Universitat Autònoma de Barcelona

Text Refós de les Normatives vigents en l'àmbit de les Tecnologies de la Informació i de la Comunicació (TIC) de la Universitat Autònoma de Barcelona

(Text refós aprovat per l'Acord del Consell de Govern de 13 de juliol de 2011)

ÍNDEX **Articles**

Preàmbul

I

El 7 d'abril de 2010 el Consell de Govern va acordar delegar a la secretària general l'elaboració d'un text refós relatiu a les normes aprovades pel Consell de Govern directament o per les seves comissions en relació amb els diversos àmbits d'aquesta Universitat, com ara l'àmbit de les tecnologies de la informació i de la comunicació.

Aquesta autorització comprèn l'actualització, l'aclariment i, quan escaigui, l'harmonització de les normes aprovades pel Consell de Govern per garantir-ne l'adequació al marc legal actual, així com la facultat per intitular els títols, els capítols i els articles dels diferents textos que s'elaborin per a cadascuna de les diferents matèries i s'agrupin en un únic text normatiu o en diversos textos segons l'objecte que tinguin.

Per acomplir l'encàrrec rebut s'ha optat per fer un únic text refós per a totes les matèries que formen part de l'àmbit concret de les tecnologies de la informació i de la comunicació.

II

El text refós s'estructura en quatre títols, cinquanta-tres articles, una disposició final i tres annexos. També s'hi inclou un sumari de l'articulat, l'objecte del qual és facilitar la utilització de la norma a les persones destinatàries mitjançant una ràpida localització i ubicació sistemàtica dels preceptes.

El text refós està basat en les normes aprovades per la Junta de Govern o Consell de Govern o les seves comissions. S'han mantingut i modificat les que estaven vigents i s'han adaptat a l'evolució de les noves tecnologies.

El títol preliminar estableix l'objecte i l'àmbit d'aplicació de la normativa.

El títol I regula el web de la UAB, també anomenat portal de la UAB, com a eina de difusió d'informació institucional i altres webs relacionats amb la Universitat, i està dividit en onze capítols, els quals regulen el tipus, l'estructura, la identificació i la llengua de les informacions que s'hi poden trobar, així com els òrgans responsables del compliment del contingut d'aquest títol i de les informacions publicades en pàgines vinculades amb el web de la UAB.

El títol II està dividit en tres capítols que fixen els diferents aspectes que configuren les comunicacions electròniques a la UAB, és a dir, les eines de què disposen els diferents col·lectius de la UAB, els criteris generals a seguir per a la difusió d'informacions per correu electrònic i les bones pràctiques en la comunicació electrònica de la UAB.

El títol III regula la publicació de material al Campus Virtual de la UAB com a eina telemàtica per afavorir la tramesa d'informació i la comunicació dins de l'ensenyament bimodal (presencial i a distància) que ofereix la Universitat.

El títol IV desenvolupa les mesures de seguretat per a les persones usuàries en relació amb els recursos tecnològics de la UAB, està dividit en cinc capítols i regula els drets d'ús dels sistemes informàtics de la Universitat, els diferents tipus d'usuari/ària que pot fer-ne ús, la responsabilitat de les persones usuàries d'aquests recursos i les mesures que s'aplicaran en cas d'incompliment de les condicions d'ús. També es recullen els objectius, les funcions i la composició del Grup de Treball per a la Coordinació d'Incidents en Sistemes Informàtics i de la Comissió de Disciplina Informàtica.

Títol preliminar. Disposicions generals

Article 1. Objecte

1. Aquest text normatiu té per objecte refondre les normatives aprovades pel Consell de Govern de la UAB que regulen l'àmbit de les tecnologies de la informació i la comunicació de la Universitat Autònoma de Barcelona en matèria del web, la comunicació electrònica, la publicació al Campus Virtual i les mesures de seguretat per als usuaris en relació amb els recursos informàtics.

2. Queda exclosa d'aquest text normatiu la regulació de l'administració electrònica i, en concret, l'ús dels mitjans electrònics en l'àmbit de la UAB, que és objecte d'un reglament específic aprovat per l'acord del Consell de Govern de 16 de novembre de 2010.

Article 2. Àmbit d'aplicació

1. El conjunt de normes recollides en aquest document són aplicables a tots els membres de la comunitat universitària (estudiantat, professorat, PAS) que facin ús de les tecnologies de la informació i la comunicació de què disposa la Universitat i a totes aquelles persones que es puguin relacionar amb aquesta institució per via telemàtica.

2. En tot allò que no estigui regulat en el present text refós, serà aplicable el que disposen les normes d'origen estatal o autonòmic que regulen la matèria.

Títol I. El web de la UAB (portal de la UAB)

Capítol I. Disposicions generals

Article 3. Objectiu

El web de la UAB (http://www.uab.cat), també anomenat *portal de la UAB*, té per objectiu difondre informació institucional de la Universitat Autònoma de Barcelona.

Article 4. Àmbit d'aplicació

El contingut d'aquest títol s'aplicarà a tots els servidors d'informació de la UAB.

Capítol II. Informació institucional

Article 5. Definició

A efectes d'aquest títol, s'entén per informació institucional la informació generada per qualsevol òrgan o unitat organitzativa de la Universitat, tant acadèmica o de recerca com administrativa en l'exercici de les seves funcions i dins el seu àmbit de competència.

Article 6. Característiques de la informació

La informació difosa al web de la UAB ha d'ajustar-se a les característiques següents:

a) Ha de ser informació institucional, segons el que s'indica en l'article anterior.

b) La informació oferta ha de ser veraç, precisa i actualitzada.

c) No s'hi podran utilitzar materials que tinguin drets d'autor, llevat del cas que es tingui l'autorització explícita del titular.

d) La incorporació de publicitat haurà tenir l'autorització expressa de la Secretaria General.

e) La informació ha de garantir el dret a la intimitat i a la pròpia imatge de les persones.

f) En cap cas no es podran difondre informacions contràries als principis fundacionals de la UAB (art. 3 i 6 dels Estatuts) i als drets reconeguts internacionalment.

Capítol III. Estructura de la informació

Article 7. Estructura

El portal de la UAB estarà format per dos tipus de pàgines institucionals que tindran l'exclusivitat de l'ús de la imatge de la Universitat. El contingut d'aquestes pàgines, desplegat de manera clara, estructurada i jerarquitzada, representarà la visió institucional de la UAB, tant a l'interior de la xarxa pròpia (intranet) com a l'exterior (Internet). Aquestes pàgines són:

a) La pàgina principal (*home page*) i altres pàgines institucionals que recullen informació general o transversal de la Universitat, les quals estaran editades principalment per l'Àrea de Comunicació i de Promoció.

b) Les pàgines vinculades, editades per qualsevol òrgan o unitat organitzativa de la Universitat, reconeguda al nomenclàtor de la UAB, que recullen informació relativa a l'àmbit de competència de la unitat organitzativa corresponent.

Article 8. Ubicació d'altres informacions

Les informacions personals de caire acadèmic i professional s'ubicaran a la pàgina de l'òrgan o unitat organitzativa a la qual pertanyi la persona interessada, sempre que aquest nivell informatiu estigui previst en els continguts de la pàgina que hi estigui vinculada.

Capítol IV. Identificació de la informació

Article 9. Imatge corporativa i protecció de dades

1. Les pàgines del web de la UAB han de respectar la imatge corporativa de la UAB.

2. Totes les pàgines hauran de respectar la Llei orgànica 15/1999, de protecció de dades de caràcter personal.

Article 10. Identificació i datació de les pàgines

Totes les pàgines identificaran clarament el nom de l'editor de la informació i la data de creació o actualització de la informació editada.

Capítol V. Llengua de la informació

Article 11. Llengua de la informació

Tota la informació institucional serà redactada en català, sense perjudici que es faci també en altres llengües.

Capítol VI. Responsabilitat de la UAB

Article 12. Òrgan responsable

El Comissionat del rector o la rectora per a la Societat de la Informació de la Universitat Autònoma de Barcelona, o persona amb un càrrec equivalent, vetllarà pel compliment del contingut del present títol.

Article 13. Funcions de l'Àrea de Comunicació i Promoció

L'Àrea de Comunicació i de Promoció tindrà les funcions següents:

a) Estructuració dels continguts del portal de la UAB i establiment dels nivells a partir dels quals es vincularan les pàgines institucionals.

b) Elaboració dels continguts de la pàgina principal i d'altres pàgines institucionals d'informació general i transversal de la Universitat.

c) Difusió del web de la UAB als buscadors d'Internet més importants.

d) Connexió de les pàgines que hi estiguin vinculades i localització en l'estructura del web.

e) Resolució dels casos de concurrència d'informació editada per dos o més servidors d'informació.

f) Supervisió d'altres pàgines amb informació d'activitats acadèmiques o de recerca en altres servidors que facin servir la seva adscripció a la UAB o la seva imatge corporativa.

