



POLÍTICA DE PASSWORDS DE LA UNIVERSIDAD POLITÉCNICA DE VALENCIA

1.- OBJETIVO Y ÁMBITO DE APLICACIÓN

Los passwords son un aspecto fundamental de la seguridad de los recursos informáticos, es la primera línea de protección para el usuario. Un password mal elegido o protegido puede resultar en un agujero de seguridad para toda la organización. Por ello, todos los usuarios de la red de la Universidad Politécnica de Valencia (UPV) son responsables de velar por la seguridad de los passwords seleccionados por ellos mismos para el uso de los distintos servicios ofrecidos a la comunidad universitaria a través de UPVnet.

La seguridad provista por un password depende de que el mismo se mantenga siempre secreto, todas las directrices suministradas por esta política tienen por objetivo mantener esta característica fundamental en los passwords de los recursos de la UPV. El objetivo fundamental de esta política es establecer un estándar para la creación de passwords fuertes, la protección de dichos passwords, y el cambio frecuente de los mismos.

El ámbito de esta política incluye a todos aquellos usuarios de los servicios y recursos informáticos de la Universidad Politécnica de Valencia que tienen o son responsables de una cuenta (o cualquier otro tipo de acceso que requiera un password) en cualquiera de los sistemas de la Universidad Politécnica de Valencia.

2.- POLÍTICA GENERAL

Todos los passwords de cuentas que den acceso a recursos y servicios de la Universidad Politécnica de Valencia deberán seguir las siguientes directrices generales:

- Todos los passwords de sistema (root, administradores NT, cuentas de administración de aplicaciones, etc...) deben ser cambiados al menos una vez cada seis meses.
- Todos los passwords de usuario (cuentas de UPVnet, cuentas de email, cuentas de servicios web, etc...) deben ser cambiados al menos una vez cada doce meses. Sin embargo, se recomienda cambiarlo con mayor frecuencia y también siempre que el usuario sospeche que la seguridad de su password pueda haber sido comprometida.
- Las cuentas de usuario que tengan privilegios de sistema a través de su pertenencia a grupos o por cualquier otro medio, deben tener passwords distintos del resto de cuentas mantenidas por dicho usuario en los servicios y recursos UPV.
- Los passwords no deben ser incluidos en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica. Tampoco deben ser comunicadas las claves en conversaciones telefónicas.
- En la medida de lo posible, los passwords serán generados automáticamente con las características recomendadas en esta política y se les comunicará a los usuarios su password siempre en estado "expirado" para obligar al usuario a cambiarlo en el primer uso que hagan de la cuenta o servicio.



- Los passwords por defecto asociados a los sistemas o aplicaciones nuevas deberán ser cambiados antes de poner estos sistemas en producción. También se desactivarán aquellas cuentas “por defecto” que no sean imprescindibles.
- Todos los passwords de sistema y de usuario de recursos y servicios UPV deben respetar las recomendaciones descritas en la presente política.

Algunos servicios en los que sea crítico el mantener la seguridad del password podrán determinar medidas adicionales de protección del mismo.

3.- SELECCIÓN Y CUSTODIA DE PASSWORDS

3.1.- Recomendaciones generales para la selección de passwords

Los passwords son usados con múltiples propósitos en la Universidad Politécnica de Valencia, como pueden ser los passwords de cuentas de usuario UPVnet, passwords de sistema de los recursos de la UPV, servicios web, cuentas de correo electrónico, protectores de pantalla en los recursos de los usuarios, administración de dispositivos remotos, etc... **Se debe poner especial atención en la selección de passwords fuertes para la autenticación en todos los recursos y servicios de la UPV.**

Los passwords **débiles** tienen alguna de las siguientes características:

- Contiene menos de 8 caracteres.
- Es una palabra que se encuentra en el diccionario (español o extranjero).
- Es una palabra de uso común, como por ejemplo:
 - Nombres de la familia, animales, compañeros de trabajo, amigos, personajes, etc...
 - Términos y marcas informáticos, comandos, compañías comerciales, hardware, software.
 - Fechas de nacimiento y cualquier otra información personal, como por ejemplo la dirección o el número de teléfono.
 - Patrones de letras o números, como ‘aaabbb’, ‘qwerty’, ‘zxywvu’, ‘123321’, etc...
 - Cualquiera de lo anterior escrito al revés.
 - Cualquiera de lo anterior precedido o seguido por un dígito, por ejemplo ‘secreto1’ o ‘1secreto’.

