# 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 tecnologies de la informació i la comunicació (TIC) per aconseguir els seus objectius. Aquests sistemes han de ser administrats amb diligència i prenent les mesures adequades per protegir-los de danys accidentals o deliberats que puguin afectar la seguretat de la informació tractada o els serveis prestats, i han d'estar sempre protegits contra les amenaces o incidents que poden 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 de les condicions de l'entorn per 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 fer un seguiment continu dels nivells de prestació dels serveis, monitorar i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als ciberincidents per garantir la continuïtat dels serveis prestats. La seguretat de les TIC és una part integral de cada etapa del cicle de vida del sistema, des de la concepció fins a la 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 s'han d'identificar i incloure 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 establia la necessitat de desenvolupar posteriorment un segon nivell normatiu sobre seguretat.

### II

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

El capítol I, dedicat a disposicions generals, s'organitza en dues seccions. La secció 1a delimita l'objecte de la normativa i l'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 persona responsable, persona administradora i persona usuària d'aquests recursos informàtics. S'hi estableix que tot dispositiu informàtic que la Universitat posa a disposició dels membres de la seva comunitat s'ha de destinar 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 gestionar-la correspon a la Vicegerència d'Estratègia Digital i Sistemes d'Informació (VEDSI).Regula la manera 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 de dispositius que incorporin mecanismes de comunicació digital (internet de les coses, IoT).

El capítol IV determina l'obligació de la Universitat de posar a disposició dels membres de la comunitat bústies de correu electrònic, i estableix que la gestió de la infraestructura i el servei per al correu electrònic correspon a la Vicegerència d'Estratègia Digital i Sistemes d'Informació.

D'altra banda, disposa que és responsabilitat exclusiva dels usuaris l'ús que es faci dels comptes de correu que se'ls assignin, i 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, i n'estableix el règim d'ús. Incideix que aquesta infraestructura tecnològica que la Universitat posa a disposició dels membres de la comunitat s'ha d'utilitzar exclusivament per a les finalitats pròpies del vincle amb la Universitat, fins i tot 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 dels proveïdors de serveis de formalitzar acords de confidencialitat i acords d'interconnexió quan, per l'objecte del contracte administratiu, hagin de tenir accés a dades de la Universitat o tinguin accés als sistemes o infraestructura de la Universitat. Així mateix, estableix l'obligació de formalitzar un acord de nivell de servei.

El capítol VIII tracta de 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'hi identifiquen els casos d'incompliment de la normativa, els quals es qualifiquen com un incompliment notori de les funcions essencials del lloc de treball o funcions encomanades i, en alguns casos, una deslleialtat o una transgressió de la bona fe contractual, a l'efecte de determinar la responsabilitat disciplinària dels usuaris. Finalment, s'hi 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 d'aquesta normativa s'ha respectat el 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

Aquesta 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

Aquesta normativa s'aplica a totes les persones que facin ús dels sistemes d'informació i recursos informàtics de la UAB i a 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 o emmagatzemament d'informació. S'hi inclouen diferents categories, com ara maquinari (dispositius), programari, xarxes o serveis al núvol.

— *Dispositiu corporatiu*: mecanisme o artifici de propietat de la UAB destinat a produir una acció electrònica prevista. Pot ser gestionat o no gestionat. En els dispositius gestionats, la Vicegerència d'Estratègia Digital i Sistemes d'Informació hi aplica la configuració i les mesures de seguretat. La resta són dispositius no gestionats.

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

— *Sistema de tecnologies de la informació i la comunicació*: conjunt d'equipaments, mètodes, procediments i personal organitzat amb eines, mètodes i sistemes digitals de manera 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 la ciutadania i les administracions públiques, com ara la gestió de tràmits electrònics. Alguns exemples són els serveis electrònics del sector públic, els serveis d'infraestructura tecnològica, els serveis d'autenticació i autorització i els serveis de protecció de la informació.

