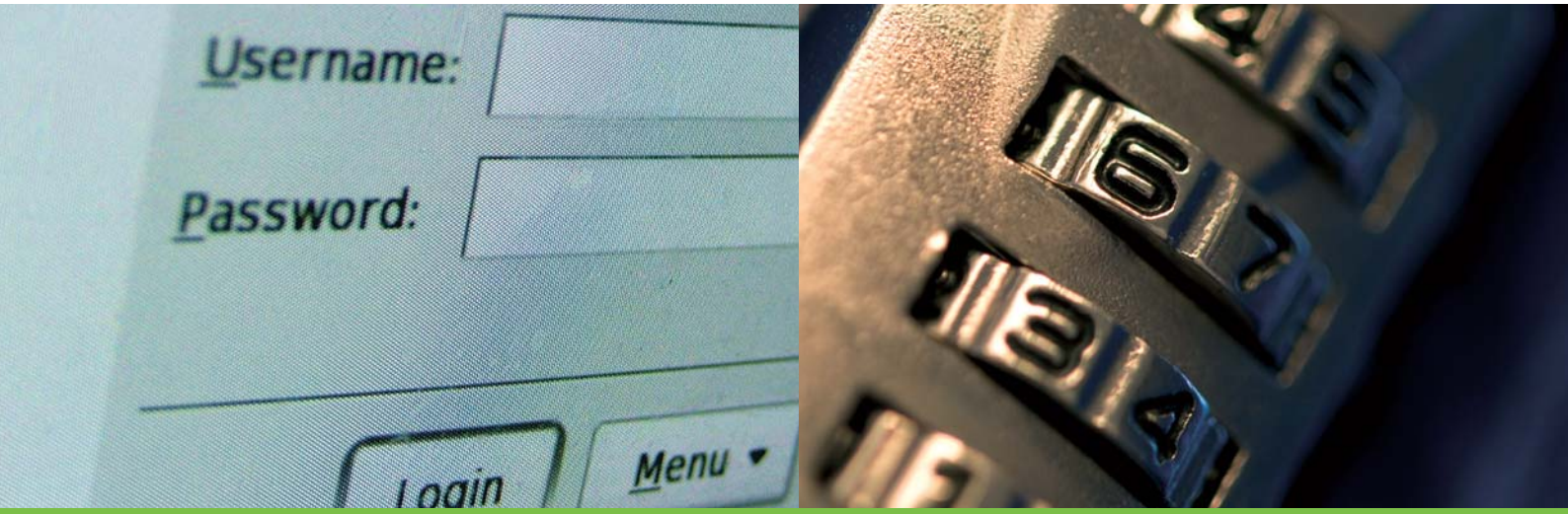
Recomendaciones básicas para **elegir una contraseña correcta**



acens
the hosting company

acens Technologies S.A.
San Rafael 14 - Pol. Ind. Alcobendas
28108 Madrid
902 90 10 20
www.acens.com

Introducción

Las contraseñas deben cumplir unas reglas básicas que las hagan difícilmente adivinables, tanto por personas como muy en especial por procesos automáticos que utilizan combinaciones basadas en palabras del diccionario y/o conmutaciones de números y letras.

Recomendaciones

1 **Nunca establezca una contraseña nula o que sea igual al nombre del usuario (p.e. usuario: prueba, contraseña: prueba).**
Aunque se trate de un acceso temporal tenga en cuenta que continuamente se realizan intentos de acceso a toda máquina conectada a Internet.

2 **No escoja una palabra que figure en algún diccionario de cualquier idioma.**
En esos "barridos" realizados contra los servidores se emplean diccionarios para probar la coincidencia de la contraseña con cada una de las palabras.

3 **No escoja un nombre propio o el nombre de una localidad.**
Suelen ser incluidos en los diccionarios como posibles contraseñas.

> "Combine minúsculas, mayúsculas, números y símbolos en la contraseña. Esto evita los ataques de diccionario y dificulta los ataques de «fuerza bruta»."

4 **Evite secuencias, frases hechas o de argot.**
No utilice secuencias de teclado, frases hechas o palabras que aunque no figuran en diccionario pertenecen al argot asociado a cierto ámbito (p.e. qwerty, 12345, noseque, foobar, devnull, homerun).

5 **No use combinaciones o permutaciones de palabras.**
Es decir, no componga una contraseña realizando operaciones de sustitución o cambio de orden en las letras de una palabra de las categorías anteriores (p.e. sustituir la letra "i" por el número "1", la letra "o" por el número "0", invertir el nombre de las letras, añadir un simple número a una palabra, etc.), como puede imaginar, las máquinas que están realizando pruebas para dar con la contraseña correcta realizan estas operaciones en cuanto han probado con todas las palabras, realizando todas las permutaciones y combinaciones posibles.

6 **Combine minúsculas, mayúsculas, números y símbolos en la contraseña**
Esto evita los ataques de diccionario y dificulta los ataques de "fuerza bruta", los símbolos deben ser "imprimibles" para evitar que se envíen comandos de control que puedan ser no aceptados por la aplicación de login.

7 **Establezca contraseñas de al menos 8 ó 10 caracteres de longitud**
Cuanto más longitud tenga la contraseña mayor será la dificultad en averiguarla.

Por último, debe saber que existen herramientas on-line para chequear la robustez de una contraseña, desde la página **http://www.securitystats.com/tools/password.php** se puede determinar el nivel de seguridad alcanzado por una contraseña y se efectúan recomendaciones para mejorarla, aunque obviamente desde la misma página se recomienda no introducir contraseñas que estemos empleando en sistemas de producción.