefels, i una en la central d'Av. Tibidabo. En el cas que per motius de seguretat, es treguin còpies fora del local, les persones autoritzades pel responsable dels fitxers han d'estar indicades en l'Annex F. El CPD de Castelldefels protegit amb accés biomètric .

2. A aquest efecte, s'ha contractat els serveis de ESABE SEGURETAT, que s'encarreguen semanalment de custodiar una còpia de seguretat. El lliurament de les cintes es realitza en uns sobre tancats i segellats, de manera que ESABE no pot accedir al contingut. ESABE gestiona els formularis i llibres de registre d'entrada i sortida de cintes. Les còpies de seguretat es protegeixen mitjançant codis d'accés.

3. En el cas que els suports siguin reutilitzables, i en algun moment hagin contingut dades de caràcter personal, haurien de ser esborrats físicament abans del seu reutilització, impedint la recuperació de les dades que van contenir anteriorment.

4. Quan un suport que ha albergat dades de caràcter personal vagi a ser rebutjat, s'esborrarà tota la informació mitjançant un sistema que no permeti el seu aprofitament. En el cas que quedin dubtes sobre la informació que pugui subsistir després del procés d'esborrat, es procedirà a la inutilització física o a la destrucció del suport.

5. L'accés al lloc de custòdia dels suports és exclusiu del Responsable dels Fitxers i administradors del sistema.

ANNEX I - FUNCIONES Y OBLIGACIONS DEL PERSONAL

L'objectiu d'aquesta normativa és definir les responsabilitats del personal respecte a l'ús de la informació empresarial i dades personals responsabilitat de la FUOC, amb la finalitat de que tots els usuaris reconeguin i acceptin consensuadament les finalitats de la seva utilització i les seves limitacions.

Així mateix, la legislació vigent en relació a la Protecció de Dades Personals, obliga a la FUOC a complir amb una sèrie de requisits legals, entre els quals destaca l'obligació de posar en coneixement de tots els treballadors amb accés a dades personals, les seves funcions i obligacions en relació al tractament d'aquestes dades, especialment, en relació a les mesures de seguretat que s'han d'adoptar per a la seva custodia i protecció, 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.

Classificació del personal

a) Responsable de los Fitxers
b) Responsable de Protecció de Dades
c) Responsable de Seguretat
d) Usuaris de los Fitxers
e) Administradores del sistema o personal informàtic

FUNCIONS

a) Encarregat del Fitxers

- És el responsable jurídic de la seguretat dels seus Fitxers i l'encarregat d'establir les normes recollides en el present document, implantar les mesures de seguretat establertes en ell, i posar a disposició tots els mitjans necessaris perquè tots els usuaris afectats per aquest document, tinguin coneixement de totes les normes que afectin al desenvolupament de les seves funcions.

- Assumirà les funcions de coordinació i control de les mesures definides en el present document.

- Inscripció de fitxers en el Registre General de Protecció de Dades, de l'Agència de Protecció de Dades.

- Elaborar i implantar la normativa de seguretat, mitjançant l'adopció d'un Document de Seguretat .i la seva actualització.

- Adoptar mesures per a limitar l'accés dels usuaris (interns o aliens) a suports o recursos del sistema d'informació, automatitzats i no automatitzats, que continguin dades de caràcter personal.

- Informar al personal de cuales són les seves funcions i obligacions en el tractament de dades a través dels sistemes d'informació.

- Assegurar que el personal rep la formació adequada referent al coneixement de les mesures de seguretat i les obligacions imposades per la LOPD i el RDLOPD.

- Adoptar mesures i mecanismes que garanteixin la correcta identificació i autenticació de tot aquell usuari, degudament autoritzat, que accedeixi al sistema d'informació.

- Garantir els drets dels afectats, pel que fa al tractament de dades personals.

- Designar un Responsable de Protecció de Dades, sense que aquesta designació suposi exoneració o delegació de responsabilitats per part del RF.