— *Persona usuària d'un recurs informàtic*: Adjudicatari/a d'ús d'un compte d'usuari personal. Als sistemes d'informació de la UAB i als seus serveis associats, cada persona usuària està representada per un compte d'usuari personal. Els comptes d'usuari 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 per donar suport als 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 ofert per la UAB que permet donar d'alta els 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'autenticació que també formen part del sistema de gestió de la identitat.

— *Connexió permanent d'un dispositiu a la xarxa*: situació que es produeix automàticament quan un ordinador o un dispositiu de IoT es connecta a la xarxa de la UAB, de manera contínua, durant més d'un mes.

**Secció 2a. Règim d'ús dels sistemes d'informació i dels recursos informàtics**

**Article 3. Assignació dels recursos informàtics dels sistemes d'informació**

1. Per aconseguir 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. Qualsevol persona amb accés als sistemes d'informació ha de ser identificada de manera inequívoca.

5. Les persones que utilitzin els sistemes d'informació han de ser prèviament autoritzades a fer-ho. Els accessos a serveis diferents dels definits per als col·lectius als quals pertany una persona s'han de sol·licitar i han de ser autoritzats expressament. El cessament de la vinculació de les persones amb la Universitat comporta, en general, la pèrdua del dret d'accés als seus sistemes d'informació.

6. L'accés a sistemes d'informació associats al desenvolupament d'un càrrec o funció està limitat a la durada d'aquest 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, i només 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, del 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 determinades per la seva vinculació amb la UAB.

**Article 5. Persona responsable dels recursos informàtics**

1. La persona responsable dels recursos informàtics és aquella que té el deure de vetllar pel bon funcionament dels recursos informàtics assignats sota la seva tutela. Compta amb el suport del personal de la Vicegerència d'Estratègia Digital i Sistemes d'Informació.

Aquests efecte són persones responsables dels recursos informàtics:

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

*b)* Les persones administradores de centre, que són responsables dels recursos informàtics destinats a la gestió del centre.

*c)* Els directors i directores de departament, que 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 vicegerent d'Estratègia Digital i Sistemes d'Informació, que és responsable dels recursos informàtics centrals, dels ordinadors personals corporatius gestionats, dels dispositius mòbils gestionats i de la xarxa de comunicacions.

*e)* La persona administradora de cada sistema personal no gestionat.

*f)* Les persones que contracten el servei d'allotjament procurat per la Vicegerència d'Estratègia Digital i Sistemes d'Informació, que són responsables dels servidors que hi tenen allotjats.

*g)* Les persones que contracten serveis de TIC al núvol amb càrrec a la UAB, que són responsables del que s'hi desplega.

2. La persona responsable dels recursos informàtics pot delegar funcions, però no la responsabilitat, quan cregui que és necessari 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 diversos recursos informàtics i treballa coordinadament amb la persona responsable dels recursos informàtics i els serveis, a la qual ha de comunicar 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 Vicegerència d'Estratègia Digital i Sistemes d'Informació en totes les qüestions vinculades a la prestació del servei, però sobretot en qüestions tècniques i de seguretat, i col·laborar 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. A l'efecte de la gestió dels riscos de seguretat informàtica, les persones administradores de recursos informàtics que puguin presentar riscos no habituals han de declarar de manera responsable el perfil de risc dels equips que administren, d'acord amb el procediment que s'estableixi. A aquests efectes, s'entenen com riscos no habituals els següents:

*a)* La instal·lació o ús d'eines que puguin alterar la configuració dels equips i afectar-ne la seguretat informàtica.

*b)* La instal·lació o ús d'eines específiques de l'àmbit de la ciberseguretat.

*c)* La instal·lació o ús de programari obsolet pel que fa a la seguretat informàtica.

No cal declarar els equips sense connexió a la xarxa de la UAB.

Quan sigui necessari instal·lar i connectar permanentment a la xarxa dispositius no gestionats per la Vicegerència d'Estratègia Digital i Sistemes d'Informació, la persona administradora del recurs ha de sol·licitar-ne l'autorització.