Capítol VII. Responsabilitat de la informació a les pàgines vinculades

Article 14. Responsabilitat de la informació a les pàgines vinculades

La persona responsable funcional de l'òrgan o unitat organitzativa definirà els continguts de les pàgines vinculades i la persona responsable orgànica tindrà cura de l'elaboració, el manteniment, l'actualització i l'edició de la informació corresponent, i assegurarà la connexió de les pàgines vinculades.

Capítol VIII. Connexió de les pàgines vinculades

Article 15. Connexió de les pàgines vinculades

Els webs dels òrgans o unitats organitzatives de la Universitat hauran de sol·licitar la seva connexió al web de la UAB i el contingut estarà supervisat per les persones responsables indicades en el capítol VI d'aquest títol.

Article 16. Sol·licituds de connexió

Les sol·licituds de connexió s'hauran d'adreçar a la persona responsable assenyalada en el capítol VI d'aquest títol, i s'hi haurà d'acreditar el compliment de les normes de connexió establertes en l'article següent.

Article 17. Normes de connexió

Els webs d'informació descentralitzada hauran de tenir els requisits següents per vincular-se al web de la UAB:

a) Hauran de complir el títol present.

b) Hauran de ser estables i funcionar les 24 hores del dia.

c) La portada del web vinculat disposarà d'un enllaç a la pàgina principal (*home page*) del web de la UAB.

d) Els continguts hauran de complir el que estableix la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD) i l'aspecte estarà d'acord amb el llibre d'estil de publicacions de pàgines web de la UAB.

Capítol IX. Suport tècnic

Article 18. Suport tècnic

Per tal que el web de la UAB es mantingui dins d'una estructura flexible, equilibrada i estable, hom disposarà del següent suport tècnic:

a) L'Àrea de Comunicació i de Promoció atendrà els responsables i els editors de pàgines vinculades pel que fa als aspectes relacionats amb els art. 4 i 11 d'aquest text normatiu i pel que fa a tots als més generals relacionats amb l'elaboració i l'estructuració de la informació descentralitzada.

b) Des del Comissionat del rector o la rectora per a la Societat de la Informació definirà el suport i decidirà qui serà la persona encarregada d'elaborar i facilitar les eines informàtiques per confeccionar les webs, de gestionar les llicències i decidir pel que fa a la ubicació de les pàgines al maquinari del Servei i podrà participar en la formació de persones usuàries en les tècniques de creació de pàgines web.

c) El Servei de Publicacions tindrà cura d'elaborar i mantenir un fons gràfic de la Universitat, d'ús lliure.

Capítol X. Contingut de la informació

Article 19. Contingut de la informació

Queda expressament prohibida la difusió d'informació que no s'ajusti a la regulació d'aquest títol.

Capítol XI. Exempció de responsabilitat de la UAB

Article 20. Exempció de responsabilitat de la UAB

La Universitat Autònoma de Barcelona declina tota responsabilitat per la difusió de qualsevol informació per via telemàtica al marge d'aquest títol i es reserva el dret d'iniciar qualsevol acció legal per aquest fet.

Títol II. Comunicació electrònica a la UAB

Capítol I. Disposicions generals

Article 21. Objecte

Aquest títol té per objecte recollir els diferents aspectes que configuren la regulació de les comunicacions electròniques a la UAB, els quals es divideixen en tres apartats: a) les eines de què disposen els col·lectius de la UAB per a la comunicació electrònica; b) els criteris generals per a la difusió d'informacions per correu electrònic utilitzant les llistes de difusió, per la intranet o pel portal d'estudiants, i c) la guia de bones pràctiques en la comunicació electrònica de la UAB.

Capítol II. Eines de què disposen els col·lectius de la UAB per a la comunicació electrònica

Article 22. Adreça de correu electrònic

1. La UAB proporciona una adreça de correu electrònic a les persones que formen part dels seus col·lectius (personal docent i investigador, personal d'administració i serveis, i estudiants) tant d'ús institucional com personal, i també assigna adreces de correu electrònic de comptes no personals amb uns criteris predefinits d'assignació de noms i domini.

2. Les adreces de correu electrònic són gestionades per l'Oficina de Coordinació Institucional, amb el suport del Servei d'Informàtica.

3. El personal docent i investigador i també l'estudiantat tenen la possibilitat de comunicar-se directament amb les persones integrants dels grups de classe que hagin estat assignades al professorat, a través de les eines integrades en el Campus Virtual. Per aquest mitjà se'ls ofereix la possibilitat d'enviar correus electrònics amb efectes únicament dins del Campus Virtual o bé amb efectes externs.

4. Aquesta eina de comunicació electrònica es gestiona a través de les infraestructures institucionals per a l'ús exclusiu dels col·lectius de la UAB i sense cost econòmic.

Article 23. Intranet

1. La UAB ofereix la possibilitat de difondre informació general emprant les pàgines d'accés restringit que corresponen als diferents col·lectius (intranet del PAS, del PDI, etc.).

2. La gestió del contingut de la intranet en qüestió correspon a les diverses àrees, que en la pràctica són responsables del contingut de la informació, i també a l'Àrea de Comunicació i Promoció de la UAB.

3. Aquesta eina de comunicació electrònica es gestiona, també, a través de les infraestructures institucionals per a l'ús exclusiu dels col·lectius de la UAB i sense cost econòmic.

Article 24. Ús del directori

1. La UAB facilita l'enviament de comunicacions del personal docent i investigador i del personal d'administració i serveis al personal del seu mateix àmbit a través de l'eina del directori, a la qual es pot accedir a partir del web institucional (dins l'apartat o pestanya que amb el nom *Directori*).

2. Aquesta és una eina autogestionada pels mateixos usuaris i a la qual es pot accedir amb la identificació institucional (NIU) i sense cost econòmic.

Article 25. Llistes de difusió institucional

1. La UAB ofereix la possibilitat de dur a terme difusió institucional a partir de llistes d'adreces de correu electrònic dels diferents col·lectius, que poden ser seleccionades per diversos criteris, com ara per centres, per departaments, etc. Amb aquestes llistes es pot fer difusió d'informació a tot el col·lectiu seleccionat, i s'aplicaran, per a aquests casos, els criteris generals que consten al capítol III d'aquest títol i que són aplicables a la difusió d'informacions mitjançant les llistes de difusió, a la intranet o al portal d'estudiants.

2. La difusió de missatges de correu electrònic a través d'aquestes llistes es gestiona des de la Secretaria General de la UAB mitjançant l'Oficina de Coordinació Institucional.

3. Els missatges de correu electrònic procedents de les llistes de difusió de caràcter institucional de la UAB són de recepció obligatòria i no és possible anul·lar-ne la subscripció. Es reben a conseqüència de la vinculació directa amb la institució, per raó de la vinculació laboral o funcionarial, el càrrec, etc.

4. Aquesta eina de comunicació electrònica es gestiona a través de les infraestructures institucionals, és per a l'ús exclusiu dels col·lectius de la UAB i no té cap cost econòmic.

Article 26. Llistes de col·laboració autogestionades

1. La UAB ofereix la possibilitat de crear llistes de correu electrònic específiques que permeten gestionar adreces de correu electrònic de manera centralitzada, i que sempre han de ser emprades per difondre informació d'una temàtica concreta a un conjunt de persones que tenen interessos comuns dins la UAB.

2. Per a cada llista hi ha una persona que se'n responsabilitza i n'assumeix l'administració, que és qui la gestiona i qui defineix les polítiques d'enviament i la publicitat de la llista.

3. Qualsevol persona que pertanyi a algun dels col·lectius de la UAB es pot subscriure a aquest tipus de llistes, i també gaudeix del dret d'anul·lar-ne la subscripció.

4. Aquesta eina de comunicació electrònica es gestiona a través de les infraestructures institucionals per a l'ús exclusiu dels col·lectius de la UAB i no té cap cost econòmic.

5. Les peticions de creació d'aquestes llistes cal que es facin a través d'un formulari que consta al web del Servei d'Informàtica, http://www.uab.cat/si, a l'apartat Correu, en el subapartat Llistes de distribució.

Article 27. Llistes de difusió autogestionades

1. La UAB ofereix la possibilitat de crear llistes de correu electrònic a partir d'una sol·licitud prèvia de la persona interessada i sempre que justifiqui adequadament la finalitat a la qual destinarà les adreces de correu electrònic de la llista. La UAB aporta el contingut de la llista de persones destinatàries.

2. Podran sol·licitar la creació d'aquestes llistes les persones titulars d'òrgans de govern unipersonals, les persones representants dels agents socials i altres persones que ocupin càrrecs de representació.

3. Les peticions de creació d'aquestes llistes s'han d'adreçar a la Secretaria General, que les gestionarà mitjançant l'Oficina de Coordinació Institucional.

