Normatives i documents

UNIVERSITAT DE BARCELONA

Política de seguretat de la informació en la utilització de mitjans electrònics de la Universitat de Barcelona

Informació d'aprovació: Consell de Govern
14 de desembre de 2022

UNIVERSITAT DE BARCELONA

Política de seguretat de la informació en la utilització de mitjans electrònics de la Universitat de Barcelona

Preàmbul

Aquesta Política de seguretat de la informació s'elabora en compliment de l'exigència del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema nacional de seguretat (en endavant, ENS), en l'àmbit de l'administració electrònica, que en l'article 12 estableix l'obligació de les administracions públiques de disposar d'una política de seguretat i indica els requisits mínims que ha de complir. El present document fixa els criteris bàsics que han de regir la forma en què la Universitat de Barcelona (en endavant, UB) gestiona i protegeix la informació que tracta i els serveis que presta.

Així mateix, la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, en l'article 13, apartat *h*, reconeix el dret de les persones que es relacionen amb les administracions públiques a la protecció de les dades personals i, en particular, a la seguretat i confidencialitat de les dades que figuren en els fitxers, els sistemes i les aplicacions de les administracions públiques.

D'altra banda, la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, preceptua en l'article 3, apartat 2, que les administracions públiques han d'utilitzar mitjans electrònics que assegurin la interoperabilitat i seguretat dels sistemes i les solucions adoptats per cadascuna d'elles, i que garanteixin la protecció de les dades personals.

A part, el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril, i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, determinen les mesures per protegir el dret fonamental a la protecció de dades personals, emparat per l'article 8 de la Carta dels drets fonamentals de la Unió Europea i per l'article 18.4 de la Constitució.

Article 1. Missió

1.1. La UB, com a institució, s'encarrega, dins del seu àmbit de competències, de la prestació del servei públic de l'ensenyament superior, mitjançant la docència, l'estudi i la recerca. Els objectius fonamentals de la UB són:

a) Crear, transmetre i difondre la cultura i els coneixements científics, tècnics i professionals, així com preparar per a l'exercici professional.

b) Fomentar el pensament crític i la cultura de la llibertat i el pluralisme, i transmetre els valors cívics i socials propis d'una societat democràtica.

c) Enriquir el patrimoni intel·lectual, cultural i científic de Catalunya, i el desenvolupament econòmic i el benestar social.

d) Difondre el coneixement i la cultura a través de l'extensió universitària, la prestació de serveis a la comunitat universitària i a la societat, i la formació continuada al llarg de tota la vida.

1.2. La UB, en el desenvolupament de les seves activitats, vetlla pel respecte a la dignitat de les persones; en l'exercici d'aquestes activitats, assumeix la defensa de la seguretat i la integritat personals, i promou la integració de les persones amb discapacitats, en adequar-hi les instal·lacions.

Article 2. Àmbit d'aplicació

2.1. Aquesta Política s'aplica als sistemes d'informació de la UB i a tots els usuaris que hi tinguin accés autoritzat, siguin o no empleats públics, i amb independència de la naturalesa de la relació jurídica que tinguin amb la Universitat.

2.2. Tots tenen l'obligació de conèixer i complir aquesta Política de la seguretat de la informació i la normativa de seguretat que en deriva, i és responsabilitat del Comitè de Seguretat de la Informació posar a l'abast els mitjans necessaris perquè la informació arribi al personal afectat.

Article 3. Objectius

3.1. La UB depèn de les tecnologies de la informació i les comunicacions (en endavant, TIC) per prestar el servei públic d'educació superior i complir les funcions que té encomanades.

3.2. Els sistemes de les TIC han de ser administrats amb diligència: s'han de prendre les mesures adequades per protegir-los enfront de danys accidentals o deliberats que puguin afectar la seguretat de la informació tractada o els serveis prestats, i han de romandre protegits sempre davant les amenaces o els incidents amb potencial per incidir en la confidencialitat, la integritat, la disponibilitat, la traçabilitat i l'autenticitat de la informació tractada i els serveis prestats.