Quan sigui necessari que un dispositiu no gestionat s'integri permanentment 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 i han de seguir les recomanacions d'utilització dels recursos informàtics donades per les persones responsables i administradores d'aquests recursos, especialment en qüestions tècniques, de protecció de dades, de continguts protegits pels drets d'autoria i en qüestions de seguretat, i sempre han d'aplicar la legislació.

Les persones usuàries han de comunicar a la persona administradora del recurs informàtic que tinguin assignat qualsevol canvi en la titularitat d'aquest. Mentre la persona usuària no l'hagi comunicat, continua sent responsable de la custòdia del recurs 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, cal contactar prèviament amb la persona usuària per comunicar-li l'acció pertinent i solucionar els problemes, excepte en els casos en què estigui compromesa la seguretat de la xarxa o de segments de la xarxa i la desconnexió sigui imperativa.

3. Les persones usuàries han de tenir el màxim de cura en la manipulació i ús dels dispositius informàtics, i de tota la infraestructura complementària. Han d'evitar 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 tenen la responsabilitat de mantenir-los actualitzats amb els pedaços de seguretat, tant del sistema operatiu com dels programaris que hi estiguin instal·lats. En cas dels sistemes difícils d'actualitzar relacionats amb equipament científic, cal 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 el sistema operatiu, els antivirus i els tallafocs actualitzats és de la Vicegerència d'Estratègia Digital i Sistemes d'Informació. En cas que les persones usuàries hi instal·lin programari addicional, s'han de responsabilitzar de mantenir-lo actualitzat.

5. Les persones usuàries han de fer un ús responsable dels recursos per reduir el risc de propagar programari maliciós a través de memòries USB, unitats compartides de xarxa, missatges de correu electrònic o programari descarregat d'internet. La Universitat ha de posar a l'abast de les persones usuàries els cursos i documentació necessaris per utilitzar correctament els recursos, i ha de donar els consells oportuns per augmentar la conscienciació i reduir els riscos.

6. Les persones usuàries han d'accedir 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 cura de la seva contrasenya i de qualsevol mètode d'autenticació actiu, que ha de mantenir en secret.

Tots els canvis de contrasenya de comptes dels sistemes d'informació s'han de dur a terme fent ús dels mecanismes i protocols definits en cada moment pels responsables dels sistemes.

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

1. La informació emmagatzemada localment en els dispositius no gestionats no és objecte de salvaguarda en els procediments corporatius de còpia de seguretat. És responsabilitat de la persona usuària fer-ne periòdicament còpies de seguretat.

2. Els sistemes d'informació gestionats per la Vicegerència d'Estratègia Digital i Sistemes d'Informació han de fer còpies de seguretat segons les polítiques i seguint els procediments determinats en el moment de la categorització del sistema.

3. Les còpies de seguretat que ja no siguin necessàries i els mitjans d'emmagatzemament que, per obsolescència o degradació, perdin la utilitat, i molt especialment els que continguin informació sensible, confidencial o protegida, s'han d'eliminar de manera segura. La persona

usuària (o la persona administradora del sistema amb els seus usuaris) ha de validar l'eliminació del contingut i 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 fix, portàtil o mòbil, ha d'estar inventariat i està 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 els danys o la sostracció de l'equipament, així com l'accés de persones no autoritzades, mitjançant les mesures de seguretat aplicables als centres, concretament a les aules de laboratori i espais de recerca, com ara clau o control d'accés i sistemes d'ancoratge d'equipament. En cas de sostracció o pèrdua d'un d'aquests dispositius, la persona usuària ho ha de comunicar perquè es puguin adoptar les mesures que corresponguin i a l'efecte de donar-lo de baixa de l'inventari.

