POLÍTICA DE SEGURETAT DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Aprovada per Consell de Govern de 6 de juny de 2024[1]

[1] Aquesta política de seguretat té el seu origen en la política de seguretat aprovada per Consell de Govern de 16 d'abril de 2019 i modificada per Consell de Govern de 10 de novembre de 2022.

1. Aprovació i entrada en vigor

Text aprovat el dia 6 de juny de 2024 per acord del Consell de Govern de la Universitat Politècnica de València.

Aquesta Política de seguretat de la informació, d'ara en avant Política, és efectiva des que s'aprove fins que siga reemplaçada per una nova política de seguretat de la informació.

2. Introducció

La Universitat Politècnica de València depèn de les TIC (tecnologies de la informació i les telecomunicacions) per a assolir els seus objectius. Aquests sistemes s'han d'administrar amb diligència. Cal prendre les mesures adequades per a protegir-los contra danys accidentals o deliberats que puguen afectar la seguretat de la informació tractada o els serveis prestats i, alhora, han d'estar sempre protegits contra les amenaces o els incidents amb potencial per a repercutir en la confidencialitat, integritat, disponibilitat, traçabilitat i autenticitat de la informació tractada i els serveis prestats.

Per a fer front a aquestes amenaces es requereix una estratègia que s'adapte als canvis en les condicions de l'entorn a fi de garantir la prestació contínua dels serveis. Això implica que els departaments 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, així mateix, preparar una resposta efectiva als ciberincidents a fi de garantir la continuïtat dels serveis prestats.

Així doncs, totes les unitats administratives de la UPV tenen present que la seguretat TIC és un procés integral de cada etapa del cicle de vida del sistema, des de la concepció fins a la retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat, basats en la gestió de riscos, 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 licitació per a projectes TIC.

Per tant, per a la Universitat Politècnica de València, l'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis. I amb aquesta finalitat actua preventivament, i implanta línies de defensa i supervisa l'activitat diària dels serveis per a detectar-hi incidents i reaccionar amb prestesa als incidents, a fi de recuperar-los tan prompte com siga possible, segons el que estableix l'article 8 de l'ENS, amb l'aplicació de les mesures que s'indiquen a continuació.

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

2.1 Prevenció

Perquè la informació i els serveis no es vegen perjudicats per incidents de seguretat, la Universitat Politècnica de València implementa les mesures de seguretat establides per l'ENS, com també qualsevol altre control addicional que haja identificat com a necessari a través d'una avaluació d'amenaces i riscos. Aquests controls, els rols i les responsabilitats de seguretat de tot el personal, estan clarament definits i documentats.

Per a garantir el compliment de la Política, la Universitat Politècnica de València:

- Autoritza els sistemes abans d'entrar en funcionament.
- Avalua regularment la seguretat dels sistemes, incloent-hi l'anàlisi dels canvis de configuració realitzats de manera rutinària.
- Sol·licita a tercers la revisió periòdica dels sistemes a fi de tenir-ne una avaluació independent.

2.2 Detecció

La Universitat Politècnica de València 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 disposa l'article 10 de l'ENS (vigilància contínua i reavaluació periòdica). Quan es produeix una desviació significativa dels paràmetres que s'hagen preestablit com a normals (segons indica l'article 9 de l'ENS, existència de línies de defensa) s'han d'establir els mecanismes de detecció, anàlisi i comunicació necessaris perquè arriben als responsables regularment.

2.3 Resposta

La Universitat Politècnica de València estableix les mesures següents:

- Mecanismes per a respondre eficaçment als incidents de seguretat.
- Designar un punt de contacte per a les comunicacions respecte a incidents detectats en altres departaments o en altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en els dos sentits, amb els equips de resposta a emergències (CERT).

2.4 Recuperació

Per a garantir la disponibilitat dels serveis, la Universitat Politècnica de València disposa dels mitjans i les tècniques necessàries que permeten garantir la recuperació dels serveis més crítics.

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

3. Missió

La missió de la Universitat Politècnica de València és la formació integral de l'estudiantat a través de la creació, el desenvolupament, la transmissió i crítica de la ciència, de la tècnica de l'art i de la cultura, des del respecte als principis ètics, amb una decidida orientació a la consecució d'una ocupació d'acord amb el nivell d'estudis assolit.