4. Les llistes han de tenir sempre un/a administrador/a, que és l'única persona que pot dur a terme les comunicacions amb els membres de la llista. Aquest/a administrador/a assumeix la responsabilitat de gestionar la llista i de complir la normativa vigent en matèria de protecció de dades de caràcter personal; a aquest efecte, prèviament, sempre ha de subscriure un document de compromís de confidencialitat i d'assumpció de responsabilitats que consta a l'annex I, i cal que l'aporti al Comissionat per a la Societat de la Informació o persona amb un càrrec equivalent abans d'iniciar les difusions. L'assumpció de responsabilitat és de caràcter personal i és vigent durant la durada en el càrrec de l'administrador/a de la llista; en cas de renovació o canvi de la persona responsable de la llista s'ha de signar un nou document.

5. Qualsevol persona que estigui inclosa en alguna d'aquestes llistes pot anul·lar-ne la subscripció i la petició d'anul·lació ha de ser atesa per la persona responsable.

6. Aquesta eina de comunicació electrònica es gestiona a través de les infraestructures institucionals per a l'ús exclusiu dels col·lectius de la UAB i sense cost econòmic.

Article 28. Llistes pròpies

1. Qualsevol persona dels col·lectius de la UAB pot confeccionar una llista pròpia d'adreces de correu electrònic per enviar missatges.

2. La persona propietària d'aquest tipus de llista assumeix directament la responsabilitat de gestionar la llista i de complir la normativa vigent en matèria de protecció de dades de caràcter personal. En aquest sentit, també assumeix la responsabilitat davant les possibles infraccions en què pugui incórrer, particularment a partir de les denúncies que poden presentar les persones incloses en una llista davant l'Agència Catalana de Protecció de Dades.

3. Els missatges enviats per aquest mitjà poden ser considerats missatges no sol·licitats (correu brossa o *spam*).

Capítol III. Criteris generals per a la difusió d'informacions per correu electrònic mitjançant les llistes de difusió institucionals, per la intranet o pel portal d'estudiants

Article 29. Criteris per a la difusió massiva d'informació

Quan se sol·liciti la realització d'una difusió massiva d'informació, ha de ser autoritzada d'acord amb els criteris següents:

1. *Publicació a la intranet o al portal d'estudiants*. Es publiquen per aquests mitjans, amb autorització prèvia, les informacions relatives als assumptes següents:

   a) Activitats acadèmiques, seminaris, cursos, ofertes de feina i beques, etc. (excepte quan estiguin dirigits a col·lectius molt reduïts i definits).
   b) Activitats o serveis oferts pels serveis de la UAB.
   c) Ofertes de formació per al personal acadèmic i el personal d'administració i serveis.
   d) Comunicats amb informació laboral o sindical, en seccions específiques.
   e) Actes acadèmics o institucionals d'interès general.

   Aquestes informacions es publiquen com a notícies a la portada de la intranet, per tal de facilitar la detecció de les novetats, independentment que també es puguin recollir en les seccions corresponents (Agenda, Formació, Serveis, etc.).

2. *Difusió per correu electrònic per llistes de difusió*. Es poden utilitzar les llistes de difusió institucional, amb autorització prèvia, en els casos següents:

   a) Informacions específiques sobre docència i recerca (convocatòries, programes especials, etc.).
   b) Informacions adreçades a col·lectius molt determinats i que es poden discriminar amb les llistes disponibles: estudiants per facultat o titulació i professorat i personal d'administració i serveis per edificis.
   c) Informació institucional rellevant per al conjunt de la comunitat, segons el parer de l'Equip de Govern.

Article 30. Òrgan responsable

Els criteris descrits en l'article anterior són implementats per la Secretaria General de la UAB mitjançant l'Oficina de Coordinació Institucional. El desenvolupament i la concreció d'aquests criteris, si escau, poden ser objecte d'una circular emesa conjuntament per la Secretaria General i el Comissionat per a la Societat de la Informació o la persona amb el càrrec equivalent.

Capítol IV. Bones pràctiques en la comunicació electrònica de la UAB

Article 31. Recomanacions

La UAB disposarà d'un protocol en el qual inclourà, entre altres aspectes, les recomanacions necessàries per a la correcta utilització de la comunicació electrònica de la UAB. Actualment, les recomanacions per a la correcta utilització de la comunicació electrònica consten a l'annex II d'aquest text refós.

Títol III. Publicació al Campus Virtual

Capítol I. Disposicions generals

Article 32. Definició

El Campus Virtual de la UAB i les eines que hi estan associades són eines telemàtiques creades per oferir a la comunitat universitària unes funcionalitats d'informació, comunicació i proposta docent dins de l'ensenyament bimodal (presencial i a distància).

Article 33. Òrgan responsable

El Comissionat del rector o la rectora per a la Societat de la Informació de la Universitat Autònoma de Barcelona, o persona amb un càrrec equivalent, vetllarà pel compliment del contingut del present títol i comptarà amb el suport de l'Oficina del Projecte Autònoma Interactiva Docent (OAID) i la Direcció TIC de la UAB. L'OAID serà la responsable del funcionament i de l'administració d'aquestes eines.

Capítol II. Material docent al Campus Virtual

Article 34. Contingut del material publicat

El professorat de la UAB podrà publicar el material docent corresponent a les assignatures de les quals és responsable al Campus Virtual de la UAB per a l'ús dels alumnes, sempre que es compleixin els requisits exigits en aquest títol. Les persones responsables d'espais acadèmics o de coordinació estaran sotmesos a la mateixes consideracions.

Article 35. Autoria del material publicat i autorització per publicar

El material docent que es vulgui publicar al Campus Virtual de la UAB ha de ser original del professorat responsable de l'assignatura, o tenir l'autorització corresponent de l'autor o autora o de la persona titular dels drets d'autor del material. En cap cas la publicació de material docent al Campus Virtual o en les eines que hi estan associades podrà atemptar contra els drets d'autor. El professorat i les persones responsables d'espais podran fer ús de material amb finalitat acadèmica i d'acord amb el que disposa el Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de propietat intel·lectual.

Article 36. Publicació del material docent

La publicació del material al Campus Virtual (o en les eines que hi estan vinculades) de la UAB serà duta a terme pel mateix professorat, sempre que això sigui possible, per l'OAID o per qui designi aquesta oficina. L'OAID en cap cas publicarà un material docent que no hagi estat facilitat pel professorat responsable de l'assignatura amb aquesta finalitat.

Article 37. Responsabilitat en la publicació de material docent

El professorat que publiqui material docent al Campus Virtual de la UAB serà responsable davant la UAB de tots els conflictes, les reclamacions i les accions que puguin derivar-se de l'incompliment del contingut d'aquest títol.

Article 38. Accés al material docent

L'accés al material docent d'una assignatura publicat al Campus Virtual de la UAB està reservat a l'alumnat matriculat de l'assignatura corresponent. No obstant això, el professorat responsable de l'assignatura podrà sol·licitar l'accés públic del material docent publicat al Campus Virtual de la UAB a l'OAID.

Article 39. Incompliment de les normes d'accés al material docent

Les activitats que comportin l'incompliment del contingut de l'article anterior se sotmetran a allò que s'estableix en el títol IV d'aquest text normatiu, que regula les mesures de seguretat per a les persones usuàries en relació amb els recursos informàtics de la UAB.

Títol IV. Mesures de seguretat per a les persones usuàries dels recursos tecnològics de la UAB

Capítol I. Disposicions generals

Article 40. Dret d'ús dels sistemes informàtics de la UAB

Els recursos informàtics de la Universitat Autònoma de Barcelona, tant els de les instal·lacions centrals com els de la resta de les instal·lacions distribuïdes, incloent-hi sistemes centrals/distribuïts, estacions de treball, ordinadors personals, xarxes internes i externes, programaris, sistemes multiusuaris, etc., són per a ús exclusiu de les tasques pròpies de la Universitat per a membres de la seva comunitat o persones autoritzades.

Article 41. Àmbit d'aplicació

1. Atès que la majoria dels sistemes informàtics de la Universitat estan connectats directament o indirectament a la xarxa general de la Universitat, i que el mal ús o la manca de sistemes de seguretat adequats en un d'aquests sistemes poden comprometre la seguretat dels altres sistemes de la Universitat o de les institucions a les quals la xarxa general de la Universitat està connectada, el contingut d'aquest títol s'aplica a tothom que faci ús dels sistemes informàtics de la Universitat o que disposi de sistemes o xarxes connectades directament o indirectament a la xarxa general.

2. Les persones que sol·licitin o disposin d'accés als sistemes informàtics (ja siguin propis o de la UAB) o d'una connexió del seu sistema o de la seva xarxa a la xarxa general de la Universitat hauran de conèixer les mesures de seguretat dels recursos informàtics, les quals estaran a la seva disposició a través del portal de la UAB.

3. La Universitat es reserva el dret d'iniciar les accions legals oportunes quan es vegin vulnerats els seus drets a conseqüència de la utilització inadequada dels seus recursos informàtics, i de posar a disposició de les autoritats competents tota la informació disponible en cas de denúncies per mala utilització i vulneració de drets de tercers.

