Acceder Al Computador Sin La Contraseña En Cualquier Sistema Operativo

Sin duda alguna la implementación de una contraseña en los equipos son una gran utilidad al momento de prevenir intrusiones, ya sea de alguna persona que desee ver nuestros archivos ó aquellos que quieran realizar una intrusión de forma remota . ¿Pero si eres una persona olvidadiza? Grave problema, ¿Verdad? . No te preocupes, en realidad nada es seguro ;) En Windows, Linux, y Mac OS X, puede acceder al computador sin la contraseña, usando algunos métodos que pueden ser bastantes útiles para extraer la información necesaria o incluso usar la terminal con acceso completo a ella.

En otros dispositivos donde no se puede obtener acceso a los archivos, pero se puede realizar un reinicio del dispositivo y tener acceso a él. Los siguientes trucos requieren acceso físico al dispositivo. Ahora si, empecemos a mirar como hacerlo en cada Sistema Operativo:

Windows

En Windows, existen distintas forma de restablecer la contraseña. Windows permite crear un **disco de restablecimiento de contraseña** que puede restablecer la contraseña de una manera «apropiada». Puedes crear el disco y usarlo cuando sea necesario. Siendo sincero, un informático, ¿De cuantos discos ó USB se puede armar? De varias, ¿Verdad? En caso dado, tendremos que buscar otras alternativas para acceder a nuestra información.

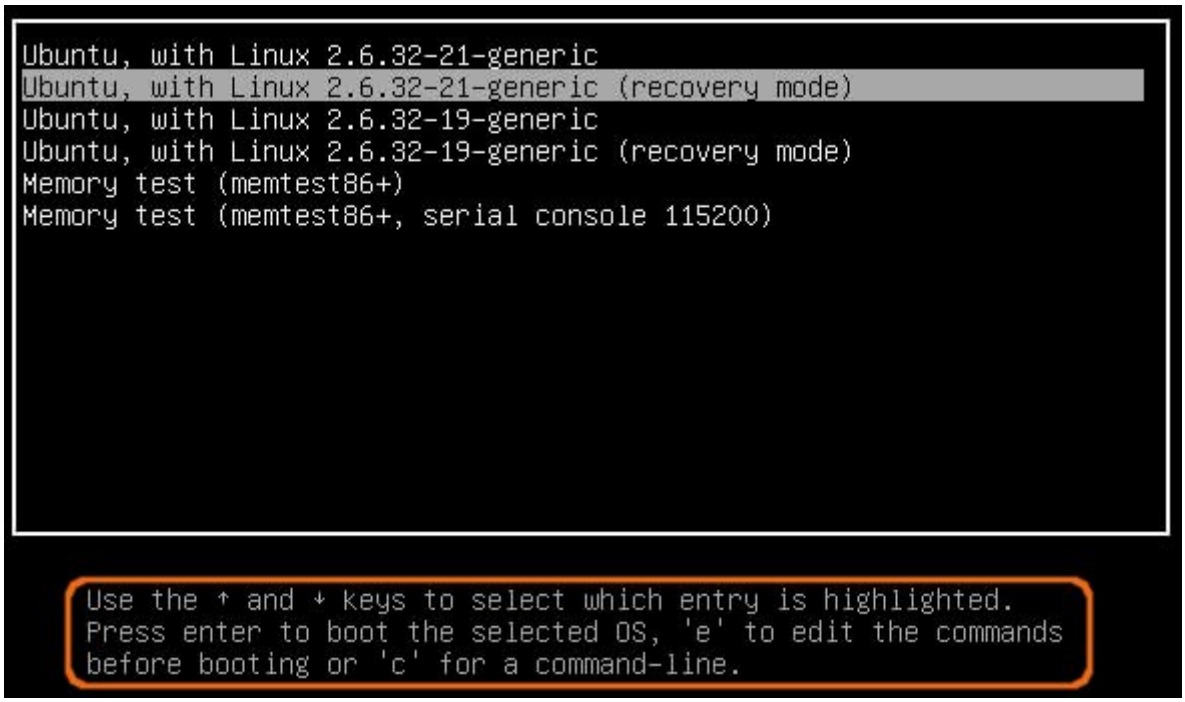
Por ejemplo, el Offline NT Password & Registry Editor nos viene como anillo al dedo para **entrar a Windows sin una contraseña**. Para esto, podemos crear una USB booteable para usar esta herramienta. Con esta herramienta se puede **editar el registro de Windows**, lo que le permite borrar la contraseña asociada a la cuenta de usuario a la cual deseas acceder. Una vez hecho esto, puede arrancar Windows e iniciar sesión en la cuenta, la cual ahora estará sin contraseña. Incluso si está usando Windows 8 con una cuenta de Microsoft, puede restablecer la contraseña del administrador de una cuenta asociada para obtener el acceso.

¿Como Protegernos?

¿Y si somos las víctimas de esto? Para evitar el ingreso de esta manera podemos configurar una contraseña a la BIOS y evitar el arranque desde dispositivos externos. Cabe recalcar que podemos configurar dos tipos de contraseña desde la BIOS, una contraseña para el acceso a esta (BIOS) y otra para el arranque del equipo. Aunque este método también tiene su falencia, ya que el «atacante» podría borrar la contraseña de la BIOS. La unica forma de evitar realmente el acceso, es cifrando la unidad del sistemas con BitLocker, ya que impediría las consulta y modificación del registro. El cifrado es la única y mejor protección.

