Pendent de correcció lingüística

Normativa de seguretat d'utilització dels recursos i Sistemes d'Informació de la Universitat Autònoma de Barcelona

(Acord del Consell de Govern de 10 de febrer de 2026)

Índex

Preàmbul

I

La Universitat Autònoma de Barcelona **-UAB-** depèn, entre d'altres, dels sistemes de les Tecnologies de la Informació i les Telecomunicacions **—TIC—** per a aconseguir els seus objectius. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per a protegir-los enfront de danys accidentals o deliberats que puguin afectar la seguretat de la informació tractada o els serveis prestats i estant sempre protegits contra les amenaces o els incidents amb potencial per a incidir en la confidencialitat, integritat, disponibilitat, traçabilitat i autenticitat de la informació tractada i els serveis prestats.

Per fer front a aquestes amenaces es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn per a garantir la prestació contínua i fiable dels serveis. Això implica que les diferents unitats o òrgans administratius en què s'estructura i organitza la Universitat han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat **—ENS—**, així com realitzar un seguiment continu dels nivells de prestació dels serveis, monitorar i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als ciberincidents per a garantir la continuïtat dels serveis prestats. La seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la seva retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en els plecs de clàusules administratives particulars i de prescripcions tècniques de les licitacions per a projectes de TIC.

Per aconseguir aquests objectius la Universitat Autònoma de Barcelona va aprovar la *'Política de Seguretat de la Informació de la Universitat Autònoma de Barcelona'* per acord núm. 92/2023, de 18 de desembre, la disposició onzena de la qual disposa la necessitat d'un posterior desenvolupament normatiu del segon nivell sobre seguretat.

II

La present normativa s'estructura en trenta-nou articles, organitzats en nou capítols, una disposició derogatòria i una disposició final.

El Capítol I, dedicat a disposicions generals, s'organitza en dos Seccions. La Secció 1a delimita l'objecte de la Normativa i el seu àmbit d'actuació. La Secció 2a identifica qui és titular del dret d'ús dels Sistemes d'Informació i dels Recursos Informàtics diferenciant les figures de la persona responsable, administradora i usuària d'aquests recursos informàtics. Es declara que tot dispositiu informàtic que la Universitat posa a disposició dels membres de la seva comunitat han de ser destinats exclusivament a les tasques pròpies de la vinculació de l'usuari amb la Universitat.

El Capítol II determina la manera segura per accedir a internet a través dels recursos informàtics que la Universitat posa a disposició dels membres de la comunitat universitària.

El Capítol III identifica la xarxa informàtica de la Universitat i estableix que la gestió li correspon a la Direcció de Tecnologies de la Informació i Comunicacions -DTIC-. Regula la forma de connectar equipament a la xarxa informàtica de la Universitat i la necessitat d'homologar la connexió per part dels serveis tècnics i el règim de funcionament. Regula singularment la connectivitat d'objectes que incorporin mecanismes de comunicació digital (internet de les coses **-IoT-**).

El Capítol IV disposa la obligació de la Universitat de posar a disposició dels membres de la comunitat bústies de correu electrònic i s'estableix que la infraestructura i el servei per al correu electrònic és gestionada per la DTIC. Es responsabilitza exclusivament als usuaris de l'ús que es

faci dels comptes de correu que se'ls assigni. Regula les llistes de difusió i els serveis de col·laboració al núvol.

El Capítol V determina la responsabilitat dels usuaris dels Sistemes d'Informació i dels Recursos Informàtics quan treballin fora de les instal·lacions de la Universitat, establint el seu règim d'ús. Incideix en que aquesta infraestructura tecnològica que la Universitat posa a disposició dels membres de la comunitat és per l'ús exclusiu per les finalitats pròpies del vincle a la Universitat, inclús quan s'utilitzi fora de les instal·lacions de la Universitat.

El Capítol VI aborda la gestió i l'ús de contrasenyes per accedir als sistemes informàtics.

El Capítol VII estableix l'obligació de formalitzar acords de confidencialitat i acords d'interconnexió als proveïdors de serveis que, per l'objecte del contracte administratiu, hagin de tenir accés a dades de la Universitat o tinguin accés als sistemes o infraestructura, respectivament. Així mateix, se'ls exigirà la formalització d'un acord de nivell de servei.

El Capítol VIII preveu la creació i l'ús de perfils públics de la UAB a les xarxes socials amb l'autorització de l'Àrea de Comunicació i Promoció de la Universitat.

El Capítol IX, com a mesura de protecció de les infraestructures informàtiques de la Universitat, regula la gestió dels incidents de seguretat. S'identifiquen els casos d'incompliment de la normativa, els quals es qualifiquen com un notori incompliment de les funcions essencials del lloc de treball o funcions encomanades o, en el seu cas, una deslleialtat o una transgressió de la bona fe contractual, als efectes de determinar la responsabilitat disciplinària dels usuaris. Finalment, s'estableix un procediment que té per objecte la restricció del dret d'ús dels Sistemes d'informació i dels Recursos Informàtics de la Universitat.

El text finalitza amb una disposició derogatòria i una disposició final sobre l'entrada en vigor de la norma.

III

En l'elaboració de la present normativa s'ha respectat allò que preveu l'article 87.3 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

Capítol I. Disposicions generals.

Secció 1a. Objecte i Àmbit d'aplicació.

Article 1. Objecte.

La present normativa té per objecte desenvolupar el segon nivell normatiu esmentat a la *'Política de Seguretat de la Informació de la Universitat Autònoma de Barcelona'* per determinar la seguretat i el règim d'ús dels Sistemes d'Informació, dels Recursos Informàtics i dels mitjans electrònics que la Universitat posa a disposició dels membres de la comunitat universitària.

Article 2. Àmbit d'aplicació.

La present normativa s'aplica a totes les persones que facin ús dels Sistemes d'Informació i Recursos Informàtics de la UAB i aquelles persones que disposin de sistemes o xarxes connectades a la xarxa informàtica de la UAB.

A aquests efectes s'entén per:

- *'Recurs informàtic'*: qualsevol component físic o lògic per a processament, producció, comunicació, emmagatzemament d'informació. Poden tenir diferents categories com ara maquinari (dispositius), programari, xarxes i/o serveis al núvol.