3.3. Amb aquest fi, la UB estableix els objectius següents de la seguretat de la informació:

a) Garantir la qualitat i la protecció de la informació.

b) Aconseguir la plena conscienciació dels usuaris respecte de la seguretat de la informació.

c) Inventariar i categoritzar els actius d'informació de la Universitat i associar-los a un responsable.

d) Implementar els mecanismes necessaris perquè qualsevol persona que accedeixi o pugui accedir als actius d'informació conegui les seves responsabilitats i, d'aquesta manera, es redueixi el risc derivat d'un ús indegut.

e) Emplaçar els actius d'informació en àrees segures, protegides per controls d'accés físics adequats al nivell de criticitat, així com protegides enfront d'amenaces físiques o ambientals.

f) Establir els procediments necessaris per aconseguir una gestió adequada de la seguretat, l'operació i l'actualització de les TIC. La informació que es transmeti a través de xarxes de comunicacions ha de ser protegida adequadament, tenint-ne en compte el nivell de sensibilitat i de criticitat, mitjançant mecanismes que en garanteixin la seguretat.

g) Limitar l'accés als actius d'informació per part d'usuaris, processos, dispositius i altres sistemes d'informació mitjançant la implantació dels mecanismes d'identificació, autenticació i autorització adients a la criticitat de cada actiu. A més a més, ha de quedar registrada la utilització del sistema de control d'accés, amb la finalitat d'assegurar la traçabilitat de l'accés i auditar-ne l'ús adequat, conforme a l'activitat de l'organització.

h) Preveure els aspectes de seguretat de la informació en totes les fases del cicle de vida dels sistemes d'informació, per garantir-ne la seguretat per defecte.

i) Implementar els mecanismes apropiats per a la identificació, el registre i la resolució correctes dels incidents de seguretat.

j) Implementar els mecanismes apropiats per assegurar la disponibilitat dels sistemes d'informació i mantenir la continuïtat dels seus processos de negoci, d'acord amb les necessitats de nivell de servei dels seus usuaris.

k) Adoptar les mesures tècniques i organitzatives que correspongui implantar per atendre els riscos

generats pel tractament de dades personals per complir la legislació en matèria de protecció de dades personals.

l) Adoptar les mesures tècniques, organitzatives i procedimentals necessàries per complir la normativa legal vigent en matèria de seguretat de la informació.

m) Participar en tots els fòrums de ciberseguretat que es considerin d'interès.

Article 4. Principis bàsics de la seguretat

4.1. Prevenció

4.1.1. Perquè la informació i/o els serveis prestats no es vegin perjudicats per incidents de seguretat, la UB ha d'implementar les mesures de seguretat establertes per l'ENS, així com qualsevol altre control addicional que hagi identificat com a necessari, a través d'una avaluació d'amenaces i riscos. Aquests controls i els rols i les responsabilitats de seguretat de tot el personal han d'estar clarament definits i documentats.

4.1.2. Per garantir el compliment de la Política, la UB:

a) Ha d'autoritzar els sistemes abans d'entrar en operació.

b) Ha d'avaluar regularment la seguretat, incloent-hi l'anàlisi dels canvis de configuració aplicats de manera rutinària.

c) Ha de sol·licitar la revisió periòdica per part de tercers, a fi d'obtenir una avaluació independent.

4.1.3. La UB ha d'evitar o, com a mínim, prevenir, en la mesura que sigui possible, que la informació o els serveis siguin perjudicats per incidents de seguretat.

4.2. Detecció

4.2.1. La UB ha d'establir controls d'operació dels seus sistemes d'informació amb l'objectiu de detectar anomalies en la prestació dels serveis i actuar en conseqüència, d'acord amb el que disposa l'article 10 de l'ENS (reavaluació periòdica).

4.2.2. Com que els serveis poden degradar-se ràpidament a causa d'incidents, amb conseqüències que poden anar des d'una simple desacceleració fins a l'aturada, s'ha de monitorar el funcionament d'aquests serveis, d'acord amb principi de vigilància continuada previst en l'article 10 de l'ENS.

4.2.3. El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 9 de l'ENS. S'han d'establir mecanismes de detecció, anàlisi i report que arribin als responsables amb regularitat i quan es produeixi una desviació significativa dels paràmetres que s'hagin establert prèviament com a normals.

4.3. Resposta

La UB ha d'establir les mesures següents:

a) Mecanismes per respondre eficaçment als incidents de seguretat.

b) Designar un punt de contacte per a les comunicacions respecte d'incidents detectats en altres

organismes.

c) Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicació, en ambdós sentits, amb els equips de resposta a emergències (CERT) i/o els equips de resposta a incidents de seguretat informàtica (CSIRT).

