



POLÍTICA DE CONTRASEÑAS DE LA UNIVERSIDAD POLITÉCNICA DE VALENCIA

1.- OBJETIVO Y ÁMBITO DE APLICACIÓN

Las contraseñas son un aspecto fundamental de la seguridad de los recursos informáticos, es la primera línea de protección para el usuario. Una contraseña mal elegida o protegida 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 las contraseñas seleccionadas por ellos mismos para el uso de los distintos servicios ofrecidos a la comunidad universitaria a través de UPVnet.

La seguridad provista por una contraseña depende de que la misma se mantenga siempre en secreto, todas las directrices suministradas por esta política tienen por objetivo mantener esta característica fundamental en las contraseñas de los recursos de la UPV. El objetivo fundamental de esta política es establecer un estándar para la creación de contraseñas fuertes, la protección de dichas contraseñas, y el cambio frecuente de las mismas.

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 una contraseña) en cualquiera de los sistemas de la Universidad Politécnica de Valencia.

2.- POLÍTICA GENERAL

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

- Todas las contraseñas de sistema (root, administradores NT, cuentas de administración de aplicaciones, etc...) deben ser cambiados al menos una vez cada seis meses.
- Todas las contraseñas de usuario (cuentas de UPVnet, cuentas de email, cuentas de servicios Web, etc...) deben ser cambiadas al menos una vez cada doce meses. Sin embargo, se recomienda cambiarla con mayor frecuencia y también siempre que el usuario sospeche que la seguridad de su contraseña 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 contraseñas distintas del resto de cuentas mantenidas por dicho usuario en los servicios y recursos UPV.
- Las contraseñas no deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica. Tampoco deben ser comunicadas las contraseñas en conversaciones telefónicas.
- En la medida de lo posible, las contraseñas serán generadas automáticamente con las características recomendadas en esta política y se les comunicará a los usuarios su contraseña siempre en estado "expirado" para obligar al usuario a cambiarla en el primer uso que hagan de la cuenta o servicio.



- Las contraseñas por defecto asociadas a los sistemas o aplicaciones nuevas deberán ser cambiadas antes de poner estos sistemas en producción. También se desactivarán aquellas cuentas “por defecto” que no sean imprescindibles.
- Todas las contraseñas 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 de la contraseña podrán determinar medidas adicionales de protección de la misma.

3.- SELECCIÓN Y CUSTODIA DE CONTRASEÑAS

3.1.- Recomendaciones generales para la selección de contraseñas

Las contraseñas son usadas con múltiples propósitos en la Universidad Politécnica de Valencia, como pueden ser las contraseñas de cuentas de usuario UPVnet, contraseñas 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 contraseñas seguras para la autenticación en todos los recursos y servicios de la UPV.**

La seguridad de este tipo de autenticación se basa en dos premisas:

- 1- La contraseña personal sólo la conoce el usuario.
- 2- La contraseña es lo suficientemente “fuerte” para no ser descifrada.

La contraseña para ser considerada “**fuerte**” (**segura**) debe poseer las siguientes características:

- Debe tener al menos 15 caracteres .
- Utiliza caracteres de tres de los cuatro grupos siguientes, y SIEMPRE QUE UNO DE ELLOS DEBERÁ SER UN SÍMBOLO:
 1. Letras minúsculas.
 2. Letras mayúsculas.
 3. Números (por ejemplo, 1, 2, 3).
 4. Símbolos (por ejemplo, ¡, @, Ñ, =, -, etc.).
- 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.

Adicionalmente, las contraseñas en UPVnet deben cumplir las siguientes recomendaciones:

- No podrá contener 3 o más caracteres consecutivos del nombre de usuario de UPVnet o del nombre completo de la persona.
- No podrá tener espacios en blanco.

Finalmente, si prevé viajar al extranjero o utilizar teclados que no sean españoles, tenga en cuenta que los símbolos que utiliza en su contraseña pueden estar en sitios diferentes del teclado; por ejemplo no use letras ‘ñ’ si viaja mucho y no conoce cómo introducirla en teclados no españoles.

Las contraseñas no deben ser almacenadas por escrito nunca. Intente crear contraseñas que pueda recordar fácilmente. Una forma de recordarlo con facilidad es crear una contraseña basada en una frase fácilmente recordable.



Por ejemplo:

La frase: 'Camarero, una de mero'
Me sugiere la contraseña: 'Camarero!,1demero'

3.2.- Recomendaciones para la protección de la contraseña

No utilice la misma contraseña 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 las mismas contraseñas en distintas cuentas y servicios UPV. Por ejemplo, utilice contraseñas distintas para su usuario UPVnet y para su correo electrónico.

No comparta las cuentas y contraseñas UPV con nadie, incluyendo administrativos, secretarías, etc... Todas las contraseñas deben ser tratadas como información sensible y confidencial.

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

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

Si alguien le pide la contraseña, refiérase 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 su contraseña pueden haber sido comprometidas, comuníquelo al ASIC y cambie las contraseñas de todas sus cuentas.

Cambie las contraseñas con la frecuencia recomendada para cada tipo de cuenta y servicio.

3.3.- Estándares 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 contraseñas, deben asegurarse de que sus programas contienen las siguientes precauciones en términos de seguridad respecto de la selección y uso de contraseñas:

- Deben soportar autenticación de usuarios individuales, no por grupos.
- No deben almacenar contraseñas 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 la contraseña del anterior.
- Deben proveer de un mecanismo para expirar las contraseñas y obligar a los usuarios al cambio de la misma.
- 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.