- *'Dispositius corporatius'*: Mecanisme o artifici per produir una acció electrònica prevista de propietat de la UAB. Poden ser gestionats o no gestionats. En els dispositius gestionats la DTIC aplica la configuració i les mesures de seguretat. La resta seran dispositius no gestionats.

- *'Sistema d'informació'*: tot el conjunt organitzat de recursos informàtics de la UAB per a què la informació es pugui recollir, emmagatzemar, processar, tractar, mantenir, compartir, distribuir, posar a disposició, presentar o transmetre.

- *'Sistema de les tecnologies de la informació i les telecomunicacions'*: conjunt d'equipaments, mètodes, procediments i personal, organitzat amb eines, mètodes i sistemes digitals de forma que permeti emmagatzemar, processar, o transmetre informació sota la responsabilitat d'una única autoritat.

- *'Servei digital'*: funcions que s'ofereixen des de la UAB, en el marc de l'administració electrònica i la infraestructura tecnològica, que faciliten la interacció entre els ciutadans i les administracions públiques, com la gestió de tràmits electrònics. Alguns exemples son els serveis electrònics del sector públic, els serveis d'infraestructura tecnològica, els serveis d'autentificació i autorització i els serveis de protecció de la informació.

- *'Usuari/a d'un recurs informàtic'*: als Sistemes d'Informació de la UAB i als seus serveis associats cada usuari/a està representat per un compte d'usuari/a personal. Els comptes d'usuari/a formen part de col·lectius ja existents amb una sèrie de serveis associats. La UAB posa bústies de correu electrònic a disposició de les persones usuàries, que s'ofereixen com una eina bàsica pel recolzament dels objectius de la Universitat en ensenyament, recerca, transferència i intercanvi del coneixement. El servei respecta els principis de llibertat d'expressió i privacitat de la informació.

- *'Sistema de gestió de la identitat'*: servei realitzat per la UAB on es donen d'alta als usuaris a través de diferents procediments establerts: matriculació d'alumnat, contractació, comunicació de personal eventual, vinculacions, col·laboracions, entre d'altres. Un cop donats d'alta els usuaris poden accedir als sistemes d'informació i serveis proporcionats per la UAB mitjançant diferents sistemes d'autentificació que també formen part del sistema de gestió de la identitat.

- *'Connexió permanent d'un dispositiu a la xarxa'*: situació que es produeix de forma automàtica quan un ordinador o un dispositiu IoT es connecta a la xarxa de la UAB, de forma continua, durant més d'un mes.

Secció 2a. Del règim d'ús dels Sistemes d'Informació i dels Recursos Informàtics.

Article 3. Assignació dels Recursos Informàtics dels Sistemes d'Informació.

1. Per la consecució de les seves finalitats, la UAB assigna Recursos Informàtics dels Sistemes d'Informació als membres de la comunitat universitària i a persones amb vinculació temporal a la Universitat que hagin estat expressament autoritzades.

2. A tots els Sistemes d'Informació que la UAB posa a disposició dels membres de la comunitat s'hi identifica una persona responsable, una persona administradora dels recursos i una persona usuària.

3. Tot recurs informàtic connectat a la xarxa de la UAB ha de tenir associat una persona responsable.

4. Tota persona amb accés als Sistemes d'Informació ha de ser identificada de manera inequívoca.

5. Tota persona que utilitzi els Sistemes d'Informació ha de ser prèviament autoritzada. Els accessos a serveis diferents dels definits per als col·lectius als que pertany la persona han de ser sol·licitats i autoritzats expressament. El cessament de la vinculació de les persones a la Universitat comportarà, en general, la pèrdua del dret d'accés als Sistemes d'Informació.

6. L'accés a Sistemes d'Informació associats al desenvolupament d'un càrrec o funció estaran limitats a la durada de dit càrrec o funció.

Article 4. Exercici del dret d'ús dels Sistemes d'Informació i dels Recursos Informàtics.

1. Els Sistemes d'Informació i els Recursos Informàtics de la UAB són per a ús exclusiu de les tasques pròpies de la Universitat, per a membres de la seva comunitat universitària o persones expressament autoritzades.

2. Tots els Recursos Informàtics de la UAB que es posen a disposició del Personal Acadèmic, Personal investigador en formació i del Personal Tècnic, de Gestió i d'Administració i Serveis **— PTGAS—** són per a ús exclusiu de les tasques pròpies de la seva vinculació funcionarial, laboral o estatuària amb la Universitat.

3. Tots els Recursos Informàtics de la UAB que es posen a disposició de l'alumnat i membres vinculats temporalment a la UAB són per desenvolupar les tasques que determinen la seva vinculació amb la UAB.

Article 5. Persona responsable dels Recursos Informàtics.

1. La persona responsable dels Recursos Informàtics és aquella que te el deure de vetllar pel bon funcionament dels Recursos Informàtics assignats sota la seva tutela. Comptarà amb el suport del personal de la DTIC.

Aquests efectes son persones responsables dels Recursos Informàtics:

a) Els degans i les deganes i el director o directora de l'Escola d'Enginyeria vetllen perquè els centres disposin dels mitjans necessaris, han d'anomenar una persona responsable dels recursos d'ús general per a la docència del centre.

b) Les persones administradores de centre, són responsables dels Recursos Informàtics destinats a la gestió del centre.

c) Els directors i les directores de departament, són responsables dels Recursos Informàtics assignats al departament, com ara Recursos Informàtics dedicats a la docència, a la recerca i a la gestió del departament.

d) El director o la directora de la DTIC, que ho és dels Recursos Informàtics centrals, ordinadors personals corporatius gestionats, dispositius mòbils gestionats i de la xarxa de comunicacions.

e) Els sistemes personals no gestionats tenen com a responsable per defecte el seu administrador.

f) Cadascuna de les persones que contracta el servei de *Housing* procurat des de la DTIC, que ho son dels servidors que hi té allotjats.

g) Cadascuna de les persones que contracta serveis TIC al núvol amb càrrec a la UAB, que ho son del que hi desplega.