2. Les persones usuàries han d'evitar, sempre que sigui 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 d'una persona usuària i això en provoqui la desvinculació de la Universitat, la persona usuària ha d'entregar el dispositiu a la UAB per tal que, si escau, se'n pugui esborrar de manera segura la informació emmagatzemada.

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

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

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

2. El programari informàtic que és propietat de la UAB o per al qual la UAB té la llicència està protegit per la legislació sobre propietat intel·lectual i, per tant, és obligatori complir els termes de la llicència.

3. S'ha d'aplicar la legislació vigent en termes de propietat intel·lectual prohibint-ne els usos no autoritzats i regulant la utilització, reproducció, distribució, transformació i comunicació pública de qualsevol obra protegida per drets de propietat intel·lectual, en els sistemes d'informació de la UAB.

4. Està prohibit, en els sistemes d'informació de la UAB, transmetre, distribuir o emmagatzemar 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 categoritzats del sistema d'informació han de tenir una persona que les administri d'acord amb els criteris i instruccions de la persona responsable. Aquesta persona és l'encarregada d'atorgar, modificar i anul·lar l'autorització d'accés de les persones usuàries a aquestes dades.

2. L'alta d'usuaris ha de ser gestionada pel sistema de gestió de la identitat, a través dels procediments establerts.

3. Una persona usuària que accedeixi als recursos corporatius no oberts al públic del sistema d'informació necessita un compte d'usuari i una autorització adequada per a 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 al col·lectiu corresponent han d'estar 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 han de conèixer aquesta normativa de seguretat i la normativa sobre protecció de dades de la UAB, les quals estan a disposició a través del portal de la UAB.

**Article 12. Identificació i autenticació**

1. Les persones usuàries disposen de codi d'usuari i contrasenya, o de mecanismes alternatius en funció de l'evolució tecnològica (targeta criptogràfica, certificat digital, etc.), per accedir als sistemes d'informació.

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

Les persones usuàries no han de tenir les seves contrasenyes per escrit, a la vista i accessibles a tercers. Si la persona usuària sospita que una altra persona està utilitzant les seves credencials, ha de canviar de contrasenya i comunicar la sospita a la Vicegerència d'Estratègia Digital i Sistemes d'Informació.

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

**Article 13. Monitoratge i auditoria de la utilització dels sistemes d'informació i els recursos informàtics**

1. En aplicació dels objectius definits a la Política de seguretat de la informació de la Universitat Autònoma de Barcelona, la UAB pot 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) del sistema d'informació i dels recursos informàtics és l'adequat en els termes legals, especialment pel que fa a la jurisprudència relacionada amb els drets a la intimitat i a la dignitat del personal.

2. La UAB, mitjançant el Comitè de Seguretat de la Informació, ha d'adoptar mesures de monitoratge i auditoria per detectar comportaments maliciosos i, en cas de detectar-ne, pot activar mesures preventives per mitigar-ne l'afectació.

Es poden 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 revisa periòdicament l'estat de l'equipament, el programari instal·lat, els dispositius i les xarxes de comunicacions.

*b)* Es monitoren els accessos a la informació continguda al sistema d'informació.

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

2. L'activitat de monitoratge s'ha de dur a terme de manera proporcional al risc, seguint els judicis d'idoneïtat, necessitat i proporcionalitat, respectant els requeriments legals i les cauteles indicades per la jurisprudència, i observant els drets de les persones usuàries.

3. La UAB té habilitat, en el seu 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 han de disposar d'accés a internet com a eina per desenvolupar la seva activitat.

2. La UAB ha de garantir l'ús adequat dels recursos informàtics d'accés a internet per:

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

*b)* Volum de trànsit extern de dades: per tal d'assegurar que l'accés a continguts necessaris per a l'activitat professional i acadèmica no es vegi perjudicat pel trànsit de continguts no vinculats a aquesta activitat.

### Article 15. Política de tallafocs

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

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

Tots els serveis oferts per la UAB als quals s'accedeixi a través d'internet estan tancats a les persones externes, excepte els serveis per als quals s'hagi declarat explícitament que hi estan oberts.