4.4. Recuperació

Per garantir la disponibilitat dels serveis crítics, la UB ha d'aplicar procediments que garanteixin la recuperació i la conservació a llarg termini dels documents electrònics, la informació i les dades produïts pels sistemes d'informació compresos en l'àmbit d'aplicació de l'ENS, quan sigui exigible.

Article 5. Marc normatiu

5.1. El marc normatiu en què es desenvolupen les activitats de la UB i, en particular, la prestació dels seus serveis electrònics està integrat per les normes següents i tota altra normativa que sigui aplicable a la UB.

5.1.1. Àmbit de l'ENS:

- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema nacional de seguretat.
- Resolució de 13 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció tècnica de seguretat de conformitat amb l'Esquema nacional de seguretat.
- Resolució de 7 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció tècnica de seguretat de l'Informe de l'estat de la seguretat.
- Resolució de 27 de març de 2018, de la Secretaria d'Estat de Funció Pública, por la qual s'aprova la Instrucció tècnica de seguretat d'auditoria de la seguretat dels sistemes d'informació.
- Resolució de 13 d'abril de 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció tècnica de seguretat de notificació d'incidents de seguretat.

5.1.2. Àmbit de la protecció de dades personals:

- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades).
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

5.1.3. Àmbit comunitari:

- Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016, relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i sistemes d'informació en la Unió Europea.

5.1.4. Àmbit estatal:

- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
- Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema nacional d'interoperabilitat en l'àmbit de l'administració electrònica.
- Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.

Article 6. Rols i Comitè de la Seguretat de la Informació

6.1. En la UB, els rols i òrgans sobre la seguretat de la informació són els següents:

a) Responsable de la informació: el secretari o secretària general.

b) Responsable dels serveis: el gerent o gerenta.

c) Responsable de seguretat de la informació: designat formalment pel rector de la Universitat, després de deliberar amb el Consell de Direcció.

El responsable de seguretat no pot ser un òrgan de govern unipersonal de la Universitat i no ha de tenir cap responsabilitat sobre la prestació dels serveis TIC, ni ha d'estar sota la dependència jeràrquica del responsable del sistema (i viceversa).

d) Responsable del sistema: el director o directora de l'Àrea TIC de la UB.

e) Comitè de Seguretat de la Informació (COMSEG):

i. Presidència: el rector o rectora, un vicerector o vicerectora o un delegat o delegada.

ii. Vocalies:

- Membres permanents:
  - Secretari o secretària del COMSEG: el secretari o secretària general.
  - Responsable del sistema (RSIS).
  - Responsable de seguretat de la informació (RSEG).
  - Responsable de la informació.
  - Responsable dels serveis.
  - Assessors que es considerin oportuns per als temes en qüestió; fins i tot, hi pot assistir un representant del Centre Criptològic Nacional (CCN) o de l'Agència de Ciberseguretat de Catalunya, amb veu però sense vot.
  - Delegat o delegada de protecció de dades, que hi participa amb veu però sense vot.

- Membres no permanents:

  El COMSEG pot convocar a les reunions tant altres representants de la Universitat com especialistes externs dels sectors públic, privat i/o acadèmic, la presència dels quals sigui necessària o aconsellable, per raó de l'experiència o la vinculació amb els assumptes tractats.

6.2. Els integrants del Comitè de Seguretat de la Informació els ha de nomenar el rector de la UB, que també ha de designar els responsables identificats en aquesta Política. El nomenament s'ha de revisar cada quatre anys o quan la plaça quedi vacant.

Article 7. Funcions dels rols de la seguretat de la informació

7.1. Són funcions dels responsables de la informació i dels serveis:

a) Establir i elevar al Comitè de Seguretat de la Informació perquè els aprovi els requisits de seguretat aplicables a la informació (nivells de seguretat de la informació) i als serveis (nivells de seguretat

dels serveis), dins del marc establert en l'annex I del Reial decret 311/2022, de 3 de maig; pot demanar una proposta al responsable de seguretat i tenir en compte l'opinió del responsable del sistema.

b) Dictaminar respecte dels drets d'accés a la informació i als serveis.

c) Acceptar els nivells de risc residuals que afecten la informació i els serveis.

d) Posar en coneixement del responsable de seguretat qualsevol variació respecte de la informació i els serveis dels quals és responsable; especialment, la incorporació de nous serveis o informació a càrrec seu. El responsable de seguretat ha de traslladar els canvis esmentats al Comitè de Seguretat de la Informació en la seva pròxima reunió.