2. 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 6. Persona administradora dels Recursos Informàtics.

1. La persona administradora dels Recursos Informàtics s'encarrega de gestionar un o més Recursos Informàtics i treballa coordinadament amb la persona responsable dels Recursos Informàtics i els serveis, a la qual comunica totes les incidències que hagi detectat i que puguin afectar el bon funcionament dels recursos.

2. La persona administradora dels Recursos Informàtics ha de treballar coordinadament amb el personal de la DTIC en totes les qüestions vinculades a la prestació del servei però sobretot en qüestions tècniques i de seguretat, i col·labora activament en la detecció, el seguiment i la identificació dels possibles incidents de seguretat. Principalment, ha d'aplicar el contingut de les normatives i recomanacions de seguretat als recursos que gestiona.

3. Als efectes de la gestió dels riscos de seguretat informàtica, aquelles persones administradores de recursos informàtics que puguin presentar riscos fora dels habituals hauran de declarar de forma responsable el perfil de risc dels equips que administren, d'acord amb el procediment que s'estableixi.

A aquests efectes, s'entendran riscos fora de l'habitual els següents:

a) La instal·lació i/o us d'eines que puguin alterar la configuració dels equips afectant la seva seguretat informàtica.

b) La instal·lació i/o us d'eines específiques de l'àmbit de la ciberseguretat.

c) La instal·lació i/o us de software obsolet pel que fa a la seva seguretat informàtica.

No caldrà declarar aquells equips sense connexió a la xarxa de la UAB.

Quan sigui necessari la instal·lació i connexió permanent a la xarxa de dispositius no gestionats des de la DTIC, la persona administradora del recurs ha de sol·licitar-ne l'autorització.

Quan sigui necessari que un dispositiu no gestionat s'integri de forma permanent a la xarxa, la persona administradora del recurs ha de sol·licitar-ne l'autorització excepte en el cas dels telèfons mòbils i tauletes tàctils.

Article 7. Persona usuària dels Recursos Informàtics.

1. Les persones usuàries dels Recursos Informàtics són responsables de la custòdia dels dispositius propietat de la UAB que se'ls assignin seguint les recomanacions, quant a la utilització dels Recursos Informàtics, de les persones responsables i administradores dels Recursos Informàtics; especialment en qüestions tècniques, de protecció de dades, de continguts protegits pels drets d'autor i en qüestions de seguretat, aplicant la legislació.

Les persones usuàries hauran de comunicar a la persona administradora del Recurs Informàtic que tingui assignat, qualsevol canvi en la titularitat del mateix. Mentre la persona usuària no realitzi

aquesta comunicació, continuarà sent la persona responsable de la custòdia i dels usos que se'n derivin.

2. En cas d'incompliment de la normativa de seguretat, la persona responsable del Recurs Informàtic pot denegar a la persona usuària, de manera preventiva i provisional, l'ús o accés a un Sistema d'Informació, o la connexió d'un sistema o xarxa a la xarxa general de la Universitat.

En cas de desconnexió de la xarxa, i sempre que sigui possible, es contactarà prèviament amb la persona usuària per comunicar-li l'acció pertinent i solucionar els problemes, excepte en els casos en que es vegi compromesa la seguretat de la xarxa o de segments de la xarxa i que sigui imperativa la seva desconnexió.

3. Les persones usuàries tindran màxima cura en la manipulació i ús dels dispositius 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.

4. Les persones usuàries amb dispositius no gestionats, es responsabilitzaran de mantenir-los actualitzats amb els pegats de seguretat, tant de sistema operatiu com dels programaris que hi estiguin instal·lats. En cas dels sistemes de difícil actualització relacionats amb equipament científic, caldrà identificar un responsable del sistema per definir i aplicar una política d'aïllament adaptada a la situació específica de l'equipament.

En els dispositius corporatius gestionats, la responsabilitat de mantenir sistema operatiu, antivirus i tallafocs actualitzats és de la DTIC. En cas que les persones usuàries hi instal·lin programari addicional, s'han de responsabilitzar de mantenir-lo actualitzat.

5. Les persones usuàries vigilaran l'ús responsable dels recursos per a reduir el risc de propagar programari maliciós a través de memòries USB, unitats compartides de xarxa, missatges de correu electrònic o programari descarregat des d'Internet. La Universitat posarà a l'abast de les persones usuàries els cursos i la documentació necessària per a la correcta utilització dels recursos i les guies i consells oportuns per augmentar la conscienciació i reduir aquest risc.

6. Les persones usuàries accediran als Recursos Informàtics seguint les normatives generals i les instruccions específiques de cada centre.

7. Els comptes d'usuari en els Sistemes d'Informació de la Universitat són personals i intransferibles. La persona usuària és responsable de tenir màxima cura de la seva contrasenya i qualsevol mètode d'autenticació actiu que ha de mantenir en secret.

Tots els canvis de contrasenyes de comptes dels Sistemes d'Informació es duran a terme fent ús dels mecanismes i protocols definits en cada moment pels responsables dels sistemes.

Article 8. Emmagatzemament i salvaguarda (còpia de seguretat) d'informació.

1. La informació emmagatzemada de forma local en els dispositius no gestionats no és objecte de salvaguarda en els procediments corporatius de còpia de seguretat. És responsabilitat de la persona usuària la realització periòdica de còpies de seguretat.

2. Els Sistemes d'Informació gestionats per la DTIC realitzaran còpies de seguretat segons les polítiques i seguint els procediments determinats en el moment de la categorització del Sistema.

3. Les còpies de seguretat, quan ja no siguin necessàries, i els mitjans d'emmagatzemament que, per obsolescència o degradació, perdin la seva utilitat, i molt especialment aquells que continguin informació sensible, confidencial o protegida, hauran de ser eliminats de forma segura. La persona usuària (o la persona administradora del sistema amb els seus usuaris) haurà de validar

l'eliminació del contingut i de la destrucció del suport si aquest conté informació confidencial, sensible o protegida.

Article 9. Equipament fix, portàtil i mòbil.

1. L'equipament informàtic propietat de la UAB, ja sigui fixe, portàtil o mòbil, estarà inventariat i estarà sota la custòdia de la persona usuària assignada i sota la responsabilitat de la persona responsable.

