Universitat Autònoma de Barcelona

Política de seguretat de la informació

(Acord del Consell de Govern d' 11 de març de 2020)

Preàmbul

El propòsit d'aquesta Política de Seguretat de la Informació és establir les bases de la fiabilitat amb la què els sistemes d'informació prestaran els seus serveis i custodiaran la informació d'acord amb les seves especificacions funcionals, sense interrupcions o modificacions fora de control i sense que la informació pugui arribar al coneixement de persones no autoritzades.

En aquest document es recull el conjunt de mesures necessàries, tècniques i organitzatives, per a aconseguir un nivell de protecció adequat per a assegurar el compliment legal, i garantir la disponibilitat i la confidencialitat de la informació.

La Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, va establir l'Esquema Nacional de Seguretat (ENS) com a pilar bàsic que permeti una protecció adequada de la informació.

Posteriorment, la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, recull l'ENS en l'article 156, apartat 2, en uns termes similars.

L'ENS està regulat pel Reial decret 3/2010, de 8 de gener , que va ser modificat pel Reial decret 951/2015 per actualitzar-ho a la llum de l'experiència obtinguda en la seva implantació, de l'evolució de la tecnologia i les ciberamenaces i del context regulador internacional i europeu.

Aquest document està basat en les guies elaborades pel Centre Criptogràfic Nacional (CCN), que s'encarrega d'elaborar i difondre normes, guies i recomanacions en relació a l'Esquema Nacional de Seguretat.

1. Marc normatiu

Aquesta política se situa dintre del marc jurídic definit per les lleis i reials decrets següents:

- Llei Orgànica 6/2001, de 21 de desembre, d'universitats (LOU), modificada per la Llei Orgànica 4/2007.
- Reial decret 3/2010, de 8 de gener, pel que es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica (ENS), modificat pel Reial Decret 951/2015, de 23 d'octubre.
- 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 la lliure circulació d'aquestes dades (RGPD).
- Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD).
- Llei 32/2010, d'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades.
- Llei 59/2003, de 19 de desembre, de firma electrònica.
- Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.
- Llei 1/2003, de 19 de febrer, d'universitats de Catalunya (LUC).
- 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.
- Decret 237/2003, de 8 d'octubre, pel qual s'aproven els Estatuts de la Universitat Autònoma de Barcelona.

2. Declaració de la política de seguretat de la informació

La UAB compta amb el suport dels sistemes TIC (tecnologies de la informació i les comunicacions) per assolir els seus objectius institucionals. Com a conseqüència, aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir-los enfront de danys accidentals o deliberats que puguin afectar la disponibilitat, la integritat, la confidencialitat, la traçabilitat o l'autenticitat de la informació tractada o dels serveis prestats.

L'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant als incidents amb prestesa.

Els sistemes TIC han d'estar protegits enfront d'amenaces d'evolució ràpida i han de tenir potencial per incidir en la confidencialitat, la integritat, la disponibilitat, la traçabilitat, l'autenticitat, l'ús previst i el valor de la informació i els serveis. Per defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn que garanteixi la prestació continuada dels serveis.

Això implica que la UAB i el seu personal han d'aplicar les mesures de seguretat exigides a l'ENS, així com dur a terme un seguiment continu dels nivells de prestació de serveis, fer el seguiment de les vulnerabilitats reportades i analitzar-les, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

La UAB ha d'assegurar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida dels sistemes, des que es conceben fins que es retiren del servei, incloent-hi les decisions de desenvolupament o adquisició i les activitats d'explotació.

L'organització ha d'estar preparada per prevenir, detectar, donar resposta i recuperar-se d'incidents, d'acord amb l'article 7 de l' ENS.

3.Principis bàsics de la seguretat

Prevenció

L'organització 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. Per això s'han d'implementar les mesures mínimes de seguretat que determina l'ENS, així com qualsevol altre control addicional identificat mitjançant una avaluació d'amenaces i riscos. Aquests controls, i els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.

Per tal de garantir el compliment de la política:

- S'han d'autoritzar els sistemes abans que comencin a funcionar.
- Se n'ha d'avaluar regularment la seguretat, incloent-hi avaluacions dels canvis de configuració que es fan de forma rutinària.
- S'ha de sol·licitar que tercers els revisin periòdicament, amb la finalitat d'obtenir una avaluació independent.

