Document pendent de revisió lingüística

UAB
Universitat Autònoma de Barcelona

Política de Seguretat de la Informació

Esquema Nacional de Seguretat

(Acord del Consell de Govern de 18 de desembre de 2023

UAB
Universitat Autònoma de Barcelona

Índex

Preàmbul

Aquest document està basat en la guia CCN-STIC 881 - Annex I. Política de Seguretat Universitats elaborada pel Centre Criptogràfic Nacional (CCN). Amb aquesta sèrie de guies, el Centre Criptogràfic Nacional, en compliment de les seves comeses i del reflectit en el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, contribueix a millorar la ciberseguretat i mantenir les infraestructures i els sistemes d'informació de totes les administracions públiques amb uns nivells òptims de seguretat.

Tot això amb la finalitat de generar confiança i garanties en l'ús d'aquestes tecnologies, protegint la confidencialitat de les dades i garantint la seva autenticitat, integritat i disponibilitat.

1. Legislació Aplicable

La present política de seguretat se situa dintre del marc jurídic definit per les lleis i reials decrets especificades en el document "Legislació Aplicable" revisat i aprovat periòdicament pel comitè de seguretat o bé quan existeixi qualsevol actualització de la legislació d'aplicació.

2. Declaració de la política de seguretat de la informació

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

Per fer front a aquestes amenaces es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn per a garantir la prestació contínua dels serveis. Això implica que les diferents unitats o òrgans administratius en que s'estructura i organitza la Universitat han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat (ENS), així com realitzar un seguiment continu dels nivells de prestació dels serveis, monitorar i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als ciberincidents per a garantir la continuïtat dels serveis prestats.

D'aquesta manera, totes les unitats administratives de la universitat tenen present que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la seva retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en els plecs de clàusules administratives particulars i de prescripcions tècniques de les licitacions per a projectes de TIC.

Per tant, per a la Universitat Autònoma de Barcelona, 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 per a detectar qualsevol incident i reaccionant amb prestesa als incidents

per a recuperar els serveis al més aviat possible, segons el que s'estableix en l'article 8 del ENS, amb l'aplicació de les mesures que es relacionen a continuació.

Prevenció

La Universitat 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

La Universitat Autònoma de Barcelona, estableix controls d'operació dels seus sistemes d'informació amb l'objectiu de detectar anomalies en la prestació dels serveis i actuar en conseqüència segons el que es disposa en l'article 10 de l'ENS (vigilància contínua i revaluació periòdica).

Quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com a normals (conforme a l'indicat en l'article 9 de l'ENS, Existència de línies de defensa), s'establiran els mecanismes de detecció, anàlisi i reporti necessaris perquè arribin als responsables regularment.

Resposta

La Universitat Autònoma de Barcelona, establirà les següents mesures:

- 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 i unitats universitàries o en altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en tots dos sentits, amb els Equips de Resposta a Emergències (CERT).

Recuperació

Per a garantir la disponibilitat dels serveis, la Universitat Autònoma de Barcelona, disposa dels mitjans i tècniques necessàries que permeten garantir la recuperació dels serveis més crítics.

3. Consecució de les finalitats de la Universitat

Per tal d'assolir les seves finalitats, la Universitat Autònoma de Barcelona posa a disposició de la ciutadania la realització de tràmits en línia i noves vies de participació que garanteixin el desenvolupament i l'eficàcia de les seves funcions.

En potenciar l'ús de les noves tecnologies en la Universitat Autònoma de Barcelona, es persegueix fomentar la relació electrònica de tots els estaments de la comunitat universitària (personal docent i/o investigador, estudiants i personal tècnic, de gestió i d'administració i de serveis).