En cambio, los passwords **fuertes** tienen las siguientes características:

- Más de 8 caracteres.
- Mezcla de caracteres alfabéticos y no alfabéticos.
- No ser ni derivarse de una palabra del diccionario, de la jerga o de un dialecto.
- No derivarse del nombre del usuario o de algún pariente cercano.
- No derivarse de información personal (del número de teléfono, número de identificación, DNI, fecha de nacimiento, etc...) del usuario o de algún pariente cercano.

Los passwords no deben almacenados por escrito nunca. Intente crear passwords que pueda recordar fácilmente. Una forma de recordarlo con facilidad es crear un password basado en una frase fácilmente recordable (letras de canción, títulos de película, o frases muy conocidas). Por ejemplo:

La frase: **‘Esto Es Una Forma Muy Facil De Recordar Mi Password’**
Me sugiere el password: **‘EE1FMFDRMP’**



3.2.- Recomendaciones para la protección del password

No utilice el mismo password que utiliza para las cuentas de recursos y servicios UPV en otras cuentas no UPV (acceso a su proveedor de servicios personal, acceso a servicios de su banco, etc...).

Cuando sea posible, no utilice los mismos password en distintas cuentas y servicios UPV. Por ejemplo, utilice passwords distintos para su usuario UPVnet y para su acceso a los servicios web.

No comparta las cuentas y passwords UPV con nadie, incluyendo administrativos, secretarías, etc... Todos los passwords deben ser tratados como información sensible y confidencial.

A continuación se presenta una lista de cosas que **NO** se deben hacer:

- No revele su password por teléfono a NADIE, incluso aunque le hablen en nombre del servicio de informática o de un superior suyo en la organización.
- No revele el password en mensajes de correo electrónico ni a través de cualquier otro medio de comunicación electrónica.
- Nunca escriba el password en papel y lo guarde. Tampoco almacene passwords en ficheros de ordenador sin encriptar o proveerlo de algún mecanismo de seguridad.
- No revele su password a sus superiores, ni a sus colaboradores.
- No hable sobre un password delante de otras personas.
- No revele su password en ningún cuestionario o formulario, independientemente de la confianza que le inspire el mismo.
- No comparta el password con familiares.
- No revele el password a sus compañeros cuando se marche de vacaciones.
- No utilice la característica de "Recordar Password" existente en algunas aplicaciones (Outlook, Netscape, Internet Explorer).

Si alguien le pide el password, refiéralo a este documento o pídale que se comunique con el Área de Sistemas de Información y Comunicaciones (ASIC) de la UPV. Si sospecha que una cuenta o password puede haber sido comprometida, comuníquelo al ASIC y cambie los passwords de todas sus cuentas.

Cambie los passwords con la frecuencia recomendada para cada tipo de cuenta y servicio.

3.3.- Estandards de desarrollo de aplicaciones

Los desarrolladores de aplicaciones informáticas para el entorno de la Universidad Politécnica de Valencia y que gestionen sus propios mecanismos de autenticación mediante passwords, deben asegurarse de que sus programas contienen las siguientes precauciones en términos de seguridad respecto de la selección y uso de passwords:

- Deben soportar autenticación de usuarios individuales, no por grupos.
- No deben almacenar passwords en texto claro o en ninguna forma fácilmente reversible.
- Deben proveer de algún tipo de mecanismo de roles, de forma que un usuario pueda tomar las funciones de otro sin necesidad de conocer el password del anterior.
- Deben proveer de un mecanismo para expirar los passwords y obligar a los usuarios al cambio del mismo.
- Se debe limitar el número de intentos de accesos sin éxito consecutivos.



4.- MEDIDAS A APLICAR

El incumplimiento de la presente Política puede llegar a comprometer la seguridad de la totalidad de la red corporativa de la Universidad Politécnica de Valencia.

Será la **Comisión de Informática de la Universidad** la que decida las acciones a tomar en el caso de incumplimiento de la presente política una vez establecidas las repercusiones que sobre los recursos y servicios informáticos de la UPV haya podido tener la violación de la misma. Todo ello sin perjuicio de las acciones disciplinarias, administrativas, civiles o penales que en su caso correspondan, a las personas presuntamente implicadas en dicho incumplimiento.

