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 3
1. Legislació aplicable 3
2. Declaració de la política de seguretat de la informació 3
Prevenció 3
Detecció 4
Resposta 4
Recuperació 4
3. Consecució de les finalitats de la Universitat 4
4. Principis bàsics 4
5. Objectius de la seguretat de la informació 5
6. Àmbit d'aplicació 6
7. Organització de la seguretat a la UAB 6
7.1. Composició del Comitè de Seguretat de la Informació 6
7.2. Funcions del Comitè de Seguretat de la Informació 7
7.3. Rols de seguretat: funcions i responsabilitats 8
Responsables de la informació i dels serveis 8
Responsable de seguretat 8
Responsable del sistema 8
Delegat de protecció de dades 9
Unitat de Seguretat Informàtica 10
7.4. Procediments de designació 11
7.5. Mecanismes de coordinació i assessorament 11
8. Dades de caràcter personal 11
9. Gestió de riscos 11
10. Gestió d'incidents de seguretat 12
11. Desenvolupament de la política de seguretat de la informació 12
12. Obligacions del personal 13
13. Terceres parts 13
14. Millora contínua 14
15. Aprovació i entrada en vigor 14
Historial de modificacions 14

Preàmbul

Aquest document es basa en la *Guía de Adecuación al ENS para Universidades* (CCN-STIC 881), especialment en l'annex primer, sobre la política de seguretat per a les universitats, elaborada pel Centre Criptogràfic Nacional (CCN). Amb aquesta sèrie de guies, el CCN, en compliment de les seves comeses i del que estipula el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), contribueix a millorar la ciberseguretat i a 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, de protegir la confidencialitat de les dades i de garantir-ne l'autenticitat, integritat i disponibilitat.

1. Legislació aplicable

La present política de seguretat se situa dins del marc jurídic definit per les lleis i reials decrets especificats al document Legislació aplicable, adjunt al present instrument, revisat i aprovat periòdicament pel Comitè de Seguretat, i incorpora les actualitzacions de la legislació que s'hi aplica.

2. Declaració de la política de seguretat de la informació

La Universitat Autònoma de Barcelona depèn, entre d'altres, de les tecnologies de la informació i la comunicació (TIC) per a aconseguir els seus objectius. Aquests sistemes s'han d'administrar 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, de manera que sempre han d'estar 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 dels 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 què s'estructura i organitza la Universitat han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat (ENS), i també han de fer un seguiment continu dels nivells de prestació dels serveis, monitorar i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als ciberincidents per garantir la continuïtat dels serveis prestats.

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

Per tant, per a la Universitat Autònoma de Barcelona, l'objectiu de la política de seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuar preventivament, supervisar l'activitat diària per detectar qualsevol incident i reaccionar amb prestesa als incidents per recuperar els serveis al més aviat possible, segons el que s'estableix a l'article 8 de l'ENS, amb l'aplicació de les mesures descrites 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 quedin 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, així com 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 manera rutinària.
- S'ha de sol·licitar que terceres parts 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 a 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'han d'establir els mecanismes de detecció, anàlisi i report necessaris perquè arribin als responsables regularment.

Resposta

La Universitat Autònoma de Barcelona ha d'establir les mesures següents:

- 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 informàtiques (CERT).

Recuperació

Per 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 garanteixen el desenvolupament i l'eficàcia de les seves funcions.

Amb la potenciació de l'ús de les noves tecnologies a la Universitat Autònoma de Barcelona es vol fomentar la relació electrònica de tots els estaments de la comunitat universitària (personal docent i 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 s'han de tenir 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 conformar un tot coherent i eficaç.
- Responsabilitat determinada: en els sistemes TIC s'ha d'identificar 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 adients per satisfer els requisits de seguretat.