7.2. Són funcions del responsable de seguretat:

a) Mantenir i verificar el nivell adequat de seguretat de la informació manejada i dels serveis electrònics prestats pels sistemes d'informació.

b) Promoure la formació i conscienciació en matèria de seguretat de la informació.

c) Designar responsables de l'execució de l'anàlisi de riscos i de la declaració d'aplicabilitat regulada en l'article 28 de l'ENS, identificar mesures de seguretat, determinar configuracions necessàries, i elaborar documentació del sistema.

d) Proporcionar assessorament per a la determinació de la categoria del sistema, en col·laboració amb el responsable del sistema i/o el Comitè de Seguretat de la Informació.

e) Participar en l'elaboració i la implantació dels plans de millora de la seguretat i, arribat el cas, dels plans de continuïtat, que ha de validar.

f) Gestionar les revisions externes o internes del sistema.

g) Gestionar els processos de certificació i auditories.

h) Elevar al Comitè de Seguretat de la Informació l'aprovació de canvis i altres requisits del sistema.

i) Aprovar els procediments de seguretat que formen part del mapa normatiu (i no són competència del Comitè) i posar en coneixement del Comitè les modificacions que s'hagin fet al llarg del període en curs.

j) Redactar propostes i presentar-les al Comitè de Seguretat de la Informació.

k) Promoure la millora continuada del sistema de gestió de la seguretat de la informació, d'acord amb l'article 27 de l'ENS.

l) Aprovar els canvis que, mitjançant una anàlisi de risc, es determini que són rellevants per a la seguretat del sistema i siguin d'un risc de nivell «alt».

m) Analitzar els informes d'autoavaluació i elevar les conclusions al responsable del sistema perquè adopti les mesures correctores adequades.

n) Proporcionar assessorament per a la determinació de la categoria del sistema, en col·laboració amb el responsable del sistema i/o el Comitè de Seguretat de la Informació.

o) Revisar els informes d'auditoria. Les conclusions de les auditories s'han de presentar al responsable del sistema perquè adopti les mesures correctores adequades.

7.3. Són funcions del responsable del sistema:

a) Desenvolupar, per si mateix o a través de recursos propis o contractats, la forma concreta d'implementar la seguretat en el sistema i de supervisar l'operació diària del mateix sistema, que pot delegar en administradors o operadors sota la seva responsabilitat.

b) Revisar les conclusions dels informes d'auditoria que emet el responsable de seguretat.

c) Desenvolupar, operar i mantenir el sistema d'informació durant tot el cicle de vida, per a la qual cosa cal elaborar els procediments operatius necessaris.

d) Definir la topologia i la gestió del sistema d'informació i establir-ne els criteris d'ús i els serveis que hi són disponibles.

e) En els casos de sistemes de categoria «alta», suspendre temporalment, si escau, el tractament d'informacions, la prestació de serveis o l'operació total del sistema fins a l'esmena o la mitigació adequada.

f) Garantir que els dispositius estan sota control i que satisfan els requisits de seguretat mentre són desplaçats d'un lloc a l'altre, fora de les zones controlades per la Universitat.

g) Rebre les conclusions dels informes d'autoavaluació i prendre les mesures correctores adequades.

h) Rebre les conclusions dels informes d'auditoria i prendre les mesures correctores adequades.

i) Cerciorar-se que les mesures específiques de seguretat s'integren adequadament dins el marc general de seguretat.

j) Proporcionar assessorament per a la determinació de la categoria del sistema, en col·laboració amb el responsable de seguretat i/o el Comitè de Seguretat de la Informació.

k) Participar en l'elaboració i la implantació dels plans de millora de la seguretat i, arribat el cas, dels plans de continuïtat.

l) Dur a terme, si escau, les funcions de l'administrador de la seguretat del sistema:

i. Gestionar, configurar i actualitzar, si escau, el maquinari i el programari en què es basen els mecanismes i serveis de seguretat.

ii. Gestionar les autoritzacions concedides als usuaris del sistema, en particular els privilegis concedits, incloent-hi el monitoratge de l'activitat desenvolupada en el sistema i la correspondència amb l'autoritzat.

iii. Aprovar els canvis en la configuració vigent del sistema d'informació.

iv. Assegurar que es compleixen estrictament els controls de seguretat establerts.

v. Assegurar que s'apliquen els procediments aprovats per manejar el sistema d'informació.

vi. Supervisar les instal·lacions de maquinari i programari i les seves modificacions i millores, per assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.

vii. Monitorar l'estat de seguretat proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica.

viii. Informar el responsable de seguretat de qualsevol anomalia, compromís o vulnerabilitat relacionat amb la seguretat.

ix. Gestionar la investigació i la resolució d'incidents de seguretat, des de la detecció fins a la resolució.