Totes les persones adoptaran les mesures necessàries per a evitar-ne danys o sostracció, així com l'accés a ells de persones no autoritzades amb les mesures de seguretat aplicables als centres com ara aules de laboratori i espais de recerca amb clau o control d'accés i l'ús de sistemes d'ancoratge d'equipament. En cas de sostracció o pèrdua d'un d'aquests dispositius, la persona usuària ho comunicarà per a l'adopció de mesures que correspongui i a efectes de baixa de l'inventari.

2. Les persones usuàries evitaran en la mesura del possible la connexió dels dispositius portàtils a xarxes públiques fora del campus per accedir als Sistemes d'Informació de la UAB.

3. Quan es modifiquin les circumstàncies funcionarials, laborals, estatutàries o acadèmiques que provoquin la desvinculació amb la Universitat, la persona usuària haurà d'entregar el dispositiu per a procedir, si s'escau, a l'esborrat segur de la informació emmagatzemada.

4. Les persones usuàries, en el cas de que tinguin l'opció, han de tenir configurats els dispositius de manera que es bloquegi la sessió d'usuari o s'activi el salva pantalles amb contrasenya passats uns minuts d'inactivitat, per tal que cap altra persona pugui fer mal ús de les seves credencials, o li pugui suplantar la identitat.

Article 10. Protecció de la propietat intel·lectual i de la dignitat de les persones

1. Està estrictament prohibida l'execució de programari informàtic en els Sistemes d'Informació de la UAB que no compleixi la corresponent llicència d'utilització. S'inclouen en aquesta categoria els programes que s'ofereixen de manera gratuïta en el mercat per a utilització d'usuaris domèstics, però no per a empreses.

2. El programari informàtic propietat o llicenciats per a la UAB està protegit per la legislació sobre propietat intel·lectual, i per tant, és obligatori complir els termes de la llicencia.

3. S'aplicarà la legislació vigent en termes de propietat intel·lectual regulant els usos no autoritzats i la utilització, reproducció, distribució, transformació i/o comunicació pública de qualsevol obra protegida per drets de propietat intel·lectual en els Sistemes d'Informació.

4. Està prohibida en els Sistemes d'Informació de la UAB tota transmissió, distribució o emmagatzemament de qualsevol material que constitueixi un atemptat contra la dignitat, l'honor, la intimitat personal i familiar i la pròpia imatge de les persones.

Article 11. Accés als Sistemes d'Informació i a les dades tractades.

1. Totes les dades gestionades per la UAB i tractades en qualsevol dels elements del Sistemaa d'Informació categoritzats han de tenir una persona que les administri d'acord amb els criteris i instruccions de la persona responsable. Aquesta persona serà l'encarregada d'atorgar, modificar i anul·lar l'autorització d'accés a aquestes dades per part de les persones usuàries.

2. L'alta d'usuaris serà gestionada pel Sistema de Gestió de la Identitat a través dels procediments establerts.

3. Un usuari que accedeixi als recursos corporatius no oberts al públic dels Sistema d'informació, necessitarà un compte d'usuari i una autorització adequada per l'ús requerit. S'estableixen nivells d'accés als sistemes d'informació i les dades diferents per als col·lectius d'usuaris de la comunitat de la UAB. Els perfils, amb nivells d'accés diferents dels definits per col·lectiu, han de ser autoritzats. Els comptes d'usuari es poden desactivar si es detecta una utilització no adequada a les normatives de seguretat.

4. Les persones que sol·licitin o disposin d'accés als Sistemes d'Informació (sigui amb dispositius 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 la present Normativa de Seguretat i la Normativa de Protecció de dades de la UAB, les quals estaran a la seva disposició a través del portal de la UAB.

Article 12. Identificació i autenticació.

1. Les persones usuàries disposaran del codi d'usuari/a i contrasenya, o de mecanismes alternatius en funció de l'evolució tecnològica (targeta criptogràfica, certificat digital, etc.) per a l'accés als Sistemes d'Informació.

2. És responsabilitat de la persona usuària la custòdia de la contrasenya, les targetes criptogràfiques i dels certificats personals.

Les persones usuàries no tindran les seves contrasenyes per escrit a la vista i accessible a tercers. Si la persona usuària té sospita que les seves credencials estan sent utilitzades per altra persona, procedirà al canvi de la seva contrasenya i comunicarà la sospita a la DTIC.

3. A més dels comptes personals, a la UAB existeixen comptes no personals, bé sigui per raó institucional, o per a execució de processos determinats. Tot compte no personal ha de tenir una única persona responsable.

Article 13. Monitorització i auditoria de la utilització dels Sistemes d'Informació i Recursos Informàtics

1. En aplicació dels objectius definits a la *'Política de Seguretat de la Informació de la Universitat Autònoma de Barcelona'*, la UAB podrà comprovar mitjançant sistemes d'auditoria informàtica que l'ús que fan els col·lectius de la Universitat (Personal Acadèmic, Personal investigador en formació, PTGAS, alumnat i membres vinculats temporalment) dels Sistema d'informació i dels Recursos Informàtics és l'adequat a aquestes finalitats, en els termes legals, especialment pel que fa a la jurisprudència relacionada amb els drets a la intimitat i a la dignitat dels treballadors.

2. La UAB, mitjançant el Comitè de Seguretat, adoptarà les mesures de monitorització i auditoria per detectar comportaments maliciosos, i en aquests casos podrà activar mesures preventives per mitigar la seva afectació.

Es podran fer auditories quan s'hagi detectat un ús irregular dels mitjans informàtics o es tinguin evidències externes o internes d'ús inadequat dels Recursos Informàtics. Aquestes actuacions es concreten en les següents:

a) Es revisarà periòdicament l'estat de l'equipament, el programari instal·lat, els dispositius i xarxes de comunicacions.

b) Es monitoritzarà els accessos a la informació continguda als Sistemaes d'linformació.

c) S'auditarà la seguretat de les credencials i aplicacions.