Capítol II. Dels sistemes informàtics

Article 42. Assignació de recursos dels sistemes informàtics

Per a l'assignació de recursos dels sistemes informàtics (institucionals, centrals o departamentals), i per a la connexió de sistemes i de xarxes a la xarxa general es reconeix un responsable dels recursos informàtics i dues categories d'usuaris/àries: l'administrador/a dels recursos informàtics i l'usuari o la usuària final.

Article 43. Responsable dels recursos informàtics

1. La persona responsable dels recursos informàtics és la persona que ha de vetllar pel bon funcionament dels recursos informàtics que té assignats sota la seva tutela sempre amb el suport dels serveis centrals i distribuïts.

2. Són responsables dels recursos informàtics:

a) Els degans i les deganes i els directors i les directores de centre són responsables dels recursos d'ús general per a la docència del centre.
b) Els directors i les directores de departament són responsables dels recursos informàtics dels laboratoris de pràctiques, dels destinats a la recerca i dels serveis informàtics de gestió del departament.

c) Els administradors i les administradores de centre són responsables dels recursos destinats a la gestió del centre.
d) Els directors i les directores dels serveis i dels instituts són responsables de tots els recursos que utilitzen.
e) El director o la directora de TIC és responsable dels recursos centrals i la xarxa de comunicacions amb el suport dels caps del serveis d'informàtica distribuïda en el cas dels centres de la UAB.

3. La persona responsable dels recursos informàtics podrà delegar les funcions, però no la responsabilitat, que cregui que són necessàries per controlar l'ús dels recursos informàtics.

Article 44. L'administrador/ora dels recursos informàtics

1. L'administrador/ora dels recursos informàtics és la persona encarregada de gestionar un o més recursos informàtics (sistemes multiusuari, estacions de treball, ordinadors personals, xarxes internes, etc.) connectats directament o indirectament a la xarxa general de la Universitat.

2. L'administrador/ora dels recursos informàtics treballarà de manera coordinada amb la persona responsable dels recursos informàtics i els serveis, a la qual comunicarà totes les incidències que hagi detectat i que puguin afectar el bon funcionament dels recursos.

3. L'administrador/ora dels recursos informàtics haurà d'aplicar el contingut d'aquest títol als recursos que gestiona i als usuaris i les usuàries que depenen d'ell/a. Igualment haurà d'aplicar les altres normatives específiques que existeixin.

4. L'administrador/ora dels recursos informàtics es compromet a treballar de manera coordinada amb els serveis centrals en totes les qüestions vinculades a la prestació del servei però sobretot en qüestions tècniques i de seguretat, i a col·laborar activament en la detecció, el seguiment i la identificació de les possibles persones implicades en la vulneració del contingut d'aquest títol.

Article 45. L'usuari o la usuària final

1. L'usuari o la usuària final és la persona que fa ús d'un recurs informàtic (propi, cedit per la UAB o de propietat de la UAB) que estigui connectat directament o indirectament a la xarxa general de la Universitat.

2. L'usuari o usuària final es compromet a seguir les recomanacions quant a la utilització dels recursos informàtics establerts per la UAB, i les de les persones responsables i administradores dels recursos informàtics especialment en qüestions tècniques, de protecció de dades de caràcter personal, de material amb drets d'autor i en qüestions de seguretat (bàsicament pel que fa a la utilització de la xarxa, l'actualització dels programes antivirus i les polítiques d'accés i custodia de la informació).

3. L'usuari o la usuària està obligat o obligada a comunicar a les persones responsables pertinents qualsevol canvi en la titularitat del recurs informàtic que tingui assignat i, mentre aquesta comunicació no es produeixi, continua sent l'única persona responsable a tots els efectes dels usos que se'n derivin.

4. La persona responsable dels recursos informàtics, per motius d'incompliment de la present normativa, podrà denegar, de manera preventiva i provisional, l'ús o accés a un sistema informàtic, o la connexió d'un sistema o xarxa a la xarxa general de la Universitat. En cas de desconnexió de la xarxa, prèviament es contactarà la persona responsable per comunicar-li l'acció pertinent i solucionar els problemes (excepte que es vegi compromesa la seguretat de la xarxa —o de segments de la xarxa— i que sigui imperativa la seva desconnexió).

Capítol III. Responsabilitats de les persones usuàries

Article 46. Protecció de dades, paraules clau i ús de recursos

1. Les persones usuàries tindran màxima cura en la manipulació i ús dels equips informàtics, i de tota la infraestructura complementària. Evitaran dur a terme qualsevol acció, que de manera voluntària o involuntària, pugui malmetre la integritat física del maquinari o de la instal·lació (destrossa, sostracció, trasllat no autoritzat, etc.), o la integritat lògica del programari o les dades.

2. Les persones usuàries accediran als recursos informàtics seguint les normatives específiques de cada centre, i accediran als sistemes informàtics seguint les recomanacions particulars que els serveis informàtics i les persones responsables de recursos hagin estipulat.

3. Els recursos informàtics de la Universitat són un bé públic i la seva finalitat és emmagatzemar, servir i tractar informació vinculada a les activitats de la Universitat. Per raons de seguretat l'administrador/a dels recursos informàtics podrà inspeccionar, de manera ordinària, la informació continguda en els sistemes informàtics que administri. En cas que, per raons de seguretat, calgui fer una inspecció més específica, l'administrador/a dels recursos informàtics haurà de justificar-ho a la persona responsable dels recursos informàtics.

4. Els comptes d'usuari en els sistemes informàtics de la Universitat són personals i intransferibles.

5. És responsabilitat de la persona usuària tenir màxima cura de la seva paraula clau, per a la qual cosa, sobretot, la mantindrà secreta, usarà paraules clau que no siguin trivials, la canviarà periòdicament i sempre que cregui o sospiti que la seva confidencialitat pugui ser violada.

6. Tots els canvis de paraules clau de comptes dels sistemes informàtics es duran a terme fent ús dels mecanismes i protocols definits en cada moment per les persones responsables dels sistemes.

7. La persona usuària es compromet a no fer servir els recursos públics (ordinadors, xarxa, punts de connexió, etc.) per fer activitats que no estiguin vinculades estrictament a l'activitat acadèmica o de recerca i serà responsabilitat seva tot el material emmagatzemant o descarregat amb drets d'autor i que no disposi de la llicència corresponent. A més, la persona usuària es compromet a respectar els termes indicats en la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal i la UAB podrà prendre les decisions oportunes en relació amb les accions que es derivin d'aquest fets.

Article 47. Incompliment de la normativa

1. Es considera incompliment de les condicions d'ús dels recursos informàtics en els supòsits següents:

a) L'ús il·lícit per part de terceres persones dels comptes d'usuari en els sistemes informàtics (amb coneixement o no de les persones usuàries legítimes), tant pel que fa a qui porta a terme l'accés indegut com pel que fa a la persona responsable del compte.

b) La desprotecció de la informació de les persones usuàries de manera que hi facilitin un accés parcial o generalitzat.

c) L'ús indegut dels serveis de xarxa i dels mitjans electrònics per comunicar-se amb altres persones usuàries dels sistemes informàtics, de la xarxa de la Universitat o de les xarxes a les quals la Universitat està connectada, quan causin molèsties (missatges molestos o ofensius, assetjament electrònic, suplantació d'adreces de xarxa, etc.), o bé no es respecti el contingut d'aquest títol o les normatives de les institucions i les xarxes amb les quals i per les quals es comuniquin. També es considerarà incompliment l'accés als paquets de comunicació per esbrinar informació de la qual no s'és propietari.

d) La cerca de paraules clau d'altres persones usuàries o qualsevol intent de trobar i explotar forats en la seguretat dels sistemes informàtics de la Universitat o de fora, o fer ús d'aquests sistemes per atacar qualsevol sistema informàtic.

e) La creació, l'ús o l'emmagatzematge de programes o d'informació que puguin ser utilitzats per atacar els sistemes informàtics de la Universitat o de fora.

f) La destrossa, la sostracció o el trasllat no degudament autoritzat a altres dependències, de qualsevol element físic de la instal·lació informàtica o d'infraestructura complementària.

g) L'alteració de la integritat de les dades.

h) Qualsevol altre actuació que vulneri la normativa vigent o que afecti o menystingui les condicions d'ús dels recursos informàtics.

Article 48. Mesures aplicables

1. L'incompliment del contingut d'aquest títol en qualsevol grau comportarà de manera preventiva la suspensió immediata de l'accés als sistemes informàtics, i/o la desconnexió dels sistemes o xarxes de la xarxa general de la Universitat.

