POLÍTICA DE CONTRASENYES DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

1. OBJECTIU I ÀMBIT D'APLICACIÓ

Les contrasenyes són un aspecte fonamental de la seguretat dels recursos informàtics: són la primera línia de protecció per a l'usuari. Una contrasenya mal triada o protegida pot ser un forat de seguretat per a tota l'organització. Per això, tots els usuaris de la xarxa de la Universitat Politècnica de València (UPV) són responsables de vetlar per la seguretat de les contrasenyes seleccionades per a usar els diferents serveis oferits a la comunitat universitària a través d'UPVnet .

La seguretat proveïda per una contrasenya depèn que es mantinga sempre en secret. Totes les directrius subministrades per aquesta política tenen per objectiu mantenir aquesta característica fonamental en les contrasenyes dels recursos de la UPV. L'objectiu fonamental d'aquesta política és establir un estàndard per a la creació de contrasenyes fortes, la protecció i el canvi freqüent d'aquestes.

L'àmbit d'aquesta política inclou aquells usuaris dels serveis i recursos informàtics de la Universitat Politècnica de València que tenen o són responsables d'un compte (o qualsevol altre tipus d'accés que requerisca una contrasenya) en qualsevol dels sistemes de la Universitat Politècnica de València.

2. POLÍTICA GENERAL

Totes les contrasenyes de comptes que donen accés a recursos i serveis de la Universitat Politècnica de València hauran de seguir les següents directrius generals:

- Totes les contrasenyes de sistema (arrel, administradors NT, comptes d'administració d'aplicacions...) han de canviar-se almenys una vegada cada sis mesos.

- Totes les contrasenyes d'usuari (comptes d'UPVnet , comptes de correu electrònic, comptes de serveis web, etc.) han de ser canviades almenys una vegada cada dotze mesos. No obstant això, es recomana canviar-la amb més freqüència i també sempre que l'usuari sospite que la seguretat de la seua contrasenya puga haver sigut compromesa.

- Els comptes d'usuari que tinguen privilegis de sistema a través de la pertinença a grups per qualsevol altre mitjà, han de tenir contrasenyes diferents de la resta de comptes mantinguts per aquest usuari en els serveis i recursos UPV.

- Les contrasenyes no s'han d'incloure en missatges de correu electrònic ni cap altre mitjà de comunicació electrònica. Tampoc s'han de comunicar en converses telefòniques.

- Les contrasenyes, en la mesura que es puga, s'han de generar automàticament amb les característiques recomanades en aquesta política i es comunicarà als usuaris la seua contrasenya sempre en estat "expirat" per obligar l'usuari a canviar-la en el primer ús que faça del compte o servei.

- Les contrasenyes per defecte associades als sistemes o aplicacions noves s'han de canviar abans de posar aquests sistemes en producció. També es desactivaran aquells comptes "per defecte" que no siguen imprescindibles.

- Totes les contrasenyes de sistema i d'usuari de recursos i serveis UPV han de respectar les recomanacions descrites en aquesta política.

Alguns serveis en què siga crític el fet de mantenir la seguretat de la contrasenya podran determinar-ne mesures addicionals de protecció.

3. SELECCIÓ I CUSTÒDIA DE CONTRASENYES

3.1. Recomanacions generals per a la selecció de contrasenyes

Les contrasenyes s'usen amb propòsits múltiples a la Universitat Politècnica de València, com ara les contrasenyes de comptes d'usuari UPVnet, contrasenyes de sistema dels recursos de la UPV, serveis web, comptes de correu electrònic, protectors de pantalla en els recursos dels usuaris, administració de dispositius remots, etc.

Cal parar una atenció especial en la selecció de contrasenyes segures per a l'autenticació en tots els recursos i serveis de la UPV.

La seguretat d'aquest tipus d'autenticació es basa en dues premisses:

a) La contrasenya personal només la coneix l'usuari.
b) La contrasenya és bastant segura per a no ser desxifrada.

La contrasenya, per a considerar-se **forta (segura),** ha de posseir les característiques següents:

- Ha de tenir almenys 15 caràcters.
- Ha d'utilitzar caràcters de tres dels quatre grups següents, i un sempre ha de ser un símbol:

    1. Lletres minúscules.
    2. Lletres majúscules.
    3. Nombres (per exemple 1, 2, 3).
    4. Símbols (per exemple , @, ñ, =, -).

- No ha de ser, ni provenir d'una paraula del diccionari, d'un argot o d'un dialecte.
- No ha de provenir del nom de l'usuari o d'algun parent proper.
- No ha de provenir d'informació personal (del número de telèfon, nombre d'identificació, DNI, data de naixement, etc.) de l'usuari o d'algun parent proper.