4. Principis bàsics

Els principis bàsics són directrius fonamentals de seguretat que han de tenir-se sempre presents en qualsevol activitat relacionada amb l'ús dels actius d'informació. S'estableixen els següents:

- Abast estratègic: La seguretat de la informació ha de comptar amb el compromís i suport de tots els nivells directius de la universitat, de manera que pugui estar coordinada i integrada amb la resta de les iniciatives estratègiques de l'organització per a conformar un tot coherent i eficaç.
- Responsabilitat determinada: En els sistemes TIC s'identificarà el Responsable de la Informació, que determina els requisits de seguretat de la informació tractada; el Responsable del Servei, que determina els requisits de seguretat dels serveis prestats; el Responsable del Sistema, que té la responsabilitat sobre la prestació dels serveis i el Responsable de la Seguretat, que determina les decisions per a satisfer els requisits de seguretat.
- Seguretat integral: La seguretat s'entendrà com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius, relacionats amb els sistemes TIC, procurant evitar qualsevol actuació puntual o tractament conjuntural. La seguretat de la informació ha de considerar-se com a part de l'operativa habitual, sent present i aplicant-se des del disseny inicial dels sistemes TIC.
- Gestió de Riscos: L'anàlisi i gestió de riscos serà part essencial del procés de seguretat. La gestió de riscos permetrà el manteniment d'un entorn controlat, minimitzant els riscos fins a nivells acceptables. La reducció d'aquests nivells es realitzarà mitjançant el desplegament de mesures de seguretat que establiran un equilibri entre la naturalesa de les dades i els tractaments, l'impacte i la probabilitat dels riscos als quals estiguin exposats i l'eficàcia i el cost de les mesures de seguretat. En avaluar el risc en relació amb la seguretat de les dades, s'han de tenir en compte els riscos que es deriven del tractament de les dades personals.
- Proporcionalitat: L'establiment de mesures de protecció, detecció i recuperació haurà de ser proporcional als potencials riscos i al valor de la informació i dels serveis afectats.
- Millora contínua: Les mesures de seguretat es revaluaran i actualitzaran periòdicament per a adequar la seva eficàcia a la constant evolució dels riscos i sistemes de protecció. La seguretat de la informació serà atesa, revisada i auditada per personal qualificat, instruït i dedicat.
- Seguretat per defecte: Els sistemes han de dissenyar-se i configurar-se de manera que garanteixin un grau suficient de seguretat per defecte.

5. Objectius de la Seguretat de la Informació

La Universitat Autònoma de Barcelona, estableix com a objectius de la seguretat de la informació els següents:

- Garantir la qualitat i protecció de la informació.
- Aconseguir la plena conscienciació dels usuaris respecte a la seguretat de la informació.
- Gestió d'actius d'informació: Els actius d'informació de la universitat es trobaran inventariats i categoritzats i estaran associats a un responsable.
- Seguretat lligada a les persones: S'implantaran 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 del seu ús indegut, aconseguint la plena conscienciació dels usuaris respecte a la seguretat de la informació.
- Seguretat física: Els actius d'informació seran emplaçats en àrees segures, protegides per controls d'accés físics adequats al seu nivell de criticitat. Els sistemes i els actius d'informació

que contenen aquestes àrees estaran prou protegits enfront d'amenaces físiques o ambientals.

- Seguretat en la gestió de comunicacions i operacions: S'establiran els procediments necessaris per a aconseguir una adequada gestió de la seguretat, operació i actualització de les TIC. La informació que es transmeti a través de xarxes de comunicacions haurà de ser adequadament protegida, tenint en compte el seu nivell de sensibilitat i de criticitat, mitjançant mecanismes que garanteixin la seva seguretat.
- Control d'accés: Es limitarà l'accés als actius d'informació per part d'usuaris, processos i altres sistemes d'informació mitjançant la implantació dels mecanismes d'identificació, autenticació i autorització concordes a la criticitat de cada actiu. A més, quedarà registrada la utilització del sistema a fi d'assegurar la traçabilitat de l'accés i auditar el seu ús adequat, conforme a l'activitat de la Universitat.
- Adquisició, desenvolupament i manteniment dels sistemes d'informació: Es contemplaran els aspectes de seguretat de la informació en totes les fases del cicle de vida dels sistemes d'informació, garantint la seva seguretat per defecte.
- Gestió dels incidents de seguretat: S'implantaran els mecanismes apropiats per a la correcta identificació, registre i resolució dels incidents de seguretat.
- Garantir la prestació continuada dels serveis: S'implantaran els mecanismes apropiats per a assegurar la disponibilitat dels sistemes d'informació i mantenir la continuïtat dels seus processos, d'acord amb les necessitats de nivell de servei i de les persones usuàries.
- Protecció de dades: S'adoptaran les mesures tècniques i organitzatives que correspongui implantar per a atendre els riscos generats pel tractament per a complir la legislació de seguretat i privacitat.
- Compliment: S'adoptaran les mesures tècniques, organitzatives i procedimentals necessàries per al compliment de la normativa legal vigent en matèria de seguretat de la informació.