- Seguretat integral: la seguretat s'entén com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius relacionats amb els sistemes TIC, i que procura evitar qualsevol actuació puntual o tractament conjuntural. La seguretat de la informació s'ha de considerar com a part de l'operativa habitual, i ha d'estar present i s'ha d'aplicar des del disseny inicial dels sistemes TIC.
- Gestió de riscos: l'anàlisi i la gestió de riscos són parts essencials del procés de seguretat. La gestió de riscos permet mantenir un entorn controlat i minimitzar els riscos fins a nivells acceptables. La reducció d'aquests nivells es fa mitjançant el desplegament de mesures de seguretat que estableixin 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. Quan s'avaluï 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 ha de ser proporcional als potencials riscos i al valor de la informació i dels serveis afectats.
- Millora contínua: les mesures de seguretat s'han de revaluar i actualitzar periòdicament per adequar-ne l'eficàcia a la constant evolució dels riscos i dels sistemes de protecció. La seguretat de la informació l'ha d'atendre, revisar i auditar personal qualificat, instruït i dedicat.
- Seguretat per defecte: els sistemes s'han de dissenyar i configurar 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 que la seguretat de la informació té els objectius següents:

- Garantia de la qualitat i la protecció de la informació.
- Plena conscienciació dels usuaris respecte a la seguretat de la informació.
- Gestió d'actius d'informació: els actius d'informació de la Universitat han d'estar inventariats i categoritzats i han d'estar associats a un responsable.
- Seguretat lligada a les persones: s'han d'implantar els mecanismes necessaris perquè qualsevol persona que accedeixi o pugui accedir als actius d'informació conegui les seves responsabilitats, i que d'aquesta manera es redueixi el risc derivat d'un ús indegut i s'aconsegueixi la plena conscienciació dels usuaris respecte a la seguretat de la informació.
- Seguretat física: els actius d'informació s'han d'emplaçar 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 han d'estar prou protegits d'amenaces físiques o ambientals.
- Seguretat en la gestió de comunicacions i operacions: s'han d'establir els procediments necessaris per aconseguir una adequada gestió de la seguretat, operació i actualització de les TIC. La informació que es transmeti a través de xarxes de comunicacions ha d'estar protegida adequadament, tenint en compte el seu nivell de sensibilitat i de criticitat, mitjançant mecanismes que en garanteixin la seguretat.
- Control d'accés: s'ha de limitar 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, ha de quedar registrada la utilització del sistema a fi d'assegurar la traçabilitat de l'accés i auditar-ne l'ús adequat conforme a l'activitat de la Universitat.
- Adquisició, desenvolupament i manteniment dels sistemes d'informació: s'han de preveure els aspectes de seguretat de la informació en totes les fases del cicle de vida dels sistemes d'informació i garantir-ne la seguretat per defecte.
- Gestió dels incidents de seguretat: s'han d'implantar els mecanismes apropiats per a la correcta identificació, registre i resolució dels incidents de seguretat.

- Garantir la prestació continuada dels serveis: s'han d'implantar els mecanismes apropiats per 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'han d'adoptar les mesures tècniques i organitzatives que correspongui implantar per atendre els riscos generats pel tractament per complir la legislació de seguretat i privacitat.
- Compliment: s'han d'adoptar les mesures tècniques, organitzatives i procedimentals necessàries per complir la normativa legal vigent en matèria de seguretat de la informació.

6. Àmbit d'aplicació

Aquesta política s'ha d'aplicar 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 altra persona usuària dels sistemes d'informació de la Universitat, incloent-hi tot el personal de les empreses contractistes de la Universitat que tinguin un equip connectat a la xarxa o que 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 tenen l'obligació de conèixer i complir aquesta Política de seguretat de la informació i la Normativa de seguretat derivada, i és responsabilitat del Comitè de Seguretat TIC disposar dels 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 al Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS) -endavant, **'RD 311/2022'**-, ha d'emprendre les accions següents per organitzar la seguretat de la informació:

i. Constituir un òrgan consultiu i estratègic per a la presa de decisions en matèria de seguretat de la informació. Aquest òrgan s'ha de constituir com un òrgan col·legiat, amb la denominació de Comitè de Seguretat de la Informació. L'ha de presidir una persona física que assumeixi la responsabilitat formal dels seus actes.

ii. Designar 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 persones següents:

- Rector o rectora, que pot delegar en el membre de l'Equip de Govern competent en matèria de Seguretat de la Informació o en la persona amb un càrrec equivalent, que n'exerceix la presidència.
- Secretari o secretària general, que pot delegar en el cap o la cap del Gabinet Jurídic.

- Responsable de seguretat: la persona designada per Gerència, que fa la funció de secretaria 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 o directora de Tecnologies de la Informació i la Comunicació.
- Administrador o administradora del sistema: responsable de la Unitat de Producció TIC.
- Delegat o delegada de Protecció de Dades.