- Haurà d'assumir i/o autoritzar totes aquelles accions, detallades en el present document que així ho estableixi el RDLOPD, o bé delegar l'autorització al Responsable de Protecció de Dades. Entre unes altres:

- Coordinar la implantació de les mesures de seguretat tècniques establertes en el Document de Seguretat, comprovant el seu compliment.

- Assegurar la realització de les còpies de seguretat planificades.

- Assignar i/o coordinar l'assignació dels password amb el nivell i perfil d'accés necessari per a les funcions assignades als distints usuaris, així com determinar el període de canvi de password previst pel RF.

- Instal·lar, actualitzar i verificar l'eficiència dels sistemes antivirus per a garantir la perdurabilidad i integritat de les dades personals del fitxer.

- Gestionar el procediment de notificació i resposta davant incidències. Revisar i avaluar el contingut del Registre d'Incidències, juntament amb el RPD, i adoptar les mesures de seguretat que procedeixin.

- Autoritzar per escrit l'execució de procediments de recuperació de les dades, deixant constància en el Registre d'incidències.

- Responsable de l'assignació de recursos compartits.

- Comprovar periòdicament l'estat dels usuaris autoritzats en el sistema d'informació, gestionant les altes, baixes o modificacions de perfils.

- Comprovar l'eficàcia de l'aplicació de les mesures de seguretat implantades, i prendre les mesures correctores o de millora que garanteixin la confidencialitat i integritat de la informació.

- Realitzar directament, o delegar en un tercer (sense exoneració de responsabilitat tant del RS com el RF), l'eliminació dels suports que continguin dades personals, o qualsevol actuació de manteniment i control de les mesures de seguretat tècniques aplicades, prèvia autorització del RF.

- Donar a conèixer les normes de seguretat que afectin al desenvolupament de les funcions dels usuaris, així com les conseqüències que poguessin incórrer en cas d'incompliment.

- Els processos de recuperació de de dades i/o arxius a través de còpies de seguretat.

- La sortida de suports amb dades de caràcter personal, fora dels locals on es troben els fitxers.

- Tractaments de dades fora de les instal·lacions del RF.

b) Responsable de Protecció de Dades

- Assegurar-se del compliment de les mesures de seguretat organitzatives que s'haurien d'implantar en els procediments de tractaments de dades que realitzi.

- Coordinar l'aplicació de les mesures de seguretat i el ple coneixement per part del personal de les obligacions derivades de la implantació de les mesures de seguretat detallades en aquest document, així com el compliment de la normativa interna i els plans de formació iniciats per l'entitat.

- Compliment del deure informació en tots els processos de captació de dades que es realitzin en l'entitat.

- Verificar que els tractaments de dades realitzades conten amb la legitimació necessària per a això. Entre altres aspectes, haurà d'informar al personal de quan els tractaments requereixen del consentiment del titular de les dades.

- Assegurar-sé que s'utilitzen els mitjans de tractament de dades adequades i facilitats per l'entitat.
- Coordinar i controlar el compliment de les obligacions relatives al deure informació, consentiment, deure secret i formació del personal.

- Garantir l'exercici dels drets d'accés, rectificació, cancel·lació i oposició determinats per la LOPD segons el procediment establert pel RDLOPD.

- Coordinar el compliment i aplicació de les mesures de seguretat contingudes en la normativa d'aplicació, així com la normativa interna adoptada per l'entitat.

- Definir, les funcions i obligacions dels usuaris amb accés a dades personals en el present document de seguretat i documentació annexa.

- Donar a conèixer les normes de seguretat que afectin al desenvolupament de les funcions dels usuaris, així com les conseqüències que poguessin incórrer en cas d'incompliment.

c) Responsable de Seguretat

- Coordinar la implantació de les mesures de seguretat tècniques establertes en el Document de Seguretat, comprovant el seu compliment.

- Col·laborar amb el RF en l'adopció de mesures perquè el personal conegui les normes en matèria de seguretat que afecten al desenvolupament de les seves funcions, i de les conseqüències que poguessin incórrer en cas d'incompliment.

- Assegurar la realització de les còpies de seguretat planificades.

- Assignar i/o coordinar l'assignació dels password amb el nivell i perfil d'accés necessari per a les funcions assignades als distints usuaris, així com determinar el període de canvi de password previst pel RF.

- Instal·lar, actualitzar i verificar l'eficiència dels sistemes antivirus per a garantir la perdurabilidad i integritat de les dades personals del fitxer.

- Gestionar el procediment de notificació i resposta davant incidències. Revisar i avaluar el contingut del Registre d'Incidències, juntament amb el RPD, i adoptar les mesures de seguretat que procedeixin, comunicant-lo al RF.

- Autoritzar per escrit l'execució de procediments de recuperació de les dades, deixant constància en el Registre d'incidències.

- Responsable de l'assignació de recursos compartits.

- Comprovar periòdicament l'estat dels usuaris autoritzats en el sistema d'informació, gestionant les altes, baixes o modificacions de perfils.

- Comprovar l'eficàcia de l'aplicació de les mesures de seguretat implantades, i prendre les mesures correctores o de millora que garanteixin la confidencialitat i integritat de la informació.

- Realitzar informes trimestrals de revisió de les mesures de seguretat, juntament amb el RPD, dels quals donarà trasllat al RF.

- Realitzar directament, o delegar en un tercer (sense exoneració de responsabilitat tant del RS com el RF), l'eliminació dels suports que continguin dades personals, o qualsevol actuació de manteniment i control de les mesures de seguretat tècniques aplicades, prèvia autorització del RF.

- Donar a conèixer les normes de seguretat que afectin al desenvolupament de les funcions dels usuaris, així com les conseqüències que poguessin incórrer en cas d'incompliment.

d) Usuaris del Fitxers

- Els usuaris expressament autoritzats en el present document de♣ seguretat s'encarreguen de les funcions de producció habitual i explotació diària de l'activitat de l'empresa. Sense perjudici que la FUOC pugui assignar funcions informàtiques a algun dels seus usuaris, aquests, en principi, no han de realitzar cap tipus activitat tècnic-informàtica.

e) Administradors del sistema o personal informàtic

- Les funcions a ocupar pel personal informàtic o els administradors del sistema, es determinen en funció de la categoria informàtica que ostentin. Aquesta classificació, no significa que necessàriament hagin d'estar presents en tots els casos, sent en algunes ocasions assumides per una mateixa persona o persones.

A.- Obligacions que afecten al responsable dels fitxers

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 administrador de sistema 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 administrador del sistema, 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. Col·laborar en la redacció de les normes internes per als usuaris

14. Publicar les normes internes

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

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

B.- Obligacions que afecten a tot el personal con accés a dades personals

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.

   - L'usuari està obligat a complir tota la normativa relacionada amb els Identificadors i claus d'accés, i especialment, està prohibit la utilització de contrasenyes toves de fàcil identificació i amb menys de 6 caràcters, així com la repetició de l'última contrasenya quan el sistema li obligui al canvi de la mateixa.

   - 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.

   - 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.

- Introduir, descarregar d'Internet, reproduir, utilitzar o distribuir programes informàtics o qualsevol tipus d'obra o material els drets de propietat intel·lectual o industrial dels quals pertanyin a tercers, quan no s'hi disposi d'autorització.

- Instal·lar o crear qualsevol programa, inclosos aquells que són estandarditzats, que impliqui tractament de dades personals, sense la deguda autorització del responsable dels fitxers o seguretat

- 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.

- Enviar o reenviar missatges en cadena o de tipus piramidal.

- L'enviament de missatges de correu electrònic on el remitent no estigui plenament identificat, o es presti confusió sobre la seva identitat.

- Variacions del contingut del correu electrònic i el seu enviament de forma maliciosa.

2.- Confidencialitat de la informació

1. No es podran utilitzar els recursos del sistema d'informació als quals es tingui accés per a fins privades o per a qualsevol altra finalitat diferent de les estrictament relacionades amb la seva funció en l'empresa. Queda expressament prohibit la realització de còpies de cap tipus dels Fitxers per a ús privat en qualsevol tipus de suport.

2. Està absolutament prohibit la comunicació de dades personals a tercers, excepte en els casos legalment prevists, i en aquells supòsits que sigui necessari per al desenvolupament de l'activitat laboral, sempre que aquestes comunicacions siguin legítimes.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.- 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.

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.

4. La navegació per pàgines d'Internet inadequades o il·legals, no limitant-se exclusivament a les pornogràfiques, i la descarrega de qualsevol tipus de continguts que no siguin per a ús empresarial.

5. La navegació per pàgines d'Internet en horari laboral que no tingui relació amb l'activitat desenvolupada.

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.

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. 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.

4. 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.

5. 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.

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. Tot el personal està obligat a atendre tota sol·licitud d'accés, rectificació i cancel·lació de dades personals sol·licitada per qualsevol persona, i ho posarà en coneixement del responsable de Protecció de Dades.

4. 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.

5. La manipulació i tractament d'imatges alienes a l'usuari de la Intrauoc i Campus Virtual.

6. La recollida de dades personals sense el degut consentiment de l'afectat i sense informar-li de les obligacions exigides en l'article 5 de la Llei de Protecció de Dades.

7. La contractació de serveis externs que impliquin comunicació de dades personals o accessos als mateixos, sense la deguda autorització i supervisió del responsable dels fitxers o responsable de protecció de dades.

Deure de secret:

1. 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.

2. Tot el personal està obligat a posar en coneixement dels seus responsables qualsevol dubte que tingui sobre l'ús i tractament de les dades personals.

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. En el cas que els tractaments de dades personals dutes a terme pels usuaris puguin ser visualitzats per persones no autoritzades, tant internes com externes, en la mesura del possible, haurien d'orientar les pantalles d'ordinador de manera que impedeixin la seva visualització.

7. 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.

8. 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.

9. Està prohibit l'ús de dispositius informàtics mòbils com ordinadors portàtils o agendes electròniques que continguin dades de caràcter personal fora dels centres de treball, sense la deguda autorització per escrit del responsable dels fitxers o seguretat.

9.- Tractament de dades personals en suport paper

1. No està permès llençar documents i papers que continguin dades personals, sense adoptar les mesures necessàries que impedeixin la seva posterior visualització, fins i tot en els recipients destinats a la deixalla del paper.

2. No està permès la reutilització de documents i papers que continguin dades de caràcter personal.

3. Tots els usuaris quan abandonin els seus llocs de treball, haurien de guardar convenientment la documentació que contingui dades personals, així com evitarà deixar documents damunt de les taules de treball.

4. Quan per l'activitat desenvolupada es manipulin cartes, paquets, documents i similars en llocs d'accés al públic, s'haurien de prendre les mesures de seguretat oportunes per a evitar accessos no autoritzats als mateixos.

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.

C- Obligacions que afecten als administradors del sistema i personal informàtic

a) Administradors del sistemes

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.

b) 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 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

ANNEX J - PROCEDIMENT DE NOTIFICACIÓ I GESTIÓ D'INCIDÈNCIES

Com registre de incidències, la UOC utilitza una eina informàtica de notificació, gestió i registre d'incidències denominat JIRA que permet la comunicació, seguiment i tancament de la incidència. Addicionalment, permet crear tipus d'incidència (problema, tasca, documentació, acta, incidència ...) i assignar-la a una altra persona que serà l'encarregat de resoldre-la.

A més, aquesta eina permet afegir observadors a la pròpia incidència, que no tenen necessàriament que participar en la resolució, però si seran informats de l'evolució de la pròpia incidència mitjançant el correu electrònic.

JIRA genera missatges de correu electrònic a l'adreça que hagi estat configurada tant per l'informador, com pel qui té l'assignació com per els observadors de la incidència en concret.

La UOC tracte 2 tipus d'incidències:

a) Incidències de seguretat
b) Incidències de alumnes

Procediment de notificació, gestió i tancament de Incidències de Seguretat

1. Procediment de notificació d'incidències:

   a. Directes pels tècnics de monitoratge dels sistemes informàtics (control 365 dies/ 24 hores).
   b. Telèfon (Call Center / Interlocutors directes).
   c. Correu electrònic.
   d. Introducció de la incidència directament a l'aplicació JIRA.

Els usuaris que no tenen accés directe al JIRA, quan pateixen una incidència ho comuniquen al seu Gestor de Demandes que avalua la incidència y s'implica.

2. Introducció de la incidència al JIRA:

   a. La persona que detecta o pateix la incidència, directament o a través del Gestor de Demandes, crea un alta de la incidència en el JIRA.

b. Creació de la incidència on queden registrades les següents dades:

- Codi de la incidència.
- Data d'alta de la incidència i de les seves actualitzacions.
- Persona que crea la incidència.
- Persona a la que s'assigna la resolució de la incidència.
- Tipus d'incidència.
- Prioritat.
- Descripció de la incidència.
- Estat de la incidència: Oberta / Tancada.
- Resolució de la incidència:
- Activitats relacionades amb la incidència (Procediments per resoldre la incidència)

c. A partir d'aquest moment la incidència queda assignada y s'inicia el procés per a la seva resolució. Tota activitat relacionada queda registrada.

d. Tancament de la incidència:

Resolta la incidència, s'introdueixen en el JIRA els resultats de la mateixa indicant:

- Resolució: Solucionat / No solucionat.
- Afectació de la resolució: Persona, departament o procés al que afecta.
- Comentaris de la resolució.
- Al JIRA queden registrades la data de tancament de la incidència y la seva resolució.

Procediment de notificació, gestió i tancament de Incidències de Alumnes

La FUOC disposa d'una aplicació per a la resolució d'incidències, de menor escala, pels estudiants.

Aquestes incidències es redueixen a dos tipus:

1. Canvis de contrasenyes
2. Problemes amb les contrasenyes (accessos)

Per a la gestió de les incidències dels estudiants, la UOC disposa d'una aplicació denominada CAU IRIS.

1. Procediment de notificació d'incidències:

   a. Ajuda informàtica – Canal telefònic / Servei d'Atenció Telefònica:

   Resolució telefònica de la incidència, prèvia identificació de l'usuari. L'actuació o gestió que afecta a les dades personals de l'alumne s'introdueix la incidència en el CAU IRIS.

   b. Canals Virtuals dels Serveis d'Atenció:

   L'estudiant es pot adreçar virtualment, a través del Campus Virtual de la UOC, al servei d'ajuda informàtica. L'alumne ha d'identificar-se prèviament amb la seva contrasenya i la petició queda automàticament registrada en el CAU IRIS.

Totes les incidències queden registrades en el CAU IRIS amb les indicacions següents:

- Nº de la incidència.
- Data de la incidència.
- Nom de l'estudiant.
- Gestor de la incidència.
- Descripció, comentaris i procediments de resolució de la incidència.
- Tancament de la incidència.

CAU IRIS disposa d'un registre d'incidències on queda registrada tota la incidència, i que permet fer cerques selectives segons:

- La seva tipologia.
- Si està en curs o històriques
- Per resultat de la gestió.
- Segons el intervinents en la seva gestió i resolució.

ANNEX K – CONTROLS DE VERIFICACIÓ I AUDITORIES

Per als Fitxers que continguin dades personals de nivell mitjà, almenys cada dos anys, es realitzarà una auditoria externa o interna que dictamini el correcte compliment i adequació de les mesures recollides en el present document de seguretat, identificant les deficiències i proposant les mesures correctores necessàries, en compliment del Títol VIII del RLOPD, referent a les mesures de seguretat, segons l'indicat en els seus articles 96 i 110 respecte de fitxers automatitzats i no automatitzats respectivament.

Amb caràcter extraordinari haurà de realitzar-se quan es duguin a terme modificacions substancials en el sistema d'informació que puguin repercutir en el compliment de les mesures de seguretat implantades, amb l'objecte de verificar l'adaptació, adequació i eficàcia de les mateixes. Aquesta auditoria inicia el còmput de dos anys assenyalat.

L'informe analitzarà l'adequació de les mesures i controls a la Llei i el seu desenvolupament reglamentari, identificarà les deficiències i proposarà les mesures correctores o complementàries necessàries.

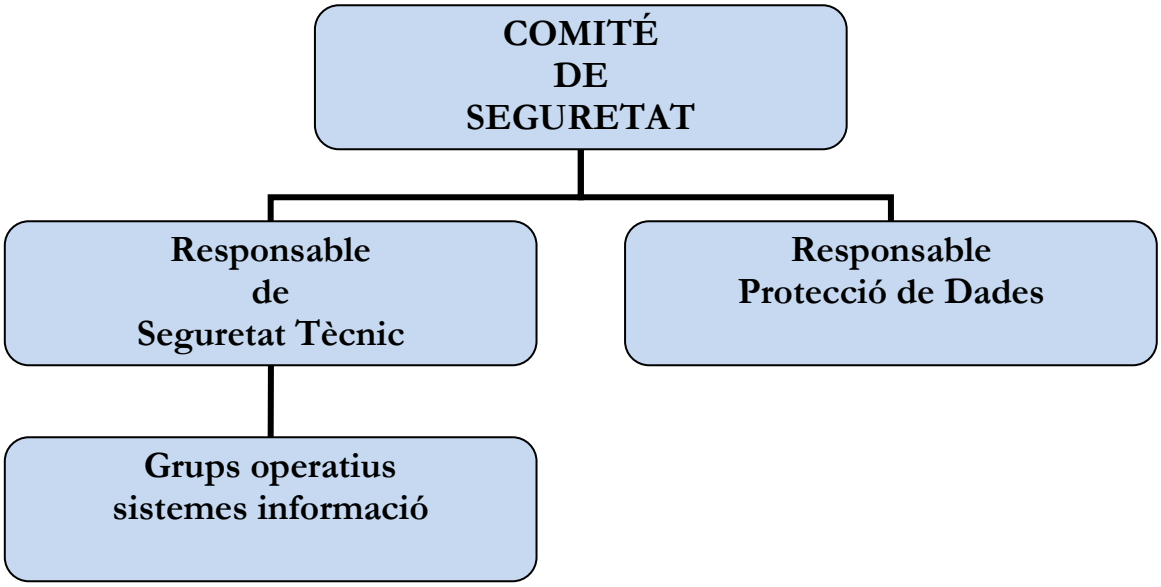
Registro de auditorías:

Nº Auditoria	Data	Estat	Auditor
1	Desembre 2009	Realitzada	Interna /Lant Advocats
2	Desembre 2011	Realitzada	Interna /Lant Advocats
3	Desembre 2013	Pendent	

ANNEX L – NOMENAMENTS

Responsable de Seguretat

Les tasques del responsable de seguretat estan encomanades a un comitè de seguretat que deriva les seves funcions en responsable de seguretat tècnic, un responsable de protecció de dades i els grups operatius del àrea de sistemes que executen les accions.



Components del Comitè de Seguretat

- President: Vice-rector de Tecnologia
- Adjunt Vice-rector de Tecnologia
- Director del Area de Persones.
- Gerent:
- Responsable de Sistemas de Informació/seguretat informàtica: Francesc Rovirosa
- Director del Gabinet Jurídic: Xavier Martinez Plaza

Responsable de Sistemas de Informació/seguretat informàtica

- Francesc Rovirosa

Responsable Protecció de Dades

- Encarna Silva
- Lant Advocats (Lant Advisors, S.L.P.)

Grups Operatius (Àrea de sistemes d'informació)

- a) Integració Tecnològica
- b) Operacions Tecnològiques
- c) Aplicacions i Desenvolupament
- d) Serveis i Suport