POLÍTICA DE SEGURETAT DE LA INFORMACIÓ DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Aprovada pel Consell de Govern de 16 d'abril de 2019 i modificada pel Consell de Govern de 10 de novembre de 2022

1. INTRODUCCIÓ

La Universitat Politècnica de València depèn dels sistemes TIC (tecnologies de la informació i les comunicacions) per a aconseguir els seus objectius. Aquests sistemes han de ser administrats amb diligència, cal garantir-ne la resiliència prenent les mesures adequades per a protegir-los davant de danys accidentals o deliberats que puguen afectar la disponibilitat, la integritat o la confidencialitat de la informació tractada o els 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 amb prestesa als incidents.

La seguretat TIC és una part integral de cada etapa del cicle de vida del sistema d'informació, des de la seua concepció fins a la seua retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC.

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per a incidir en la confidencialitat, la integritat, la disponibilitat, l'ús previst i el valor de la informació i els serveis. Per a defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapte als canvis en les condicions de l'entorn per a garantir la prestació contínua dels serveis. Això implica que s'han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat (ENS), regulat pel Reial decret 3/2010, de 8 de gener, i també dur a terme un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per a garantir la continuïtat dels serveis prestats.

Tots els membres de la comunitat universitària, el personal i els responsables de les estructures organitzatives i dels serveis universitaris de la Universitat Politècnica de València han d'interioritzar i incorporar a la seua pràctica diària el valor de la seguretat. La Universitat ha d'estar preparada per a prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'article 7 de l'Esquema Nacional de Seguretat.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

I[1]

Mitjançant acord del Consell de Govern de 16 d'abril de 2019 va ser aprovada la Política de seguretat de la informació de la Universitat Politècnica de València.

D'altra banda, la Guia de Seguretat de les TIC, CCN-STIC 881, que arreplega la Guia d'adequació a l'Esquema Nacional de Seguretat (ENS) per a la Universitat, es va publicar al maig de 2022, juntament amb el seu annex en el qual es descriu com hauria de ser la redacció de la Política de Seguretat de les Universitats. Entre altres qüestions, en l'epígraf 3.1 de la Guia s'arreplega la composició del Comitè de Seguretat de la Informació, assenyalant que entre els membres permanent del mateix haurà de figurar el Responsable de Seguretat de la Informació, indicant que serà designat pel Rector de la Universitat o l'equip de direcció.

Així doncs, atès que la Política de Seguretat de la Informació de la Universitat Politècnica de València arreplega en el seu apartat 6.2 el procediment de designació del Responsable de Seguretat de la Informació, no sent coincident amb el proposat en la Guia de Seguretat de les TIC abans assenyalada, resulta necessari realitzar l'adaptació d'aquest apartat de la Política de Seguretat de la Informació de la Universitat Politècnica de València.

Per tot això, el Consell de Govern, a proposta de la Comissió Permanent, proposa l'aprovació de la següent proposta de modificació de la Política de Seguretat de la Informació de la Universitat Politècnica de València.

2. ÀMBIT D'APLICACIÓ

Aquesta política s'aplica a tots els sistemes TIC de la Universitat Politècnica de València i a tots els membres de la comunitat universitària, sense excepcions.

3. MISSIÓ

La Universitat Politècnica de València forma persones per a potenciar les seues competències; investiga i genera coneixement, amb qualitat, rigor i ètica, en els àmbits de la ciència, la tecnologia, l'art i l'empresa, amb l'objectiu d'impulsar el desenvolupament integral de la societat i contribuir al seu progrés tecnològic, econòmic i cultural.

En l'acompliment d'aquesta missió, la seguretat compleix una funció essencial per a afermar els objectius de la Universitat mitjançant l'ús dels seus sistemes d'informació, amb la finalitat última de garantir els drets fonamentals dels seus usuaris.

4. MARC NORMATIU

Els Estatuts de la Universitat Politècnica de València, juntament amb la normativa que els desenvolupen, constitueixen el marc en el qual enquadrar aquesta política.

[1] Text introduït per l'Acord del Consell de Govern de 10 de novembre de 2022

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

Així mateix, es tindrà en compte la legislació vigent quant a protecció de dades, propietat intel·lectual i ús d'eines telemàtiques. I, en concret, el Reglament de la Unió Europea 2016/679, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades, la Llei orgànica 3/2018 de protecció de dades personals i garantia dels drets digitals, la Llei 39/2015 de procediment administratiu comú de les administracions públiques, la Llei 40/2018 de règim jurídic del sector públic i el Reial decret 3/2010, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica.

5. DADES DE CARÀCTER PERSONAL

La Universitat Politècnica de València tracta dades de caràcter personal, i aplica en aquest tractament les mesures de seguretat adequades tenint en compte l'estat de la tècnica, els costos d'aplicació i la naturalesa, l'abast, el context i les finalitats del tractament, així com els riscos de probabilitat i gravetat variables per als drets i les llibertats de les persones físiques.