7.4. Quan la complexitat del sistema ho justifiqui, el responsable del sistema pot designar els responsables de sistema delegats que consideri necessaris, els quals en tenen dependència funcional directa i són responsables en el seu àmbit de totes les accions que els deleguin. De la mateixa manera, també pot delegar funcions concretes de les responsabilitats que se li atribueixen.

7.5. Les funcions del delegat o delegada de protecció de dades són les que estableix l'article 39 del Reglament (UE) 2016/679, de 27 d'abril, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades).

Article 8. Funcions i règim de funcionament del Comitè de Seguretat de la Informació

8.1. Són funcions del Comitè de Seguretat de la Informació:

a) Estar informat permanentment de la normativa que regula la certificació de conformitat amb l'ENS, incloent-hi les normes d'acreditació, certificació, guies, manuals, procediments i instruccions tècniques.

b) Estar informat permanentment de la relació d'entitats de certificació acreditades i organitzacions, públiques i privades, certificades.

c) Estar informat permanentment de la relació d'esquemes de certificació de la seguretat amb els quals l'Administració pública té establerts arranjaments i acords de reconeixement mutu de certificats.

d) Proposar directrius i recomanacions, que s'han de recollir en les actes corresponents de les reunions del Comitè, a les quals la Presidència ha de donar una resposta adequada.

e) Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació per assegurar que siguin consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.

f) Atendre les inquietuds en matèria de seguretat de la informació de l'Administració i de les diferents àrees, i informar regularment sobre l'estat de la seguretat de la informació al Consell de direcció.

g) Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i/o entre diferents unitats administratives, i elevar els casos en què no tingui prou autoritat per decidir.

h) Assessorar en matèria de seguretat de la informació, sempre que se li requereixi.

i) Revisar la Política de seguretat de la informació, abans que l'aprovi el Consell de Govern.

j) Aprovar la Normativa sobre l'ús de mitjans electrònics per a tot el personal.

k) Aprovar el mapa de normativa amb la llista de normativa i procediments de seguretat per a la implantació de l'ENS.

l) Aprovar els requisits de seguretat aplicables a la informació i als serveis, a proposta dels responsables de la informació i dels serveis.

m) Aprovar els plans de millora de la seguretat.

8.2. La periodicitat de les reunions i l'adopció d'acords s'han de regir pels següents punts:

a) Durant el desenvolupament del projecte d'adequació a l'ENS, per avaluar-ne el desenvolupament i possibilitar-ne el seguiment adequat, el Comitè de Seguretat de la Informació s'ha de reunir, almenys, un cop al trimestre.

b) Un cop assolida la certificació de conformitat amb l'ENS dels serveis prestats per la Universitat, el Comitè de Seguretat de la Informació s'ha de reunir, almenys, dues vegades l'any amb caràcter semestral, sense perjudici que, en atenció a les necessitats derivades del compliment dels seus fins i atribucions, es requereixi més freqüència en les reunions.

c) En qualsevol cas, les reunions les ha de convocar la Presidència, a través del secretari o secretària, a iniciativa seva o per majoria dels membres permanents.

d) Les decisions s'han d'adoptar per consens dels membres permanents.

8.3. El secretari o secretària del Comitè ha de fer les convocatòries i ha d'aixecar actes de les reunions del Comitè de Seguretat de la Informació. A les sessions del Comitè de Seguretat de la Informació, poden assistir-hi en qualitat d'assessors les persones que en cada cas estimi pertinents la Presidència.

8.4. Els representants de la UB en els grups de treball sobre seguretat de la informació en què participin han de traslladar al Comitè de Seguretat de la Informació totes les informacions, els projectes i les deliberacions que s'hi produeixin.

Article 9. Gestió dels riscos

9.1. Tots els sistemes afectats per aquesta Política de seguretat de la informació estan subjectes a una anàlisi de riscos, amb l'objectiu d'avaluar les amenaces i els riscos a què estan exposats.

9.2. Aquesta anàlisi s'ha de repetir:

a) Almenys un cop cada dos anys.

b) Quan canviïn de manera significativa la informació i/o els serveis manejats.

c) Quan s'esdevingui un incident greu de seguretat o es detectin vulnerabilitats greus.