2. En els casos d'incompliment de la normativa, les persones responsables dels recursos informàtics, prèvia audiència de la persona interessada, podran aplicar preventivament la mesura prevista en aquest article, si bé aquesta mesura haurà de ser confirmada per la Comissió de Disciplina Informàtica. A la vista dels fets i les circumstàncies que hi concorrin, aquesta comissió establirà la durada i, si escau, la periodificació en què caldrà confirmar la mesura.

3. Contra les resolucions d'aquests òrgan, les persones interessades podran interposar recurs ordinari davant el rector o la rectora o la persona en qui delegui.

4. La persona responsable dels recursos informàtics podrà elevar a la Comissió de Disciplina Informàtica aquells casos que, sense estar explícitament contemplats en el present títol, pugui considerar sancionables.

5. Les mesures esmentades en aquest article s'aplicaran sense perjudici de les accions disciplinàries, civils o penals que escaigui aplicar a les persones presumptament implicades, així com de la reparació dels danys ocasionats.

Capítol IV. Grup de Treball per a la Coordinació d'Incidents en Sistemes Informàtics (CSIRT-UAB)

Article 49. Objectius i funcions

L'objectiu d'aquest grup és treballar i assessorar en temes de seguretat informàtica i gestió d'incidents en les xarxes telemàtiques de la UAB. Aquest grup tindrà com a objectius principals:

a) Coordinar les polítiques de treball sobre vulnerabilitats de seguretat i amenaces.
b) Definir les línies de treball per divulgar i posar a la disposició de la comunitat informació que permeti prevenir i resoldre incidents de seguretat.
c) Formular les polítiques de difusió i educació de la comunitat en l'àmbit de la seguretat informàtica.
d) Definir les regles d'actuació per dur a terme investigacions (proactives) relacionades amb la seguretat informàtica.

Article 50. Membres del Grup

El Grup de Treball per a la Coordinació d'Incidents en Sistemes Informàtics està integrat, com a Responsables per les persones següents:

a) Comissionat/ada per a la Societat de la Informació o persona amb un càrrec equivalent.
b) Director/ora de Tecnologies de la Informació i la Comunicació o persona amb un càrrec equivalent.
c) Director/ora del Departament d'Arquitectura de Computadors i Sistemes Operatius o persona/ones en qui delegui.

d) Director/a del Departament d'Enginyeria de la Informació i de les Comunicacions o persona/ones en qui delegui.
e) Cap de Seguretat del Servei d'Informàtica o persona amb un càrrec equivalent.

Aquest grup de treball estarà assistit per un equip de personal tècnic (amb un nombre mínim de components no restringit i en funció de les necessitats) del qual formaran part:

a) Membre/s del Departament d'Arquitectura de Computadors i Sistemes Operatius.
b) Membre/s del Departament d'Enginyeria de la Informació i de les Comunicacions.
c) Cap de Seguretat del Servei d'Informàtica o persona amb un càrrec equivalent.
d) Responsables d'àrea del Servei d'Informàtica (accés, comunicacions, producció...).
e) Representació dels Servei d'Informàtica Distribuïda (SID).

Article 51. Polítiques de treball, serveis i formularis

Les polítiques de treball, serveis i formularis per a l'informe d'incidents es troben definits en el document annex III.

Capítol V. La Comissió de Disciplina Informàtica

Article 52. Nomenament i funcions

El Consell de Govern de la Universitat Autònoma de Barcelona nomenarà una Comissió de Disciplina Informàtica, que tindrà les funcions següents:

a) Vetllar per la bona gestió i funcionament dels recursos informàtics en l'àmbit general de la UAB.
b) Confirmar, si escau, els incompliments considerats en el títol present. La Comissió escoltarà les parts implicades abans de ratificar o modificar les mesures aplicades de manera preventiva per les persones responsables dels recursos informàtics.
c) Resoldre els casos no previstos en aquest títol, sens perjudici de les competències que corresponen als òrgans de la Universitat, d'acord amb la normativa vigent.
d) Escoltar els membres de la comunitat universitària que li elevin queixes o suggeriments.
e) Proposar al Consell de Govern la modificació i actualització del contingut d'aquest títol quan escaigui.
f) Informar el Consell de Govern de les incidències que s'han produït i de les mesures que s'han acordat, en cas que es requereixi.

Article 53. Composició

La Comissió de Disciplina Informàtica estarà formada per:

a) El president o la presidenta, que serà el comissionat o la comissionada del rector per a la Societat de la Informació o persona amb un càrrec equivalent.
b) Dos/dues degans/anes o directors/ores de centres.
c) Dos/dues directors/ores de departament.
d) Un membre dels Serveis Informàtics centrals.
e) Tres persones usuàries: un/a professor/a o investigador/a, un/a estudiant i un membre del PAS.

En cas que en qualsevol moment o per qualsevol causa la Comissió no es pugui constituir, les seves funcions seran assumides de manera excepcional pel seu president o la seva presidenta o la persona o les persones en qui delegui.

Disposició addicional

A proposta de la persona comissionada per a la Societat de la Informació, la Comissió d'Economia i Organització adoptarà les mesures necessàries per al desenvolupament i aplicació de la present normativa pel que fa a les responsabilitats, la publicació i ús del Dipòsit Digital de Documents de la UAB.

Disposició derogatòria. Normativa que es deroga

Queden derogades totes les normes de rang igual o inferior aprovades per la Universitat Autònoma de Barcelona que s'oposin al present text refós i, particularment, les següents:

1. Acord de la Junta de Govern de 26 de juny de 1997 pel qual s'aprova la Normativa sobre el web de la UAB.

2. Acord del Consell de Govern de 7 de juliol de 2010 pel qual s'aprova el Protocol sobre comunicació electrònica a la UAB.

3. Acord de la Junta de Govern de 27 de gener de 2000 pel qual s'aprova la Normativa de publicació de material docent al Campus Virtual de la UAB.

4. Acord del Consell de Govern de 7 de juny de 2007 pel qual s'aprova la creació, composició i funcions de la Comissió d'Universitat Electrònica (E-Universitat).

5. Acord de la Junta de Govern de 25 d'abril de 1996 pel qual s'aprova la Normativa de seguretat per als usuaris dels recursos informàtics de la UAB.

Disposició final

Aquest text refós entrarà en vigor l'endemà de la seva aprovació pel Consell de Govern.

Annexos

Annex I: Compromís de confidencialitat i assumpció de responsabilitats per a la creació d'una llista de difusió autogestionada

XXXXXXXXXX, amb DNI número XXXXXXX, actuant en nom i representació de XXXXXX en la seva condició de XXXXXX,

Exposo:

Que la UAB posa a la meva disposició una llista de distribució autogestionada que inclou les adreces de correu electrònic corresponents a XXXX.

Manifesto el meu compromís de:

Primer. Dur a terme el tractament de les dades incloses en la llista de difusió, complint el que disposa la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant LOPD) i el Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el reglament de desenvolupament de la Llei, i la resta de normatives sobre la matèria (*aquest compromís sobre les dades que consten a la llista de difusió s'estén també amb posterioritat a la meva vinculació com a XXX*)**,** i en especial la relativa a l'assumpció de responsabilitat, la qualitat de les dades, la seguretat i el deure de secret.

Segon. Tractar les dades que m'han estat facilitades d'acord amb el que disposa la normativa interna de la UAB i fer servir la llista de distribució per a l'ús concret de comunicació amb el col·lectiu representat, per a l'àmbit de què és objecte la meva representació i sempre respectant el drets de les persones representades d'acord amb el que estableix la LOPD.

Tercer. Complir el secret professional respecte a les dades que són objecte de tractament, mantenint l'absoluta confidencialitat i reserva sobre qualsevol dada que pugui conèixer amb ocasió del compliment de la meva responsabilitat, i no comunicar a terceres persones les dades subministrades, ni tan sols a fi de conservar-les.

Quart. Assumir les obligacions legals que corresponen a la persona responsable del tractament respecte de les dades que li han estat facilitades i, per tant, afrontar la responsabilitat en cas que les dades es destinin a finalitats diferents de les estipulades, es comuniquin o s'utilitzin de manera que s'incompleixin les responsabilitats pròpies de l'òrgan de representació; i respondre de les infraccions en què es pugui incórrer, de les reclamacions de tercers i dels procediments a què insti l'Agència de Protecció de Dades o aquell òrgan que sigui competent en relació amb la matèria.

Cinquè. Ser la persona responsable de la custòdia de les paraules d'accés per gestionar la llista de difusió i de les mesures de seguretat que es facin servir per a la custòdia. No obstant això, la UAB és responsable, en el sentit que disposa l'article 9 de la LOPD, de complir les mesures d'índole tècnica i organitzatives necessàries que garanteixin la seguretat de les dades tractades, d'acord amb el nivell de protecció que correspongui (reglament aprovat mitjançant el Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal).