Així mateix, s'aplicaran les mesures tècniques i organitzatives apropiades per a garantir un nivell de seguretat adequat al risc detectat, amb la finalitat d'assegurar la confidencialitat, la integritat, la disponibilitat i la resiliència permanents dels sistemes i serveis de tractament.

6. ORGANITZACIÓ DE LA SEGURETAT

6.1. ROLS: FUNCIONS I RESPONSABILITATS

6.1.1. La persona responsable de seguretat de la informació

Té entre les seues funcions:

a. Mantenir la seguretat de la informació manejada i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat, d'acord amb el que s'estableix en la política de seguretat de l'organització.
b. Promoure la formació i la conscienciació en matèria de seguretat de la informació dins del seu àmbit de responsabilitat.
c. Participar en les anàlisis de risc, ajudant a determinar la categoria del sistema i establint la declaració d'aplicabilitat i les mesures de seguretat addicionals.
d. Acordar la suspensió del maneig d'una certa informació o la prestació d'un cert servei si se l'informa de deficiències greus de seguretat que puguen afectar la satisfacció dels requisits establits.

6.1.2. El Comitè de Seguretat TIC

Actua com a responsable de la informació a la Universitat Politècnica de València, i és el responsable d'establir els requisits de la informació en matèria de seguretat.

El Comitè de Seguretat TIC té el rol de responsable del servei a la Universitat, i té la potestat de determinar els nivells de seguretat dels serveis, atesos els requisits de seguretat de la informació i afegint els requisits de disponibilitat, accessibilitat, interoperabilitat, etc. necessaris.

El Comitè de Seguretat de la Informació no és un comitè tècnic, però recaptarà regularment del personal tècnic propi o extern la informació pertinent per a prendre decisions. El Comitè de Seguretat de la Informació s'assessorarà dels temes sobre els quals haja de decidir o emetre una opinió. Aquest assessorament es determinarà en cada cas, i es podrà materialitzar de diferents formes i maneres mitjançant:

a. Grups de treball especialitzats interns, externs o mixtos.
b. Assessoria externa.
c. Assistència a cursos o un altre tipus d'entorns formatius o d'intercanvi d'experiències

6.1.3. Prefectures de servei de l'àmbit competent en matèria TIC

Les persones que exerceixen les prefectures de servei de l'àmbit competent en matèria TIC tenen la funció de responsables de sistemes.

Tenen com a responsabilitats:

a. Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida, les seues especificacions, la instal·lació i la verificació del seu funcionament correcte.
b. Definir la topologia i sistema de gestió del sistema d'informació establint els criteris d'ús i els serveis disponibles en aquest.
c. Cerciorar-se que les mesures específiques de seguretat s'integren adequadament dins del marc general de seguretat.
d. Actuen com a administradores de la seguretat dels sistemes les persones amb el càrrec de cap de servei de l'àmbit competencial en matèria TIC. Entre les seues funcions hi ha:
    d.1. La implementació, gestió i manteniment de les mesures de seguretat aplicables al sistema d'informació.
    d.2. La gestió, configuració i actualització, si s'escau, del maquinari i programari en què es basen els mecanismes i serveis de seguretat del sistema d'informació.
    d.3. La gestió de les autoritzacions concedides als usuaris i usuàries del sistema, en particular els privilegis concedits, inclòs el monitoratge que l'activitat desenvolupada en el sistema s'ajusta a allò autoritzat.
    d.4. L'aplicació dels procediments operatius de seguretat.
    d.5. Aprovar els canvis en la configuració vigent del sistema d'informació.
    d.6. Assegurar que els controls de seguretat establits es compleixen estrictament.
    d.7. Assegurar que s'apliquen els procediments aprovats per a manejar el sistema d'informació.
    d.8. Supervisar les instal·lacions de maquinari i programari, i les seues modificacions i millores per a assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.

d.9. Monitorar l'estat de seguretat del sistema proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica implementats en el sistema.
d.10. Informar les persones responsables de la seguretat i del sistema de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
d.11. Col·laborar en la investigació i resolució d'incidents de seguretat, des de la detecció fins a la resolució.

6.2. PROCEDIMENTS DE DESIGNACIÓ

El nomenament del Responsable de Seguretat de la Informació i la designació dels Responsables identificats en aquesta Política, es realitzaran pel rector o rectora de la Universitat Politècnica de València. El nomenament es revisarà, almenys, cada quatre anys o quan el lloc quede vacant.

6.3. POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

És missió del Comitè de Seguretat TIC la revisió anual d'aquesta política de seguretat de la informació i la proposta de revisió o manteniment d'aquesta.

La política serà aprovada pel Consell de Govern i es difondrà perquè la coneguen totes les parts afectades.