Tots els serveis externs als sistemes locals als quals s'accedeix des de la UAB, com ara els localitzats als proveïdors al núvol, han de ser 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 tres mesos consecutius poden 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 poder accedir a alguns recursos restringits a serveis des de fora de la Universitat. Per defecte, els accessos que es puguin fer a través de la XPV no s'obriran en el tallafoc perimetral.

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

3. Per 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 XPV s'ha de sol·licitar i justificar.

## 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 tasques de recerca, docència, transferència i intercanvi del coneixement i gestió de la institució i d'institucions amb conveni. La gestió i el manteniment de la xarxa i l'aplicació de les instruccions derivades de les normatives aprovades són responsabilitat de la Vicegerència d'Estratègia Digital i Sistemes d'Informació.

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

1. L'equipament que s'ha de connectar a la xarxa inclou els dispositius personals, els portàtils, les impressores, els servidors i en general qualsevol dispositiu connectable a la xarxa amb cable (xarxa fixa) o amb capacitat de wifi diferent dels que configuren la infraestructura central de xarxa.

2. Tot equip connectat permanentment a la xarxa fixa de la UAB ha d'estar registrat i identificat i ha de tenir assignades una persona responsable, una persona administradora i una persona usuària. La gestió d'aquesta identificació i l'assignació de noms i adreces es fa des de la Vicegerència d'Estratègia Digital i Sistemes d'Informació.

3. Per defecte, l'equip que es connecta a la 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 ho compleix, se'n pot denegar l'accés a la xarxa o l'accés a internet. Si a través d'un dispositiu es fa un mal ús de la xarxa o s'incompleixen les normatives de seguretat, també es pot bloquejar l'accés des d'aquest dispositiu.

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

6. Tots els equips amb sistema operatiu Windows connectats a la xarxa de la UAB han de tenir instal·lat, al dia i en funcionament el sistema de protecció contra programari maliciós (com antivirus i d'altres). S'han d'establir protocols de protecció especials per a aquells sistemes difícils d'actualitzar o substituir.

7. Tots els equips connectats a la xarxa de la UAB han de tenir funcionant el sistema automàtic d'actualitzacions del sistema operatiu. S'han d'establir protocols de protecció especials per a aquells sistemes difícils d'actualitzar o substituir.

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

9. La Vicegerència d'Estratègia Digital i Sistemes d'Informació ha de mantenir actualitzada la tipologia de dispositius admesos i no admesos per a la 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 l'ha d'homologar la Vicegerència d'Estratègia Digital i Sistemes d'Informació. De manera explícita, no es permet connectar 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 l'aprovació de la Vicegerència d'Estratègia Digital i Sistemes d'Informació. Si es requereix instal·lar algun d'aquests elements, cal posar-se en contacte amb la Vicegerència d'Estratègia Digital i Sistemes d'Informació per fer-ho dins la infraestructura de xarxa.

**Article 21. Valoració de l'impacte dels dispositius sobre la xarxa i de la necessitat de desconnectar-los**

1. Si es preveu que un dispositiu farà un ús intensiu i continuat de la xarxa, la Vicegerència d'Estratègia Digital i Sistemes d'Informació n'ha de fer una valoració de l'impacte abans de connectar-lo a la xarxa, per tal d'evitar efectes sobre la resta d'usuaris.

2. Si, en qualsevol moment, es detecta que l'ús que es fa d'un equip incideix negativament en el rendiment d'altres dispositius de la xarxa, aquest es pot desconnectar de la xarxa puntualment fins que es corregeixi el problema.

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

1. No es permet 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'ha de retirar el material original de la safata d'entrada.

**Article 23. Dispositius d'internet de les coses (IoT)**

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

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

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

4. La persona responsable del dispositiu ha de sol·licitar i rebre l'autorització de la Vicegerència d'Estratègia Digital i Sistemes d'Informació abans de la connectar-lo a la xarxa de la UAB.