Sisè: Ser la persona responsable de fer efectives les noves subscripcions i les baixes que es produeixin en aquesta llista de difusió i que obeeixen als drets de les persones representats, de gestionar els missatges, de moderació i de les accions de manteniment de la llista, així com d'establir els condicionants tècnics i els mecanismes d'actualització dels nous membres del col·lectiu representat, amb el suport dels Serveis Informàtics de la UAB i a través de la persona comissionada del rector o la rectora per a la Societat de la Informació o càrrec polític equivalent.
Pel que fa al personal de nova adscripció, s'establirà el mecanisme adient —a través de les àrees responsables— per tal que es garanteixi l'actualització de la llista amb una freqüència semestral. Aquesta acció es durà a terme

sota la coordinació del Comissionat de del rector o la rectora per a la Societat de la Informació o càrrec polític equivalent.

Setè: Gestionar, en els casos de canvi de la persona responsable, el traspàs de les claus d'accés gestionades a la nova persona escollida. El traspàs no podrà fer-se efectiu fins que no sigui signat el document de compromís per la nova persona entrant i aportat aquest compromís a la UAB.

Vuitè: Sol·licitar per escrit la finalització de la vigència d'aquest document amb un preavís de cinc dies hàbils al Comissionat del rector o la rectora per a la Societat de la Informació o càrrec polític equivalent.

Bellaterra (Cerdanyola del Vallès), XX de XX de 20XX.

Signat

Annex II: Guia de bones pràctiques en la comunicació electrònica de la UAB

1. Recomanacions de caràcter general

a) Mantenir al dia les actualitzacions del programari i del sistema operatiu, especialment l'antivirus, i, en la mesura que es pugui, fer servir el programari recomanat. (Consulteu l'apartat Maquinari i programari recomanat a http://www.uab.cat/si.)

b) Controlar periòdicament la bústia de correu (la capacitat de la qual és limitada), a fi d'evitar que es quedi sense espai lliure (per exemple, traspassar els correus que es vol conservar a les carpetes locals i fer còpies de seguretat d'aquestes; es fan còpies de la bústia institucional automàticament). Les persones que us envien correus us agrairan que no tingueu la bústia plena (no els arribarà un missatge de rebuig) i també us ho agrairà el servidor de correu.

c) Descarregar els fitxers adjunts que siguin útils (sense imprimir el contingut del missatge si no és realment necessari, ja que el cost d'espai en disc equivalent és més de 150.000 vegades més baix que el cost d'impressió) i eliminar el missatge (o també moure'l a una carpeta local). Recordar de buidar la paperera i la carpeta de correus enviats sempre que sigui possible.

d) Protegir les paraules clau d'accés a les bústies de correu electrònic i evitar-ne la divulgació a terceres persones. En cas de pèrdua o de desconfiança que algú les pugui fer servir, canviar-les tan aviat com sigui possible a través de la pàgina http://sia.uab.es/gestio_pwd.html.

e) Donar amb moderació l'adreça de correu institucional i intentar tenir, sempre que sigui possible, un compte gratuït (Gmail, Yahoo, Hotmail, etc.) per registrar-vos en webs i per enviar i rebre correu no institucional, per evitar la publicitat no desitjada.

f) No acceptar documents ni arxius adjunts provinents de persones desconegudes o de persones conegudes que tinguin un origen poc fiable o del qual es desconfia. En tot cas, tenir molta cura amb els arxius adjunts i, si no s'està segur, contactar la persona remitent o deixar primer el fitxer en una carpeta i, sense fer-hi un doble clic a sobre, passar-hi l'antivirus actualitzat. No fer cas, tampoc, de peticions de canvi de paraules clau ni d'adhesió a grups externs (MySpace, Facebook, etc.), ja que la majoria són fraus per obtenir les paraules clau i informació personal de l'usuari (accions conegudes com a *phishing*).

g) Fer servir les unitats de disc compartides (en procés d'actualització i modernització per facilitar-hi l'accés) o el Campus Virtual. Si és per a ús no institucional, utilitzar sistemes gratuïts (amb capacitat de fins a uns quants gigabytes) com ara Megaupload, Dropbox, File Dropper, Skydrive, etc., ja que el correu electrònic no és el mecanisme adequat ni més eficient per transferir fitxers.

h) Evitar l'ús del correu per enviar imatges, vídeos o altres fitxers adjunts no necessaris o no sol·licitats. Per exemple, és millor copiar el text d'un document al cos del missatge (si és d'informació i no cal conservar-ne el format) que afegir un fitxer adjunt, i si s'ha d'enviar informació adjunta, sempre és millor enviar-la en format PDF si no és necessari modificar el document. Valorar, segons la grandària del fitxer adjunt, la possibilitat d'enviar el fitxer comprimit (el format de compressió de fitxers més comú és Zip, però n'hi ha molts d'altres) per millorar la rapidesa en l'enviament i l'espai en el servidor. Fer servir l'opció de comprimir del propi sistema operatiu (si està disponible) o utilitats específiques gratuïtes per comprimir o descomprimir el fitxer adjunt en un fitxer Zip.

i) No facilitar dades personals a persones desconegudes i no fer servir mai el correu per enviar dades de caràcter financer o personal si el correu no és xifrat (o com a mínim segur, com per exemple IMAPS o HTTPS).

j) No respondre mai el correu no sol·licitat (*spam*). Respondre el correu no sol·licitat és una manera d'augmentar la quantitat de correu brossa, ja que indica a la persona remitent que el compte està actiu. A https://webmail.uab.es, en l'apartat Opcions, es poden introduir, modificar i verificar els filtres de correu que s'apliquen a la bústia institucional.

k) Evitar participar en el reenviament de correu no sol·licitat (acudits, cadenes de missatges, rumors, publicitat, etc.) o d'enganys i trucs (*hoax* en anglès). Les cases comercials i els centres d'alerta legítims tenen per norma redirigir els correus a servidors web que donen informació de manera fiable i detallen les accions que cal prendre.

l) Respectar la privadesa dels missatges i el destinatari. No reenviar missatges sense el permís de la persona remitent, sobretot aquells que tenen un contingut sensible, conflictiu o confidencial.

m) No abusar de les funcionalitats, com ara l'avís de recepció; tenen una eficàcia escassa quan s'utilitzen de manera indiscriminada o continuada i arriben a molestar la persona destinatària. Activar-les només en els casos en què realment sigui necessari.

2. Recomanacions d'actitud i de redacció

a) Tenir present que el correu electrònic és una eina de comunicació i, per tant, respondre tan aviat com sigui possible o, en cas que el missatge es derivi en un procediment o el volum de missatges per processar sigui molt gran, respondre breument per informar de la situació simplement dient que es tractarà el tema tan aviat com sigui possible (les bones pràctiques aconsellen respondre generalment com a màxim quatre dies hàbils després de rebre el correu i, si cal més temps, recomanen enviar una resposta curta per avisar).

b) Fer servir un nom d'usuari de correu electrònic que pugui reconèixer la persona destinatària, ja que, en cas contrari, el missatge podria ser esborrat sense ser llegit. Per al correu institucional es compleix aquesta norma, però si es fa servir un altre tipus de correu s'ha de tenir en compte.

c) Escriure una línia d'assumpte que descrigui clarament el contingut del missatge.

d) Donar un aspecte clar i ordenat al text del correu, tenir cura de la sintaxi i l'ortografia, no superar els 80 caràcters per línia (per facilitar-ne la lectura), fer servir la negreta, la cursiva i el subratllat només quan sigui necessari, i signar sempre el missatge (sobretot si és un missatge no personal, p. ex. d'una àrea, una oficina, etc.) en la part inferior del missatge perquè la persona destinatària pugui saber qui és el remitent i com posar-s'hi en contacte. La signatura ha d'incloure el nom, la responsabilitat o el càrrec, la institució i el telèfon per facilitar la comunicació; cal mostrar moderació en la informació posada per evitar que ocupi més que el missatge enviat. (Es pot configurar el programa de correu electrònic per incloure automàticament la signatura en tots els missatges de correu electrònic de sortida.)

e) No fer servir totes les lletres en majúscula, tant en la línia d'assumpte com en el missatge, en cas que el text no sigui realment important. Fer servir majúscules és equivalent a cridar. Considerar si cal fer servir el telèfon en cas que el missatge sigui crític, important o d'alerta per a una persona. En els missatges de correu electrònic, una paraula en majúscules sovint és eficaç però més d'una, tot el contrari.

f) Incloure el missatge original sota la resposta quan es fa un «Respon» (*Reply*) (configurar el programari perquè es faci automàticament) i eliminar tota la informació supèrflua del missatge original (aquesta última recomanació és aplicable també a l'opció Reenvia, *Forward*).

g) No enviar missatges amb còpia en obert (CC, *carbon copy*) a un nombre molt gran d'usuaris (o usuaris no habituals o de fora de la institució) excepte si les persones receptores estan d'acord a rebre'ls. En alguns casos es pot incórrer en una falta de LOPD (susceptible de ser sancionada amb multes de 600 € o més). En enviar còpies de missatges a usuaris no habituals o de fora de la institució, fer servir la còpia oculta només en els casos que sigui necessari enviar còpies (BCC, *blind carbon copy*).

h) Establir una resposta automàtica en el compte de correu electrònic (Missatge de vacances, en les opcions de configuració de http://webmail.uab.es) en els casos d'absència d'un període perllongat de temps (per vacances, conferències, malaltia, etc.) en què no es pugui consultar el correu periòdicament.

i) Valorar si és adient que la comunicació es faci per correu electrònic, sobretot en les comunicacions de caràcter institucional o en relació amb qüestions sensibles o personals: de vegades, el correu electrònic no és la millor manera de comunicar-se atès que el missatge pot ser percebut com a poc important o irrespectuós.