7.2. Funcions del Comitè de Seguretat de la Informació

Les atribucions del Comitè de Seguretat de la Informació són les següents:

a) Estar permanentment informat 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 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 acords de reconeixement mutu de certificats.
d) Proposar directrius i recomanacions, que s'han de recollir 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 assegurar que siguin consistents i alineats amb l'estratègia decidida en la matèria i per 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 o entre diferents unitats o òrgans administratius, i elevar aquells casos en els quals no tingui prou 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 a l'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 les normatives 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, el Comitè de Seguretat de la Informació s'ha de reunir, com a mínim, una vegada al trimestre per a avaluar-ne el desenvolupament i possibilitar-ne un seguiment adequat.
2. Una vegada aconseguida la certificació de conformitat amb l'ENS dels serveis prestats per la Universitat, el Comitè de Seguretat TIC s'ha de reunir, com a mínim, dues vegades a l'any, sense perjudici que, en atenció a les necessitats derivades del compliment dels seus fins i atribucions, calgui augmentar la freqüència de les reunions.
3. En qualsevol cas, les reunions les convoca el president o presidenta del Comitè a través del secretari o secretària, a iniciativa seva o a sol·licitud de la majoria dels membres permanents.

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

7.3. Rols de seguretat: funcions i responsabilitats

Responsables de la informació i dels serveis

- Establir i elevar, perquè el Comitè de Seguretat de la Informació els aprovin, 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 a l'Annex I del RD 311/2022 , si cal amb 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, i traslladar aquests canvis al Comitè de Seguretat de la Informació en la seva pròxima reunió.
- Comunicar al delegat de protecció de dades els incidents de seguretat que puguin afectar 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 la conscienciació en matèria de seguretat de la informació.
- Designar responsables de l'execució de l'anàlisi de riscos i de la declaració d'aplicabilitat, identificar mesures de seguretat, determinar configuracions necessàries i elaborar documentació del sistema.
- Proporcionar assessorament per determinar la categoria del sistema, en col·laboració amb el responsable del sistema o el Comitè de Seguretat de la Informació.
- Participar en l'elaboració i la implantació dels plans de millora de la seguretat i, si escau, en els plans de continuïtat, i procedir a validar-los.
- 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 que no són competència del Comitè) i posar en coneixement del Comitè les modificacions que s'hagin fet al llarg del període en curs.

Responsable del sistema

- Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida i elaborar els procediments operatius necessaris.
- Definir la topologia i la gestió del sistema d'informació i establir els criteris d'ús i els serveis disponibles.
- Aturar l'accés a la informació o la prestació de servei si té el coneixement que aquests presenten deficiències greus de seguretat.
- Cerciorar-se que les mesures específiques de seguretat s'integren adequadament dins del marc general de seguretat.
- Proporcionar assessorament per determinar la categoria del sistema, en col·laboració amb el responsable de seguretat o el Comitè de Seguretat de la Informació.

- Participar en l'elaboració i la implantació dels plans de millora de la seguretat i, si escau, en els plans de continuïtat.
- Dur a terme, si escau, les funcions de l'administrador de la seguretat del sistema:
  - Gestionar, configurar i actualitzar, si escau, el maquinari i programari en els quals es basen els mecanismes i serveis de seguretat.
  - 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 seva correspondència amb l'autoritzat.
  - Aprovar els canvis en la configuració vigent del sistema d'informació.
  - Assegurar que els controls de seguretat establerts es compleixen estrictament.
  - Assegurar que s'apliquen els procediments aprovats per gestionar el sistema d'informació.
  - Supervisar les instal·lacions de maquinari i programari, i les modificacions i millores que s'hi facin, per 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 detecció fins a la resolució.

