POLÍTICA DE SEGURETAT DE LA INFORMACIÓ DE LA FUNDACIÓ UNIVERSITÀRIA BALMES

Aprovada pel Consell de Govern de la UVic-UCC el 22/10/25 i per la Comissió Executiva del Patronat de la Fundació Universitària Balmes el 27/10/25

FUB

FUNDACIÓ
UNIVERSITÀRIA
BALMES

Preàmbul

La informació constitueix un actiu fonamental per a la Fundació Universitària Balmes (FUBalmes), per al desenvolupament de les seves activitats i per a la confiança de la comunitat universitària, col·laboradors i altres parts interessades. En un entorn cada vegada més digitalitzat i interconnectat, protegir la confidencialitat, integritat i disponibilitat de la informació és una responsabilitat estratègica i operativa.

Aquesta Política de seguretat de la informació estableix el marc general per garantir la protecció dels actius d'informació, mitjançant l'aplicació de mesures tècniques, organitzatives i procedimentals adequades. L'objectiu és prevenir i minimitzar els riscos derivats d'amenaces internes i externes, complint els requisits legals i normatius aplicables, com ara el Reglament general de protecció de dades (RGPD), la Llei orgànica de protecció de dades personals i garantia dels drets digitals (LOPDGDD), la norma ISO/IEC 27001 i el Reial decret 311/2022, de 3 de maig, pel que es regula l'Esquema Nacional de Seguretat (ENS), principalment.

Aquesta Política és d'aplicació a tota la comunitat universitària que depèn de la FUBalmes, així com a tercers que accedeixin o gestionin informació de l'organització, i forma part del compromís continu de millora de la gestió de la seguretat de la informació.

Primer. Objecte

Aquesta Política té com a finalitat protegir la informació, els sistemes informàtics i la infraestructura tecnològica de la Fundació Universitària Balmes (FUBalmes).

L'objecte principal és prevenir incidents que posin en risc la disponibilitat, integritat, confidencialitat, autenticitat i traçabilitat de la informació i els serveis digitals.

Segon. Àmbit d'aplicació

Aquesta Política és d'aplicació obligatòria per a:

a) La comunitat universitària vinculada a la FUBalmes.
b) Qualsevol persona que utilitzi els sistemes d'informació de la FUBalmes.
c) Persones o empreses externes que col·laborin amb la Fundació mitjançant la prestació de serveis o altres tipus de relació que suposi l'accés a serveis digitals.
d) Totes les instal·lacions i tots els dispositius que accedeixin als sistemes d'informació de la FUBalmes.

Tercer. Objectius i actuacions per a la seguretat de la informació

Els objectius principals per a la seguretat de la informació són:

a) Contribuir als objectius de la Fundació mitjançant una gestió eficaç de la seguretat.
b) Complir la normativa legal, especialment pel que fa a la protecció de dades personals i serveis digitals.
c) Garantir la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de la informació.
d) Protegir els recursos tecnològics davant de qualsevol amenaça, interna o externa. Aquesta protecció s'ha d'integrar des del disseny fins a la retirada dels sistemes de les TIC i incloure els requisits de seguretat en la planificació, adquisició i operació dels projectes tecnològics.
e) Assegurar la qualitat de la informació i la prestació constant dels serveis.
f) Fomentar la conscienciació de tot el personal en matèria de seguretat.
g) Protegir la informació davant de danys accidentals o intencionats.
h) Assegurar la continuïtat dels serveis, responent als incidents amb agilitat.
i) Actuar de forma preventiva, detectant anomalies i responent-hi amb rapidesa, aplicant les mesures adequades, tal com es preveu a l'Esquema Nacional de Seguretat (ENS), o altres protocols que es creguin convenients.

Quart. Principis bàsics i directrius de la seguretat de la informació

4.1. Principis bàsics

Aquests principis són la base per garantir un ús segur i responsable de la informació i dels sistemes.

a) Seguretat com a part integral: la seguretat s'ha d'aplicar a totes les etapes i els processos relacionats amb la informació i els sistemes de les TIC, des del disseny fins a la retirada.
b) Diverses línies de defensa: cal implementar diferents capes de seguretat, com la física, lògica i organitzativa, per reduir els riscos i fer front als incidents amb eficàcia.
c) Vigilància i actualització contínua: els sistemes han d'estar en constant supervisió per detectar-hi anomalies i adaptar-se als nous riscos. La seguretat es revisa i s'audita periòdicament per personal qualificat.
d) Assignació clara de responsabilitats: tothom ha de conèixer el seu rol en matèria de seguretat. Es designen responsables específics per a la informació, els serveis, els sistemes i la seguretat.
e) Gestió de riscos: els riscos es gestionen per reduir-los a nivells acceptables, aplicant mesures adequades en funció del valor de la informació, l'impacte dels riscos i el cost de les solucions. També es tenen en compte els riscos derivats del tractament de dades personals.