6. Àmbit d'aplicació

Aquesta Política s'aplicarà als sistemes d'informació de la Universitat Autònoma de Barcelona relacionats amb l'exercici de les seves competències i a totes les persones que els utilitzen amb accés autoritzat, siguin o no empleats públics i amb independència de la naturalesa de la seva relació jurídica amb la universitat.

Així mateix és aplicable a tota altre persona usuària dels sistemes d'informació de la Universitat, incloent-hi tot el personal de les empreses contractistes de la Universitat 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.

Tots ells tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la seva Normativa de Seguretat derivada, sent responsabilitat del Comitè de Seguretat TIC disposar els mitjans necessaris perquè la informació arribi al personal afectat.

7. Organització de la seguretat a la UAB

La Universitat Autònoma de Barcelona, tenint en compte el que s'estableix en l'avantdit Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), per a organitzar la seguretat de la informació emprendrà les següents accions:

i. Constituirà un òrgan consultiu i estratègic per a la presa de decisions en matèria de Seguretat de la Informació. Aquest òrgan es constituirà com un òrgan col·legiat i es denominarà Comitè de Seguretat de la Informació. Serà presidit per una persona física que serà la que assumirà la responsabilitat formal dels seus actes.

ii. Designarà rols de seguretat: Responsables dels Serveis, Responsables de la Informació, Responsable de la Seguretat, Responsable del Sistema i Delegat de protecció de dades.

7.1. Composició del Comitè de Seguretat de la Informació

El Comitè de Seguretat de la Informació està format per les següents persones:

- Rector/a qui pot delegar en el membre de l'equip de govern competent en matèria de Seguretat de la Informació o persona amb un càrrec equivalent, que n'exerceix la presidència.
- Secretari/ària general qui pot delegar en el/la cap del Gabinet Jurídic.
- Responsable de Seguretat: La persona designada per Gerència, que farà la funció de secretariat del comitè.
- Responsable de la Informació: Cap de l'Oficina de Govern de les Dades 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.

7.2. Funcions del Comitè de Seguretat de la Informació

Atribucions del Comitè de Seguretat de la Informació:

a) Estar permanentment informat de la normativa que regula la Certificació de Conformitat amb l'ENS, incloent-hi les seves normes d'acreditació, certificació, guies, manuals, procediments i instruccions tècniques.
b) Estar permanentment informat de la relació d'Entitats de Certificació acreditades i organitzacions, públiques i privades, certificades.
c) Estar permanentment informat de la relació d'esquemes de certificació de la seguretat amb els quals l'Administració Pública té establerts arranjaments o acords de reconeixement mutu de certificats.
d) Proposar directrius i recomanacions, que seran recollides en les corresponents actes de les reunions del Comitè de Seguretat de la Informació.
e) Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per a assegurar que aquests 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 la Universitat i de les seves diferents unitats o òrgans administratius, informant regularment de l'estat de la seguretat de la informació a la Direcció.
g) Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i/o entre diferents unitats o òrgans administratius, elevant aquells casos en els quals no tingui suficient autoritat per a decidir.
h) Assessorar en matèria de seguretat de la informació, sempre que li sigui requerit.
i) Revisar la Política de Seguretat de la Informació prèvia aprovació per l'Òrgan Superior.

j) Aprovar la Normativa d'Ús de Mitjans electrònics per a tots els membres de la comunitat universitària.
k) Aprovar el Mapa de Normativa amb la llista de Normativa i Procediments de seguretat per a la implantació de l'ENS.

Periodicitat de les reunions i adopció d'acords:

1. Durant el desenvolupament del Projecte d'Adequació a l'ENS, per a avaluar el desenvolupament del mateix i possibilitar el seu adequat seguiment, el Comitè de Seguretat de la Informació es reunirà, almenys, una vegada al trimestre.
2. Una vegada aconseguida la Certificació de Conformitat amb l'ENS dels serveis prestats per la Universitat, el Comitè de Seguretat TIC es reunirà, almenys, dues vegades a l'any, sense perjudici que, en atenció a les necessitats derivades del compliment dels seus fins i atribucions, requereixi d'una major freqüència en les reunions.
3. En qualsevol cas, les reunions es convocaran per la seva Presidència, a través del/ de la Secretari/ària, a la seva iniciativa o a sol·licitud de la majoria dels seus membres permanents.
4. Les decisions s'adoptaran per consens dels membres permanents.

