UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Política de seguretat de la informació de la UPC

Acord CG/2023/07/34, de 5 de juliol de 2023, del Consell de Govern, pel qual s'aprova la política de seguretat de la informació de la UPC

Vicerector d'Estratègia Digital

- Document amb l'informe favorable de la Comissió d'Economia i Infraestructures de 27/06/2023

Acord de Consell d'actualització de la Política de Seguretat de la Informació

FETS I FONAMENTS DE DRET

La UPC disposa d'una política de seguretat de la informació, en el context de l'ENS (Esquema Nacional de Seguretat), aprovada per Consell de Govern CG 04/2019 a 4 de juliol de 2019. Tanmateix, aquesta política requereix una revisió, i si cal una modificació bianual. El propi ENS va ser modificat en el RD 311/2022.

L'actualització que es proposa ara introdueix un canvi principal en definir un Comitè tècnic addicional i més operatiu que el Comitè de Seguretat de l'ENS.

Aquesta introducció es fa necessària en el context actual, amb atacs molt més freqüents i de més envergadura, que requereixen un seguiment i atenció més continuats. A més a més, es fan canvis menors per tal d'adaptar la nova política a l'actualització de l'ENS.

En virtut del que precedeix, el Consell de Govern, en exercici de les funcions que li atorguen l'article 59 dels vigents estatuts i l'article 46 de la Llei orgànica dels Sistema Universitari, adopta el següent

ACORD

Primer. Aprovar l'actualització de la Política de Seguretat de la Informació

Segon. Aquest reglament entrarà en vigor l'endemà del dia que l'aprovi el Consell de Govern.

Barcelona, 5 de juliol de 2023

ÍNDEX

0. Preàmbul

L'**Esquema Nacional de Seguretat** (ENS) està constituït pels principis bàsics i requisits mínims que permetin una protecció adequada de la informació de les entitats del sector públic.

El principal requisit de l'ENS és que cada administració pública disposi d'una Política de Seguretat de la informació, que contingui el conjunt de directrius que regeixen la forma en què es gestiona i es protegeix la informació que tracta, així com els serveis que presta.

1. Entrada en vigor

Text aprovat el dia XX de juliol de 2023 pel Consell de Govern de la Universitat Politècnica de Catalunya.
Aquesta política de seguretat de la informació és efectiva des d'aquesta data i fins que sigui reemplaçada per una nova política.

2. Declaració de la política de seguretat de la informació

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

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

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

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

La UPC ha d'assegurar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida dels sistemes, des que es conceben fins que es retiren del servei, incloent-hi les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les seves necessitats de finançament han d'estar identificats i s'han d'incloure en la planificació, en la sol·licitud d'ofertes i en els plecs de licitació per als projectes TIC.

La UPC ha d'estar preparada per prevenir i detectar incidents de seguretat, i per reaccionar-hi i recuperar-se'n, d'acord amb el que s'estableix en l'ENS.

2.1. Prevenció

La UPC 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 dins la Universitat, han d'estar clarament definits i documentats.

Per tal de garantir el compliment de la política:

- El Responsable del Sistema ha 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.

2.2. Detecció

Com que els serveis poden degradar-se ràpidament a causa d'incidents, amb conseqüències que poden anar des d'una simple desacceleració fins a l'aturada, s'ha de monitorar el funcionament d'aquests serveis de manera continuada per detectar anomalies en els nivells de prestació dels serveis i actuar-hi en conseqüència.

S'han d'establir mecanismes de detecció d'incidents i vulnerabilitats, anàlisi i report que arribin als responsables amb regularitat i quan es produeixi una desviació significativa dels paràmetres que s'hagin establert prèviament com a normals.

2.3. Resposta

La UPC ha de:

- Establir mecanismes per respondre eficaçment als incidents de seguretat.
- Designar un punt de contacte per a les comunicacions respecte dels incidents en matèria de seguretat de la informació detectats.

- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions a les autoritats competents en la matèria, en tots dos sentits, amb els equips de resposta a emergències (CERT, de l'anglès *computer emergency response team*).

2.4. Recuperació

Per garantir la disponibilitat dels serveis crítics, la UPC ha de desenvolupar plans de continuïtat dels sistemes TIC com a part del seu pla general de continuïtat del negoci i les activitats de recuperació.

3. Abast

L'objectiu d'aquesta política de seguretat de la informació és protegir els membres de la comunitat universitària UPC d'accions il·legals o perjudicials d'individus, sigui conscientment o inconscientment.

Aquesta política de seguretat està elaborada d'acord amb l'anàlisi de riscos i de vulnerabilitats dels serveis i infraestructures informàtiques de la institució; per tant, l'abast d'aquesta política està subjecta als actius de la Universitat.

