UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Modificació de la Política de Seguretat de la Informació

Acord CG/2019/04/31, de 4 de juliol de 2019, del Consell de Govern, pel qual s'aprova la modificació de la Política de Seguretat de la Informació.

Gerència

- Document presentat a la Comissió d'Economia i Infraestructures de 26/06/2019

MODIFICACIÓ DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

FETS I FONAMENTS DE DRET

El Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'Administració electrònica, té per objecte determinar la política de seguretat en la utilització de mitjans electrònics en el seu àmbit d'aplicació i està constituït pels principis bàsics i requisits mínims que permetin una protecció adequada de la informació.

L'apartat 1 de l'article 11 de l'ENS indica el següent: "Tots els òrgans superiors de les administracions públiques han de disposar formalment de la seva política de seguretat que articuli la gestió continuada de la seguretat, que ha de ser aprovada pel titular de l'òrgan superior corresponent".

El Consell de Govern de la UPC va aprovar la **Política de seguretat de la informació** per mitjà de l'acord 88/2017 de 13 de juliol de 2017.

El mes d'abril de 2016 es va aprovar el Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades) (DOUE 4.5.2016), essent d'obligat compliment el 25 de maig de 2018.

El desembre de 2018 va entrar en vigor la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD).

El maig de 2019 es publica una actualització de la Guia CCN-STIC-801 sobre responsabilitats i funcions en l'ENS. Concretament es recull les responsabilitats generals en la gestió de la seguretat dels sistemes d'informació de les entitats del sector públic. El document indica que aquestes entitats hauran, prenent com a base les directrius assenyalades en la nova guia, d'establir i aprovar la seva pròpia Organització de Seguretat, d'acord amb la seva naturalesa, estructura, dimensió i recursos disponibles, que haurà d'estar recollida en la Política de Seguretat de la Informació de l'entitat.

A la vista dels canvis legislatius, i de les recomanacions fetes per les autoritats, s'ha valorat la conveniència de modificar la **Política de Seguretat de la Informació** de la Universitat per incorporar les noves lleis citades, i adaptar-la a les recomanacions de la guia indicada, amb la intenció que els canvis que afecten aspectes com, la incorporació del rol de Delegat de Protecció de Dades al Comitè de Seguretat de l'ENS de la UPC, i la incorporació dels mecanismes de resolució de controvèrsies, quedin recollits en el text.

D'acord amb el que s'exposa, el Consell de Govern pren el següent

ACORD

PRIMER. Aprovar les següents modificacions de la Política de seguretat de la informació:

- Actualitzar en el punt 5 “Marc normatiu” les legislacions en matèria de protecció de dades.
- Incorporar en el punt 6.1 “Comitès: Funcions i responsabilitats” les recomanacions fetes a la Guia CCN-STIC-801 sobre responsabilitats i funcions en l'ENS, pel que fa a la figura del delegat o delegada de protecció de dades.
- Incorporar en el punt 6.2 “Comitès: Funcions i responsabilitats” les recomanacions fetes a la Guia CCN-STIC-801 sobre les garanties d’independència i absència de conflicte d’interessos.
- Actualitzar el punt 7 “Dades de caràcter personal” adaptant-lo al nou RGPD i a la nova LOPDGDD.
- Incorporar un nou punt 15 “Resolució de controvèrsies” seguint la recomanació feta a la Guia CCN-STIC-801.

SEGON. Aprovar el text consolidat de la Política de seguretat de la informació, que inclou les modificacions esmentades a l’apartat primer i que s'adjunta com a annex a aquest acord.

TERCER. Aquestes modificacions entraran en vigor l'endemà del dia que les aprovi el Consell de Govern.

Barcelona, 4 de juliol de 2019

Annex

POLÍTICA DE SEGURETAT DE LA INFORMACIÓ TEXT CONSOLIDAT

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Política de seguretat[1] de la informació

ESQUEMA NACIONAL DE SEGURETAT

Versió:	2
Data de creació:	4/07/2019
Creada per:	Comitè de Seguretat de l'ENS
Aprovada per:	Consell de Govern CG 04/2019
Nivell de confidencialitat:	Baix

[1] Aquesta política de seguretat està basada en la guia elaborada a aquest efecte pel **Centre Criptogràfic Nacional**, que s'encarrega d'elaborar i difondre les normes, guies i recomanacions en relació amb l'Esquema Nacional de Seguretat.