7.3. Rols de seguretat: funcions i responsabilitats

Responsables de la Informació i dels Serveis

- Establir i elevar per a la seva aprovació al Comitè de Seguretat de la Informació 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 RD ENS, podent recaptar una proposta del Responsable de Seguretat i tenint en compte l'opinió del Responsable del Sistema.
- Dictaminar respecte als drets d'accés a la informació i als serveis.
- Acceptar els nivells de risc residual que afecten la informació i els serveis.
- Posar en comunicació del Responsable de Seguretat qualsevol variació respecte a la Informació i els Serveis dels quals és responsable, especialment la incorporació de nous Serveis o Informació al seu càrrec. El qual donarà trasllat d'aquests canvis, al Comitè de Seguretat de la Informació, en la seva pròxima reunió.
- Comunicar al delegat de protecció de dades quan els incidents de seguretat puguin afectar a dades de caràcter personal.

Responsable de Seguretat

- Mantenir i verificar el nivell adequat de seguretat de la Informació tractada i dels Serveis electrònics prestats pels sistemes d'informació.
- Promoure la formació i conscienciació en matèria de seguretat de la informació.
- Designar responsables de l'execució de l'anàlisi de riscos, de la Declaració d'Aplicabilitat, identificar mesures de seguretat, determinar configuracions necessàries, elaborar documentació del sistema.
- Proporcionar assessorament per a la determinació de la Categoria del Sistema, en col·laboració amb el Responsable del Sistema i/o Comitè de Seguretat de la Informació.
- Participar en l'elaboració i implantació dels plans de millora de la seguretat i, arribat el cas, en els plans de continuïtat, procedint a la seva validació.
- Gestionar les revisions externes o internes del sistema.
- Gestionar els processos de certificació.
- Elevar al Comitè de Seguretat l'aprovació de canvis i altres requisits del sistema.

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

Responsable del Sistema

- Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida, elaborant els procediments operatius necessaris.
- Definir la topologia i la gestió del Sistema d'Informació establint els criteris d'ús i els serveis disponibles en aquest.
- Detenir l'accés a informació o prestació de servei si té el coneixement que aquests presenten deficiències greus de seguretat.
- Cerciorar-se que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.
- Proporcionar assessorament per a la determinació de la Categoria del Sistema, en col·laboració amb el Responsable de Seguretat i/o Comitè de Seguretat de la Informació.
- Participar en l'elaboració i implantació dels plans de millora de la seguretat i arribat el cas en els plans de continuïtat.
- Dur a terme, en el seu cas, les funcions de l'administrador de la seguretat del sistema:
    - La gestió, configuració i actualització, en el seu cas, del maquinari i programari en els quals es basen els mecanismes i serveis de seguretat.
    - La gestió de 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 seva correspondència amb l'autoritzat.
    - Aprovar els canvis en la configuració vigent del Sistema d'Informació.
    - Assegurar que els controls de seguretat establerts són complerts estrictament.
    - Assegurar que són aplicats els procediments aprovats per a manejar el Sistema d'Informació.
    - Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per a assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
    - Monitorar l'estat de seguretat proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica.
    - Informar el Responsable de Seguretat de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
    - Col·laborar en la recerca i resolució d'incidents de seguretat, des de la seva detecció fins a la seva resolució.

Quan la complexitat del sistema ho justifiqui, el Responsable del Sistema podrà designar els responsables de sistema delegats que consideri necessaris, que en tindran dependència funcional directa i seran responsables en el seu àmbit de totes aquelles accions que els delegui el mateix. D'igual manera, també podrà delegar en un/s altre/s funcions concretes de les responsabilitats que se li atribueixen.