Detecció

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració fins a la seva aturada, s'ha de monitoritzar l'operació de manera contínua per detectar anomalies en els nivells de prestació dels serveis i actuar-hi en conseqüència, segons el que estableix l'article 9 de l'ENS.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 de l'ENS. S'establiran mecanismes de detecció, anàlisi i informe que arribin als responsables regularment i quan es produeixi una desviació significativa dels paràmetres que s'hagin preestablert com a normals.

Resposta

L'organització ha de:

- Establir mecanismes per respondre eficaçment als incidents de seguretat.
- Designar un punt de contacte per a les comunicacions pel que fa a incidents detectats en altres serveis universitaris o en altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident.

Recuperació

Per garantir la disponibilitat dels serveis crítics, es desenvoluparan plans de continuïtat dels sistemes TIC com a part del pla general de continuïtat del serveis i les activitats de recuperació que s'escaiguin.

4. Àmbit d'aplicació

Aquesta política de seguretat de la informació s'aplica a tota la comunitat Universitària de la Universitat Autònoma de Barcelona, als seus actius d'informació i a tots els sistemes d'informació afectats.

Així mateix és aplicable a tots contractistes, consultors, personal eventual i altres usuaris de la Universitat, incloent-hi tot el personal extern que tingui un equip connectat a la xarxa o interaccioni amb els sistemes informàtics o la xarxa de la UAB així com tots els equips i serveis propietaris o arrendats que, d'alguna manera, hagin d'utilitzar localment o remotament la xarxa o recursos tecnològics de la institució, així com els serveis i l'intercanvi d'arxius i programes.

5. Organització de la seguretat a la UAB

La gestió de la seguretat de la informació a la UAB serà coordinada a través del Comitè de Seguretat de la Informació.

5.1. Composició:

El comitè està format per les següents persones:

- Comissionat/da per l'àmbit de les Tecnologies de la Informació i de la Comunicació o persona amb un càrrec equivalent, que n'exerceix la presidència.
- Responsable de Seguretat: La persona designada per Gerència, que farà la funció de secretari del comitè.
- Responsable de la Informació: Cap de la Oficina de Gestió de la Informació i de la Documentació o persona en qui delegui.
- Responsable dels Serveis: Cap de l'Àrea de Transformació Digital i Organització o persona en qui delegui.
- Responsable del Sistema: Director/a de Tecnologies de la Informació i la Comunicació.
- Administrador/a del Sistema: Responsable de la Unitat de Producció TIC.
- Delegat/da de Protecció de Dades.

5.2. Funcions del Comitè.

Les funcions del Comitè de Seguretat de la Informació són:

- Divulgar la política i les normatives de seguretat TIC de la UAB.
- Aprovar normatives i procediments de seguretat i altres documents derivats de la política de seguretat TIC.
- Revisar la política de seguretat de la informació i proposar a l'òrgan competent la seva modificació, si escau.
- Difondre la política de seguretat perquè la coneguin totes les parts afectades.
- Desenvolupar el procediment de designació de rols.
- Supervisar i aprovar les tasques de seguiment de l'Esquema Nacional de Seguretat: adequació, anàlisi de riscos i auditoria bianual.
- Promoure la millora contínua del sistema de gestió de la seguretat de la informació.
- Elaborar l'estratègia d'evolució de la UAB pel que fa a la seguretat de la informació.
- Determinar els nivells de seguretat requerits pels diferents serveis.
- Avaluar l'acompliment dels processos de gestió d'incidents de seguretat.
- Definir el desplegament en la UAB dels principis de seguretat identificats en la present política.
- Reportar al rector o rectora els resultats de la coordinació en matèria de seguretat de la informació.

5.3. Rols: funcions i responsabilitats

Responsable de la Informació

Les funcions són les següents:

- Establir els requisits de la informació en matèria de seguretat.
- Treballar en col·laboració amb els responsables de Seguretat i del Sistema en el manteniment dels sistemes catalogats segons l'annex I de l'Esquema Nacional de Seguretat.

Responsable dels Serveis

Les funcions del Responsable de Serveis són els següents:

- Establir els requisits dels serveis en matèria de seguretat TIC.
- Treballar en col·laboració amb els responsables de Seguretat i del Sistema en el manteniment dels sistemes catalogats segons l'annex I de l'Esquema Nacional de Seguretat.
- Vetllar per la inclusió de clàusules sobre seguretat en els contractes amb terceres parts i perquè es compleixin.

