

ANEXO RECOMENDACIONES SOBRE USO DE CONTRASEÑAS.

Índice de contenido

| | |
|--|---|
| 1.- OBJETIVO Y ÁMBITO DE APLICACIÓN..... | 1 |
| 2.- RECOMENDACIONES GENERALES..... | 1 |
| 3.- ELECCIÓN Y PROTECCIÓN DE CONTRASEÑAS..... | 2 |
| 3.1.- Recomendaciones generales para la elección de contraseñas..... | 2 |
| 3.2.- Recomendaciones para la protección de contraseñas..... | 2 |

1.- OBJETIVO Y ÁMBITO DE APLICACIÓN.

El uso de contraseña es un aspecto fundamental de la seguridad de los recursos informáticos; una contraseña mal elegida o protegida pueden generar problemas de seguridad en la organización.

El objetivo fundamental de este documento es establecer un estándar para la creación de contraseñas fuertes, favorecer su protección, así como el cambio frecuente de las mismas.

El ambito de estas recomendaciones incluye a todos aquellos usuarios de los servicios y recursos informáticos de la Universidad de Murcia que tienen o son responsables de una cuenta (o cualquier otro tipo de acceso que requiera contraseña) en cualquiera de los sistemas de la Universidad de Murcia.

2.- RECOMENDACIONES GENERALES

Todo usuario de la Universidad de Murcia es responsable de velar por la seguridad de las contraseñas seleccionadas por él mismo para el uso de los distintos servicios y recursos ofrecidos. Cualquier contraseña es de uso exclusivo, y por tanto intransferible, del usuario al que se ha otorgado

Han de seguirse las siguientes directrices:

- Todas las contraseñas de sistema (cuentas de administrador, cuentas de administración de aplicaciones, etc...) deberán cambiarse con una periodicidad de al menos una vez cada seis meses.
- Todas las contraseñas de usuario (cuentas de correo, cuentas de servicios web, etc...) deberán cambiarse al menos una vez cada doce meses.
- Ante la sospecha de que una contraseña haya sido comprometida, se cambiará la misma de forma inmediata, y se procederá a avisar del incidente de seguridad por los cauces establecidos (sistema DUMBO).
- Las cuentas de usuario que tengan privilegios de sistema a través de su pertenencia a grupos o por cualquier otro medio, deberán tener contraseñas distintas a otras cuentas mantenidas por dicho usuario en los servicios y recursos.
- En la medida de lo posible, las contraseñas serán generados 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 cambiarlo en el primer uso que hagan de la cuenta o servicio.

3.- ELECCIÓN Y PROTECCIÓN DE CONTRASEÑAS

3.1.- Recomendaciones generales para la elección de contraseñas

Se debe poner especial atención en la selección de contraseñas fuertes para la autenticación en todos los recursos y servicios de la Universidad de Murcia.

Una contraseña *fuerte* tiene, entre otras, las siguientes características:

- Más de ocho 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.

Las contraseñas deben crearse de forma que puedan recordarse fácilmente, bien de forma directa o a través de reglas nemotécnicas

3.2.- Recomendaciones para la protección de contraseñas

Se recomienda proteger la contraseña elegida con las siguientes recomendaciones:

- Usar contraseñas diferenciadas en función del uso (por ejemplo no debe usarse la misma para una cuenta de recursos y servicios que la usada para acceso a servicios bancarios).
- Si se dispone de diferentes cuentas de acceso a servicios y recursos en la Universidad, deben usarse distintas claves para cada una de ellas.
- No compartir de ninguna forma cuentas y contraseñas. Son estrictamente personales e intransferibles.
- No revelar ni compartir su contraseña por teléfono, correo electrónico, anotándola o de cualquier otra forma a nadie, incluso aunque le hablen en nombre de ATICA o de un superior suyo en la organización.

- Nunca escribir la contraseña, ni almacenarla en ficheros sin encriptar, ni comunicarla en el texto de mensajes de correo electrónico, ni en ningún otro medio de comunicación electrónica.
- No se comunicarán en conversaciones telefónicas.
- Cambiar las contraseñas con la frecuencia recomendada para cada tipo de cuenta y servicio.