S'inclouen en l'abast d'aquesta política els sistemes afectats per l'ENS, és a dir, els sistemes relacionats amb l'exercici de drets per mitjans electrònics, amb el compliment dels deures per mitjans electrònics i amb l'accés a la informació o al procediment administratiu.

4. Missió

La missió de la UPC és contribuir a la construcció d'un món sostenible i just, mitjançant la recerca, la transferència de tecnologia, la difusió del coneixement i la formació de professionals en enginyeria, arquitectura, ciència i tecnologia amb esperit crític i capacitat per treballar en equips interdisciplinaris i multiculturals, adaptar-se als canvis i aprendre al llarg de la vida.

5. Marc normatiu

Aquesta política se situa dintre del marc jurídic definit per les lleis i reials decrets que s'especifiquen al registre Politica de Seguretat de la Informació: Registre normativa aplica…

6. Organització de la seguretat

6.1. Comitè de Seguretat de la Informació: funcions i responsabilitats

El **Comitè de Seguretat de la Informació** coordina la seguretat de la informació i dels serveis a la Universitat Politècnica de Catalunya, i està format per les persones següents:

- **Responsable de la Informació**: la persona titular de la Secretaria General.
- **Responsable del Servei**: la persona titular de la Gerència de la Universitat.
- **Responsable de Seguretat**: la persona designada pel rector o rectora.
- **Responsable del Sistema**: la persona de l'equip de Gerència responsable de l'àmbit TIC.
- El delegat o delegada de Protecció de Dades, nomenat pel rector o rectora.
- La persona titular del vicerectorat que s'ocupi de les polítiques TIC o la persona en qui delegui el rector o rectora aquestes polítiques.
- La persona de l'equip de Gerència responsable de l'àmbit jurídic.
- La persona de l'equip de Gerència responsable de l'àmbit d'organització.

El Comitè de Seguretat de la Informació ha de nomenar un secretari o secretària, que tindrà les funcions següents:

- Convocar les reunions del Comitè de Seguretat de la Informació.
- Preparar els temes que s'han de tractar en les reunions del Comitè, sobre les quals ha d'aportar informació concreta per a la presa de decisions.
- Elaborar l'acta de les reunions.
- Executar directament o per delegació les decisions del Comitè.

El Comitè de Seguretat de la Informació ha de reportar al rector o rectora els resultats de la coordinació en matèria de seguretat de la informació.

El Comitè de Seguretat de la Informació té les funcions següents:

- Divulgar la política i les normatives de seguretat TIC de la UPC.
- Aprovar la política i les normatives de seguretat TIC de la UPC.
- Revisar la política de seguretat de la informació, proposar que el Consell de Govern l'aprovi, i fer-ne difusió perquè la coneguin totes les parts afectades.
- Desenvolupar el procediment de designació de rols.
- Designar els rols i responsabilitats.
- Supervisar i aprovar les tasques de seguiment de l'Esquema Nacional de Seguretat: tasques d'adequació, anàlisi de riscos i auditoria bianual.

6.2. Rols: funcions i responsabilitats

Les funcions i responsabilitats dels membres del Comitè estan definides per garantir-ne la necessària independència i l'absència de conflicte d'interessos.

Responsable de la Informació

El responsable de la Informació de la UPC té les funcions següents:

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

Responsable dels Serveis

El responsable dels Serveis de la UPC té les funcions següents:

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

Responsable de Seguretat[1]

El responsable de Seguretat de la UPC té les funcions següents:

- Mantenir la seguretat de la informació que tracten i els serveis que presten els sistemes TIC en el seu àmbit de responsabilitat.
- Realitzar o promoure les auditories periòdiques que permetin verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Promoure la formació i conscienciació del personal TIC dins del seu àmbit de responsabilitat.
- Verificar que les mesures de seguretat establertes són adequades per a la protecció de la informació que es tracta i els serveis que es presten.
- Analitzar, completar i aprovar tota la documentació relacionada amb la seguretat dels sistemes.

[1] En el cas que la figura del Responsable de Seguretat depengui jeràrquicament del Responsable del Sistema es garantirà la independència de les seves decisions.

- Monitorar l'estat de seguretat dels sistemes proporcionat per les eines de gestió d'esdeveniments de seguretat i els mecanismes d'auditoria implementats en els sistemes.
- Donar suport a la investigació dels incidents de seguretat, des que es notifiquen fins que es resolen, i supervisar-la.
- Elaborar l'informe periòdic de seguretat per al responsable del Sistema, que ha d'incloure els incidents més rellevants del període.
- Aprovar els procediments de seguretat elaborats pel responsable del Sistema.
- Elaborar la normativa de seguretat de l'entitat.