Addicionalment, les contrasenyes en UPVnet han de complir les recomanacions següents:

- No ha de contenir tres o més caràcters consecutius del nom d'usuari d'UPVnet o del nom complet de la persona.
- No ha de tenir espais en blanc.

Finalment, si preveieu viatjar a l'estranger o utilitzar teclats que no siguen espanyols, cal tenir en compte que els símbols que s'utilitzen en la contrasenya poden estar en llocs diferents del teclat; per exemple, no podreu usar lletres *ñ* si viatja molt i no coneix com introduir-la en teclats no espanyols.
Les contrasenyes no han de ser emmagatzemades per escrit mai. Intenteu crear contrasenyes que pugueu recordar fàcilment. Una forma de recordar-les amb facilitat és crear una contrasenya basada en una frase fàcilment recordable, com ara, la frase: 'Setze jutges d'un jutjat' em suggereix la contrasenya: '16jutgesd1jutjat'.

3.2. Recomanacions per a la protecció de la contrasenya

No s'ha utilitzar la mateixa contrasenya que s'utilitza per als comptes de recursos i serveis UPV en altres comptes de fora de la UPV (accés al proveïdor de serveis personal, accés a serveis del banc, etc.).

Quan siga possible, cal no utilitzar les mateixes contrasenyes en diferents comptes i serveis UPV. Per exemple, utilitzeu contrasenyes diferents per a l'usuari UPVnet i per al correu electrònic.

No s'han de compartir els comptes i les contrasenyes UPV amb ningú, tampoc amb els administratius, secretàries, etc. Totes les contrasenyes han de ser tractades com a informació sensible i confidencial.

A continuació, presentem una llista de coses que **NO** s'han de fer:

- No reveleu la contrasenya per telèfon a ningú, fins i tot encara que li parlen en nom del Servei d'Informàtica o d'un superior en l'organització.
- No reveleu la contrasenya en missatges de correu electrònic ni a través de qualsevol altre mitjà de comunicació electrònica.
- No escriviu mai la contrasenya en paper i no la guardeu. Tampoc emmagatzemeu contrasenyes en fitxers d'ordinador sense encriptar o proveïu-lo d'algun mecanisme de seguretat.
- No reveleu la contrasenya als superiors, ni col·laboradors.
- No parleu sobre una contrasenya davant d'altres persones.
- No reveleu la contrasenya en cap qüestionari o formulari, independentment de la confiança que li inspire.
- No compartiu la contrasenya amb familiars.
- No reveleu la contrasenya als companys quan marxen de vacances.
- No utilitzeu la característica de "Recordar contrasenya" que hi ha en algunes aplicacions (Outlook, Netscape, Internet Explorer).

Si algú us demana la contrasenya, esmenteu aquest document o demaneu que es comunique amb l'Àrea de Sistemes d'Informació i Comunicacions (ASIC) de la UPV. Si sospiteu que un compte o la contrasenya poden haver sigut compromesos, comuniqueu-ho a l'ASIC i canvieu les contrasenyes de tots els comptes.
Canvieu les contrasenyes amb la freqüència recomanada per a cada tipus de compte i servei.

3.3. Estàndards de desenvolupament d'aplicacions

Els desenvolupadors d'aplicacions informàtiques per a l'entorn de la Universitat Politècnica de València i que en gestionen els mecanismes d'autenticació mitjançant contrasenyes han d'assegurar-se que els programes contenen les precaucions següents en termes de seguretat respecte de la selecció i l'ús de contrasenyes:

- Han de suportar autenticació d'usuaris individuals, no de grups.
- No han d'emmagatzemar contrasenyes en text clar o en cap forma fàcilment reversible.
- Han de proveir el sistema d'algun tipus de mecanisme de rols, de manera que un usuari puga prendre les funcions d'un altre sense necessitat de conèixer la contrasenya de l'anterior.
- Han de proveir el sistema d'un mecanisme per a fer expirar les contrasenyes i obligar els usuaris a canviar-la.
- Han de limitar el nombre d'intents d'accessos sense èxit consecutius.

4. MESURES QUE CAL APLICAR

L'incompliment d'aquesta política pot arribar a comprometre la seguretat de la xarxa corporativa de la Universitat Politècnica de València.

La Comissió d'Informàtica de la Universitat serà l'òrgan que decidisca les accions que s'han de dur a terme en el cas que s'incomplisca aquesta política, una vegada establides les repercussions de la violació d'aquesta sobre els recursos i serveis informàtics de la UPV. Tot això sense perjudici de prendre les accions disciplinàries, administratives, civils o penals que, si escau, s'imposen a les persones presumptament implicades en aquest incompliment.