3. Bones pràctiques en els enviaments massius

a) Contactar el Servei d'Informàtica per obtenir assessorament sobre l'enviament massiu (congressos, activitats, etc.).

b) Fer ús de les eines adients per a l'enviament massiu (llistes de distribució). Consulteu: http://www.uab.es/si, en el subapartat Llistes de distribució de l'apartat Correu.

c) Tenir sempre en compte que la responsabilitat dels enviaments massius és de la persona que fa l'enviament (la UAB, per normativa, té un registre de tots els correus enviats i rebuts a bústies institucionals). En cas que es faci l'enviament massiu per la bústia institucional, dividir els destinataris en diversos grups o subllistes de distribució de manera que el volum de correu quedi repartit de manera equitativa (com més grups i menys nombre de destinataris per grup millor). Recordar que un volum molt gran de missatges similars enviats des d'un ordinador poden ser considerats correu brossa i els filtres dels diferents servidors pels quals passen els missatges els bloquejaran i cap missatge arribarà als destinataris.

d) Fer els enviaments en hores vall i espaiar els enviaments entre grups.

e) Dur a terme un manteniment periòdic de les llistes de correu d'usuaris subscrits i usuàries subscrites, tractar d'evitar subscripcions no desitjades, adreces de correu sospitoses i adreces de correu que rebutgen constantment els missatges que s'hi envien.

f) Tenir present la LOPD a l'hora d'enviar missatges que poden ser considerats no desitjats per les persones destinatàries, i exercir el dret de no rebre comunicacions, amb responsabilitat directa per a la persona remitent.

Annex III: Grup de Treball per a la Coordinació d''Incidents en Sistemes Informàtics (Computer Security Incident Response Team) (CSIRT-UAB)

Objectius

Aquest document defineix les bases i les tasques que realitzarà el Grup de Treball per a la Coordinació d'Incidents en Sistemes Informàtics de la UAB.

L'objectiu d'aquest grup és treballar i assessorar en temes de seguretat informàtica i gestió d'incidents en les xarxes telemàtiques de la UAB. Els objectius principals d'aquest grup estan definits en l'article 49 del Text refós de les normatives vigents en l'àmbit de les tecnologies de la informació i de la comunicació de la UAB.

Antecedents

Avui dia els termes CERT i CSIRT s'utilitzen de manera similar. El terme CSIRT és normalment el que més s'utilitza a Europa enlloc del terme protegit CERT, registrat als Estats Units pel CERT Coordination Center (CERT/CC) i ubicat a la Carnegie Mellon University, a Pittsburgh. Els diferents CSIRT i CERT són coordinats a nivell internacional pel Forum of Incident Response and Security Teams (FIRST) i a nivell europeu existeix l'agència ENISA (European Network and Information Security Agency*)* que té la finalitat de coordinar els esforços que realitzen els diferents CERT i CSIRT dels països de la UE i els grups de delictes informàtics dels cossos de seguretat.

D'acord amb els documents consultats i amb la informació existent, hi ha diferències en la constitució d'un grup de treball en funció dels clients atesos i del tipus d'entorn al qual s'orienten els serveis que es presten, així com de la relació i coordinació amb altres grups. És per això que la constitució d'un grup de treball d'aquestes característiques comporta, a més d'unes obligacions internes (amb dotació de recursos propis per desenvolupar els objectius definits), unes obligacions externes importants, tant a nivell nacional com internacional.

Per tant, es considera adient treballar per fases i, en primera instància, constituir un grup del tipus CSIRT, propi de la UAB i sense responsabilitats externes, que permeti reorientar i reforçar el model de seguretat dels sistemes d'informació de la UAB i millorar en funció dels recursos disponibles. Aquesta definició de grup no evadeix els drets i deures en relació amb Iris-CERT (http://www.rediris.es/cert/) ni amb l'Equip de Resposta a Incidents de l'Anella Científica (ERIAC) del CESCA (http://www.cesca.es/es/comunicacions/addicionals.html#12), i es deixa per a fases futures l'assumpció de responsabilitats tant d'àmbit nacional com internacional.

CSIRT-UAB. Descripció (d'acord a la RFC 2350)

Nom del Grup:

CSIRT-UAB: UAB University Computer Security Incident Response Team

Adreça

Edifici D. Campus Bellaterra. UAB. Bellaterra. 08193. Barcelona

Zona horària

GMT+0100/0200 DST

Telèfon de contacte

+34 93 581 21 00

Número de Fax

+34 93 581 20 94 (No és un fax segur)

Altres punts de comunicació

https://csirt.uab.cat

Adreça de correu electrònic

csirt@uab.cat
Es tracta d'un àlies de correu electrònic que transmet a l'equip de servei.

Claus públiques i certificats digitals

CatCert, PGP *públic key*.

Membres del Grup

El Grup de Treball per a la Coordinació d'Incidents en Sistemes Informàtics està integrat per les persones que consten en l'article 50 del Text refós de la normativa vigent en l'àmbit de les tecnologies de la informació i de la comunicació de la UAB.

Altra informació

La informació general sobre el CSIRT-UAB, així com enllaços als recursos de seguretat (recomanats), es pot trobar a https: //csirt.uab.cat.

Tipus de contacte recomanat

El mètode preferit per contactar el CSIRT-UAB és per mitjà del correu electrònic a csirt@uab.cat, les comunicacions rebudes a aquesta adreça s'enviaran automàticament al personal responsable immediatament. Per tal d'obtenir ajuda urgent, indiqueu "URGENT" a la línia d'assumpte.

Si no és possible (per raons de seguretat) utilitzar el correu electrònic, el CSIRT pot ser contactat per telèfon al Servei de CAS, al número de telèfon: 93 581 21 00, de 8.00 a 22.00 de dilluns a divendres,i de 8.00 a 20.00 els caps de setmana.

Si és possible, en presentar l'informe, cal utilitzar el formulari de presentació d'informes d'incidents.

Declaració de la missió

El propòsit del CSIRT-UAB és ajudar els membres de la comunitat universitària de la UAB en la resposta a incidents de seguretat, sempre que es produeixin, d'acord amb els objectius principals a què es refereix l'article 49 del Text refós de la normativa vigent en l'àmbit de les tecnologies de la informació i de la comunicació de la UAB.

Constitució

La circumscripció CSIRT-UAB és la comunitat universitària de la UAB i compta amb el suport parcial de la comunitat RedIRIS i del CESCA. No obstant això, cal tenir present que els serveis del CSIRT-UAB es proporcionen als sistemes de la UAB exclusivament.

Afiliació

La UAB, mitjançant els pressupostos derivats al Servei d'Informàtica, finança les accions del CSIRT-UAB en el 100% dels costos operatius, infraestructura, espai i servei telefònic.

Autoritat

El CSIRT funciona sota la responsabilitat del Comissionat per a la Societat de la Informació (o persona amb un càrrec equivalent) i amb el suport de personal acadèmic del Departament d'Enginyeria de la Informació i de les Comunicacions i del Departament d'Arquitectura de Computadors i Sistemes Operatius, i membres del Servei d'Informàtica i d'Informàtica Distribuïdes. La prestació del servei es delega al personal tècnic del Servei d'Informàtica de la UAB i als Serveis d'Informàtica Distribuïts de la UAB.

El CSIRT-UAB treballarà en cooperació amb el personal administrador de sistemes i persones usuàries de la UAB sempre que sigui possible, per tal d'evitar les relacions d'autoritat i dependència. No obstant això, si les circumstàncies ho justifiquen, el CSIRT pot demanar als Serveis d'Informàtica exercir la seva autoritat directa o indirectament, segons que sigui necessari.

Els membres del CSIRT i dels Serveis d'Informàtica difondran les directrius a la comunitat de la UAB i establiran els protocols per a l'aplicació de les normes de seguretat i resolució d'incidències en els sistemes informàtics, en cas necessari.

Polítiques

Tipus d'incidències i nivell de suport

El CSIRT-UAB està autoritzat per fer front a tot tipus d'incidents de seguretat informàtica que es produeixen o amenacen de produir-se en la seva àrea d'influència.