Delegat de protecció de dades

- Informar i assessorar a la Universitat de Autònoma de Barcelona, i a les persones usuàries que s'ocupin del tractament, de les obligacions que els incumbeixen en virtut de la normativa vigent en matèria de Protecció de Dades.
- Supervisar el compliment del que es disposa en normativa de seguretat i de les polítiques internes de la Universitat Autònoma de Barcelona, en matèria de protecció de dades, inclosa

l'assignació de responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament, i les auditories corresponents.
- Oferir l'assessorament que se li sol·liciti sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar la seva aplicació.
- Cooperar amb l'Autoritat Catalana de Protecció de Dades quan aquesta ho requereixi, actuant com a punt de contacte amb aquesta per a qüestions relatives al tractament de dades.
- Exercir les seves funcions parant esment als riscos associats a les operacions de tractament. Per a això ha de ser capaç de:
    - Recaptar informació per a determinar les activitats de tractament.
    - Analitzar i comprovar la conformitat de les activitats de tractament.
    - Informar, assessorar i emetre recomanacions al responsable o l'encarregat del tractament.
    - Recaptar informació per a supervisar el registre de les operacions de tractament.
    - Assessorar en el principi de la protecció de dades per disseny i per defecte.
    - Assessorar sobre si es duu a terme o no les avaluacions d'impacte, metodologia, salvaguardes a aplicar, etc.
    - Prioritzar activitats sobre la base dels riscos.
    - Assessorar el Responsable de Tractament sobre àrees a realitzar auditories i activitats de formació i operacions de tractament a dedicar més temps i recursos.

Unitat de Seguretat Informàtica

La Unitat de Seguretat Informàtica presta serveis de ciberseguretat, desenvolupant la capacitat de vigilància i detecció d'amenaces en l'operació diària dels sistemes TIC, alhora que millora la capacitat de resposta del sistema davant qualsevol atac. Per a la seva composició es proposa:

- Cap de projectes de la Unitat de Seguretat Informàtica, que actuarà com a enllaç, a través del Responsable de Seguretat, amb el Comitè de Seguretat TIC.
- Responsable de Seguretat (RSEG).
- Responsables tècnics especialistes TIC-seguretat informàtica.

La Unitat de Seguretat Informàtica desenvolupa les següents funcions:

- Vigilar i monitorar la seguretat dels sistemes, i dels dispositius de defensa, ja sigui mitjançant interfícies previstes o instal·lant les corresponents sondes. Per a això es valdrà tant d'eines gestionades per la pròpia Unitat de Seguretat Informàtica com de les gestionades pels equips de la Unitat d'Operacions i Sistemes i de la Unitat de Comunicacions.
- Analitzar i correlar els esdeveniments de seguretat i registres d'activitat dels sistemes.
- Realitzar operacions de seguretat sobre els dispositius de defensa.
- Realitzar un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions respecte d'ells.
- Comunicar al Delegat de protecció de dades quan els incidents de seguretat puguin afectar a dades de caràcter personal.
- Proveir el Servei d'Alerta Primerenca d'alertes de seguretat en les xarxes corporatives i en les connexions a Internet dels sistemes.
- Gestionar les vulnerabilitats (anàlisis i determinació de les accions d'esmena/posat de pegats) d'aplicacions i serveis.
- Fer les anàlisis forenses digitals i de seguretat quan s'escaigui.
- Proveir de servei de cibervigilància que possibiliti la prospectiva sobre la ciberamenaça.

Addicionalment, es troben les següents competències, relacionades amb les següents àrees de treball: adequació a l'ENS, normativa i gestió de riscos, anàlisis i millora contínua, seguretat en les interconnexions i connectivitat i altres funcions derivades del reial decret:

- Gestió i operativa de la seguretat del Projecte d'adequació, implantació i gestió de la Conformitat en el ENS, anàlisi i gestió de riscos, explotació, normativa i manteniment.
- Redacció i presentació de propostes al Comitè de Seguretat TIC. Elaborarà els aspectes relacionats amb la ciberseguretat i els debatrà en primera instància, per a ser traslladats al Comitè de Seguretat TIC a través del Responsable de Seguretat.
- Promoció de la millora contínua del sistema de gestió de la Seguretat de la Informació. Per a això s'encarregarà de:
    - Revisar regularment la Política de Seguretat de la Informació per al seu trasllat al Comitè de Seguretat TIC per a la seva revisió i posterior aprovació de l'òrgan superior.
    - Col·laborar en l'elaboració de la normativa de Seguretat de la Informació per a la seva aprovació pel Responsable de Seguretat, amb coneixement del Comitè de Seguretat TIC.
    - Verificar els procediments de seguretat de la informació i altra documentació per a la seva aprovació.
    - Col·laborar en l'elaboració de programes de formació destinats a formar i sensibilitzar al personal en matèria de seguretat de la informació i protecció de dades.
    - Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de seguretat de la informació.
    - Proposar plans de millora de la seguretat de la informació, prioritzant les actuacions en matèria de seguretat quan els recursos siguin limitats.
    - Realitzar un seguiment dels principals riscos residuals assumits i recomanar possibles actuacions respecte d'ells.
    - Promoure la realització de les auditories periòdiques ENS i RGPD que permetin verificar el compliment de les obligacions de la universitat en matèria de seguretat de la Informació i protecció de dades.