9.3. El responsable de la seguretat és l'encarregat que es faci l'anàlisi de riscos, així com d'identificar carències i debilitats i posar-les en coneixement del Comitè de Seguretat de la Informació.

9.4. El Comitè de Seguretat de la Informació ha de dinamitzar la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes i ha de promoure inversions de caràcter horitzontal.

9.5. El procés de gestió de riscos ha de comprendre les fases següents:

a) Categorització dels sistemes.

b) Anàlisi de riscos.

c) Selecció de mesures de seguretat que cal aplicar: el Comitè de Seguretat de la Informació les ha de seleccionar i han de ser proporcionals als riscos i han d'estar justificades.

9.6. Les fases d'aquest procés s'han de fer segons el que disposen els annexos I i II del Reial decret 311/2022, de 3 de maig, pel qual es regula l'ENS, i seguint les normes, instruccions, guies CCN-STIC i recomanacions per aplicar-lo elaborades pel Centre Criptològic Nacional. De la mateixa manera, s'han de seguir les normes, instruccions i recomanacions de l'Agència de Ciberseguretat de Catalunya.

9.7. En particular, per fer l'anàlisi de riscos s'ha d'utilitzar, com a norma general, una metodologia reconeguda d'anàlisi i gestió de riscos.

Article 10. Gestió de les notificacions d'incidents de seguretat

10.1. De conformitat amb el que disposen els articles 33 i 34 del Reial decret 311/2022, de 3 de maig, pel qual es regula l'ENS, la UB ha de notificar al Centre Criptològic Nacional els incidents que tinguin un impacte significatiu en la seguretat de la informació manejada i dels serveis prestats en relació amb la categorització de sistemes recollida en l'annex I del cos legal esmentat. De la mateixa manera, aquests incidents s'han de notificar a l'Agència de Ciberseguretat de Catalunya.

10.2. Quan aquests incidents afectin dades personals, s'han de comunicar al responsable del tractament de la UB (Secretaria General) i al delegat o delegada de protecció de dades.

Article 11. Obligacions del personal

11.1. Tots els membres de la UB tenen l'obligació de conèixer i complir aquesta Política de seguretat de la informació i les normatives de seguretat TIC que en deriven, i és responsabilitat del Comitè de Seguretat de la Informació disposar dels mitjans necessaris perquè la informació arribi als afectats.

11.2. Tot el personal de la UB comprès dins l'àmbit de l'ENS ha d'assistir a una o diverses sessions de conscienciació en matèria de seguretat i protecció de dades, almenys una vegada a l'any. S'ha d'establir un programa de conscienciació continuada per atendre tot el personal i, en particular, el de nova incorporació.

11.3. Les persones amb responsabilitat en l'ús, l'operació o l'administració de sistemes d'informació han de rebre formació per manejar d'una manera segura els sistemes en la mesura en què la necessitin per fer la seva feina. La formació és obligatòria abans d'assumir una responsabilitat, tant si és la primera assignació com si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest lloc.

Article 12. Terceres parts

12.1. Quan la UB presti serveis a altres organismes o manegi informació d'altres organismes, se'ls ha de fer partícips d'aquesta Política de seguretat de la informació. S'han d'establir canals per al report i la

coordinació dels comitès de seguretat de la informació respectius i s'han d'establir procediments d'actuació per reaccionar davant d'incidents de seguretat.

12.2. Quan la UB utilitzi serveis de tercers o cedeixi informació a tercers, se'ls ha de fer partícips d'aquesta Política de seguretat de la informació i de la normativa de seguretat que pertoqui a aquests serveis o informació. La tercera part esmentada queda subjecta a les obligacions que estableixi la normativa mencionada i pot desenvolupar els seus propis procediments operatius per satisfer-la. S'han de fixar procediments específics de report i resolució d'incidències. S'ha de garantir que el personal de tercers està conscienciat adequadament en matèria de seguretat, almenys al mateix nivell que el que preveu aquesta Política de seguretat.

12.3. Quan una tercera part no pugui satisfer algun aspecte d'aquesta Política de seguretat de la informació segons el que requereixen els paràgrafs anteriors, s'ha de demanar un informe del responsable de seguretat que precisi els riscos en què s'incorre i la forma de tractar-los. S'ha de requerir que aprovin aquest informe els responsables de la informació i els serveis afectats abans de continuar endavant.