5. Els dispositius han d'estar actualitzats pel que fa als pedaços de seguretat.

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

7. Els dispositius han d'estar configurats de manera segura. Les contrasenyes han de ser robustes, i en cap cas les que es creen per defecte. Si l'objecte inclou una configuració dinàmica, la persona administradora ha de comprovar la seguretat de la interfície, revisant els valors per defecte, els controls de bloqueig després de diversos intents fallits d'accés, el xifratge de les connexions i 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 de IoT han de tenir en compte la normativa sobre 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 d'altres eines de col·laboració

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

1. La Vicegerència d'Estratègia Digital i Sistemes d'Informació gestiona la infraestructura i el servei per al correu electrònic, i supervisa els servidors de correu dins la xarxa de la UAB. La Vicegerència pot desconnectar de la xarxa els servidors de correu desconeguts o amb configuracions que permetin pràctiques abusives de tercers.

2. Les persones usuàries són responsables de totes les activitats dutes a terme amb les bústies de correu electrònic que se'ls posin a disposició, i és responsabilitat seva protegir-les d'accessos indeguts. Les persones usuàries han de vetllar per mantenir la confidencialitat de les seves credencials d'accés, no usar contrasenyes poc robustes i no accedir a les bústies de correu des de dispositius d'ús públic o insegurs.

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

### Article 25. Monitoratge i auditoria del correu electrònic

1. Es poden rebutjar, bloquejar o enviar a la paperera els missatges rebuts o enviats en què, de manera automatitzada, es detectin problemes de seguretat o incompliments normatius. S'ha d'informar els 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 un ús abusiu poden 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, particularment la normativa sobre 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 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 l'ocasional, així com les connexions remotes durant les estades fora de la Universitat.

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

1. Les persones usuàries poden accedir als elements del sistema d'informació i a les eines i aplicacions de la UAB des de fora de les instal·lacions de la Universitat tan sols per a les finalitats pròpies del seu vincle amb la institució.

2. Per poder treure fora de les dependències de la UAB dispositius informàtics no portàtils cal tenir-ne l'autorització.

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

*a)* Preveure la gestió de contrasenyes segons el que es determina al capítol VI d'aquesta normativa, referent a la creació i utilització de contrasenyes.

*b)* En acabar la feina, tancar la sessió en els ordinadors i activar la pantalla de bloqueig en els mòbils i tauletes tàctils.

*c)* Xifrar la informació sensible, confidencial o protegida que s'hagi de transmetre 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 evitar furts que comprometin la informació emmagatzemada. La informació en els dispositius mòbils ha d'estar xifrada.

5. Els navegadors utilitzats per accedir a internet han d'estar actualitzats amb la darrera versió i correctament configurats.

6. Quan s'acabi la sessió de treball en un equip compartit amb altres usuaris, és obligatori tancar-la per evitar que algú altre la utilitzi.

7. Com a norma general, s'han de desactivar les opcions de recordar contrasenyes en el navegador en sistemes compartits amb altres usuaris.

8. Com a norma general, s'ha d'activar l'opció d'esborrament automàtic d'informació sensible en tancar el navegador per a qualsevol informació sensible que s'hi hagi registrat: historial de navegació, descàrregues, formularis, memòria cau, galetes, contrasenyes, sessions autenticades.

9. Cal evitar, sempre que sigui possible, activar complements per al navegador que provinguin de desenvolupadors externs a la UAB que no estiguin orientats a millorar la seguretat del sistema.

## Capítol VI. Creació i utilització de contrasenyes

### Article 29. Requeriment de contrasenyes robustes.

1. L'ús de contrasenyes s'ha de regular quan 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 accedir als diferents recursos que configuren el sistema d'informació de la UAB han de ser virtualment impossibles d'esbrinar i han de complir els criteris següents:

*a)* Han de tenir una longitud mínima de 8 caràcters.

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

*c)* No poden ser iguals que les darreres contrasenyes utilitzades, ni es poden formar a partir de modificacions d'aquestes.

3. S'han de substituir si hi ha evidències o se sospita que han estat compromeses, i també quan hagi passat un temps prèviament estipulat.

4. Només es poden emmagatzemar contrasenyes de manera segura, preferiblement mitjançant un gestor de contrasenyes o una caixa forta. En cap cas es poden apuntar en un paper a l'abast de tercers.

5. Les contrasenyes per als serveis de la UAB no s'han d'utilitzar 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 seguretat de les contrasenyes. Aquests gestors han de comparar la nova contrasenya amb llistes negres de contrasenyes inacceptables pel fet de ser àmpliament utilitzades: paraules de diccionaris, caràcters repetitius, seqüències, codi d'usuari, etc. La Vicegerència d'Estratègia Digital i Sistemes d'Informació ha de proporcionar una llista de gestors recomanats i principis bàsics d'ús.

**Article 30. Limitació del nombre d'intents d'accés**

Qualsevol sistema de verificació de contrasenya dels diferents recursos que configuren el sistema d'informació de la UAB ha de limitar el nombre d'intents d'accés sense èxit. Aquesta mesura s'ha de complementar amb la limitació del nombre d'intents en un període donat.

**Article 31. Autenticació de doble factor**

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

*a)* Contrasenya i un altre factor d'autenticació, quan es fa 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 Vicegerència d'Estratègia Digital i Sistemes d'Informació ha de dur a terme anàlisis de riscos periòdiques dels diferents recursos que configuren el sistema d'informació, en les quals s'han de recollir 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 requereixi tenir accés a dades de la UAB, s'han de complementar amb:

*a)* Un acord de confidencialitat que descrigui la naturalesa del servei que requereix accés a les dades, i que estableixi que l'intercanvi d'informació s'ha de fer a través de canals adequats.

*b)* Un acord d'interconnexió, quan per la naturalesa del servei aquestes entitats tinguin accés als sistemes o infraestructura de la UAB.

*c)* Un acord de nivell de servei, que cal revisar periòdicament.

## 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 sobre protecció de dades de caràcter personal, a la legislació sobre protecció del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge, sobre propietat intel·lectual i sobre serveis de la societat de la informació, i a l'Esquema Nacional de Seguretat.

2. Els comptes en xarxes socials que representin 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 una persona responsable que pertanyi a la UAB.

### Article 34. Delegació de l'ús del compte corporatiu

Els comptes en xarxes socials es poden delegar a persones del col·lectiu de la UAB que la persona responsable designi. S'ha d'informar d'aquesta delegació l'Àrea de Comunicació i 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 de les xarxes socials és responsabilitat de la persona responsable o de la persona a qui n'hagi delegat l'ús, i s'ha de seguir aquesta normativa per gestionar-les.

## 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 s'ha de comunicar per tal de fer-ne el registre al CAS.

2. Els incidents que afectin la protecció de dades han de seguir el canal de comunicació descrit a la normativa sobre protecció de dades de caràcter personal.

### Article 37. Supòsits d'incompliment de la normativa

1. Es considera que s'incompleixen les condicions d'ús dels recursos informàtics en els casos següents:

*a)* 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 per part de qui porta a terme un accés indegut com per part de la persona responsable del compte.

*b)* Facilitació o oferiment a altres persones de l'ús del compte i la bústia personal.

*c)* Desprotecció de la informació de manera que faciliti un accés indegut.

*d)* Ús dels serveis de xarxa i dels mitjans electrònics per comunicar-se de manera indeguda amb altres persones. A aquest efecte, 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)* Accés al mitjà físic o als paquets de comunicació per esbrinar informació de la qual no s'és propietari, excepte en els casos en què s'hagi permès aquest accés per tasques docents o de recerca en situacions controlades.

*f)* Utilització intencionada de programari que faci un ús abusiu de la xarxa o dels recursos compartits.

*g)* Instal·lació o utilització de programari que vulneri la legislació vigent.

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

*i)* Cerca de contrasenyes d'altres persones usuàries o qualsevol intent de trobar forats en la seguretat de sistemes d'informació de la Universitat o de fora, o de fer ús dels sistemes o recursos per atacar qualsevol sistema informàtic, excepte en tasques de comprovació de seguretat i en situacions docents o de recerca controlades.

*j)* Creació, ús o emmagatzematge de programes o d'informació que es puguin utilitzar per atacar els sistemes d'informació de la Universitat o de fora, excepte en tasques de comprovació de seguretat i en situacions docents o de recerca controlades.

*k)* Destrossa, sostracció o trasllat no degudament autoritzat a altres dependències, de qualsevol element físic de la instal·lació informàtica o d'infraestructura complementària.

*l)* Alteració intencionada o negligent de la integritat de les dades.

*m)* Desinstal·lació o desactivació no autoritzada del programari corporatiu de protecció contra amenaces o de qualsevol altra peça de programari que la Vicegerència d'Estratègia Digital i Sistemes d'Informació hagi incorporat als ordinadors personals per gestionar-los i protegir-los.

*n)* Ús abusiu de l'accés a internet. Es considera ús abusiu:

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

II. L'accés per a la 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)* Ús abusiu del correu electrònic i dels serveis al núvol. Es considera ús abusiu, entre d'altres:

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

1. La promoció d'interessos personals.

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

3. L'enviament de missatges que continguin amenaces i ofenses a la dignitat de les persones o que, per 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 reenviar correus amb un usuari de la UAB.

III. Els atacs amb l'objecte d'impossibilitar o dificultar el servei, tant els dirigits a un usuari com al sistema de correu mateix.

IV. La subscripció indiscriminada a llistes de correu de 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 o continguts de la UAB amb el propòsit de violar-ne la integritat o seguretat.

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

X. L'establiment o habilitació d'accessos compartits a una bústia de correu sense el coneixement i l'aprovació de la Vicegerència d'Estratègia Digital i Sistemes d'Informació.

XI. La facilitació o oferiment a tercers de l'ús del compte i la bústia personals.

2. Els casos d'incompliment de les condicions d'ús dels recursos informàtics identificats a l'apartat 1 d'aquest article suposen un incompliment notori de les funcions essencials del lloc de treball o funcions encomanades i, en alguns casos, una deslleialtat o una transgressió de la bona fe contractual. Es consideraran faltes molt greus, greus o lleus segons les circumstàncies en què es portin a terme i 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 un 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, o la desconnexió dels sistemes o xarxes de la xarxa general de la Universitat.

2. El procediment l'ha d'instruir el vicegerent o vicegerenta d'Estratègia Digital i Sistemes d'Informació, o la persona que delegui, ha d'incloure una audiència amb la persona interessada i l'ha de resoldre el Comitè de Seguretat de la Informació.

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

4. Les mesures esmentades en aquesta normativa s'apliquen sens perjudici de les accions disciplinàries, civils o penals que escaigui aplicar a les persones presumptament implicades, i de la reparació dels danys ocasionats. La Universitat pot iniciar les accions legals que estimi oportunes quan es vulnerin els seus drets a conseqüència de la utilització inadequada dels seus recursos informàtics, i posar 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 del mateix rang aprovades per la Universitat Autònoma de Barcelona que s'oposin a aquesta normativa i, de manera expressa, el Text refós de les normatives vigents en l'àmbit de les tecnologies de la informació i la comunicació (TIC) de la Universitat Autònoma de Barcelona, aprovat per acord del Consell de Govern de 13 de juliol de 2011 i modificat per acord del Consell de Govern de 25 d'abril de 2012.

**Disposició final. Entrada en vigor**

Aquesta normativa entra en vigor l'endemà que l'aprovi el Consell de Govern.