Responsable del Sistema

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

- Desenvolupar, fer funcionar i mantenir el sistema durant tot el seu cicle de vida, incloent-ne la instal·lació i la verificació del funcionament correcte i el seguiment de les especificacions.
- Definir la topologia i els procediments de gestió del sistema, i establir-ne els criteris d'ús i els serveis disponibles.
- Definir la política de connexió o desconnexió d'equips i usuaris nous en el sistema.
- Aprovar els canvis que afecten la seguretat del mode d'operació del sistema.
- Decidir les mesures de seguretat que hauran d'aplicar els subministradors de components del sistema durant les etapes de desenvolupament, instal·lació i prova.
- Implantar i controlar les mesures específiques de seguretat del sistema i assegurar-se que aquestes s'integrin adequadament dins del marc general de seguretat.
- Determinar la configuració autoritzada del hardware i el software que s'han d'utilitzar en el sistema.
- Aprovar tota modificació substancial de la configuració de qualsevol element del sistema.
- Portar a terme el procés preceptiu d'anàlisi i de gestió de riscos en el sistema.
- Determinar la categoria del sistema segons el procediment descrit a l'annex I de l'ENS i determinar les mesures de seguretat que han d'aplicar-s'hi segons el que es descriu a l'annex II de l'ENS.
- Elaborar la documentació de seguretat del sistema.
- Delimitar les responsabilitats de cada entitat involucrada en el manteniment, explotació, implantació i supervisió del sistema.
- Vetllar pel compliment de les obligacions de l'administrador de seguretat del sistema (ASS).

- Investigar els incidents de seguretat que afectin el sistema i, si s'escauen, comunicar-los al responsable de Seguretat o a qui s'hagi determinat.
- Establir plans de contingència i emergència, i dur a terme de manera freqüent exercicis per al personal perquè s'hi familiaritzi.
- A més, el responsable del Sistema pot decidir la suspensió de l'ús d'una certa informació o la prestació d'un cert servei si se l'informa de deficiències greus de seguretat que puguin afectar la satisfacció dels requisits establerts. Aquesta decisió ha de ser consultada amb els responsables de la informació afectada i del servei afectat, i amb el suport del responsable de Seguretat abans d'executar-la.
- Elaborar els procediments de seguretat necessaris per a l'operativa del sistema.

6.3. Comitè Tècnic de Seguretat de la Informació: funcions i responsabilitats

El Comitè Tècnic de Seguretat coordina la seguretat a un nivell més detallat, àgil i continu que el comitè principal.

Les seves funcions principals són:

- Aprovar Instruccions i Procediments de seguretat.
- Proposar Normatives de seguretat
- Revisar la resolució dels incidents més greus.
- Revisar la correcció de les vulnerabilitats greus dels pentests.

Està format per les persones següents:

- Responsable de Seguretat.
- Responsable del Sistema.
- El delegat o delegada de Protecció de Dades.
- La persona titular del vicerectorat que s'ocupi de les polítiques TIC o la persona en qui delegui el rector o rectora aquestes polítiques.

Addicionalment pot convidar com a consultors:

- Proveïdors i experts en seguretat.
- Membres de la comunitat per debatre l'impacte de les normatives, instruccions i procediments.

7. Gestió de riscos

Per tots els sistemes subjectes a aquesta política s'ha de realitzar una anàlisi de riscos, en què s'avaluïn les amenaces i els riscos als quals estan exposats. Aquesta anàlisi s'ha de repetir:

- Regularment, com a mínim cada 2 anys.
- Quan canviï el tipus d'informació que es gestioni.
- Quan canviïn els serveis prestats.
- Quan s'esdevingui un incident greu de seguretat.
- Quan es reportin vulnerabilitats greus.

Per tal d'harmonitzar les anàlisis de riscos, el Comitè de Seguretat de la Informació ha d'establir una valoració de referència per als diferents tipus d'informació que s'utilitzen i els diferents serveis prestats. El Comitè de Seguretat de la Informació ha de dinamitzar la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

8. Dades de caràcter personal

Quan els sistemes d'informació tractin dades personals, els hi serà d'aplicació la normativa vigent en matèria de protecció de dades, així com els criteris que estableixin les autoritats de control competents. En aquests casos, de forma prèvia a la realització de les operacions que comportin tractament de dades personals, la Universitat elaborarà una anàlisi de riscos o una avaluació d'impacte relativa a la protecció de dades amb l'assessorament del seu delegat/da de protecció de dades. D'aquesta manera, la Universitat determinarà les mesures i els mecanismes necessaris per afrontar els riscos detectats i garantir-ne la protecció.