2. Tota activitat de monitorització es realitzarà de manera proporcional al risc, sota els judicis d'idoneïtat, necessitat i proporcionalitat, respectant els requeriments legals i les cauteles indicades per la jurisprudència, observant els drets de les persones usuàries.

3. La UAB habilita, en els seus Sistema d'informació, un registre dels accessos i modificacions de la informació requerits per l'ENS.

Capítol II. Accés a internet.

Article 14. Accés a internet des de la UAB.

1. Amb caràcter general, les persones usuàries dels Recursos Informàtics de la UAB disposaran d'accés a Internet com a eina per al desenvolupament de la seva activitat.

2. La UAB ha de garantir l'ús adequat dels Recursos Informàtics d'accés a Internet per:

a) Seguretat: degut als riscos de seguretat informàtica, com ara el d'infecció per codi maliciós.

b) Volum de tràfic extern de dades: s'assegura que l'accés a continguts que són necessaris per a l'activitat professional i acadèmica no es vegi perjudicat pel tràfic generat per continguts no vinculats a aquestes activitats.

Article 15. Política de tallafocs.

1. La UAB ha de disposar de tallafocs perimetral per poder limitar quan calgui l'accés a serveis, tant dins de la xarxa interna de Campus com cap a i des d'Internet.

2. La UAB ha de gestionar els accessos a serveis no estrictament necessaris per a l'activitat professional i acadèmica, podent restringir aquest tràfic.

Tots els serveis oferts per la UAB que s'accedeixin via internet estaran tancats a les persones externes, excepte els declarats explícitament.

Tots els serveis externs als sistemes locals accedits des de la UAB, com ara els localitzats als proveïdors al núvol, estaran gestionats per la UAB. Es poden aplicar restriccions a aquests serveis externs per motius de seguretat.

Article 16. Registre de servidors.

1. El registre de servidors manté la llista activa dels serveis ubicats a servidors de la UAB que han de tenir visibilitat des d'Internet.

2. Els serveis declarats que no tinguin activitat durant 3 mesos consecutius podran ser donats de baixa seguint un procediment previ de notificació a la persona responsable.

Article 17. La xarxa privada virtual.

1. La UAB habilita el sistema de xarxa privada virtual —XPV— per a poder accedir a alguns recursos restringits a serveis des de fora de la Universitat. Per defecte, els accessos que es puguin fer via XPV no s'obriran en el tallafocs perimetral.

2. En general, els serveis que només estiguin dirigits al personal UAB (Personal Acadèmic i PTGAS) i no a la ciutadania en general, estaran disponibles exclusivament a través d'una connexió de xarxa privada virtual.

3. Per a declarar explícitament un servei, la persona responsable ha de sol·licitar-ho a través dels procediments establerts. Qualsevol excepció respecte a l'accés a un servei fora de la via XPV haurà de ser sol·licitada i justificada.

Capítol III. Connexió a la Xarxa.

Article 18. La xarxa de la UAB.

La xarxa informàtica de la UAB és un recurs compartit propietat de la Universitat per a ús en tasques de recerca, docència, transferència i intercanvi del coneixement i gestió de la pròpia institució i institucions amb conveni. La gestió, manteniment i aplicació de les instruccions derivades de les normatives aprovades és responsabilitat de la DTIC.

Article 19. Connexió d'equipament a la xarxa de la UAB

1. L'equipament a connectar són els dispositius personals, els portàtils, les impressores, els servidors i en general qualsevol dispositiu connectable en xarxa amb cable (xarxa fixa) o amb capacitat WiFi diferents que els que conformen la infraestructura central de xarxa.

2. Tot equip connectat de forma permanent a la xarxa fixa de la UAB ha d'estar registrat, identificat, i amb persona responsable, administradora i usuària assignada. La gestió d'aquesta identificació i l'assignació de noms i adreces es fa des de la DTIC.

3. Per defecte, l'equip que es connecta a xarxa ha d'estar configurat per rebre la configuració de xarxa per DHCP.

4. Tots els dispositius que es connecten a la xarxa han de tenir les actualitzacions de seguretat al dia. Si un dispositiu no compleix, se li podrà treure l'accés a la xarxa o l'accés a Internet. Si un dispositiu fa mal ús de la xarxa o incompleix les normatives de seguretat també se li podrà treure l'accés.

5. Tots els ordinadors connectats a la xarxa de la UAB han de tenir configurat i activat un tallafocs.

6. Tot equip amb sistema operatiu Windows connectat a la xarxa de la UAB ha de tenir instal·lat, al dia i en funcionament el sistema de protecció contra programari maliciós (com antivirus i d'altres). S'establiran protocols de protecció especials per a aquells sistemes de difícil actualització o substitució.

7. Tot equip connectat a la xarxa de la UAB ha de tenir funcionant el sistema automàtic d'actualitzacions del sistema operatiu. S'establiran protocols de protecció especials per a aquells sistemes de difícil actualització o substitució.

8. Els dispositius que no tinguin activitat s'hauran de desconnectar de la xarxa d'acord amb el protocol que s'estableixi.

9. La DTIC mantindrà actualitzada la tipologia de dispositius admesos i no admesos per a connexió a la xarxa WiFi de la UAB.

Article 20. Homologació de dispositius connectats a la xarxa.

La connexió de dispositius a la xarxa fixa ha de ser homologada per la DTIC. De manera explícita, no es permet la connexió de dispositius d'infraestructura de xarxa com ara concentradors, commutadors, encaminadors o punts d'accés a la xarxa sense fils (Access Points) sense el coneixement i aprovació de la DTIC. Si es requereix la instal·lació d'algun d'aquests elements es posarà en contacte amb la DTIC per a la seva instal·lació dintre de la infraestructura de xarxa.

Article 21. Valoració de l'impacte a la xarxa i de la desconnexió dels dispositius.

1. Els dispositius que es prevegi que puguin fer un ús intensiu de forma continuada de la xarxa se sotmetran a una valoració per part de la DTIC prèvia a la seva connexió per evitar efectes sobre la resta d'usuaris.

2. Si, en qualsevol moment, es detecta que un equip es comporta de manera que incideix negativament en el rendiment d'altres dispositius de la xarxa, aquest es podrà desconnectar de la xarxa de forma puntual fins que es corregeixi el problema.