Historial de modificacions

Data	Versió	Autor	Descripció de la modificació
03/07/2017	1	Comitè de Seguretat de l'ENS	Versió 1 del document
14/06/2019	2	Comitè de Seguretat de l'ENS	Actualització del marc normatiu amb referències a l'RGPD i la LOPDGDD de 2018. Adaptació a la nova versió de la guia CCN-STIC-801 de març de 2019 sobre "Responsabilidades y Funciones".

ÍNDEX

0. Preàmbul

La Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, va establir l'**Esquema Nacional de Seguretat**, que, aprovat mitjançant el Reial decret 3/2010, de 8 de gener, **té per objecte determinar la política de seguretat en la utilització de mitjans electrònics en el seu àmbit d'aplicació** i està constituït pels principis bàsics i requisits mínims que permetin una protecció adequada de la informació. Posteriorment, la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, recull l'Esquema Nacional de Seguretat en l'article 156, apartat 2, en uns termes similars.

El 2015 es va publicar la modificació de l'Esquema Nacional de Seguretat mitjançant el Reial decret 951/2015, de 23 d'octubre, en resposta a l'evolució de l'entorn regulador, especialment de la Unió Europea, de les tecnologies de la informació i de l'experiència de la implantació de l'Esquema.

1. Entrada en vigor

Text aprovat el dia 4 de juliol de 2019 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 (en endavant, 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 la disponibilitat, la integritat, la confidencialitat, la traçabilitat o l'autenticitat de la informació tractada o dels serveis prestats.

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

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

Això implica que la UPC i el seu personal han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, 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 l'article 7 de l'Esquema Nacional de Seguretat (en endavant, **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 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.

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, segons el que estableix l'article 9 de l'ENS.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 de l'ENS. S'han d'establir mecanismes de detecció, 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 detectats en altres parts de l'entitat 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, 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 de la publicació d'aquesta política de seguretat de la informació és protegir el personal de la Universitat d'accions il·legals o perjudicials d'individus, ja 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'Esquema Nacional de Seguretat, 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 UPC és una institució pública de recerca i d'educació superior en els àmbits de l'enginyeria, l'arquitectura i les ciències.

En un context altament creatiu i de compromís amb l'entorn i amb el canvi, els projectes de recerca, docència i gestió de la UPC es fonamenten en els principis de llibertat, justícia, democràcia, solidaritat, cooperació, sostenibilitat, eficiència, transparència i responsabilitat social.

Des del rigor intel·lectual, l'esperit crític, la transversalitat en el coneixement, la innovació docent i l'emprenedoria, la UPC forma persones i professionals competents amb capacitats i habilitats per fer front als reptes presents i futurs.

L'activitat dels seus campus i centres fan de la UPC un punt de referència i, en complicitat amb el teixit productiu, un agent i motor de canvi econòmic i social, en aportar valor a la recerca bàsica i aplicada, i transferir tecnologia i coneixement a la societat.

La Universitat Politècnica de Catalunya disposa d'infraestructures científiques i tecnològiques que posa al servei dels grups i centres de recerca, investigadors i estudiants, professionals, empreses i institucions.

5. Marc normatiu

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

- Llei orgànica d'universitats (6/2001) i la llei orgànica de modificació de la LOU (4/2007).
- Esquema Nacional de Seguretat (RD 3/2010 + RD 951/2015).
- Llei d'accés electrònic dels ciutadans als serveis públics (11/2007).
- Reglament general de protecció de dades (UE 2016/679), RGPD.
- Llei orgànica de protecció de dades personals i garanties dels drets digitals (3/2018), LOPDGDD.
- Llei de signatura electrònica (59/2003).
- Llei de serveis de la societat de la informació i de lliure comerç electrònic (34/2002).
- Llei de serveis de la societat de la informació (de 12 d'octubre de 2002).
- Llei d'universitats de Catalunya (1/2003).
- Llei del procediment administratiu comú de les administracions públiques (39/2015).
- Llei de règim jurídic del sector públic (40/2015).
- Estatuts de la Universitat Politècnica de Catalunya (2012).

6. Organització de la seguretat

6.1. Comitès: funcions i responsabilitats

El **Comitè de Seguretat de l'ENS** 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 dels Serveis**: 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 l'ENS ha de nomenar un secretari o secretària, que tindrà les funcions següents:

- Convocar les reunions del Comitè de Seguretat de l'ENS.
- 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 l'ENS ha de reportar al rector o rectora els resultats de la coordinació en matèria de seguretat de la informació.

El Comitè de Seguretat de l'ENS 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 i 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[2]

El responsable de Seguretat de l'ENS 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.

[2] En el cas que les figures del responsable de l'ENS i la de delegat o delegada de Protecció de Dades recaiguin en una mateixa persona, aquesta no podrà rebre instruccions respecte a l'acompliment de les seves funcions per part dels altres membres del Comitè.

- Monitorar l'estat de seguretat dels sistemes proporcionat per les eines de gestió d'esdeveniments de seguretat i els mecanismes d'auditoria implementats en els sistemes.
- Donar suport a la investigació dels incidents de seguretat, des que es notifiquen fins que es resolen, i supervisar-la.
- Elaborar l'informe periòdic de seguretat per al propietari del sistema, que ha d'incloure els incidents més rellevants del període.
- Aprovar els procediments de seguretat elaborats pel responsable del Sistema.
- Elaborar 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 acordar la suspensió de l'ús d'una certa informació o la prestació d'un cert servei si se l'informa de deficiències greus de seguretat que puguin afectar la satisfacció dels requisits establerts. Aquesta decisió ha de ser acordada amb els responsables de la informació afectada i del servei afectat, i amb el responsable de Seguretat abans d'executar-la.
- Elaborar els procediments de seguretat necessaris per a l'operativa del sistema.

7. Dades de caràcter personal

La UPC tracta dades personals. La LOPDGDD estableix que els subjectes vinculats al sector públic, com ho són les universitats públiques, han de fer públic un inventari de les seves activitats respecte del tractament accessible per mitjans electrònics, on hi ha de constar la informació prevista a l'article 30 de l'RGPD, on s'ha d'especificar, a més, la base legal del tractament. Aquest registre d'activitats de tractament de la UPC es pot consultar en aquest enllaç: https://rat.upc.edu, i recull activitats de tractament concretes, vinculades a una finalitat bàsica comuna a totes. Tots els sistemes d'informació de la UPC s'han d'ajustar als nivells de seguretat que estableix la normativa segons la naturalesa i la finalitat de les dades personals.

El personal de la UPC ha d'estar assabentat de l'obligació de llegir i complir el Manual UPC de protecció de dades (https://www.upc.edu/normatives/ca/documents/proteccio-dades).

8. Gestió de riscos

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

- Regularment, com a mínim cada 2 anys.
- Quan canviï la 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 l'ENS 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 l'ENS ha de dinamitzar la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

9. Directrius per estructurar la documentació de seguretat del sistema, 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'aquestes normes.

El Comitè de Seguretat de l'ENS aprova les normatives i procediments de seguretat descrits anteriorment.

El Comitè de Seguretat de l'ENS estableix les limitacions a l'accés, ús i reutilització per a l'usuari o receptor d'aquests documents (per exemple, es pot especificar que un document determinat sigui accessible però no es pugui reproduir, per motius de seguretat).

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 l'ENS. 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.

Per tal de garantir-ne la conservació, aquests documents s'hauran de conservar preferentment en un format corresponent a un estàndard obert que preservi al llarg del temps la integritat del contingut del document, de la seva signatura, si s'escau, i de les metadades que l'acompanyin.

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:

- Manual UPC de protecció de dades – **Protocol intern de seguretat**

Aquesta política de seguretat de la informació que estableix els requisits i criteris de seguretat TIC en l'àmbit de la Universitat, s'ha de desenvolupar per mitjà de normatives 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

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

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 en deriven, i és responsabilitat del Comitè de Seguretat de l'ENS disposar dels mitjans necessaris perquè la informació arribi als afectats.

S'haurà de convocar tot el personal de la UPC a una sessió de conscienciació en matèria de seguretat TIC com a mínim una vegada a l'any. 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 a altres organismes o utilitzi informació d'altres organismes, els haurà de fer partícips d'aquesta política de seguretat de la informació, haurà d'establir canals per informar-ne els comitès de seguretat TIC respectius i coordinar-los, i haurà d'establir procediments d'actuació per reaccionar adequadament davant d'incidents de seguretat.

Quan la 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 seguir 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 l'ENS.

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

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

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

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

Tota nova versió d'aquest document s'haurà de comunicar segons l'abast del canvi del document i el nivell de difusió que calgui, de manera que el personal pugui actualitzar la versió del document obsolet.

14. 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 als col·lectius de la normativa en matèria disciplinària vigent en cada moment.

A més, la UPC podrà exercir les accions oportunes previstes en el codi civil i, fins i tot, en el penal, especialment en el cas que, per causa d'un treballador o treballadora de la UPC, se sancioni la Universitat de conformitat amb la legislació vigent.

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.