7.4. Procediments de designació

La creació del Comitè de Seguretat de la Informació, el nomenament dels seus integrants, excepte els que siguin per raó del càrrec, i la designació dels Responsables identificats en aquesta Política, es realitzarà pel rector de la Universitat Autònoma de Barcelona per un període de 4 anys renovable.

7.5. Mecanismes de coordinació i assessorament

El Comitè de Seguretat de la Informació estarà assistit per personal tècnic dels àmbits de la UAB:

- Jurídic.
- Arquitectura i Logística.
- Economia.
- Organització.
- DTIC (Direcció de Tecnologia de la Informació i la Comunicació).

8. Dades de caràcter personal

La Universitat Autònoma de Barcelona només recollirà i tractarà dades personals quan els tractaments siguin adequats, pertinents i no excessius i aquests es trobin en relació amb l'àmbit i les finalitats per

als quals s'hagin obtingut. D'igual manera, adoptarà les mesures d'índole tècnica i organitzatives necessàries per al compliment de la normativa de Protecció de Dades.

La Universitat Autònoma de Barcelona publicarà en la Seu Electrònica la seva Política de Privacitat.

El personal de la Universitat Autònoma de Barcelona ha d'estar assabentat de l'obligació de llegir i complir la Política de Protecció de Dades descrita al Web Institucional de la UAB.

9. Gestió de riscos

Tots els sistemes afectats per la present Política de Seguretat de la Informació estan subjectes a una anàlisi de riscos amb l'objectiu d'avaluar les amenaces i els riscos als quals estan exposats. Aquesta anàlisi es repetirà:

- Quan canviïn la informació i/o els serveis de manera significativa.
- Quan esdevingui un incident greu de seguretat o es detectin vulnerabilitats greus.

El Responsable de la Seguretat serà l'encarregat que es realitzi l'anàlisi de riscos, així com d'identificar mancances i febleses i posar-les en coneixement del Comitè de Seguretat de la Informació.

El Comitè de Seguretat de la Informació dinamitzarà la disponibilitat de recursos per a atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

El procés de gestió de riscos comprendrà les següents fases:

- Categorització dels sistemes.
- Anàlisi de riscos.
- El Comitè de Seguretat de la Informació procedirà a la selecció de mesures de seguretat a aplicar que hauran de ser proporcionals als riscos i estar justificades.
- Les fases d'aquest procés es realitzaran segons el que es disposa en els Annexos I i II del Reial decret 311/2022, de 8 de gener, i seguint les normes, instruccions, Guies CCN-STIC i recomanacions per a l'aplicació del mateix elaborades pel Centre Criptològic Nacional.

En particular, per a realitzar l'anàlisi de riscos, com a norma general s'utilitzarà una metodologia reconeguda d'anàlisi i gestió de riscos.

10. Gestió d'incidents de seguretat

De conformitat amb el que es disposa en l'article 33 del RD 311/2022, de 3 de maig, la Universitat Autònoma de Barcelona, notificarà al Centre Criptològic Nacional aquells incidents que tinguin un impacte significatiu en la seguretat de la informació tractada o en els serveis prestats. Aquesta notificació pot fer-se a través de l'Agència de Ciberseguretat de Catalunya, el CERT de referència de la Universitat.

S'ha d'informar internament al Delegat de protecció de dades quan els incidents de seguretat puguin afectar a dades de caràcter personal, perquè, en el cas que afectin, es realitzi la notificació a l'Autoritat Catalana de Protecció de Dades en un termini de 72 hores.