Article 22. Utilització d'impressores, escàners i fotocopiadores en xarxa.

1. No és permès deixar documentació desatesa a les safates de les impressores.

2. En el cas de fotocopiadores o escàners, una vegada finalitzat el procés de còpia o digitalització, s'haurà de retirar el material original de la safata d'entrada.

Article 23. Dispositius Internet de les coses - IoT.

1. Els objectes que incorporin mecanismes de comunicació digital Internet de les coses (IoT) usaran la xarxa que correspongui segons les seves característiques d'abast, energia o connectivitat.

2. Tot dispositiu IoT que es connecti a la xarxa de la UAB haurà de tenir una persona responsable.

3. Els dispositius IoT que es connectin a Internet i a la xarxa de la UAB hauran de tenir una configuració que permeti comprovar que estan certificats com a lliures de vulnerabilitats conegudes i que poden rebre actualitzacions de seguretat.

4. La persona responsable del dispositiu haurà de sol·licitar autorització per la DTIC abans de la seva connexió a la xarxa de la UAB.

5. Els dispositius hauran d'estar actualitzats pel que fa als pegats de seguretat

6. Els dispositius hauran d'utilitzar protocols estàndards i tecnologies no obsoletes per a les comunicacions, el xifrat i la interconnexió amb altres elements.

7. Els dispositius hauran d'estar configurats de manera segura. Les contrasenyes han de ser robustes i en cap cas la per defecte. Si l'objecte inclou configuració dinàmica, la persona administradora ha de comprovar la seguretat de la interfície, revisant els valors per defecte, els controls de bloqueig després de varis intents fallits d'accés, el xifrat de les connexions, la capacitat d'activació de registre d'esdeveniments de seguretat i activar, si és possible, l'autenticació mitjançant la verificació de dos o més factors.

8. Tots els processos gestionats mitjançant dispositius IoT hauran de tenir en compte la Normativa sobre de Protecció de Dades de caràcter personal i considerar-los en el moment de fer l'anàlisi de riscos i de gestionar-los.

Capítol IV. Ús del correu electrònic i altres eines de col·laboració.

Article 24. Responsabilitats d'ús del correu electrònic corporatiu.

1. La DTIC gestiona la infraestructura i el servei per al correu electrònic. Els servidors de correu dins la xarxa de la UAB estaran supervisats per la DTIC. La DTIC podrà desconnectar de la xarxa els servidors de correu desconeguts o amb configuracions que permetin pràctiques abusives per part de tercers.

2. Les persones usuàries són responsables de totes les activitats realitzades amb les bústies de correu electrònic que se li posin a disposició, essent responsabilitat de la persona usuària protegir-la d'accessos indeguts. Les persones usuàries vetllaran per mantenir la confidencialitat de les seves credencials d'accés, no usaran contrasenyes poc robustes, i no accediran a les bústies de correu des de dispositius d'ús públic i/o insegurs.

3. Si per a temes de caràcter aliè al treball o estudi a la Universitat s'ha de treballar amb adreces de proveïdors externs, no ha de suposar una interferència en el rendiment del servei, de les tasques pròpies dels gestors del servei, ni suposar cap cost per a la Universitat.

Article 25. Monitorització i auditoria del correu electrònic.

1. Podran ser rebutjats, bloquejats o enviats a la paperera aquells missatges rebuts o enviats on, de forma automatitzada, s'hi detectin problemes de seguretat o incompliments normatius.

S'informarà als usuaris d'aquestes mesures i de les conseqüències d'un potencial problema de seguretat derivat d'aquests missatges.

2. Els comptes de correu denunciats repetidament per ús abusiu podran ser bloquejats.

Article 26. Les llistes de difusió.

Les llistes de difusió autogestionades han de tenir sempre una persona responsable i alhora administradora. Aquesta persona assumeix la responsabilitat de gestionar la llista i de complir la legislació vigent i particularment la Normativa sobre ~~de~~ Protecció de Dades de caràcter personal. L'assumpció de responsabilitat és de caràcter personal i és vigent mentre la persona sigui administradora del recurs informàtic; en cas de renovació o canvi de la persona administradora de la llista, s'ha d'informar d'aquesta circumstància.

Capítol V. Seguretat per a treballar fora de les instal·lacions de la UAB.

Article 27. El treball fora de les instal·lacions de la UAB.

El treball fora de les instal·lacions de la UAB comprèn tant el teletreball habitual com el ocasional dels usuaris, així com les connexions remotes realitzades durant estades fora de la Universitat.

Article 28. Accés a les eines o aplicacions accessibles des de la xarxa interna de la UAB.

1. L'accés als elements del Sistema d'informació i a les eines i aplicacions de la UAB per les persones usuàries fora de les instal·lacions de la UAB tant sols han de ser utilitzats per a finalitats pròpies del seu vincle amb la Universitat.

2. La sortida fora de les dependències de la UAB de dispositius informàtics no portàtils ha de ser prèviament autoritzada.

3. La transmissió d'informació i l'accés remot s'ha de fer únicament a través dels canals establerts, tot seguint els protocols i els procediments definits, tenint cura, especialment:

a) De contemplar la gestió de contrasenyes segons el que es determina al capítol VI referent a la "Creació i utilització de les contrasenyes" de la present normativa.

b) De tancar la sessió sempre en acabar la feina en ordinadors i d'activació de pantalles de bloqueig en mòbils i tauletes tàctils.

c) De xifrar la informació sensible, confidencial o protegida que hagi de ser transmesa per correu electrònic o qualsevol altre canal que no permeti preservar la confidencialitat de les dades.

4. Els arxius que contenen documentació i els dispositius mòbils propietat de la UAB han d'estar vigilats i sota control per a evitar furts que comprometin la informació emmagatzemada. La informació en els dispositius mòbils ha d'estar xifrada.

5. Els navegadors utilitzats per a accés a Internet han d'estar actualitzats a la darrera versió i correctament configurats.

6. Una vegada acabada una sessió de treball en un equip compartit amb altres usuaris, és obligatòria la desconnexió d'aquesta sessió de manera que s'elimini la possibilitat de reutilització de la mateixa.