Responsable de Seguretat

El Responsable de seguretat té les funcions següents:

- Mantenir les condicions de seguretat dels sistemes TIC, pel que fa a la informació que tracten i als serveis que presten.
- Gestionar les auditories periòdiques que permetin verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Promoure la formació i conscienciació del personal TIC dins del seu àmbit de responsabilitat.
- Verificar que les mesures de seguretat establertes són adequades per a la protecció de la informació que es tracta i els serveis que es presten.
- Analitzar, completar i aprovar tota la documentació relacionada amb la seguretat dels sistemes.
- Monitorar l'estat de seguretat dels sistemes proporcionat per les eines de gestió d'esdeveniments de seguretat i els mecanismes d'auditoria implementats en els sistemes.
- Donar suport a la investigació dels incidents de seguretat, des que es notifiquen fins que es resolen, i supervisar-la.
- Elaborar l'informe periòdic de seguretat per al propietari del sistema, que ha d'incloure els incidents més rellevants del període.
- Aprovar els procediments de seguretat elaborats pel responsable del Sistema.
- Elaborar les normatives de seguretat de l'entitat.

Responsable del Sistema

El responsable del Sistema té, dins de la seva àrea d'actuació, les funcions següents:

- Desenvolupar, fer funcionar i mantenir el sistema de forma segura durant tot el seu cicle de vida, incloent-ne la instal·lació i la verificació del funcionament correcte i el seguiment de les especificacions de seguretat.
- Definir la topologia i els procediments de gestió del sistema atenent a la seguretat.
- Definir la política de connexió o desconnexió d'equips i usuaris nous en el sistema.
- Aprovar els canvis que afecten la seguretat del mode d'operació del sistema.
- Decidir les mesures de seguretat que hauran d'aplicar els subministradors de components del sistema durant les etapes de desenvolupament, instal·lació i prova.
- Implantar i controlar les mesures específiques de seguretat del sistema i assegurar-se que aquestes s'integrin adequadament dins del marc general de seguretat.
- Determinar la configuració autoritzada del hardware i el software que s'han d'utilitzar en el sistema.
- Aprovar tota modificació substancial de la configuració de qualsevol element del sistema.
- Portar a terme el procés preceptiu d'anàlisi i de gestió de riscos en el sistema.
- Determinar la categoria del sistema segons el procediment descrit a l'annex I de l'ENS i determinar les mesures de seguretat que han d'aplicar-s'hi segons el que es descriu a l'annex II de l'ENS.
- Elaborar la documentació de seguretat del sistema.
- Delimitar les responsabilitats de cada entitat involucrada el manteniment, explotació, implantació i supervisió del sistema.
- Vetllar pel compliment de les obligacions de l'administrador de seguretat del Sistema.
- Investigar els incidents de seguretat que afectin el sistema, comunicar-los al responsable de Seguretat o a qui s'hagi determinat, i, si s'escau, al DPD i al responsable de la informació.
- Establir plans de contingència i emergència, i dur a terme de manera freqüent exercicis per al personal perquè s'hi familiaritzi.
- A més, el responsable del Sistema pot acordar la suspensió de l'ús d'una certa informació o la prestació d'un cert servei si se l'informa de deficiències greus de seguretat que puguin afectar la satisfacció dels requisits establerts. Aquesta decisió ha de ser acordada amb els responsables de la informació afectada i del servei afectat, i amb el responsable de Seguretat abans d'executar-la.

- Elaborar els procediments de seguretat necessaris per a l'operativa del sistema amb la implicació de les parts afectades.

5.4. Mecanismes de coordinació i assessorament

El Comitè de Seguretat de la Informació estarà assistit per personal tècnic dels àmbits:
- Jurídic.
- Arquitectura i Logística.
- Economia.
- Organització.
- CSIRT (Centre de Resposta a Incidents de Seguretat) de la UAB.
- DTIC (Direcció de Tecnologia de la Informació i la Comunicació) de la UAB.

6. Dades de caràcter personal

La LOPDGDD estableix que els subjectes vinculats al sector públic, com ho són les universitats públiques, han de fer públic un inventari de les seves activitats respecte del tractament de dades personals accessible per mitjans electrònics, on hi ha de constar la informació prevista a l'article 30 de l'RGPD, i on s'ha d'especificar, a més, la base legal del tractament. Aquest registre d'activitats de tractament de la UAB es publicarà al Web Institucional de la UAB, apartat "Protecció de Dades". Tots els sistemes d'informació de la UAB s'han d'ajustar als nivells de seguretat que estableix la normativa segons la naturalesa i la finalitat de les dades personals.
El personal de la UAB ha d'estar assabentat de l'obligació de llegir i complir la Política de Protecció de Dades descrita al Web Institucional de la UAB.