A aquests efectes, també s'haurà de tenir en compte la normativa interna de la Universitat en matèria de protecció de dades.

9. Directrius per la documentació de seguretat del sistema, com gestionar-la i accedir-hi

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

La UPC estructura la documentació de seguretat TIC en tres tipus de documents:

- La present **política de seguretat de la informació**, que estableix els requisits i criteris de seguretat TIC en l'àmbit de la Universitat i que serveix de guia per a la creació de normes de seguretat (apartat 13 d'aquest document).
- Les **normatives de seguretat**, que defineixen què cal protegir i els requisits de seguretat TIC necessaris (apartat 10 d'aquest document).
- Els **procediments de seguretat TIC**, en els quals s'ha de concretar com s'ha de protegir el que estableixen les normes i les persones o rols responsables de la implantació, manteniment, revisió i seguiment d'aquests procediments.

El Comitè de Seguretat de la Informació aprova les normatives i procediments de seguretat descrits anteriorment.

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

La revisió de cada document i la proposta de noves versions realitzada per qualsevol de les àrees afectades o pels òrgans de la Universitat s'han de notificar al responsable de Seguretat, que canalitzarà les propostes a través del Comitè de Seguretat de la Informació. Les noves versions de qualsevol d'aquests documents s'hauran de comunicar, segons el seu àmbit d'ús i el nivell de difusió que requereixin, de manera que el personal afectat pugui eliminar les versions obsoletes.

10. Desenvolupament de la política de seguretat

Aquesta política de seguretat de la informació complementa les polítiques de seguretat de la UPC en diferents matèries, com ara aquelles establertes en matèria de protecció de dades.

S'han de desenvolupar per mitjà de normatives, instruccions i procediments de seguretat que afrontin aspectes específics. Les normatives de seguretat hauran d'estar a disposició de tots els membres de la UPC que necessitin conèixer-les, en particular per al personal que utilitzi, faci funcionar o administri els sistemes d'informació i comunicacions.

Les normatives de seguretat hauran d'estar disponibles a la intranet corporativa, a l'adreça següent: https://serveistic.upc.edu/ca/politiques-i-normatives.

11. Obligacions del personal i usuaris

Aquesta política és aplicable a tots els membres la comunitat universitària (el personal d'administració i serveis, el personal de docència i investigació i l'estudiantat), a qualsevol persona externa que faci ús dels sistemes o els recursos de la Universitat i a les persones físiques i/o jurídiques que prestin serveis o proveeixin solucions a la Universitat. Aquesta

política és aplicable també a tots els equips i serveis de propietat, arrendats o contractats que, d'alguna manera, hagin d'utilitzar localment o remotament la xarxa o recursos tecnològics de la institució, així com els serveis i l'intercanvi d'arxius i programes.

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

S'haurà de proveir a tot el personal de la UPC de formació i conscienciació en matèria de seguretat TIC. S'haurà d'establir un programa continu de conscienciació per atendre tots els membres de la UPC, en particular els de nova incorporació.

Les persones amb responsabilitat en l'ús, funcionament o administració de sistemes TIC hauran de rebre formació per utilitzar de forma segura els sistemes en la mesura que ho necessitin per dur a terme la seva feina.

12. Terceres parts

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

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

13. Gestió del document Política de seguretat de la informació

El responsable de Seguretat ha d'elaborar aquest document per indicació del Comitè de Seguretat de la Informació.

El document haurà d'estar sempre actualitzat, mitjançant una revisió periòdica biennal, i s'haurà de revisar sempre que es produeixin canvis rellevants en els sistemes de tractament, en el tipus d'informació tractada, en els sistemes d'informació o en l'organització de la UPC.

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

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

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

Tota nova versió d'aquest document s'haurà de comunicar segons l'abast del canvi del document i el nivell de difusió que calgui.

14. Conseqüències de l'incompliment de la política de seguretat

L'incompliment de les obligacions i mesures de seguretat establertes en el present document comportarà l'aplicació de la normativa corresponent vigent en cada moment.

15. Resolució de controvèrsies

En el cas que, per causa de l'execució d'aquesta política de seguretat de la informació, ja sigui pel que fa a l'abast, la missió o l'organització de la seguretat (Comitè, rols i funcions), es produís una controvèrsia o conflicte d'interessos, aquesta s'haurà d'avaluar de forma interna i s'haurà de determinar si s'ha pres una decisió correcta i de conformitat amb les normes. La controvèrsia haurà de ser resolta pel rector o rectora.