4.2. Criteris d'actuació

S'ha de donar compliment als principis esmentats prenent en consideració les directrius o criteris que es relacionen a continuació:

a) Proporcionalitat i gestió del risc: les mesures de seguretat s'apliquen segons el risc i l'impacte potencial.
b) Acceptació dels riscos: només es poden acceptar riscos amb l'aprovació d'un nivell directiu competent.
c) Propietat i classificació: tota la informació ha de tenir un responsable que la classifiqui i en controli l'accés.
d) Accés per necessitat: només accedeix a la informació qui realment ho necessita per la seva feina.

e) Qualitat i responsabilitat: la informació, especialment la digital, ha de ser fiable, precisa i protegida.
f) Compliment legal: s'ha de seguir la normativa vigent en matèria de seguretat i protecció de dades.
g) Formació i conscienciació: s'ha de promoure el coneixement de les bones pràctiques i els protocols de seguretat entre tots els usuaris.
h) Ús legítim: els recursos de les TIC només poden utilitzar-se per a finalitats relacionades amb les activitats de la Fundació.
i) Separació de funcions: s'assignen responsabilitats diferenciades per evitar conflictes d'interès i millorar la seguretat.
j) Seguiment i auditories: es fa un control continu del sistema de seguretat i es fan auditories per millorar-lo.

Cinquè. Àmbits d'actuació per garantir la seguretat de la informació

5.1. Tipus d'accions per garantir la seguretat

Són actuacions de prevenció, detecció, resposta i recuperació de la informació.

5.1.1. Prevenció:

a) Es defineixen i documenten les responsabilitats i mesures de seguretat.
b) Els sistemes es revisen abans de posar-los en funcionament.
c) Es fan avaluacions periòdiques de seguretat, també per part d'auditors externs.

5.1.2. Detecció:

a) Es monitoritzen els sistemes per detectar-hi anomalies.
b) S'analitzen i informen els incidents als responsables quan hi ha desviacions de funcionament significatives.

5.1.3. Resposta:

a) Es defineixen mecanismes per actuar davant d'incidents.
b) S'estableixen punts de contacte interns i externs.
c) Es creen protocols per compartir informació amb equips d'emergència.

5.1.4. Recuperació:

Es desenvolupen plans de recuperació de la informació per garantir la continuïtat dels serveis crítics com a part del pla general de continuïtat del negoci.

5.2. Àmbits d'actuació:

a) Gestió dels actius: tots els actius d'informació estan inventariats i tenen un responsable assignat.
b) Seguretat vinculada a les persones: s'assegura que tothom conegui les seves responsabilitats per reduir riscos.
c) Seguretat física: els espais amb informació crítica disposen de controls d'accés físic adequats.
d) Gestió operativa i de comunicacions: es protegeixen les comunicacions i es garanteix el correcte funcionament de les TIC.
e) Control d'accés: l'accés a la informació es limita i es registra per garantir-ne un ús correcte.
f) Cicle de vida dels sistemes: la seguretat s'aplica en totes les fases dels sistemes d'informació.
g) Gestió d'incidents: es disposa de mecanismes per detectar, registrar i resoldre incidents de manera eficient.
h) Continuïtat del servei: es garanteix la disponibilitat dels sistemes d'informació per assegurar la continuïtat dels serveis d'acord amb els nivells requerits pels usuaris.
i) Protecció de dades: es prenen les mesures necessàries per protegir les dades personals i complir la legislació vigent.
j) Compliment normatiu: es despleguen accions per garantir l'adequació legal en matèria de seguretat de la informació.

Sisè. Organització de la seguretat de la informació

D'acord amb la normativa aplicable i per donar compliment als objectius i principis de la seguretat de la informació, la Fundació disposa d'una estructura de supervisió i coordinació de la seguretat que s'organitza de la següent manera:

6.1. Comissió Executiva del Patronat

La Comissió Executiva és el màxim òrgan responsable d'establir i aprovar els requisits de seguretat per aconseguir els objectius de seguretat de les TIC a curt, mitjà i llarg termini, i establir els mecanismes necessaris per verificar i supervisar la implementació de les accions per garantir aquesta seguretat.

Les seves funcions principals són:

a) Ésser la responsable que la FUBalmes aconsegueixi els objectius de seguretat de les TIC a curt, mitjà i llarg termini.
b) Donar suport explícit a la FUBalmes per les activitats de seguretat de les TIC.
c) Expressar les seves inquietuds quant a la seguretat de la informació al Comitè de Seguretat de les TIC.
d) Aprovar la Política de seguretat de la FUBalmes.
e) Delegar el seguiment de la seguretat en el Comitè de Seguretat de les TIC.

6.2. Comitè de Seguretat de les TIC (COMSEGTIC)

6.2.1. Les funcions principals són:

a) Coordinar i divulgar la Política de seguretat.
b) Proposar normatives i canvis al Consell de Govern o al Patronat.
c) Supervisar auditories i aprovar procediments operatius.
d) Assessorar i informar sobre l'estat de la seguretat de la Fundació.
e) Estar informat sobre la normativa i certificacions en seguretat (ENS, acreditacions, acords).
f) Proposar directrius i recomanacions per millorar la seguretat.

g) Coordinar les àrees internes per garantir la coherència de l'actuació i evitar duplicacions.

h) Gestionar conflictes de responsabilitat i assessorar sobre seguretat.

i) Revisar, coordinar i divulgar la Política i normativa de seguretat.

j) Aprovar plans i requisits de seguretat, així com nivells de risc.

6.2.2. Composició:

a) Presidència: director o directora general, o persona en qui delegui.

b) Secretaria: responsable de seguretat, o persona en qui delegui.

c) Vocals permanents: responsable de la informació, responsable del servei, responsable del sistema, responsable de seguretat i delegat de protecció de dades (DPD).

d) Assistents: persones convidades pel president o presidenta amb veu però sense vot.

6.2.3. Règim de funcionament

Es reuneix a instància del seu president o presidenta tantes vegades com faci falta, i també a petició del responsable de seguretat de la informació.

En qualsevol cas, es reuneix de forma ordinària dues vegades l'any, una el primer semestre i una el segon, i, de manera extraordinària, tantes vegades com calgui, a instància del president o presidenta o de la persona responsable de seguretat de la informació.

Les decisions es prenen per consens dels membres.

6.3. Responsables segons els diferents rols de seguretat

6.3.1. Responsabilitat de la informació

- Rol: definir els requisits de seguretat de la informació.
- Responsable: el secretari o secretària general de la Fundació o persona en qui delegui.
- Funcions:
  - Defineix els requisits de seguretat de la informació.
  - Vetlla pel bon ús i integritat de les dades.
  - Col·labora amb els responsables de seguretat i sistemes en la gestió dels sistemes segons l'ENS.
  - Informa de canvis al Comitè.

6.3.2. Responsabilitat del servei

- Rol: definir els requisits de seguretat dels serveis prestats.
- Responsable: el gerent o gerenta o persona en qui delegui.
- Funcions:
  - Defineix els requisits de seguretat dels serveis de les TIC.
  - Col·labora en la gestió i el manteniment dels sistemes.
  - Garanteix l'existència de clàusules de seguretat en contractes amb tercers.

6.3.3. Responsabilitat de seguretat

- Rol: vetllar per la seguretat global de la informació, decidir els requisits de seguretat de la informació i dels serveis, supervisar la implantació de les mesures necessàries per garantir que se satisfacin els requisits, sense dependència jeràrquica del responsable del sistema.
- Responsable: persona designada pel director o directora general.
- Funcions:
  - Manté i verifica la seguretat dels sistemes de les TIC.
  - Participa en plans de millora i continuïtat.
  - Fomenta la formació i les auditories periòdiques.
  - Aprova canvis rellevants segons el risc.
  - Supervisa incidents i assessora sobre la categoria del sistema.
  - Coordina la documentació, les revisions i les certificacions.
  - Informa la resta de membres del Comitè i promou la millora contínua.

6.3.4. Responsabilitat del sistema

- Rol: aplicar i supervisar la seguretat dels sistemes de les TIC.
- Responsable: el director o directora de l'Àrea de les TIC.
- Funcions:
  - Desenvolupa, manté i supervisa el sistema de les TIC al llarg del seu cicle de vida.
  - Aprova canvis i configura el sistema (hardware/software).
  - Implanta mesures específiques de seguretat.
  - Realitza l'anàlisi i la gestió de riscos.
  - Determina la categoria del sistema segons l'ENS.
  - Pot suspendre serveis si hi ha riscos greus (amb acord dels altres responsables). Pot delegar responsabilitats en funció de la complexitat del sistema.

6.3.5. Delegat de protecció de dades (DPD)

- Rol: vetllar pel compliment de la normativa de protecció de dades personals dins de l'organització.
- Funcions:
  - Informar i assessorar la Fundació i els usuaris sobre les seves obligacions segons la normativa de protecció de dades.
  - Supervisar el compliment de la normativa de seguretat i les polítiques internes, incloent la formació i les auditories.
  - Assessorar en l'avaluació d'impacte de protecció de dades i supervisar-ne l'aplicació.
  - Cooperar i ser el punt de contacte amb l'Autoritat Catalana de Protecció de Dades.
  - Proposar l'adopció de mesures tècniques i organitzatives per complir la normativa per tal que tots els sistemes compleixen amb els nivells de seguretat exigits segons la naturalesa de les dades.

– Redactar i proposar l'aprovació del registre d'activitats de tractament a la web, amb tota la informació legal.

Setè. Obligacions dels empleats

Sense perjudici de l'assignació de rols i responsabilitats segons l'estructura organitzativa establerta en aquest document, tots els empleats de la Fundació són responsables del correcte tractament de les dades personals dins del seu àmbit d'activitat, han de conèixer les directrius de seguretat establertes per les TIC i els procediments de la seva competència, i estan obligats a informar de qualsevol incident de seguretat observat durant la seva activitat laboral diària, sent compromisos inherents a les seves obligacions laborals. Específicament s'estableix que:

a) La Política de seguretat de la informació s'aplica a tots els empleats, col·laboradors i personal amb accés a la xarxa o recursos tecnològics.
b) Tots els empleats han de conèixer i complir la Política i normatives de seguretat.
c) S'ha de garantir que la informació arribi a tothom.
d) Cal promoure la difusió i la formació per conscienciar sobre seguretat, especialment per a noves incorporacions.
e) En qualsevol cas, els empleats amb funcions vinculades als sistemes de les TIC han de rebre formació adequada per fer-ne un ús segur.

Vuitè. Gestió de riscos

Tots els sistemes han de passar per una anàlisi de riscos per identificar amenaces i vulnerabilitats.

Aquesta anàlisi es fa:

a) Com a mínim cada 2 anys.
b) Quan canvien les dades o els serveis.
c) Quan hi ha incidents greus o s'hi detecten vulnerabilitats.

El responsable de seguretat fa l'anàlisi i n'informa al Comitè.

El Comitè assigna recursos i decideix mesures proporcionals als riscos.

El procés segueix la normativa i guies oficials com el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat i el Centre Criptològic Nacional.

Es fa servir una metodologia reconeguda per a l'anàlisi i la gestió de riscos.

Novè. Desenvolupament de la Política de seguretat

La Política de seguretat de la informació es complementa amb normatives i recomanacions tècniques.

El Comitè de Seguretat estableix els criteris i la periodicitat de revisió de la Política de seguretat de la informació, efectua propostes de millora i estructura els nivells de la normativa aplicable a la Fundació. Totes aquestes mesures han de ser aprovades pel Patronat o per la seva Comissió Executiva.

La seguretat de la informació és un procés en constant evolució que s'adapta als canvis organitzatius, tecnològics, legislatius i a les amenaces mitjançant actuacions de revisió de la política de seguretat, anàlisis anuals de riscos, auditories internes o externes, revisió i actualització de serveis, mesures, normes i procediments, i altres accions que es creguin oportunes.

La normativa està disponible al Campus Virtual de la UVic.

Desè. Aprovació i entrada en vigor

Aquesta Política de seguretat de la informació (PSI) entra en vigor després de la seva aprovació i corresponent publicació.