Quan la complexitat del sistema ho justifiqui, el responsable del sistema pot designar els responsables de sistema delegats que consideri necessaris, que en tenen dependència funcional directa i són responsables en el seu àmbit de totes les accions que els delegui. Igualment, també pot delegar en altres persones 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 dades, de les obligacions que els incumbeixen en virtut de la normativa vigent en matèria de protecció de dades.
- Supervisar el compliment del que disposen la normativa de seguretat i les polítiques internes de la Universitat Autònoma de Barcelona en matèria de protecció de dades, incloent-hi 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-ne l'aplicació.
- Cooperar amb l'Autoritat Catalana de Protecció de Dades quan aquesta ho requereixi i actuar 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 la qual cosa ha de ser capaç de:
  - Recollir informació per determinar les activitats de tractament.
  - Analitzar i comprovar la conformitat de les activitats de tractament.
  - Informar i assessorar el responsable o l'encarregat del tractament i emetre recomanacions.
  - Recollir informació per 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 duen a terme o no les avaluacions d'impacte, metodologia, salvaguardes que cal aplicar, etc.
  - Prioritzar activitats sobre la base dels riscos.

  - Assessorar el responsable del tractament sobre les àrees on cal fer auditories i les activitats de formació i operacions de tractament en que cal dedicar més temps i recursos.

Unitat de Seguretat Informàtica

La Unitat de Seguretat Informàtica presta serveis de ciberseguretat i desenvolupa 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 de qualsevol atac. Es proposa que tingui la composició següent:

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

La Unitat de Seguretat Informàtica desenvolupa les funcions següents:

- Vigilar i monitorar la seguretat dels sistemes i dels dispositius de defensa, ja sigui mitjançant interfícies previstes o instal·lant les sondes corresponents. Per a fer-ho ha d'emprar tant eines gestionades per la Unitat de Seguretat Informàtica com eines gestionades pels equips de la Unitat d'Operacions i Sistemes i de la Unitat de Comunicacions.
- Analitzar i correlar els esdeveniments de seguretat i els registres d'activitat dels sistemes.
- Dur a terme operacions de seguretat sobre els dispositius de defensa.
- Fer un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions a partir d'aquestes.
- Comunicar al delegat de protecció de dades els incidents de seguretat que puguin afectar 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 d'aplicacions i serveis (anàlisi i determinació de les accions d'esmena/aplicació de pedaços).
- Fer les anàlisis forenses digitals i de seguretat quan s'escaigui.
- Proveir un servei de cibervigilància que possibiliti la prospectiva sobre les ciberamenaces.

Addicionalment hi ha altres competències relacionades amb les àrees de treball següents: adequació a l'ENS, normativa i gestió de riscos, anàlisis i millora contínua, seguretat en les interconnexions i connectivitat i altres funcions derivades del RD 311/2022:

- Gestió i operativa de la seguretat del projecte d'adequació, implantació i gestió de la conformitat amb l'ENS, anàlisi i gestió de riscos, explotació, normativa i manteniment.
- Redacció i presentació de propostes al Comitè de Seguretat TIC. Ha d'elaborar els aspectes relacionats amb la ciberseguretat i debatre'ls en primera instància, per tal que el responsable de seguretat els traslladi al Comitè de Seguretat TIC.
- Promoció de la millora contínua del sistema de gestió de la seguretat de la informació. S'encarrega de:
  - Revisar regularment la Política de seguretat de la informació i traslladar al Comitè de Seguretat TIC les revisions proposades per la seva revisió i posterior aprovació per part de l'òrgan superior competent.
  - Col·laborar en l'elaboració de la normativa de seguretat de la informació perquè l'aprovi el responsable de seguretat, amb coneixement del Comitè de Seguretat TIC.

- Verificar els procediments de seguretat de la informació i altra documentació perquè s'aprovi.
- 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 la seguretat de la informació.
- Proposar plans de millora de la seguretat de la informació i prioritzar les actuacions en matèria de seguretat quan els recursos siguin limitats.
- Fer un seguiment dels principals riscos residuals assumits i recomanar possibles actuacions.
- Promoure auditories periòdiques de l'aplicació de l'ENS i del Reglament general de protecció de dades (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 la duu a terme el rector o rectora 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 està assistit per personal tècnic dels àmbits de la UAB següents:

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

8. Dades de caràcter personal

La Universitat Autònoma de Barcelona només ha de recollir i tractar dades personals quan els tractaments siguin adequats, pertinents i no excessius i estiguin relacionats amb l'àmbit i les finalitats per als quals s'han obtingut. D'igual manera, ha d'adoptar les mesures d'índole tècnica i organitzatives necessàries per al compliment de la normativa de protecció de dades. La Universitat Autònoma de Barcelona ha de publicar a 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 s'ha de repetir:

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

El responsable de la seguretat és l'encarregat que es dugui a terme 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 ha de dinamitzar la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes i promoure inversions de caràcter horitzontal.