7. Gestió de riscos

Tots els sistemes subjectes a aquesta política han de realitzar una anàlisi de riscos, en què s'avaluïn les amenaces i els riscos als quals estan exposats. Aquesta anàlisi s'ha de repetir:
- Regularment, com a mínim cada 2 anys.
- Quan canviï l'estructura de la informació que es gestioni.
- Quan canviïn els serveis prestats.
- Després de la resolució d'un incident greu de seguretat.
- Quan canviïn les condicions tecnològiques.
- Quan es reportin vulnerabilitats greus

Per tal d'harmonitzar les anàlisis de riscos, el Comitè de Seguretat de la Informació ha d'establir una valoració de referència per als diferents tipus d'informació que s'utilitzen i els diferents serveis prestats.

8. Gestió d'incidents de seguretat

La UAB disposarà d'un servei de resposta davant d'incidents de seguretat (CSIRT) que estigui dotat dels mitjans necessaris per implantar i gestionar totes i cadascuna de les mesures de seguretat requerides en cada sistema d'informació per donar resposta als incidents de seguretat que es produeixin. La gestió d'incidents contemplarà detecció, anàlisi, registre, contenció, erradicació, recuperació i les notificacions que s'escaiguin.

Aquest servei podrà efectuar les auditories de seguretat que consideri oportunes i necessàries sobre qualsevol equip connectat a la xarxa de la Universitat, podent procedir a la seva desconnexió o aïllament en aquells casos que suposin un risc potencial o real per a la resta dels sistemes d'informació o usuaris de la UAB.

Tanmateix, qualsevol usuari ha de traslladar incidents, suggeriments i/o debilitats que puguin tenir relació amb la seguretat de la informació i les directrius contingudes en la present política.

9. Desenvolupament de la política de seguretat de la informació

Aquesta Política de Seguretat serà desenvolupada per normatives i procediments de seguretat que estaran a disposició de tots els membres de la comunitat universitària que necessitin conèixer-la.

10. Documentació de seguretat

1.La documentació de seguretat TIC s'estructura en tres tipus:

- La present política de seguretat de la informació, que estableix els requisits i criteris de seguretat TIC en l'àmbit de la Universitat i que serveix de guia per a la creació de normes de seguretat.
- Les normatives de seguretat, que defineixen què cal protegir i els requisits de seguretat TIC necessaris.
- Els procediments de seguretat TIC, en els quals s'ha de concretar com s'ha de protegir el que estableixen les normes i les persones o rols responsables de la implantació, manteniment, revisió i seguiment d'aquestes normes.

2. S'ha d'assegurar la creació i la gestió de documents de seguretat del sistema autèntics, fiables, íntegres i utilitzables capaços de donar suport a les funcions i les activitats de seguretat TIC de la Universitat, durant el temps que sigui necessari, així com preservar-los.

3. Els documents seran públics llevat que el seu contingut faci difusió de dades personals o comporti un risc per a la seguretat dels sistemes. El seu format estarà en un estàndard obert.

El Comitè de Seguretat de la Informació estableix les limitacions a l'accés, ús i reutilització per a l'usuari o receptor d'aquests documents.

La revisió de cada document i la proposta de noves versions realitzada per qualsevol de les àrees afectades o pels òrgans de la Universitat s'han de notificar al responsable de Seguretat, que canalitzarà les propostes a través del Comitè de Seguretat de la Informació.

4. El Comitè de Seguretat de la Informació aprova les normatives i procediments de seguretat i altres documents derivats d'aquesta política.

Les noves versions de qualsevol d'aquests documents s'hauran de comunicar, segons el seu àmbit d'ús i el nivell de difusió que requereixin, de manera que el personal afectat sempre disposi de la darrera versió.

11. Obligacions del personal

Tots els membres de la UAB 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 les persones afectats.

Es formarà adequadament a tota la comunitat universitària en matèria de seguretat i protecció de dades i s'establirà un programa de conscienciació contínua per atendre tots els membres de la UAB, en particular els de nova incorporació. Les persones amb responsabilitat en l'ús, operació o administració de sistemes TIC rebran formació per al maneig segur dels sistemes. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seva primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en el mateix.