La contribució al desenvolupament cultural, social i econòmic de la societat valenciana i espanyola mitjançant el suport científic, tècnic i artístic.

El desenvolupament d'un model d'institució caracteritzada pels valors d'excel·lència, internacionalització, solidaritat i eficàcia; una institució oberta que incentiva la participació d'institucions, empreses i professionals en tots els aspectes de la vida universitària.

Per a complir aquesta missió, la Universitat Politècnica de València posa a la disposició de la ciutadania la realització de tràmits en línia i noves vies de participació que garantisquen el desenvolupament i l'eficàcia de les seues funcions i comeses.

La potenciació de l'ús d'aquestes tecnologies persegueix fomentar la relació electrònica de totes les parts implicades (docents, estudiants, investigadors, personal d'administració i serveis, etc.) amb la UPV.

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 principis bàsics següents:

- Abast estratègic: la seguretat de la informació ha de comptar amb el compromís i suport de tots els nivells directius de la UPV, de manera que puga estar coordinada i integrada amb les altres iniciatives estratègiques de l'organització per a desplegar de manera coherent i eficaç la implantació del procés de seguretat.
- 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 per a 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 cal procurar evitar qualsevol actuació ocasional o tractament conjuntural. La seguretat de la informació ha de considerar-se com una part del funcionament habitual i s'ha de fer present i aplicar-se des del disseny inicial dels sistemes TIC.
- Gestió de riscos: l'anàlisi i la gestió de riscos formen part essencial del procés de seguretat. La gestió de riscos permet mantenir un entorn controlat en què els riscos es minimitzen fins a nivells acceptables. La reducció d'aquests nivells s'efectua mitjançant l'aplicació de mesures de seguretat, en què s'estableix un equilibri entre la naturalesa de les dades i els tractaments, la repercussió i la probabilitat dels riscos a què estiguen exposades i l'eficàcia i el cost de les mesures de seguretat. Quan s'avalua 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 riscos potencials i a la criticitat i el valor de la informació i dels serveis afectats.
- Millora contínua: les mesures de seguretat s'han de reavaluar i actualitzar periòdicament a fi que l'eficàcia s'adeqüe a l'evolució constant dels riscos i sistemes de protecció. La seguretat de la informació ha de ser atesa, revisada i auditada per personal qualificat, instruït i dedicat.
- Seguretat per defecte: els sistemes han de dissenyar-se i configurar-se de manera que garantisquen un grau suficient de seguretat per defecte. Cal aplicar els requisits mínims d'autorització i control d'accés, protecció de les instal·lacions, adquisició de productes de seguretat i contractació de serveis de seguretat, protecció de la informació, prevenció respecte a altres sistemes d'informació interconnectats, registre de l'activitat i detecció de codi nociu, incidents de seguretat i privilegi mínim.

5. Objectius de la seguretat de la informació

La Universitat Politècnica de València estableix com a objectius de la seguretat de la informació els següents:

- Garantir la qualitat i protecció de la informació.
- Aconseguir la plena conscienciació dels usuaris respecte a la seguretat de la informació.
- Gestió d'actius d'informació: els actius d'informació de la UPV han d'estar inventariats, categoritzats i anar associats a un responsable.
- Seguretat lligada a les persones: cal implantar els mecanismes necessaris perquè qualsevol persona que accedisca o puga accedir als actius d'informació conega les seues responsabilitats i, així, es reduïsca el risc derivat d'un ús indegut i s'aconseguisca la plena conscienciació dels usuaris respecte a la seguretat de la informació.

- Seguretat física: els actius d'informació s'han de situar en àrees segures, protegides per controls d'accés físics adequats al nivell de criticitat. Els sistemes i els actius d'informació que contenen aquestes àrees han d'estar protegits contra amenaces físiques o ambientals.
- Seguretat en la gestió de comunicacions i operacions: s'han d'establir els procediments necessaris per a aconseguir una gestió adequada de la seguretat, del funcionament i de l'actualització de les TIC. La informació que es transmeta a través de xarxes de comunicacions ha de protegir-se adequadament, tenint en compte el nivell de sensibilitat i de criticitat d'aquestes dades, mitjançant mecanismes que garantisquen la seguretat del procés.
- Control d'accés: cal limitar a usuaris, a processos i a altres sistemes d'informació l'accés als actius d'informació mitjançant la implantació de mecanismes d'identificació, autenticació i autorització d'acord amb la criticitat de cada actiu. A més, l'ús del sistema ha de quedar registrat a fi d'assegurar la traçabilitat de l'accés i auditar-ne l'ús adequat, d'acord amb l'activitat de l'organització.
- Adquisició, desenvolupament i manteniment dels sistemes d'informació: els elements de seguretat de la informació s'han d'incloure en totes les fases del cicle de vida dels sistemes d'informació a fi de garantir la seguretat d'aquests sistemes 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.
- Garantia de prestació continuada dels serveis: s'han d'implantar els mecanismes apropiats per a assegurar la disponibilitat dels sistemes d'informació i mantenir la continuïtat dels processos de negoci, d'acord amb les necessitats de nivell de servei dels usuaris.
- Protecció de dades: s'han d'adoptar les mesures tècniques i organitzatives necessàries per a gestionar els riscos generats pel tractament a fi de complir la legislació de seguretat i privacitat.
- Compliment: s'han d'adoptar les mesures tècniques, organitzatives i procedimentals necessàries a fi de complir la normativa legal vigent en matèria de seguretat de la informació.

6. Abast

Aquesta Política s'ha d'aplicar als sistemes d'informació de la Universitat Politècnica de València relacionats amb l'exercici de les seues competències i a tots els usuaris amb accés autoritzat a aquests sistemes, siguen empleats públics o no i amb independència de la naturalesa de la relació jurídica que tinguen amb la UPV. Tots tenen l'obligació de conèixer i complir aquesta Política de seguretat de la informació i la Normativa de seguretat derivada. El Comitè de Seguretat de la Informació té la responsabilitat de disposar els mitjans necessaris perquè la informació arribe al personal afectat.

7. Marc normatiu

El marc normatiu en què es despleguen les activitats de la Universitat Politècnica de València i, en particular, la prestació dels serveis electrònics està integrat per les normes que s'indiquen en l'annex: "Annex legal. Política de seguretat de la informació de la Universitat Politècnica de València":

8. Organització de la seguretat de la informació

8.1 Criteris per a l'organització de la seguretat de la informació

La Universitat Politècnica de València, tenint en compte el que estableix el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), emprèn les accions següents per a organitzar la seguretat de la informació:

i. Designació de rols de seguretat: responsables dels serveis, responsables de la informació, responsable de seguretat, responsable del sistema i delegat/ada de protecció de dades.
ii. Constitució d'un òrgan consultiu i estratègic per a prendre decisions en matèria de seguretat de la informació. Aquest òrgan es constitueix com un òrgan col·legiat i es denomina Comitè de Seguretat de la Informació. El presideix una persona física que ha d'assumir la responsabilitat formal de les accions que emprenga.

8.2 Rols i òrgans de la seguretat de la informació

A la Universitat Politècnica de València, en el marc de l'ENS, els rols i els òrgans de la seguretat de la informació són els següents:

- Responsable de la informació i els serveis
- Responsable de seguretat de la informació
- Responsable del sistema
- Comitè de Seguretat de la Informació

8.2.1. Procediments de designació

- La creació del Comitè de Seguretat de la Informació, el nomenament dels integrants i la designació dels responsables identificats en aquesta Política són atribucions del rector de la Universitat Politècnica de València.
- El nomenament s'ha de revisar cada quatre anys o quan el lloc quede vacant.

Està format pels membres següents:

Membres permanents:

Composició:

- President/a: vicerector/a de Planificació, Oferta Acadèmica i Transformació Digital.
- Vicepresident/a, que substitueix el president/a en cas de vacant, absència o malaltia: director/a de l'Àrea de Ciberseguretat.
- Secretari/ària: un/a tècnic/a de l'Àrea de Sistemes d'Informació i les Comunicacions designat pel vicerector/a de Planificació, Oferta Acadèmica i Transformació Digital.

Vocals:

- El secretari/ària general.
- El gerent/a.
- Dos tècnics o tècniques de l'Àrea de Sistemes d'Informació i les Comunicacions designats pel vicerector/a de Planificació, Oferta Acadèmica i Transformació Digital.
- Tres persones designades pel Rectorat entre els òrgans de govern, els serveis universitaris, les escoles o facultats i els departaments.

Membres no permanents:

Vocals:

- Direccions de serveis vinculades amb els assumptes per tractar.
- El delegat/ada de protecció de dades de la Universitat.
- Especialistes externs del sector públic, privat o acadèmic la presència dels quals, per raó d'experiència o de vinculació amb els assumptes tractats, siga necessària o aconsellable.

La presidència convoca les direccions dels serveis segons els assumptes que calga tractar.

El delegat o delegada de protecció de dades participa amb veu i sense vot en les reunions del Comitè de Seguretat de la Informació quan es tracten qüestions relacionades amb el tractament de dades de caràcter personal, i també sempre que es requerisca que hi participe. En tot cas, si un assumpte se sotmet a votació, cal fer consignar en acta l'opinió del delegat o delegada de protecció de dades.

El secretari o secretària del Comitè fa les convocatòries i estén l'acta de les reunions del Comitè de Seguretat de la Informació. Poden assistir a les sessions del Comitè de Seguretat de la Informació, en qualitat d'assessors, les persones que el president considere pertinents en cada cas.

8.3 Responsabilitats dels rols associats a l'Esquema Nacional de Seguretat

8.3.1 Responsable de la informació i dels serveis

La persona responsable de la informació i dels serveis té les funcions següents:

- Establir els requisits de seguretat aplicables a la informació (nivells de seguretat de la informació) i als serveis (nivells de seguretat dels serveis) en matèria de seguretat. Pot demanar una proposta al responsable de la seguretat i ha de tenir en compte l'opinió del responsable del sistema
- Dictaminar respecte als drets d'accés a la informació i els serveis.
- Acceptar els nivells de risc residual que afecten la informació i els serveis.
- Comunicar al responsable de seguretat qualsevol variació respecte a la informació i els serveis, especialment la incorporació de nous serveis o informació

8.3.2 Responsable de seguretat de la informació

La persona responsable de seguretat de la informació té les funcions següents:

- 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 conscienciació en matèria de seguretat de la informació.
- Designar responsables de l'execució de l'anàlisi de riscos, de la declaració d'aplicabilitat, identificar mesures de seguretat, determinar configuracions necessàries i elaborar documentació sobre el sistema.
- Proporcionar assessorament per a determinar la categoria del sistema, en col·laboració amb el responsable del sistema o amb el Comitè de Seguretat de la Informació.
- Participar en l'elaboració i la implantació dels plans de millora de la seguretat i, si arriba el cas, en els plans de continuïtat, i 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 comunicar al Comitè les modificacions realitzades al llarg del període en curs.

8.3.3 Responsable del sistema

La persona responsable del sistema té les funcions següents:

- Elaborar els procediments operatius necessaris per a desenvolupar, fer funcionar i mantenir el sistema d'informació durant tot el cicle de vida.
- Definir la topologia i la gestió del sistema d'informació i establir els criteris d'ús i els serveis disponibles.
- Detenir l'accés a informació o a la prestació de servei si té coneixement que hi ha deficiències greus de seguretat.
- Cerciorar-se que les mesures específiques de seguretat s'integren adequadament en el marc general de seguretat.
- Proporcionar assessorament per a determinar la categoria del sistema, en col·laboració amb el responsable de seguretat o amb el Comitè de Seguretat de la Informació.
- Participar en l'elaboració i la implantació dels plans de millora de la seguretat i, si s'escau, en els plans de continuïtat.
- Dur a terme, si s'escau, les funcions de l'administrador de la seguretat del sistema:
    - La gestió, configuració i actualització, si cal, del maquinari i programari en què es basen els mecanismes i serveis de seguretat.
    - La gestió de 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 correspondència amb l'activitat autoritzada.
    - Aprovar els canvis en la configuració vigent del sistema d'informació.
    - Assegurar que els controls de seguretat establits es compleixen de manera estricta.
    - Assegurar que s'apliquen els procediments aprovats per a manejar el sistema d'informació.
    - Supervisar les instal·lacions de maquinari i programari i, també, les modificacions i millores a fi de garantir 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'incidents de seguretat i pels mecanismes d'auditoria tècnica.
    - Comunicar al responsable de seguretat qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
    - Col·laborar en la investigació i resolució d'incidents de seguretat, des de la detecció fins a la resolució.

Quan la complexitat del sistema ho justifique, el responsable del sistema pot designar els responsables de sistema delegats que considere necessaris. Aquests responsables tenen dependència funcional directa d'aquell i són responsables en el seu àmbit de totes les accions que els delegue. Així mateix, també pot delegar en altres responsables funcions concretes de les responsabilitats que té atribuïdes.

8.3.4 Delegat de protecció de dades

El delegat de protecció de dades té les funcions següents:

- Informar i assessorar la Universitat Politècnica de València i els usuaris que s'ocupen del tractament sobre les obligacions que els incumbeixen en virtut de la normativa vigent en matèria de protecció de dades.
- Supervisar el compliment del que disposa la normativa de seguretat i les polítiques internes de la Universitat Politècnica de València, 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 li sol·liciten sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar-ne l'aplicació.
- Cooperar amb l'Agència Espanyola de Protecció de Dades quan aquesta ho requerisca i actuar com a punt de contacte amb aquesta entitat per a qüestions relatives al tractament de dades.
- Actuar com a punt de contacte (finestreta única) amb les persones interessades quant al tractament de les seues dades personals i l'exercici de drets sobre aquestes dades.

El delegat de protecció de dades exerceix les seues funcions parant atenció als riscos associats a les operacions de tractament. I per això ha de ser capaç de:

- Obtenir informació per a determinar les activitats de tractament.
- Analitzar i comprovar la conformitat de les activitats de tractament.
- Oferir informació, assessorament i recomanacions al responsable o encarregat del tractament.
- Obtenir informació per a supervisar el registre de les operacions de tractament.
- Assessorar en el principi de la protecció de dades des del disseny i per defecte.
- Assessorar sobre si es duen a terme o no les avaluacions d'impacte, metodologia, salvaguardes per aplicar, etc.
- Prioritzar activitats segons els riscos.
- Assessorar el responsable del tractament sobre àrees que s'han de sotmetre a auditories, activitats de formació i operacions de tractament a les quals cal dedicar més temps i recursos.

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

8.3.5 Comitè de Seguretat de la Informació

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

a) Estar permanentment informat sobre la normativa que regula el certificat de conformitat amb l'ENS, incloent-hi les normes d'acreditació, certificació, guies, manuals, procediments i instruccions tècniques.
b) Estar permanentment informat sobre la llista d'entitats de certificació acreditades i organitzacions, públiques i privades, certificades.
c) Estar permanentment informat sobre la llista d'esquemes de certificació de la seguretat amb els quals l'Administració pública té establits convenis o acords de reconeixement mutu de certificats.
d) Proposar directrius i recomanacions, que s'han d'incloure en les actes corresponents de les reunions del Comitè, a les quals el president ha de donar complida resposta.
e) Coordinar els esforços de les diverses àrees en matèria de seguretat de la informació a fi d'assegurar que siguen consistents, alineats amb l'estratègia decidida en la matèria i evitar duplicitats d'esforços.
f) Atendre les inquietuds, en matèria de seguretat de la informació, de l'Administració i de les diverses àrees, i informar regularment la direcció sobre l'estat de la seguretat de la informació.
g) Resoldre els conflictes de responsabilitat que puguen aparèixer entre els responsables o departaments i elevar els casos en què no tinga prou autoritat per a decidir.
h) Assessorar en matèria de seguretat de la informació sempre que li ho demanen.
i) Revisar, amb l'aprovació de l'òrgan superior, la Política de seguretat de la informació.
j) Aprovar la normativa d'ús de mitjans electrònics per a tot el personal.
k) Aprovar el mapa de normativa amb la llista de normativa i procediments de seguretat per a la implantació de l'ENS.
l) Actuar com a responsable de la informació i dels serveis.

Periodicitat de les reunions i adopció d'acords:

- Durant el desenvolupament del projecte d'adequació a l'ENS, a fi d'avaluar-ne el procés i possibilitar-ne un seguiment adequat, el Comitè de Seguretat de la Informació s'ha de reunir, almenys, una vegada al trimestre.
- Una vegada obtingut el certificat de conformitat amb l'ENS dels serveis prestats per la UPV, el Comitè de Seguretat de la Informació s'ha de reunir, almenys, dues vegades a l'any amb caràcter semestral, sense perjudici que, considerant les necessitats derivades del compliment dels seus fins i atribucions, calga reunir-se amb més freqüència.
- Les reunions les convoca el president, a través del secretari, per iniciativa pròpia o per iniciativa de la majoria dels membres permanents.
- Les decisions s'adopten per consens dels membres permanents.

9. Dades personals

La Universitat Politècnica de València només arreplega i tracta dades personals quan siguen adequades, pertinents, no excessives i tinguen relació amb l'àmbit i les finalitats per a les quals s'hagen obtingut. Així mateix, adopta les mesures de tipus tècnic i organitzatives necessàries per a complir la normativa de protecció de dades.

La Universitat Politècnica de València publica a la seu electrònica la seua política de privacitat i el Registre d'Activitats de Tractament.

10. Obligacions del personal

Tot el personal de la Universitat Politècnica de València comprès dins de l'àmbit de l'ENS ha d'assistir, almenys una vegada a l'any, a una o més sessions de conscienciació en matèria de seguretat i protecció de dades. S'ha d'establir un programa de conscienciació contínua per a atendre tot el personal, en particular el de nova incorporació.
Les persones amb responsabilitat en l'ús, en el funcionament o en l'administració de sistemes d'informació han de rebre formació per a l'ús segur dels sistemes en la mesura que la necessiten per a la faena. 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 el lloc de treball.

11. Gestió de riscos

Tots els sistemes afectats per aquesta Política de seguretat de la informació estan subjectes a una anàlisi de riscos amb l'objectiu d'avaluar les amenaces i els riscos a què estan exposats. Aquesta anàlisi s'ha de fer:

- Almenys una vegada a l'any.
- Quan canvie la informació o els serveis gestionats de manera significativa.
- Quan ocórrega un incident greu de seguretat o es detecten vulnerabilitats greus.

El responsable de la seguretat és l'encarregat que es faça l'anàlisi de riscos i, també, d'identificar mancances i febleses i comunicar-les al Comitè de Seguretat de la Informació.

El Comitè de Seguretat de la Informació dinamitza la disponibilitat de recursos per a cobrir les necessitats de seguretat dels diversos sistemes i promou inversions de caràcter horitzontal.

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

El procés de gestió de riscos comprèn les fases següents:

- Categorització dels sistemes.
- Anàlisi de riscos.
- El Comitè de Seguretat de la Informació selecciona les mesures de seguretat que cal aplicar. Aquestes mesures han de ser proporcionals als riscos i estar justificades.

Les fases d'aquest procés han d'ajustar-se al que disposen els annexos I i II del Reial decret 311/2022, de 8 de gener, i han de seguir les normes, instruccions, guies CCN-STIC i recomanacions per a l'aplicació d'aquest procés elaborades pel Centre Criptològic Nacional.
En particular, per a fer l'anàlisi de riscos s'empra, com a norma general, una metodologia reconeguda d'anàlisi i gestió de riscos.

11.1 Riscos derivats del tractament de dades personals

Quan s'avalua el risc en relació amb la seguretat de les dades cal tenir en compte els riscos que es deriven del tractament de les dades personals, com ara destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra forma, o la comunicació o l'accés no autoritzats a aquestes dades, susceptibles en particular d'ocasionar danys i perjudicis físics, materials o immaterials.

S'ha de publicar el registre d'activitats del tractament de les dades i la gestió de riscos s'efectua a través d'una anàlisi de riscos i EPID, en cas que siga necessari.

12. Notificació d'incidents

De conformitat amb el que disposa l'article 33 del RD 311/2022, de 3 de maig, la Universitat Politècnica de València notifica al Centre Criptològic Nacional els incidents que tinguen repercussió significativa en la seguretat de la informació gestionada i dels serveis prestats en relació amb la categorització de sistemes que apareix en l'annex I d'aquest cos legal.

13. Desplegament de la Política de seguretat de la informació

Aquesta Política de seguretat de la informació s'ha de complementar amb diversa normativa 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 la revisió anual i el manteniment d'aquesta Política i, en cas que siga necessari, proposar-hi millores.

El cos normatiu sobre seguretat de la informació s'ha de construir en tres nivells per àmbit d'aplicació, nivell de detall tècnic i obligatorietat de compliment, de manera que cada norma d'un cert nivell de desplegament es fonamente en les normes de nivell superior. Aquests nivells de desplegament normatiu són els següents:

1. Primer nivell normatiu: polítiques de seguretat.
2. Segon nivell normatiu: normatives de seguretat.
3. Tercer nivell normatiu: procediments, guies i instruccions tècniques. Són documents que compleixen el que s'ha exposat en la Política de seguretat de la informació i determinen les accions o tasques que cal fer en l'acompliment d'un procés.

Correspon al Consell de Govern de la Universitat Politècnica de València aprovar la Política de seguretat de la informació i la Normativa de seguretat de la UPV. El Comitè de Seguretat de la Informació és l'òrgan responsable de l'aprovació dels altres documents i, també, és responsable de la difusió perquè les parts afectades els coneguen.

Així mateix, aquesta Política de seguretat de la informació complementa la política de privacitat de la Universitat Politècnica de València en matèria de protecció de dades.

La Normativa de seguretat i, molt especialment, la Política de seguretat de la informació ha de ser coneguda i estar a la disposició de tots els membres de la UPV, en particular per a aquells que usen, facen funcionar o administren els sistemes d'informació i comunicacions. Aquesta documentació, custodiada per l'Àrea de Sistemes d'Informació i Comunicacions, ha d'estar disponible per a la consulta en la intranet i en suport paper.

14. Terceres parts

Quan la Universitat Politècnica de València preste serveis a altres organismes o manege informació d'altres organismes, els ha de comunicar aquesta Política de seguretat de la informació. S'han d'establir canals per a la comunicació i la coordinació dels comitès de seguretat de la informació respectius i procediments d'actuació per a la reacció en cas d'incidents de seguretat.

Quan la Universitat Politècnica de València use serveis de tercers o cedisca informació a tercers, els ha de comunicar aquesta Política de seguretat i la Normativa de seguretat que afecte aquests serveis o informació. Aquesta tercera part resta subjecta a les obligacions establides en aquesta Normativa i pot crear els propis procediments operatius per a satisfer-les. S'han d'establir procediments específics de comunicació i resolució d'incidències. S'ha de garantir que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que el que estableix aquesta Política de seguretat.

Quan algun aspecte d'aquesta Política de seguretat de la informació no puga ser satisfet per una tercera part segons requereixen els paràgrafs anteriors, es requerirà un informe al responsable de seguretat que precise els riscos en què s'incorre i la manera de tractar-los. Abans de continuar endavant, els responsables de la informació i els serveis afectats han d'aprovar aquest informe.

15. Millora contínua

La gestió de la seguretat de la informació és un procés subjecte a actualització permanent. Els canvis en l'organització, les amenaces, les tecnologies o la legislació són motius pels quals és necessària una millora contínua dels sistemes. Per això és menester implantar un procés permanent que comporta, entre altres accions:

a) Revisió de la Política de seguretat de la informació.
b) Revisió i categorització dels serveis i de la informació.
c) Execució amb periodicitat anual de l'anàlisi de riscos.
d) Realització d'auditories internes o, quan calga, d'auditories externes.
e) Revisió de les mesures de seguretat.
f) Revisió i actualització de les normes i els procediments.

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