8. Com a norma general, es desactivaran les característiques de recordar contrasenyes en el navegador en sistemes compartits amb altres usuaris.

9. Com a norma general, s'activarà l'opció d'esborrat automàtic d'informació sensible al tancament del navegador, de tota informació sensible registrada al mateix: històric de navegació, descàrregues, formularis, caché, cookies, contrasenyes, sessions autenticades.

10. S'evitarà, en la mesura del possible, l'activació d'addons en el navegador de desenvolupadors externs a la UAB que no estiguin orientats a millorar la seguretat del sistema.

Capítol VI. Creació i utilització de les contrasenyes.

Article 29. Requeriment de contrasenyes robustes.

1. L'ús de contrasenyes ha de ser regulat quan aquest sigui el mecanisme d'autenticació per a l'accés als diferents recursos que configuren el Sistema d'informació de la UAB.

2. Les contrasenyes utilitzades per a l'accés als diferents recursos que configuren el Sistema d'informació de la UAB han de ser virtualment impossibles d'esbrinar i han de complir els següents criteris:

a) Han de tenir una longitud mínima de 8 caràcters;

b) No hauran d'estar compostes per dades que altra persona pugui esbrinar fàcilment (nom, cognoms, data de naixement, número de telèfon...), ni tampoc ser frases famoses;

c) No hauran de ser iguals a les darreres utilitzades, ni formades per modificacions d'elles;

3. Han de ser substituïdes si existeix evidència o sospita de que han estat compromeses. També quan hagi passat un temps prèviament estipulat d'antiguitat.

4. Només es podran emmagatzemar contrasenyes de forma segura, preferiblement mitjançant un gestors de claus o una caixa forta. En cap cas es podran apuntar en un paper a l'abast de tercers.

5. Les contrasenyes per als serveis de la UAB no han d'utilitzar-se per a altres serveis fora de la universitat.

6. En el cas d'emmagatzemament en gestors de contrasenyes, és convenient que aquests aportin informació sobre la fortalesa de les contrasenyes. Aquests gestors han de comparar la nova contrasenya amb llistes negres de contrasenyes inacceptables per ser àmpliament utilitzades: paraules de diccionaris, caràcters repetitius, seqüències, codi d'usuari/a, etc. DTIC proporcionarà una llista de gestors recomanats i principis bàsics d'ús.

Article 30. Limitació de número d'intents d'accessos.

Tot sistema de verificació de contrasenya dels diferents recursos que configuren el Sistema d'informació de la UAB ha de limitar el número d'intents d'accés sense èxit. Aquesta mesura es complementarà amb la limitació del número d'intents en un període donat.

Article 31. Doble factor d'autenticació.

Quant als mecanismes d'autenticació del personal propi o contractat o circumstancial, que pugui tenir accés a la informació continguda en el sistema, es podrà utilitzar els següents factors d'autenticació:

a) Contrasenya i un altre factor d'autenticació quan es realitza l'accés des de fora del campus.

b) Certificats digitals.

Capítol VII. Prestació de serveis per part de tercers.

Article 32. Intercanvi d'informació. Acords de confidencialitat i d'interconnexió

1. La DTIC ha d'efectuar anàlisis de riscos periòdics als diferents recursos que configuren el Sistema d'informació on s'hi recullin les amenaces detectades en els serveis prestats per tercers.

2. Els contractes administratius signats amb entitats que prestin serveis, quan la naturalesa d'aquests serveis requereixin tenir accés a dades de la UAB, han de complementar:

a) Un Acord de Confidencialitat que descrigui la naturalesa del servei que requereixi accés a les dades, i que requereixi que l'intercanvi d'informació es realitzi a través de canals adequats .

b) Un Acord d'Interconnexió quan la naturalesa del servei els doni accés als sistemes o infraestructura.

c) Un Acord de Nivell a revisar de manera periòdica.

Capítol VIII. Ús de les xarxes socials.

Article 33. Autorització, identificació i autenticació. Verificació dels comptes

1. La creació i utilització de perfils públics de la UAB a les xarxes socials s'ha d'ajustar a la Normativa de Protecció de Dades de caràcter particular a la legislació de protecció del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge, de Propietat Intel·lectual i sobre serveis de la Societat de la Informació i a l'ENS.

2. Els comptes en xarxes socials que representin a grups, centres, titulacions o serveis de la UAB s'han de crear des de comptes de correu no personals de la UAB, sempre que la xarxa social ho permeti, i han de tenir sempre una persona responsable que pertanyi a la UAB.

Article 34. Delegació de l'ús del compte corporatiu

Els comptes en xarxes socials podran ser delegats a persones del col·lectiu UAB que la persona responsable designi. Aquesta delegació també ha de ser informada a l'Àrea de Comunicació i de Promoció.

Article 35. Custòdia de les contrasenyes. Compliment de la normativa de creació i d'utilització de contrasenyes a la UAB

La custòdia de les contrasenyes dels perfils del les xarxes socials és responsabilitat de la persona responsable o en qui hagi delegat el seu ús, i s'ha de seguir la present normativa respecte a la gestió de les mateixes.

Capítol IX. Protecció dels Sistemes d'Informació i dels Recursos Informàtics.

Article 36. Incidents de seguretat

1. Qualsevol anomalia o incident de seguretat que pugui comprometre el bon ús i funcionament dels Sistemes d'Informació de la UAB ha de ser comunicada pel seu registre al CAS.

2. Els incidents que afectin a protecció de dades seguiran el canal de comunicació descrit en la Normativa de Protecció de Dades de caràcter particular.

Article 37. Supòsits d'incompliment de la normativa.

1. Es considera incompliment de les condicions d'ús dels Recursos Informàtics els supòsits següents:

a) L'ús il·lícit no denunciat per part de terceres persones dels comptes d'usuari en els diferents recursos que configuren el Sistema d'informació, tant pel que fa a qui porta a terme l'accés indegut com pel que fa a la persona responsable del compte.

b) Facilitar i/o oferir a tercer l'ús del compte i bústia personal.

c) La desprotecció de la informació de manera que faciliti un accés indegut.

d) L'ús dels serveis de xarxa i dels mitjans electrònics per comunicar-se de forma indeguda amb altres persones. A aquests efectes s'entén per comunicació indeguda: l'enviament de missatges amb ànim d'ofendre, l'assetjament electrònic, la suplantació d'adreces de xarxa, i la suplantació d'identitat.

e) L'accés al mitjà físic o als paquets de comunicació per esbrinar informació de la qual no s'és propietari, excepte en els casos que s'hagi permès aquest accés per tasques docents o de recerca en situacions controlades.

f) De forma intencionada, la utilització intencionada de programari que faci un ús abusiu de la xarxa o dels recursos compartits.

g) La instal·lació o utilització de programari que vulneri la legislació vigent.

h) La instal·lació o utilització de programari en dispositius corporatius sense complir les condicions d'utilització d'aquest programari.

i) La cerca de contrasenyes d'altres persones usuàries o qualsevol intent de trobar ~~de trobar~~ forats en la seguretat del~~s~~ Sistema d'informació de la Universitat o de fora, o fer ús dels sistemes o recursos per atacar qualsevol sistema informàtic, excepte en els casos de tasques de comprovacions de seguretat i en situacions docents o de recerca controlades.

j) La creació, l'ús o l'emmagatzematge de programes o d'informació que puguin ser utilitzats per atacar el Sistema informàtic de la Universitat o de fora, excepte en els casos de tasques de comprovacions de seguretat i en situacions docents o de recerca controlades.

k) 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.

l) L'alteració intencionada o negligent de la integritat de les dades.

m) La desinstal·lació o desactivació no autoritzada del programari de protecció contra amenaces corporatiu o qualsevol altra peça de programari que la DTIC hagi incorporat als ordinadors personals per a la seva gestió i protecció.

n) L'ús abusiu de l'accés a Internet. Se'n considera ús abusiu:

   I. L'accés a altres xarxes amb el propòsit de violar-ne la seva integritat o seguretat, excepte en els casos de tasques de comprovacions de seguretat i en situacions docents o de recerca controlades.

   II. L'accés per a promoció d'interessos personals no relacionats amb les activitats acadèmiques.

   III. La publicació o enviament d'informació no sol·licitada amb fins comercials.

   IV. La publicació o enviament d'informació sensible, confidencial o protegida a persones no autoritzades o a sistemes d'informació externs no autoritzats.

o) L'ús abusiu del correu electrònic i dels serveis al núvol. Se'n considera ús abusiu, entre d'altres:

   I. La utilització del correu electrònic per a finalitats diferents a les derivades de les activitats pròpies de la UAB i, de manera especial:

      1. La promoció d'interessos personals.

      2. L'enviament de missatges no sol·licitats de forma massiva i amb interès comercial.

3. L'enviament de missatges que continguin amenaces i ofenses a la dignitat de les persones o que, per la seva naturalesa, constitueixin complicitat amb delictes.

4. La revelació de dades confidencials o de secrets empresarials propietat de la UAB.

ii. La difusió de correus electrònics mitjançant canals no autoritzats, és a dir, l'ús no autoritzat d'un servidor de correu aliè a la UAB per a reenviar correu amb un usuari UAB.

iii. Atacs amb l'objecte d'impossibilitar o dificultar el servei, tant dirigits a un usuari com al propi sistema de correu.

iv. Subscripció indiscriminada a llistes de correu a fonts externes a la UAB sense el consentiment dels usuaris.

v. La falsificació de les capçaleres de correu electrònic.

vi. La utilització d'encaminadors de correu que no siguin els que posa a disposició la Universitat.

vii. L'enviament de missatges professionals en representació de la UAB utilitzant adreces externes als dominis de la UAB.

viii. L'accés als serveis i/o continguts de la UAB amb el propòsit de violar la seva integritat o seguretat.

ix. La publicació d'informació confidencial propietat de la UAB a persones o sistemes d'informació no autoritzats.

x. Establir o habilitar accessos compartits a una bústia de correu sense el coneixement i aprovació de la DTIC.

xi. Facilitar i/o oferir a tercers l'ús del compte i bústia personals.

2. L'incompliment de les condicions d'ús dels Recursos Informàtics identificats a l'apartat 1r del present article, suposa un notori incompliment de les funcions essencials del lloc de treball o funcions encomanades o, en el seu cas, una deslleialtat o una transgressió de la bona fe contractual, les quals seran qualificades com a faltes molt greus, greus o lleus, d'acord amb les circumstàncies en base a les quals es portin a terme, la legislació de règim disciplinari aplicable.

Article 38. Mesures aplicables en cas d'incompliment de la normativa.

1. L'incompliment de les condicions d'ús dels Recursos Informàtics és causa per iniciar expedient que tingui per objecte determinar la imposició d'una mesura temporal consistent en la restricció del dret d'ús dels diferents recursos que configuren el Sistema d'informació i dels Recursos Informàtics de la Universitat i/o la desconnexió dels sistemes o xarxes de la xarxa general de la Universitat.

2. El procediment serà instruït pel director o directora de la DTIC o persona en qui delegui, es donarà audiència a la persona interessada i serà resolt pel Comitè de Seguretat de la Informació.

3. Contra les resolucions del Comitè de Seguretat de la Informació, les persones interessades podran interposar recurs d'alçada davant el rector o la rectora o la persona en qui delegui.

4. Les mesures esmentades en aquesta normativa 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. La Universitat iniciarà les accions legals que estimi oportunes quan es vegin vulnerats els seus drets a conseqüència de la utilització inadequada dels seus Recursos Informàtics, i posarà a disposició de les autoritats competents tota la informació disponible en cas de denúncies per mala utilització i vulneració de drets de tercers.

Disposició derogatòria. Normativa que es deroga.

Queden derogades totes les normes d'igual rang, aprovades per la Universitat Autònoma de Barcelona que s'oposin a la present Normativa i, de forma expressa, el 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, Acord del Consell de Govern de 13 de juliol de 2011 i modificat per Acord de Consell de Govern de 25 d'abril de 2012.

Disposició final. Entrada en vigor.

Aquesta Normativa entrarà en vigor l'endemà de la seva aprovació pel Consell de Govern.