El procés de gestió de riscos, que es duu a terme segons el que es disposa als annexos I i II del RD 311/2022, i seguint les normes, instruccions, guies CCN-STIC i recomanacions per a l'aplicació d'aquest procés elaborades pel Centre Criptològic Nacional, comprèn les fases següents:

- Categorització dels sistemes.
- Anàlisi de riscos.
- Selecció de mesures de seguretat que cal aplicar, les quals han de ser proporcionals als riscos i estar justificades, per part del Comitè de Seguretat de la Informació.

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

10. Gestió d'incidents de seguretat

De conformitat amb el que es disposa a l'article 33 del RD 311/2022, la Universitat Autònoma de Barcelona ha de notificar 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 es pot fer 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 dades de caràcter personal, perquè, si és així, faci 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 es complementa per mitjà de diferents normatives 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 revisar-la i mantenir-la, i proposar-hi millores, si escau.

El cos normatiu sobre seguretat de la informació es desenvolupa 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 fonamenta 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 que reguli l'ús de recursos i sistemes d'informacióq de la UAB i les directrius

generals de seguretat aplicables a les unitats o òrgans administratius de la Universitat als quals és aplicable 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, d'acord amb la Política de seguretat de la informació, determinen les accions o tasques que cal dur a terme 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. El Comitè de Seguretat de la Informació és l'òrgan responsable de l'aprovació dels restants documents, i també és responsable de fer-ne 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 el Reglament d'ús dels mitjans electrònics en l'àmbit de la UAB, l'ha de conèixer tots els membres de la Universitat i ha d'estar a la seva disposició, en particular per a aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions. Ha d'estar disponible perquè es pugui consultar al portal de la Universitat. Els procediments de seguretat han d'estar disponibles en una zona restringida del web.

12. Obligacions del personal

Tot el personal de la Universitat Autònoma de Barcelona comprès dins de l'àmbit de l'ENS ha de participar, en la mesura del possible, en 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 contínua per a tot el personal, en particular per al de nova incorporació.

Les persones amb responsabilitat en l'ús, l'operació o l'administració de sistemes d'informació han de rebre formació per al maneig segur dels sistemes en la mesura en què la necessitin per a fer la seva feina. En la mesura del possible, la formació ha de ser obligatòria abans d'assumir una responsabilitat, tant si és la seva primera assignació com si es tracta d'un canvi de lloc de treball o de responsabilitats.

13. Terceres parts

Quan la Universitat Autònoma de Barcelona presti serveis a altres entitats o tracti informació d'altres organismes els ha de fer partícips d'aquesta Política de seguretat de la informació. S'han d'establir canals per a reportar i coordinar els respectius comitès de seguretat de la informació i s'han d'establir procediments d'actuació per reaccionar davant d'incidents de seguretat.

Quan la Universitat Autònoma de Barcelona utilitzi serveis de tercers o cedeixi informació a tercers, els ha de fer partícips d'aquesta Política de seguretat i de la normativa de seguretat relativa a aquests serveis o informació. Aquesta tercera part queda subjecta a les obligacions establertes en aquesta normativa, i pot desenvolupar els seus propis procediments operatius per a satisfer-la. S'han d'establir procediments específics per a reportar i resoldre incidències. S'ha de garantir 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 de la Política de seguretat de la informació no pugui ser satisfet per una tercera part d'acord amb el que es requereix en els paràgrafs anteriors, cal un informe del responsable de seguretat que detalli els riscos en què s'incorre i la manera de tractar-los. Cal l'aprovació d'aquest informe per part dels 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 una actualització permanent. Els canvis en la Universitat, les amenaces, les tecnologies i la legislació són exemples en els quals és necessària una millora contínua dels sistemes. Per això cal implantar un procés permanent que inclou, entre altres, les accions següents:

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, si escau, 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.

La present Política de seguretat de la informació és efectiva des de la data d'aprovació i fins que sigui reemplaçada per una de nova.

Historial de modificacions

Data	Versió	Autor	Descripció
11.3.2020	1	Comitè de Seguretat de l'ENS	Primera versió del document
18.12.2023	2	Comitè de Seguretat de la Informació	Actualització del document