12. Terceres parts

Quan la UAB presti serveis a altres organismes o utilitzi informació d'altres organismes, els haurà de fer partícips d'aquesta política de seguretat de la informació, haurà d'establir canals per informar-ne els comitès de seguretat TIC respectius i coordinar-los, i haurà d'establir procediments d'actuació per reaccionar adequadament davant d'incidents de seguretat.

Quan la UAB utilitzi serveis de tercers o cedeixi informació a tercers, els haurà de fer partícips d'aquesta política de seguretat i de la normativa de seguretat relacionada amb aquests serveis o aquesta informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en la normativa esmentada i podrà desenvolupar procediments operatius propis per complir-la. S'hauran d'establir procediments específics per reportar i resoldre incidències. S'haurà de garantir que el personal de tercers està conscienciat adequadament en matèria de seguretat, si més no al mateix nivell que el que estableix aquesta política. Quan una tercera part no pugui satisfer algun aspecte d'aquesta política, segons el que estableixen els paràgrafs anteriors, el responsable de Seguretat haurà d'elaborar un informe en què especifiqui els riscos a què està exposada i la forma de tractar- los. Els responsables de la informació i els serveis afectats hauran d'aprovar aquest informe abans de seguir endavant.

13. Gestió del document de Política de Seguretat UAB

El Responsable de Seguretat ha d'elaborar les revisions d'aquest document per indicació del Comitè de Seguretat de la informació. El document haurà d'estar sempre actualitzat, mitjançant una revisió periòdica biennal, i s'haurà de revisar sempre que es produeixin canvis rellevants en els sistemes de tractament, en la informació tractada, en els sistemes d'informació o en l'organització de la UAB.

És responsabilitat del Comitè de Seguretat de la Informació la revisió d'aquest document, la proposta d'actualització o el manteniment, quan sigui necessari.
Es considera com a canvi rellevant qualsevol que pugui repercutir en el compliment de les mesures de seguretat implantades.

El contingut del document s'haurà d'adequar, sempre, a les disposicions vigents en la matèria de l'Esquema Nacional de Seguretat.
Tota nova versió d'aquest document s'haurà 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.

14. Resolució de controvèrsies

En cas de conflicte entre els diferents responsables, aquest es resoldrà pel superior jeràrquic dels mateixos. En defecte de l'anterior, prevaldrà la decisió el Comitè de Seguretat de la Informació de la UAB.

15. Aprovació i entrada en vigor

Aquesta Política de Seguretat entrarà en vigor des de la data d'aprovació pel Consell de Govern de la Universitat Autònoma de Barcelona (UAB).

Glossari de termes

Els termes de ciberseguretat es poden consultar als glossaris del Centres de Ciberseguretat de referència (Agència de ciberseguretat de Catalunya i Centro Criptológico Nacional). Particularment, alguns dels esmentats a aquest document:

Anàlisi de riscos
Utilització sistemàtica de la informació disponible per identificar perills i estimar els riscos.

Dades de caràcter personal
Qualsevol informació sobre una persona física identificada o identificable.

Delegat/da de protecció de dades
Persona designada o nomenada per la UAB per exercir les funcions establertes en l'article 39 del Reglament europeu de protecció de dades.

Gestió d'incidents
Pla d'acció per a atendre les incidències que es donen. A més de resoldre-les, ha d'incorporar mesures d'acompliment que permeten conèixer la qualitat del sistema de protecció i detectar tendències abans que es converteixin en grans problemes.

Gestió de riscos
Activitats coordinades per dirigir i controlar una organització respecte els riscos.

Incident de seguretat
Succés inesperat o no desitjat amb conseqüències que van en detriment de la seguretat del sistema d'informació, el servei o la informació en si mateixa.

Servei
Funció o prestació exercida per alguna entitat oficial destinada a cuidar interessos o a satisfer necessitats dels ciutadans.

Sistema d'informació
Conjunt organitzat de recursos perquè la informació es pugui recollir, emmagatzemar, processar o tractar, mantenir, usar, compartir, distribuir, posar a disposició, presentar o transmetre.

Historial de modificacions

Data	Versió	Autor	Descripció
	1	Comitè de Seguretat de l'ENS	Primera versió del document