11. Desenvolupament de la política de seguretat de la informació

La present Política de Seguretat de la Informació serà complementada per mitjà de diversa normativa i recomanacions de seguretat (normatives i procediments de seguretat, procediments tècnics de seguretat, informes, registres i evidències electròniques). Correspon al Comitè de Seguretat de la Informació la seva revisió i/o manteniment, proposant-hi, en cas que sigui necessari, millores.

El cos normatiu sobre seguretat de la informació es desenvoluparà 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 desenvolupament es fonamenti en les normes de nivell superior. Aquests nivells de desenvolupament normatiu són els següents:

a) Primer nivell normatiu: constituït per la present Política de Seguretat de la Informació, la Normativa Interna de l'Ús dels Mitjans Electrònics i les directrius generals de seguretat aplicables a les unitats o òrgans administratius de la universitat als quals sigui d'aplicació aquests documents.
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, complint amb l'exposat en la Política de Seguretat de la Informació, determinen les accions o tasques a realitzar en l'acompliment d'un procés.

Correspon al Consell de Govern de la Universitat Autònoma de Barcelona l'aprovació de la Política de Seguretat de la Informació, sent el Comitè de Seguretat de la Informació l'òrgan responsable de l'aprovació dels restants documents, sent també responsable de la seva difusió perquè la coneguin les parts afectades.

De la mateixa manera, la present Política de Seguretat de la Informació complementa la Política de Privacitat de la Universitat Autònoma de Barcelona, en matèria de protecció de dades.

La normativa de seguretat i, molt especialment, la Política de seguretat de la Informació i la Normativa Interna de l'Ús dels Mitjans Electrònics, serà coneguda i estarà a la disposició de tots els membres de la universitat, en particular per a aquells que utilitzin, operin o administrin els sistemes d'informació i comunicacions. Estarà disponible per a la seva consulta en el portal de la Universitat.

Els procediments de seguretat estaran disponibles en zona restringida.

12. Obligacions del personal

Tot el personal de la Universitat Autònoma de Barcelona, comprès dins de l'àmbit de l'ENS, atendrà en la mesura del possible, una o diverses sessions de conscienciació en matèria de seguretat i protecció de dades, almenys una vegada a l'any. S'establirà un programa de conscienciació contínua per a atendre a tot el personal, en particular al de nova incorporació.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes d'informació rebran formació per al maneig segur dels sistemes en la mesura en què la necessitin per a fer el seu treball. En la mesura del possible, 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 aquest.

13. Terceres parts

Quan la Universitat Autònoma de Barcelona, presti serveis a altres entitats o tracti informació d'altres organismes, se'ls farà partícip d'aquesta Política de Seguretat de la Informació. S'establiran canals per al reporti i la coordinació dels respectius Comitès de Seguretat de la Informació i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.

Quan la Universitat Autònoma de Barcelona utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícip d'aquesta Política de Seguretat i de la normativa de seguretat que concerneixi a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, podent desenvolupar els seus propis procediments operatius per a satisfer-la. S'establiran procediments específics de reporti i resolució d'incidències. Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta Política de Seguretat.

Quan algun aspecte d'aquesta Política de Seguretat de la Informació no pugui ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que precisi els riscos en què s'incorre i la manera de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir endavant.

14. Millora contínua

La gestió de la seguretat de la informació és un procés subjecte a permanent actualització. Els canvis en la Universitat, les amenaces, les tecnologies i/o la legislació són un exemple en els quals és necessària una millora contínua dels sistemes. Per això, és necessari implantar un procés permanent que comportarà, entre altres accions:

a) Revisió de la Política de Seguretat de la Informació.
b) Revisió dels serveis i informació i la seva categorització.
c) Execució de l'anàlisi de riscos.
d) Realització d'auditories internes o, quan procedeixin, externes.
e) Revisió de les mesures de seguretat.
f) Revisió i actualització de les normes i procediments.

15. Aprovació i entrada en vigor

Text aprovat el dia 18 de desembre de 2023 per Acord del Consell de Govern de la Universitat Autònoma de Barcelona.

Aquesta “Política de Seguretat de la Informació”, d'ara endavant Política, serà efectiva des de la seva data d'aprovació i fins que sigui reemplaçada per una nova Política.

Historial de modificacions

Data	Versió	Autor	Descripció
11/03/2020	1	Comitè de Seguretat de l’ENS	Primera versió del document

18/12/2023	2	Comitè de Seguretat de la informació	Actualització del document