El nivell de suport proporcionat pel CSIRT pot variar segons el tipus i la gravetat de l'incident o el problema, el tipus de components i la mida de la comunitat d'usuaris afectats, encara que en tots els casos es compromet a donar una resposta en un període màxim de **tres dies** hàbils.

Els incidents es prioritzaran d'acord al seu nivell aparent de severitat i extensió. Aquests incidents seran avaluats pel que fa a la seva gravetat pel CSIRT i d'acord amb els seus criteris.

No hi haurà suport directe d'informació de seguretat per als usuaris i les usuàries finals, sinó a través de les persones responsables de centre o departaments i dels seus respectius administradors i administradores de sistemes, administrador o administradora de la xarxa. En cas de no disposar de personal qualificat es responsabilitzarà els usuaris i les usuàries finals de resoldre l'incident amb el suport dels SID o personal equivalent.

Tot i que hi ha una gran heterogeneïtat en el nivell de coneixements en seguretat informàtica a la Comunitat UAB, el CSIRT s'esforçarà per presentar la informació i l'assistència en un nivell adequat a cada persona. En cap cas, però, es podrà assumir la formació dels administradors del sistema sobre la marxa, tot i que es coordinaran les accions necessàries per a la resolució del problema quan sigui necessari.

El CSIRT,a través del Servei d'Informàtica, es compromet a mantenir al dia la informació sobre les possibles vulnerabilitats, i quan sigui possible, informarà la comunitat d'aquestes vulnerabilitats abans que siguin explotades activament a través de la pàgina https://csirt.uab.cat.

Cooperació, interacció i divulgació de la informació

Per defecte, el CSIRT-UAB mantindrà la confidencialitat de tota la informació relativa als incidents.

El CSIRT es compromet a protegir la identitat dels membres de la comunitat afectats i/o causants de la incidència, però es reserva el dret de prendre les accions oportunes en cas que hi hagi accions de faltes o delictes en relació amb persones o infraestructures de la UAB.

La informació sense dades de caràcter personal podrà ser utilitzada per explicar o ajudar altres persones a resoldre o prevenir els incidents de seguretat.

Comunicació i autentificació

En funció del tipus d'informació que es vulgui comunicar, el CSIRT recomana fer-ho per correu electrònic, amb un missatge signat digitalment o xifrat en cas que la informació contingui dades de caràcter personal o per qüestions de confidencialitat. La informació de sortida del CSIRT-UAB sempre anirà signada digitalment i la informació pública serà penjada a la pàgina segura https://csirt.uab.es.

Les claus arrel per validar les signatures digitals es poden obtenir a http://catcert.cat.

Serveis

Resposta a incidents

El CSIRT-UAB proporcionarà assistència o assessorament pel que fa als següents aspectes de la gestió d'incidents:

Selecció d'incidents: Normes per investigar si efectivament s'ha produït un incident. Determinar l'abast de l'incident.

Coordinació d'incidents: Determinació de la causa inicial de l'incident (vulnerabilitat explotada). Facilitar el contacte amb altres llocs que poden estar-hi involucrats. Realització d'informes a altres CERT-CSIRT. Redacció d'anuncis per als usuaris i les usuàries, si escau.

Determinació de les formes de resolució d'incidents: Indicacions per a l'eliminació de la vulnerabilitat. Regles per protegir el sistema contra els efectes de l'incident. Recollir estadístiques relatives als incidents que es produeixin a la UAB o involucrin la comunitat quan sigui necessari per col·laborar en la protecció contra atacs coneguts.

Activitats proactives: El CSIRT definirà les polítiques i coordinarà les accions, en la mesura que sigui possible, en funció dels seus recursos, a través de llistes de contactes de seguretat dels serveis distribuïts i departaments/centres. També donarà el vistiplau a l'ús del repositori d'eines de seguretat i documentació per a administradors i administradores de sistemes a través de https://csirt.uab.cat.

El CSIRT-UAB farà les recomanacions necessàries als serveis de formació de PDI-PAS sobre la impartició de cursos relacionats amb temes de seguretat informàtica.

El CSIRT-UAB també definirà les accions i els protocols de cerca proactiva per investigar possibles forats de seguretat en les infraestructures de la UAB i en les que hi estiguin vinculades, sense accedir a dades de caràcter personal, amb l'únic objectiu de trobar possibles vulnerabilitats.

Serveis d'arxiu: Es mantindran els registres d'incidents de seguretat, que seran confidencials, i es podran utilitzar amb finalitats documentals i fins estadístics.

Avís legal

Si bé s'han pres totes les precaucions que cal adoptar en la preparació de la informació, notificacions i alertes, el CSIRT no assumeix cap responsabilitat per errors o omissions, ni pels danys resultants de l'ús de la informació continguda en aquest document.

Formularis

CSIRT-UAB: formulari d'informe d'incidents

El CSIRT-UAB ha desenvolupat aquest formulari per ajudar-vos recopilar informació sobre l'incident en seguretat informàtica en màquines que pertanyen a la UAB o que estan connectades a la xarxa de la UAB. Si sospiteu que aquestes màquines estan involucrades en un incident, si us plau, completeu el formulari que hi ha a continuació. Això ens ajudarà a evitar retards a l'hora detectar l'incident.

Tota la informació continguda en aquest formulari és confidencial i podrà ser utilitzada únicament i exclusivament per a la resolució de l'incident de seguretat. A més, pel que fa a la informació de caràcter personal, d'acord amb el que disposa la LOPD, podeu exercir els drets d'accés, de rectificació i de cancel·lació davant la Secretaria General de la UAB.

Informació de contacte:

CSIRT-UAB: UAB University Computer Security Incident Response Team
Edifici D. Campus de Bellaterra. UAB. Bellaterra. 08193. Barcelona
Telèfon: +34 93 581 21 00
Fax: +34 93 581 20 94 (No és un fax segur)

Servidor web: https://csirt.uab.cat
Correu electrònic: csirt@uab.cat

Si us plau, contacteu-nos si teniu cap comentari o suggeriment. Gràcies per endavant.

CSIRT-UAB

✂----------

Envieu aquest formulari a csirt@uab.cat

Si no podeu fer servir el correu electrònic, podeu enviar-lo per fax al núm.: +34 93 581 20 94

1. INFORMACIÓ DE CONTACTE
-Nom del departament, centre, institut, etc.:
-Nom de la persona de contacte per a aquest incident:
-Adreça de correu electrònic (camp obligatori):
-Telèfon/fax:
-Entitat certificadora si feu servir correu digital signat (recomanat):
-Altres:

2. APARELLS DE PERSONES AFECTADES
-Nom de la màquina:
-Adreça IP:
-Ubicació física (laboratori, despatx...) i identificació de la roseta de connexió a xarxa (número de damunt el punt de connexió a la xarxa a la paret):
-Sistema operatiu i versió:
-Té instal·lades les actualitzacions de seguretat (*security patches*) recomanades de proveïdors de programari i/o

del CSIRT-UAB? (Sí/No/No ho sap):
-Altres (serveis oberts, mesures de seguretat, propòsit de la màquina, etc.):

3. FONT DE L'ATAC (si es coneix)
-Nom de màquina:
-Adreça IP:
-Heu contactat el responsable d'aquesta màquina? (Sí/No):
-Informació addicional:

4. DESCRIPCIÓ DE L'INCIDENT
Si us plau, incloeu les dades que considereu necessàries, incloent-hi (si disposeu d'aquesta informació) els mètodes o les eines d'intrusió, els detalls de les vulnerabilitats explotades, o qualsevol altra informació pertinent.

-Sabeu si l'ordinador ha estat utilitzat per llançar atacs a altres màquines? (Sí/No/No ho sap).
-En cas afirmatiu, duplicar aquesta informació per a cada equip de destinació:
Nom de host, adreça IP, informació addicional.

Si us plau, envieu qualsevol arxiu de registre, el missatge de correu electrònic i arxius que podrien ajudar a gestionar l'incident.

5. ALLIBERAMENT D'INFORMACIÓ
-Excloent-ne les dades de caràcter personal, doneu el vostre vistiplau per fer pública la informació relativa a aquest incident? (Sí/No):
-Comentaris:

Formulari adaptat des d'Iris-CERT (http://www.rediris.es/cert/tareas/servicios/iris-cert/).

CSIRT-UAB: Formulari de comentaris i/o suggeriments:

Tota la informació continguda en aquest formulari és confidencial i podrà ser utilitzada únicament i exclusivament per a la millora del servei. A més, pel que fa a la informació de caràcter personal, d'acord amb el que disposa la LOPD, podeu exercir els drets d'accés, de rectificació i de cancel·lació davant la Secretaria General de la UAB.

✂----------
Envieu aquest formulari a csirt@uab.cat

1. INFORMACIÓ DE CONTACTE
-Nom del departament, centre, institut, etc.:
-Nom de la persona de contacte per a aquest comentari/suggeriment:
-NIU:
-Adreça de correu electrònic (indispensable):
-Telèfon/fax (opcional):

Comentari o suggeriment: