DOCUMENT DE SEGURETAT DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

Acord del Consell de Govern de 19 de gener de 2006

FUNCIONS I OBLIGACIONS DEL PERSONAL

FUNCIONS I OBLIGACIONS DEL PERSONAL

5.1 Funcions i Obligacions del Personal

Amb l'objecte de donar degut compliment al que estableix l'art. 8.2.c del Reial Decret 994/1999 d'11 de juny, la **UNIVERSITAT AUTÒNOMA DE BARCELONA** obliga el seu personal al coneixement i compliment de les següents obligacions, les quals hauran d'ésser conegudes, acceptades i respectades per tot el personal.

Tindrà la consideració d'usuari qualsevol persona autoritzada a accedir a dades o recursos inclosos dins l'àmbit d'aplicació del Document de Seguretat de la Institució.

Dins del col·lectiu d'usuaris cal diferenciar un cas especial: els usuaris administradors. Com a conseqüència de la seva activitat professional poden tenir un accés a la informació, sense les restriccions que tenen la resta d'usuaris. Aquests privilegis són necessaris per a la correcta gestió dels sistemes d'informació on resideixen els fitxers amb dades de caràcter personal.

Donada aquesta circumstància caldrà que aquests usuaris estiguin explícitament identificats, així com el rol a desenvolupar (administradors de bases de dades, tècnics de sistemes, responsables d'aplicacions informàtiques, operadors, manteniment d'equips informàtics, etc.).

En cas que existeixin usuaris que no formin part del personal al servei de la **UNIVERSITAT AUTÒNOMA DE BARCELONA,** les seves obligacions i responsabilitats hauran d'estar clarament especificades mitjançant la formalització d'un contracte, pacte, acord o qualsevol altre acte equivalent que permeti acreditar l'establiment de les obligacions i responsabilitats corresponents, així com el compromís d'acomplir-les.

Obligacions de tot el personal de la UNIVERSITAT AUTÒNOMA DE BARCELONA

Confidencialitat de la Informació:

1. Els usuaris dels sistemes d'informació i dels fitxers amb dades de caràcter personal hauran de guardar, per temps indefinit, la màxima reserva i no divulgar ni utilitzar directament ni a través de terceres persones o

empreses, les dades, documents, metodologies, claus, anàlisi, programes i la resta d'informació a què tinguin accés durant la seva relació laboral amb la **UNIVERSITAT AUTÒNOMA DE BARCELONA** tant en suport material com electrònic. Aquesta obligació continuarà vigent després de l'extinció de la seva relació amb el titular del fitxer o el seu responsable.

2. Queda prohibit trametre informació confidencial de l'Organització a l'exterior, mitjançant suports materials, o a través de qualsevol mitjà de comunicació, incloent la simple visualització o accés, excepte autorització expressa del Responsable de Fitxer.

3. Cap col·laborador haurà de posseir, per a usos no propis de la seva responsabilitat, cap material o informació propietat de l'Organització, tant ara com en el futur.

4. En el cas que, per motius directament relacionats amb el lloc de treball, l'empleat entri en possessió d'informació confidencial sota qualsevol tipus de suport, haurà d'entendre's que la citada possessió és estrictament temporal, amb obligació de secret i sense que això li atorgui cap dret de possessió, o titularitat o còpia, cobri la referida informació.

5. Així mateix, el treballador haurà de tornar els citats materials a l'Organització o destruir-los, immediatament després de la finalització de les tasques que han originat l'ús temporal dels mateixos, i en qualsevol cas, a la finalització de la relació laboral.

Codis d'identificació i Claus d'Accés:

1. Queda prohibit 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 posar-ho en coneixement del responsable del sistema, a fi que li assigni una nova clau. Davant d'una baixa o absència temporal de l'usuari, el responsable del departament podrà sol·licitar al responsable del sistema la cessió de clau o dades a la persona per ell designada, havent de quedar registrada per escrit la citada autorització.

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

3. Estan expressament prohibides les següents activitats:

    - Compartir o facilitar l'identificador d'usuari i la clau d'accés facilitats per l'organització amb una altra persona física o jurídica, inclòs el personal de la pròpia organització. 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 d'activitat històrics (LOG) del Sistema.

    - Intentar desxifrar les claus, sistemes o algoritmes de xifrat i qualsevol altre element de seguretat que intervingui en els processos telemàtics de l'organització.

    - 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 intentar accedir a àrees restringides dels sistemes informàtics de l'Organització o de tercers.

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

Utilització dels Recursos Informàtics:

Els usuaris amb accés als sistemes informàtics i de xarxa hauran d'esforçar-se en fer servir i promoure un ús eficient d'aquests recursos, a fi d'evitar tràfic innecessari i interferències en el treball d'altres usuaris.

Per això, estaran expressament prohibides les següents activitats:

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

- Obstaculitzar voluntàriament l'accés d'altres usuaris a la xarxa mitjançant el consum massiu dels recursos informàtics i telemàtics de l'organització, així com realitzar accions que danyin, interrompin o generin errors en els sistemes citats.

- Trametre missatges de correu electrònic de forma massiva o amb finalitats comercials o publicitàries sense el consentiment del destinatari (Spam).

- 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, seguint les directrius marcades pels serveis informàtics, d'utilitzar els programes antivírics i les actualitzacions per prevenir l'entrada en el sistema de qualsevol element destinat a destruir o corrompre les dades informàtiques.

- Introduir, descarregar d'internet, reproduir, utilitzar o distribuir programes informàtics no autoritzats expressament per l'organització, o qualsevol altre tipus d'obra o material els drets de propietat intel·lectual o industrial que pertanyin a tercers, quan no es disposi d'autorització per a això.

- Instal·lar còpies il·legals de qualsevol programa, inclosos els estandarditzats i els de caràcter gratuït.

- Esborrar qualsevol dels programes instal·lats legalment.

- Utilitzar els recursos telemàtics de l'organització, inclosa la xarxa Internet, per a activitats que no es trobin directament relacionades amb el lloc de treball de l'usuari.

- Introduir continguts obscens, immorals o ofensius i, en general, mancats d'utilitat per als objectius de l'organització, a la xarxa corporativa de l'Organització.

- Trametre o retransmetre missatges en cadena o de tipus piramidal.

Utilització del Correu Electrònic:

1. El sistema informàtic, la xarxa corporativa i els terminals utilitzats per cada usuari són propietat de l'organització.

2. Es considerarà correu electrònic tant l'intern, entre terminals de la xarxa corporativa, com l'extern, dirigit o provenint d'altres xarxes públiques o privades i especialment internet. Cap missatge de correu electrònic serà

considerat com a privat.

3. El servei de correu electrònic ha d'ésser usat únicament per a la comunicació d'aspectes relacionats amb el negoci i/o el compliment de les obligacions laborals.

4. L'organització vetllarà pel correcte ús del correu electrònic dels usuaris de la xarxa corporativa i els arxius de registres històrics d'activitat (LOG) del servidor, a fi de comprovar el compliment d'aquestes normes i prevenir activitats que puguin afectar a l'organització com a responsable civil subsidiària del mal ús d'aquest recurs.

5. Qualsevol fitxer introduït a la xarxa corporativa o al terminal de l'usuari a través de missatges de correu electrònic que provinguin de xarxes externes, haurà de complir els requisits establerts en aquestes normes i, en especial, les referides a propietat intel·lectual i industrial i a control de virus.

Utilització de l'Accés a Internet:

1. L'ús del sistema informàtic de l'organització per accedir a xarxes públiques com internet, es limitarà als temes directament relacionats amb l'activitat de l'organització i les funcions del lloc de treball de l'usuari.

2. L'accés a debats en temps real (Xat / 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 queda estrictament prohibit.

3. L'accés a pàgines Web, grups de notícies (Newsgroups) i altres fonts d'informació com FTP, telnet, etc. es limita a aquells que continguin informació relacionada amb l'activitat de l'organització o amb les funcions del lloc de treball de l'usuari.

4. L'organització es reserva el dret de monitoritzar i comprovar, de forma aleatòria i sense previ avís, qualsevol sessió d'accés a internet iniciada per un usuari de la xarxa corporativa.

5. Qualsevol fitxer introduït a la xarxa corporativa o al terminal de l'usuari des d'Internet, haurà de complir els requisits establerts en aquestes normes i, en especial, les referides a propietat intel·lectual i industrial i a control de virus.

Propietat Intel·lectual i Industrial:

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

Gestió d'Incidències:

S'entén per incidència qualsevol anomalia que afecti o pugui afectar a la seguretat de les dades.

1. És obligació de tot el personal de l'organització comunicar al responsable del sistema qualsevol incidència que es produeixi en els sistemes d'informació a què tinguin accés.

2. La citada comunicació haurà de realitzar-se immediatament i, en qualsevol cas, en un termini de temps no superior a una hora (1) des del moment en què es conegui la citada incidència.

Protecció de dades:

Es consideraran actes prohibits:

1. Crear fitxers de dades personals sense l'autorització del Responsable de Fitxer.

2. Utilitzar les dades personals per a finalitats incompatibles amb aquelles per les que s'hagin recaptat o per a finalitats diferents de les comunicades a l'Agència de Protecció de Dades.

3. Creuar informació relativa a dades de diferents fitxers o serveis a fi d'establir perfils de personalitat, hàbits de consum o qualsevol altre tipus de preferències, sense l'autorització expressa del Responsable de Fitxer.

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.

5.2 Comunicació

Correspon a la institució l'adopció de les mesures que permetin al personal conèixer les normes de seguretat relacionades amb el desenvolupament de les seves funcions, així com de les conseqüències del seu incompliment.

Les normes contingudes en el paràgraf anterior s'inclouran en el Document "*Normes de Seguretat dels Sistemes d'Informació*" i es donaran a conèixer formalment i de forma individualitzada entre tot el personal que presti servei actualment a la institució. A tots els efectes signaran la recepció de les normes i el seu coneixement.

En aquest mateix document, s'integraran de forma explicativa les conseqüències i responsabilitats que l'incompliment de les esmentades funcions li pot suposar a tots els nivells, incloent el laboral.

Les persones que entren a prestar servei a la institució amb caràcter temporal o indefinit, procediran a rebre formalment i de forma individualitzada les normes de seguretat dels sistemes d'informació, en el moment de firmar el contracte de treball, contracte administratiu o acta de presa de possessió.

Aquesta mateixa política, on s'inclouen totes les obligacions genèriques que afecten als empleats en quant a la seguretat dels tractaments de dades i l'ús dels sistemes d'informació, pot penjar-se a la intranet o a qualsevol sistema d'informació massiu.

Sempre que sigui necessari, i en qualsevol cas, amb una periodicitat mínima anual, es remetrà una circular informativa fent referència a les possibles modificacions produïdes en les normes de seguretat dels sistemes d'informació.

5.3 Responsabilitat

L'incompliment de les obligacions per part del personal serà sancionat disciplinadament, prèvia instrucció del preceptiu expedient.

D'igual manera, sense perjudici de la responsabilitat disciplinària corresponent que pugui incórrer el personal, s'exigirà d'ofici la corresponent responsabilitat pels danys i perjudicis ocasionats als particulars, sempre que hagi existit dol o culpa greu.

La responsabilitat penal i la responsabilitat civil derivada del delicte en què hagi incorregut el personal, s'exigirà de conformitat amb la legislació corresponent.