7. PREVENCIÓ

La Universitat Politècnica de València ha d'evitar o almenys prevenir en la mesura que siga possible, que la informació o els serveis es vegen afectats per incidents de seguretat. Per a això s'han d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat a través d'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 a garantir el compliment d'aquesta política, la Universitat ha de:

a. Autoritzar els sistemes abans d'entrar en operació, aplicant els principis de seguretat des del disseny i per defecte.
b. Avaluar regularment la seguretat, incloent-hi avaluacions dels canvis de configuració fets de forma rutinària.
c. Sol·licitar la revisió periòdica per part de tercers amb la finalitat d'obtenir una avaluació independent.

8. DETECCIÓ

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració fins a la seua detenció, els serveis han de monitorar l'operació de manera

contínua per a detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons el que s'estableix en l'article 9 de l'Esquema Nacional de Seguretat.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 de l'Esquema Nacional de Seguretat. S'establiran mecanismes de detecció, anàlisi i informe que arriben a les persones responsables regularment i quan es produeix una desviació significativa dels paràmetres que s'han preestablit com a normals.

9. RESPOSTA

La Universitat Politècnica de València ha de:

a. Establir mecanismes per a respondre eficaçment als incidents de seguretat.
b. Designar punt de contacte per a les comunicacions respecte a incidents detectats en altres departaments o en altres organismes.
c. 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).

10. RECUPERACIÓ

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

11. GESTIÓ DE RISCOS

Tots els sistemes subjectes a aquesta política hauran de realitzar una anàlisi de riscos, i avaluar les amenaces i els riscos als quals estan exposats.

Aquesta anàlisi es durà a terme en els supòsits següents:

a. De forma regular, almenys una vegada cada dos anys.
b. En el cas que es canvie la informació manejada.
c. En el cas que canvien els serveis prestats.
d. Sempre que ocórrega un incident greu de seguretat.
e. En tot cas quan es reporten vulnerabilitats greus.
f. En qualsevol moment que siga necessari d'acord amb el que s'estableix en la normativa de protecció de dades personals.

Per a l'harmonització de les anàlisis de riscos, el Comitè de Seguretat TIC establirà una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats. El Comitè de Seguretat TIC dinamitzarà la disponibilitat de recursos per a atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

12. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Aquesta política es desenvoluparà per mitjà de normativa de seguretat que afronte aspectes específics. La normativa de seguretat estarà a disposició de tots els membres de la Universitat Politècnica de València que necessiten conèixer-la, en particular, aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions.

La normativa de seguretat estarà disponible en la intranet de la Universitat Politècnica de València.

13. OBLIGACIONS DEL PERSONAL

Tots els membres de la Universitat Politècnica de València tenen l'obligació de conèixer i complir aquesta política de seguretat de la informació i la normativa de seguretat, sent responsabilitat del Comitè de Seguretat TIC disposar els mitjans necessaris perquè la informació arribe a les persones afectades.

Tots els membres de la Universitat Politècnica de València assistiran a sessions de conscienciació en matèria de seguretat TIC. S'establirà un programa de conscienciació contínua per a atendre tots els membres d'aquesta, en particular els de nova incorporació.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes TIC rebran formació per al maneig segur dels sistemes en la mesura que la necessiten per a fer el seu treball. La formació és obligatòria abans d'assumir una responsabilitat, tant si és la primera assignació com si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest.

14. TERCERES PARTS

Quan la Universitat Politècnica de València preste serveis a altres organismes o faça servir informació d'altres organismes, se'ls farà partícips d'aquesta política de seguretat de la informació; s'establiran canals per a informes i coordinació dels respectius comitès de seguretat TIC, i s'establiran procediments d'actuació per a la reacció davant d'incidents de seguretat.

Quan la Universitat Politècnica de València utilitze serveis de tercers o cedisca informació a tercers, se'ls farà partícips d'aquesta política de seguretat i de la normativa de seguretat que concernisca a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establides en aquesta normativa, podent desenvolupar els seus propis procediments operatius per a satisfer-la. S'establiran procediments específics d'informe i resolució d'incidències. Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establit en aquesta política.

Quan algun aspecte de la política no puga ser satisfet per una tercera part (d'acord amb el que es requereix en els paràgrafs anteriors), es requerirà un informe de la persona responsable de seguretat a fi que precise els riscos en què s'incorre i la manera de tractar-los. Es requereix l'aprovació d'aquest informe per part de les persones responsables de la informació i els serveis afectats, abans de continuar avant.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

15. ENTRADA EN VIGOR
    a. Aquesta política de seguretat de la informació és efectiva des de l'aprovació pel Consell de Govern i fins que siga reemplaçada per una nova política.
    b. Així mateix, aquesta política de seguretat de la informació serà publicada en el Butlletí Oficial de la Universitat Politècnica de València (BOUPV).

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen