BOUPV
Butlletí Oficial de la Universitat Politècnica de València

Núm. 2024/0089 16/07/2024 1

NORMATIVA DE SEGURETAT DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Aprovada per Consell de Govern de 6 de juny de 2024

Contingut

CAPÍTOL I
DISPOSICIONS GENERALS

Article 1. Objecte

Aquesta Normativa té per objecte regular la norma d'ús segur dels mitjans tecnològics que formen part dels sistemes d'informació de la Universitat Politècnica de València, amb la finalitat de minimitzar la probabilitat que es materialitzen les amenaces que posen en risc la seguretat dels sistemes d'informació.

Article 2. Definicions

1. Sistemes d'informació: conjunt d'elements (maquinari, programari, dades, processos i personal) que permeten recopilar, emmagatzemar, processar i transmetre informació per a gestionar operacions i prendre decisions.
2. Recursos i serveis TIC: recursos tecnològics i serveis relacionats, com ara maquinari, programari, bases de dades, xarxes i serveis de telecomunicacions, que s'usen per a donar suport i administrar sistemes d'informació.
3. Xarxa corporativa: conjunt de xarxes i sistemes interconnectats que permeten la comunicació i transmissió de dades entre diverses àrees d'una organització.
4. Correu electrònic corporatiu: sistema de comunicació per correu electrònic que pertany a una organització i que s'usa per a comunicacions oficials entre treballadors i amb altres agents d'interès.
5. Galetes: petits fitxers de dades que un lloc web emmagatzema en el dispositiu de l'usuari. S'usen per a recordar informació de l'usuari, com ara preferències de navegació i detalls d'inici de sessió.
6. EDR (*endpoint detection and response*): eines i solucions de seguretat dissenyades per a tasques de detecció, anàlisi i resposta en cas d'amenaces i activitats sospitoses en dispositius finals (com ara ordinadors personals, ordinadors portàtils, servidors i dispositius mòbils).
7. Informació classificada: informació l'accés a la qual queda restringit a persones amb autorització específica, generalment per motius de seguretat o confidencialitat.
8. Infraestructura de xarxa: conjunt de maquinari, programari i sistemes interconnectats que formen la base per a comunicar i transmetre dades en una xarxa.
9. Sistemes físics: components tangibles d'un sistema, com ara servidors, ordinadors personals, dispositius de xarxa i altres elements de maquinari.
10. Sistemes lògics: components intangibles d'un sistema, com ara programari, aplicacions, bases de dades i algorismes que funcionen sobre sistemes físics per a gestionar dades i processos.

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

Article 3. Àmbit d'aplicació

1. Aquesta normativa és d'obligat compliment i s'aplica a les persones que tenen la consideració d'usuaris dels recursos i serveis TIC de la Universitat Politècnica de València.

2. Tenen la consideració d'usuaris:

a) Els membres de la comunitat universitària (PDI, PAS, PI i estudiants).
b) El personal de les fundacions i organitzacions dependents de la Universitat Politècnica de València, sempre que tinguen accés als recursos i serveis TIC de la Universitat Politècnica de València.
c) El personal de les organitzacions proveïdores de serveis, sempre que la prestació dels seus serveis requerisca accedir als recursos i serveis TIC de la Universitat Politècnica de València. Quan aquest personal siga integrador de tecnologia en el sistema és obligatori complir les normatives d'usuaris avançats.
d) Les persones que, encara que no formen part de cap dels col·lectius anteriors, estan habilitades per a l'ús dels recursos TIC de la Universitat Politècnica de València, sempre que s'haja establit un acord de col·laboració o una autorització explícita que així ho permeta.

CAPÍTOL II
USOS DELS RECURSOS I SERVEIS TIC

Article 4. Ús dels recursos TIC

1. La Universitat Politècnica de València posa a la disposició dels usuaris de la comunitat universitària diverses connexions a la xarxa corporativa. Aquestes connexions s'assignen segons les característiques de la vinculació de l'usuari amb la Universitat Politècnica de València.

2. El conjunt de serveis i recursos TIC que la Universitat Politècnica de València pot prestar i posar a la disposició dels usuaris es pot modificar, i també deixar de prestar-se, segons la disponibilitat de recursos i els canvis en la vinculació de l'usuari amb la institució.

3. Els recursos i serveis TIC (dispositius, programes, serveis informàtics, etc.) que la Universitat Politècnica de València posa a la disposició dels usuaris s'han d'usar fonamentalment per a la realització de les funcions encomanades; és a dir, per a fins professionals o acadèmics.

4. Amb caràcter general, els equips informàtics propietat de la Universitat Politècnica de València els gestiona i els configura el personal tècnic de la Universitat. Cap usuari no ha de fer canvis en la configuració d'aquests equips ni executar-hi o desar-hi fitxers que no siguen de confiança.

5. Els equips propietat de la Universitat Politècnica de València que es traslladen fora de les seues instal·lacions han de ser vigilats, estar sota control dels usuaris i cal assegurar-se que es transporten de manera segura per a evitar furts, pèrdues o accessos no autoritzats.

6. Tots els equips que es connecten a la xarxa de la Universitat Politècnica de València han de mantenir el sistema operatiu convenientment actualitzat, a fi d'evitar vulnerabilitats, i han de disposar de l'antivirus i sistema EDR oficials de la Universitat Politècnica de València convenientment actualitzats i operatius. No es poden connectar a la xarxa els equips informàtics en què el sistema operatiu estiga fora del període d'assistència del fabricant. Els equips que es connecten a la xarxa de la Universitat Politècnica de València des de fora dels campus a través de la VPN han de complir igualment aquests requisits.

7. Quan per raons justificades un usuari té permisos per a administrar ordinadors de la Universitat Politècnica de València, a més de complir el que disposa l'apartat anterior, s'ha d'assegurar d'instal·lar-hi exclusivament programes amb llicència.

8. Quan, per raons justificades, un dispositiu ha de tenir habilitada alguna tecnologia que permeta accedir directament a aquest equip des d'Internet, com l'accés web o altres accessos, les aplicacions de control remot o qualsevol altre tipus de connexió remota per qualsevol port de comunicacions, el procediment que cal seguir és el següent:

a) L'administrador d'aquest equip ha de justificar els motius pels quals és necessari aquest accés des d'Internet mitjançant una declaració responsable en què especifique el propòsit de l'equip, els ports que cal obrir i la tecnologia que s'emprarà, el temps de vigència d'aquesta circumstància excepcional i el compromís de mantenir l'equip permanent actualitzat, a fi d'evitar vulnerabilitats, i de tenir activat i actualitzat permanentment el sistema antivirus i el sistema EDR oficials de la Universitat Politècnica de València.

b) L'Àrea de Sistemes d'Informació i Comunicacions (ASIC), en vista del compromís descrit, ha d'autoritzar l'obertura dels ports requerits abans que aquesta obertura siga efectiva.

c) Qualsevol incompliment dels compromisos assumits en la declaració responsable implica la desconnexió immediata de l'equip de la xarxa acordada pel responsable de seguretat de la informació.

Article 5. Credencials i contrasenyes

1. La Universitat Politècnica de València proporciona als usuaris un compte d'accés consistent en credencials, a través del qual pot usar els recursos i serveis TIC per als quals tinga habilitació. La finalització de la relació que vincula els usuaris amb la Universitat Politècnica de València comporta la finalització del dret de fer ús dels recursos i serveis TIC subministrats per la institució.

2. Les credencials proporcionades per la Universitat Politècnica de València als usuaris són personals, intransferibles i identifiquen l'usuari de manera inequívoca.

3. Es prohibeix comunicar les contrasenyes a terceres persones, tinguen vinculació amb la Universitat Politècnica de València o no. La custòdia i l'ús diligent d'aquestes contrasenyes és responsabilitat de l'usuari.

4. La Universitat Politècnica de València ha de garantir la inviolabilitat d'aquests recursos i serveis, de manera que només el titular puga accedir als recursos associats al seu compte, excepte en els casos i amb les garanties en què l'ordenament jurídic ho permeta.

5. L'usuari ha de canviar les contrasenyes quan el sistema ho demane i sempre ha d'usar contrasenyes segures.

Article 6. Impressió i digitalització de documents

1. Amb caràcter general, s'han d'usar impressores en xarxa i fotocopiadores propietat de l'organització i autoritzades.

2. Tota la digitalització s'ha de fer amb els mitjans tècnics corporatius i s'ha d'evitar en tot moment fer ús de dispositius aliens a la Universitat Politècnica de València, com ara fotografies amb telèfons mòbils personals, etc.

3. Quan es digitalitza algun document cal posar especial cura en la destinació d'aquest document.

4. Quan s'imprimeix documentació ha d'estar el temps més curt possible a les safates d'eixida de les impressores, a fi d'evitar que terceres persones hi puguen accedir.

5. Les fotocòpies o còpies descartades no es poden reaprofitar si contenen dades personals o informació classificada; en aquest cas, cal destruir-les immediatament.

6. Queda prohibit deixar abandonats documents amb informació classificada a la impressora, a la fotocopiadora o en dispositius similars, o desatesos al lloc de treball.

Article 7. Ús de la infraestructura de xarxa

1. Els equips informàtics de propietat particular es poden connectar a la xarxa de la Universitat Politècnica de València tant sense fils com per cable. En el segon cas han de disposar de l'autorització corresponent de la persona responsable de seguretat de la informació.

2. La connexió dels equips informàtics particulars a la xarxa de la Universitat Politècnica de València es pot restringir o limitar per motius tècnics i per a garantir la seguretat del sistema.

3. No es permet connectar equips mitjançant cable a la xarxa de la Universitat Politècnica de València que no disposen de persona de contacte o de mecanismes que garantisquen que en tot moment es pot identificar la persona que usa l'equip.

4. No es permet posar en marxa infraestructures o serveis, locals o remots, que permeten accedir a la xarxa corporativa, utilitzables per l'usuari o per terceres persones, ni en obert ni amb accés controlat, sense demanar autorització expressa de l'ASIC.

5. Els serveis informàtics de la UPV, a través del personal tècnic propi o d'entitats proveïdores de serveis, és l'únic autoritzat a accedir físicament als sistemes de comunicacions, cablatge, punts d'accés sense fil i qualsevol altre equipament de la xarxa, administrar-los i manipular-los.

6. Per motius tècnics, i a fi de garantir el bon funcionament de les comunicacions en la xarxa de la Universitat Politècnica de València, el personal tècnic pot revertir qualsevol actuació no autoritzada realitzada sobre algun element connectat a la xarxa corporativa. Qualsevol perjudici generat per aquesta mena d'actuacions és responsabilitat del personal no autoritzat que ha fet una tal acció.

Article 8. Lloc de treball endreçat

1. En la mesura possible, s'ha de mantenir el lloc de treball net, ordenat i endreçat, sense més material damunt de la taula que el requerit per a l'activitat que es fa en cada moment.

2. La documentació, una vegada usada, s'ha d'alçar en un lloc tancat, especialment quan el lloc de treball queda desatès i en acabar-se la jornada.

3. No està permès apuntar les contrasenyes en notes adhesives o similars i guardar-les al lloc de treball.

4. Quan l'usuari s'absenta del lloc de treball ha de ser caut i no mostrar en la pantalla documents de treball.

5. En cada ordinador s'ha d'activar el blocatge automàtic de pantalla si transcorre un cert temps sense activitat, amb una validació de contrasenya. Aquest blocatge no s'ha de desactivar mai i, així mateix, és aconsellable blocar manualment la pantalla abans d'abandonar el lloc per un temps prolongat, amb la finalitat que no hi haja accessos indeguts.

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

6. En els ordinadors d'ús compartit és obligatori tancar la sessió quan s'abandona el lloc.

7. Es considera ús indegut la sostracció o el trasllat no autoritzat degudament a altres dependències de qualsevol element físic de la instal·lació informàtica o de la infraestructura complementària, com també causar danys a aquests elements.

Article 9. Ús del correu electrònic

1. El correu electrònic corporatiu és una eina de treball que s'ha d'utilitzar per a la realització de les funcions acadèmiques, de recerca i administratives pròpies de la UPV. Se'n permet l'ús en l'àmbit privat si es tracta de motius personals o domèstics, si no és abusiu i no perjudica la seguretat dels sistemes d'informació de l'organització ni el desenvolupament normal de les funcions encomanades.

2. L'usuari és responsable de les accions realitzades a través del seu compte de correu.

3. El personal tècnic pot accedir als registres d'ús dels comptes de correu electrònic quan aquest accés és necessari per a garantir la seguretat, la disponibilitat, la integritat i el correcte funcionament dels recursos TIC.

4. Els usuaris han de ser especialment diligents a l'hora d'obrir correus electrònics que inclouen fitxers adjunts i enllaços (URL). No s'ha d'obrir cap fitxer que provinga de fonts que no siguen de confiança ni cap enllaç d'aparença no legítima.

En cas de sospites o dubtes raonables sobre la fiabilitat dels fitxers i enllaços rebuts, cal notificar aquesta circumstància a l'ASIC a través del sistema de notificació d'incidències Gregal o a través del compte de correu antifrau de la Universitat Politècnica de València: fraudeinternet@upv.es.

5. Es prohibeix l'ús del compte de correu electrònic corporatiu per a:

a) Tramesa de correus electrònics amb contingut inadequat, il·legal, ofensiu, difamatori, inapropiat o discriminatori per raó de sexe, raça, edat, discapacitat, que continguen programes informàtics (programari) sense llicència, que vulneren drets de propietat intel·lectual, d'alerta de virus falsos o difusió de virus reals i codi maliciós, o qualsevol altre tipus de contingut que puga perjudicar els usuaris, la identitat i la imatge corporativa i els mateixos sistemes d'informació de l'organització.
b) Tramesa de correu brossa, correus massius i propagació de correus encadenats.
c) Tramesa de missatges relacionats amb activitats il·legals o fraudulentes.
d) Qualsevol altra acció incompatible amb les finalitats de la Universitat Politècnica de València i, en general, qualsevol contravenció de les finalitats que consten en aquesta normativa o en el reglament aplicable.

Article 10. Protecció de la navegació web

1. L'ús d'Internet s'ha de limitar a l'obtenció d'informació relacionada amb la faena que s'exerceix. Cal evitar, per tant, tot ús que no tinga una mínima relació amb les funcions encomanades a l'usuari.

2. No es permet l'accés a pàgines de contingut ofensiu, inapropiat, pornogràfic o discriminatori per raons de gènere, ètnia, opció sexual, discapacitat o qualsevol altra circumstància personal o social, excepte per raons justificades de recerca o docència, i sempre amb l'autorització deguda del responsable de seguretat de la informació.

3. L'ús de pàgines web s'ha de fer a través del protocol segur HTTPS. Els accessos mitjançant el protocol HTTP no segur només es permeten en els serveis que per motius tècnics no ofereixen un mitjà segur de connexió. I cal tenir la precaució de no transmetre dades personals ni informació classificada a través d'aquestes connexions no segures.

4. Els usuaris han de verificar que els certificats tramesos per serveis HTTPS els tramet una autoritat de certificació de confiança. Qualsevol error o alerta creada pel navegador a conseqüència de la validació del certificat s'ha de revisar acuradament amb la finalitat de comprovar-ne la licitud.

5. Amb la finalitat de reduir l'exposició a les galetes, cal usar perfils d'usuaris diferenciats en els navegadors web a fi de separar les activitats relacionades amb l'organització de les personals.

Article 11. Ús de les instal·lacions tècniques

1. L'accés físic a àrees restringides només es permet al personal autoritzat, excepte en els supòsits d'urgència o emergència.

2. L'accés als centres de processament de dades (CPD) i a les infraestructures de comunicacions de la Universitat Politècnica de València queda restringit al personal dels serveis informàtics de la Universitat Politècnica de València i al personal autoritzat.

3. En cas que personal que no siga membre dels serveis informàtics de la UPV necessite accedir a algun CPD o a la infraestructura de comunicacions, la persona responsable de la visita ha de formalitzar la sol·licitud d'autorització corresponent.

4. Els CPD han de disposar d'un sistema de control d'entrades a fi de registrar tots els accessos.

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

Article 12. Ús indegut dels recursos TIC

Es considera ús indegut dels recursos TIC i en cap cas no es poden emprar per a cap de les finalitats següents:

a) Activitats il·lícites o il·legals de qualsevol classe i, particularment, difusió de continguts de caràcter racista, xenòfob, pornogràfic, sexista, d'apologia del terrorisme, que atempten contra els drets humans o que actuen en perjudici dels drets a la intimitat, a l'honor, a la pròpia imatge o contra la dignitat de les persones.

b) Difondre continguts contraris als principis inspiradors dels Estatuts de la Universitat Politècnica de València.

c) Congestionar intencionadament la xarxa de la Universitat Politècnica de València o interferir en el funcionament d'aquesta xarxa.

d) Establir mecanismes o sistemes que permeten aprofitaments indeguts dels recursos de xarxa proporcionats, com ara revenda o reutilització per a fins privats, lucratius o delictius, entre d'altres.

e) Danyar els sistemes físics i lògics, introduir o difondre en la xarxa virus informàtics o programari nociu i fer qualsevol altra classe d'activitat susceptible de provocar danys a la Universitat Politècnica de València, als seus membres, proveïdors o terceres persones.

f) Obtenir dades personals, tant de manera directa com mitjançant tractaments invisibles, excepte els directament relacionats amb les funcions pròpies de la Universitat, o fer qualsevol tractament de dades personals que no siguen titularitat de la Universitat Politècnica de València i que no s'haja autoritzat abans.

g) Instal·lar programari per al qual no es disposa de llicència; executar o guardar fitxers que no són de confiança.

h) Publicar o difondre dades, documents o fitxers que afecten terceres persones o subjectes a drets de privacitat en la protecció de dades i garantia dels drets digitals o de propietat intel·lectual, com també qualsevol altre dret o interès legítim, sense el consentiment exprés de les persones afectades i del titular dels drets

i) Fer ús dels recursos TIC amb finalitats comercials, llevat dels casos autoritzats expressament.

j) Enviar comunicacions amb finalitats comercials o correu massiu no sol·licitat amb finalitats publicitàries (correu brossa) des dels comptes de correu electrònic.

k) Vulnerar els drets de propietat intel·lectual o industrial de tercers.

l) Cercar o usar identificadors i contrasenyes d'altres usuaris o qualsevol intent de trobar i explotar errors en la seguretat dels sistemes informàtics de la UPV o de fora, o fer ús dels sistemes per a atacar algun sistema informàtic.

CAPÍTOL III
TRACTAMENT DE LA INFORMACIÓ

Article 13. Classificació de la informació

La Universitat Politècnica de València posa a la disposició dels usuaris un procediment de classificació d'informació que s'ha d'emprar per a l'exercici de les funcions encomanades.

Article 14. Ús i tractament de la informació

1. Els usuaris tenen el deure de guardar la confidencialitat deguda, de conformitat amb la legislació vigent, respecte de la informació tractada. Aquest deure de confidencialitat es manté fins i tot una vegada acabada la relació de l'usuari amb la Universitat Politècnica de València.

2. En cas que es dispose d'informació en suport paper, s'ha de conservar i custodiar amb la diligència deguda.

3. Les còpies, els extractes i les traduccions fetes per usuaris amb accés autoritzat a la informació estan subjectes als mateixos requisits de seguretat que els documents originals.

4. Queda expressament prohibit l'intercanvi d'informació classificada mitjançant plataformes no corporatives o no autoritzades.

5. Els arxius o fitxers classificats per la Universitat Politècnica de València no es poden usar per a ús particular o de tercers. Durant el temps que els fitxers o arxius estiguen en l'equip o suport informàtic de la seua propietat s'ha de restringir l'accés a la informació que contenen i l'ús d'aquesta informació.

6. No es pot copiar o enviar la informació continguda en els fitxers en què s'emmagatzemen dades de caràcter personal o un altre tipus d'informació de la Universitat Politècnica de València en ordinadors propis, memòries USB, discos extraïbles o qualsevol altre suport informàtic.

7. En cas necessari, els arxius o fitxers classificats per la Universitat Politècnica de València s'han d'eliminar quan han deixat de ser útils per als fins que en motivaren la creació.

8. Abans d'abandonar sales d'ús comú s'han de netejar adequadament les pissarres de les sales de reunió i despatxos i assegurar-se que no hi queda cap mena d'informació classificada o que pot ser reutilitzada.

Article 15. Emmagatzematge de la informació

1. La informació només es pot emmagatzemar en recursos oficials, com ara la unitat de xarxa individual (W:), la unitat de xarxa compartida amb el servei (V:), el servei de OneDrive corporatiu i, també, en els que autoritze expressament la Universitat Politècnica de València.

2. L'usuari és el responsable de tota la informació que ha emmagatzemat i que s'extraga fora de la Universitat Politècnica de València.

CAPÍTOL IV
RÈGIM DE VIGILÀNCIA I RESPONSABILITAT

Article 16. Responsabilitat dels usuaris

1. Els usuaris han de custodiar, i fer-ne un bon ús, els recursos TIC que la Universitat Politècnica de València posa a disposició seua per a desenvolupar-ne les funcions dins de la institució.

2. Cada usuari és responsable de les accions realitzades a través del seu compte i dels recursos TIC posats a disposició seua.

3. En cas d'incompliment del deure de custòdia del compte, la Universitat Politècnica de València pot iniciar un procediment administratiu per a assegurar el funcionament correcte dels serveis prestats i adoptar les mesures correctores i disciplinàries necessàries, entre les quals hi ha el blocatge temporal del compte d'usuari com a mesura provisional.

4. Els usuaris tenen l'obligació de conèixer i complir aquesta normativa i qualsevol altra norma o instrucció que puga afectar l'ús correcte de les TIC, tant a la Universitat Politècnica de València com en les xarxes de les quals la UPV forma part.

5. La Universitat Politècnica de València no és responsable, ni directament ni subsidiàriament, de les opinions expressades pels membres de la comunitat universitària o per qualssevol altres, ni dels continguts publicats en els recursos de debat públic en línia proporcionats per la institució.

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

Article 17. Incidents de seguretat

Si un usuari detecta alguna anomalia o incidència de seguretat que pot comprometre el bon ús i funcionament de les instal·lacions o dels sistemes d'informació de la Universitat Politècnica de València, ha de comunicar-la immediatament a través del sistema Gregal o del procediment que té disponible en aquest moment en cas d'urgència.

Article 18. Anàlisi i monitoratge de seguretat

1. La Universitat Politècnica de València, per motius legals, de seguretat i qualitat del servei, i complint els requisits de la legislació que l'afecten, disposa d'un sistema de ciberseguretat que monitora l'estat del SGSI (Sistema de Gestió de la Seguretat de la Informació), per la qual cosa:

a) Revisa periòdicament l'estat dels equips, el programari instal·lat, els dispositius i les xarxes de comunicacions sota responsabilitat seua.

b) Monitora els accessos a la informació i a les xarxes continguda en els seus sistemes.

c) Audita la seguretat de les credencials i aplicacions.

d) Monitora els serveis d'Internet, el correu electrònic i altres eines de col·laboració.

2. La Universitat Politècnica de València du a terme aquestes activitats de monitoratge de manera proporcional al risc, amb les cauteles legals pertinents i respectant plenament els drets dels usuaris.

3. El sistema que proporciona el servei de navegació pot tenir filtres d'accés que bloquen l'accés a pàgines web amb contingut inadequat, programes lúdics de descàrrega massiva o pàgines potencialment insegures o que contenen virus o codi nociu. Així mateix, el sistema pot registrar les pàgines a què s'ha accedit i deixar-ne traça, com també el temps d'accés, el volum i la grandària dels fitxers descarregats.

4. La Universitat Politècnica de València pot suspendre l'ús dels recursos als usuaris, de manera temporal o definitiva, quan se'n detecta un ús inadequat o s'incompleixen les directrius de seguretat, a fi de garantir la seguretat dels sistemes d'informació.

Article 19. Incompliment de la normativa

1. Els sistemes de la Universitat Politècnica de València es configuren per a prevenir accions que es puguen considerar contràries a aquest reglament o a qualsevol altra norma o protocol aprovat. Aquests sistemes poden adoptar les mesures preventives corresponents.

2. El responsable de seguretat, en l'exercici de les seues funcions, en cas d'un possible incompliment d'aquesta normativa que puga comportar un perjudici per als sistemes i recursos de la Universitat Politècnica de València, pot suspendre de manera cautelar el servei prestat o blocar temporalment els sistemes, comptes o accessos a la xarxa de manera preventiva, amb la finalitat de garantir el bon funcionament dels serveis de la institució.

2. En els altres supòsits d'incompliment, s'envia un avís a l'infractor. En cas que l'usuari no responga a l'avís o l'ignore, el Comitè de Seguretat de la Informació de la Universitat Politècnica de València pot sol·licitar al rector, o al vicerector en qui aquest haja delegat, l'adopció de les mesures de suspensió provisional dels serveis prestats o el blocatge dels sistemes.

Tot això sense perjudici d'iniciar les accions disciplinàries, administratives, civils o penals que corresponguen en cada cas, en relació amb les persones presumptament implicades en aquest incompliment.

La Universitat Politècnica de València comunica a l'autoritat judicial i les forces i cossos de seguretat de l'Estat les infraccions que poden ser constitutives de delicte.

Article 20. Revisió i avaluació

El Comitè de Seguretat és competent per a:

a) Interpretar els dubtes que puguen aparèixer en l'aplicació d'aquesta normativa.
b) Revisar aquesta normativa quan siga necessari a fi d'actualitzar-ne el contingut o si es compleixen els terminis màxims establits per a revisar-la.
c) Verificar l'efectivitat de les mesures adoptades per raó d'aquesta normativa.

Anualment, aquest document s'ha de sotmetre a revisió i aprovació de les possibles modificacions.

La modificació i la revisió s'orienta tant a la identificació d'oportunitats de millora en la gestió de la seguretat de la informació, com a l'adaptació als canvis esdevinguts en el marc legal, en la infraestructura tecnològica, en l'organització general, etc.

2. El responsable de seguretat de la informació és la persona encarregada de difondre la informació i les directrius incloses en aquesta normativa.

Disposició derogatòria única

Queda derogat el Reglament d'ús dels serveis i recursos informàtics de la Universitat Politècnica de València de data 17 de maig de 2007 i qualsevol altra norma que contravé a aquesta Normativa.

Disposició final única

Aquesta Normativa entra en vigor el mateix dia en què es publica en el BOUPV.

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