Article 13. Gestió de la Política de seguretat i millora continuada

13.1. És responsabilitat del Comitè de Seguretat de la Informació revisar aquest document i la proposta d'actualització o el manteniment, quan sigui necessari.

13.2. Es considera com a canvi rellevant qualsevol que pugui repercutir en el compliment de les mesures de seguretat implantades.

13.3. El contingut del document s'ha d'adequar sempre a les disposicions vigents en la matèria de l'ENS i de protecció de dades personals.

13.4. Tota nova versió d'aquesta Política s'ha de comunicar segons l'abast del canvi del document i el nivell de difusió que calgui, de manera que el personal pugui actualitzar la versió del document obsolet.

13.5. Per garantir-ne la millora continuada, s'ha d'implantar un procés permanent que comporti, entre altres accions, les següents:

a) Revisar la Política de seguretat de la informació.

b) Revisar els serveis i la informació i la seva categorització.

c) Executar amb periodicitat anual l'anàlisi de riscos.

d) Fer auditories internes o, quan escaigui, externes.

e) Revisar les mesures de seguretat.

f) Revisar, actualitzar i crear les normes i els procediments que es creguin oportuns.

Article 14. Incompliment de la Política de seguretat

14.1. L'incompliment de les obligacions i mesures de seguretat establertes en aquest document comporta aplicar als col·lectius la normativa en matèria disciplinària vigent en cada moment.

14.2. A més, la UB pot exercir les accions oportunes previstes en el Codi civil i, fins i tot, en el penal, especialment en el cas que, per causa d'un treballador o treballadora de la UB, se sancioni la Universitat de conformitat amb la legislació vigent.

Article 15. Resolució de controvèrsies

En el cas que per causa de l'execució d'aquesta Política de seguretat de la informació es produís una controvèrsia o un conflicte d'interessos, s'ha d'avaluar de manera interna i s'ha de determinar si s'ha pres una decisió correcta i d'acord amb les normes. La controvèrsia l'ha de resoldre el rector o rectora.

Article 16. Desplegament de la Política de seguretat

16.1. Aquesta Política de seguretat de la informació s'ha de complementar mitjançant diverses normatives i recomanacions de seguretat (normatives i procediments de seguretat, procediments tècnics de seguretat, informes, registres i evidències electròniques).

16.2. El cos normatiu sobre seguretat de la informació s'ha de desplegar en tres nivells, per àmbit d'aplicació, nivell de detall tècnic i obligatorietat de compliment, de manera que cada norma d'un determinat nivell de desplegament es fonamenti en les normes del nivell superior. Els nivells de desplegament normatiu són els següents:

a) Primer nivell normatiu: constituït per aquesta Política de seguretat de la informació, la Normativa interna sobre l'ús de mitjans electrònics i les directrius generals de seguretat aplicables als organismes o unitats de la universitat a què siguin aplicables els documents esmentats.

b) Segon nivell normatiu: constituït per les normes de seguretat derivades de les anteriors.

c) Tercer nivell normatiu: constituït per procediments, guies i instruccions tècniques. Són documents que, en compliment del que exposa la Política de seguretat de la informació, determinen les accions o tasques que s'han de fer en l'exercici d'un procés.

16.3. Correspon al Consell de Govern de la UB aprovar la Política de seguretat de la informació i la Normativa interna sobre l'ús de mitjans electrònics de la Universitat, mentre que el Comitè de Seguretat de la Informació és l'òrgan responsable d'aprovar la resta de documents i també és responsable de difondre la Política perquè la coneguin les parts afectades.

16.4. De la mateixa manera, aquesta Política de seguretat de la informació complementa les instruccions i altres indicacions que emeti el responsable del tractament de la UB en matèria de protecció de dades personals.

16.5. La normativa de seguretat i, molt especialment, la Política de seguretat de la informació i la Normativa interna sobre l'ús de mitjans electrònics, les han de conèixer tots els membres de la Universitat i han d'estar a disposició seva; en particular, els qui utilitzen, operen o administren els sistemes d'informació i comunicacions. Ha d'estar disponible per ser consultada en el Portal de la Transparència. Així mateix, l'Àrea TIC ha de crear i mantenir un registre amb tot el cos normatiu sobre seguretat de la informació.

Disposició final única. Entrada en vigor

Aquesta Política entra en vigor de l'endemà d'haver estat aprovada pel Consell de Govern.