Linux

Vamos a utilizar a Ubuntu como ejemplo. Ubuntu ofrece un **modo de recuperación en su menú de arranque** Grub, puede seleccionar Opciones avanzadas y luego seleccionar el modo de recuperación. Verá el menú de inicio al arrancar el ordenador; si no lo hace, puede mantener pulsada la tecla Mayús mientras se arranca y aparecerá el menú. Puede abrir sin problemas un editor de comandos.



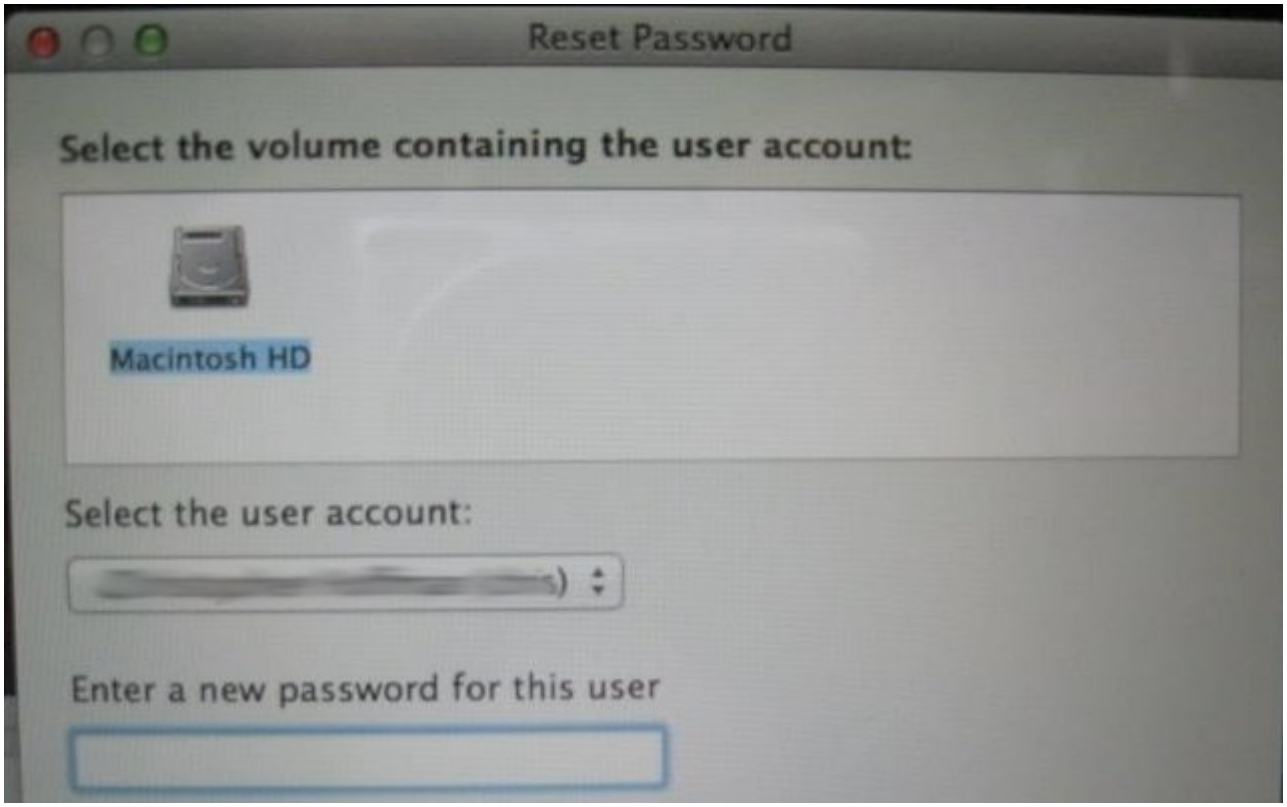
Esta opción no es necesaria, ya que sólo tiene que pulsar el botón e para editar las opciones de arranque de Ubuntu y arrancar directamente en una consola. A continuación, puede ser capaz de usar la linea de comandos como root y con esto cambiar las contraseñas en el sistema. Si el menú de arranque Grub está bloqueado y protegido por contraseña, aún puede iniciar desde el modo Live y cambiar su contraseña desde allí.

¿Como Protegernos?

Una vez más, el cifrado protege la lectura y modificación de los archivos. Utilizamos Ubuntu como un ejemplo, pero casi todas las distribuciones de Linux usan Grub como el gestor de arranque y pocas personas establecen una contraseña para el Grub.

Mac OS X

Los equipos con Mac, cuentan con una herramienta integrada para restablecer la contraseña, y es muy fácil de acceder a ella. Esta opción está disponible en el modo de recuperación. Cuando el equipo se reinicie, pulse y mantenga las teclas **Comando + R** y se iniciara en el modo de recuperación.



Haga clic en el menú Herramientas en modo de recuperación, seleccione Terminal, escriba **resetpassword** en el terminal, y pulse Enter. Verás la utilidad de restablecimiento de contraseña, que le permite **restablecer la contraseña de cualquier cuenta de usuario en el Mac**.

¿Como Protegernos?

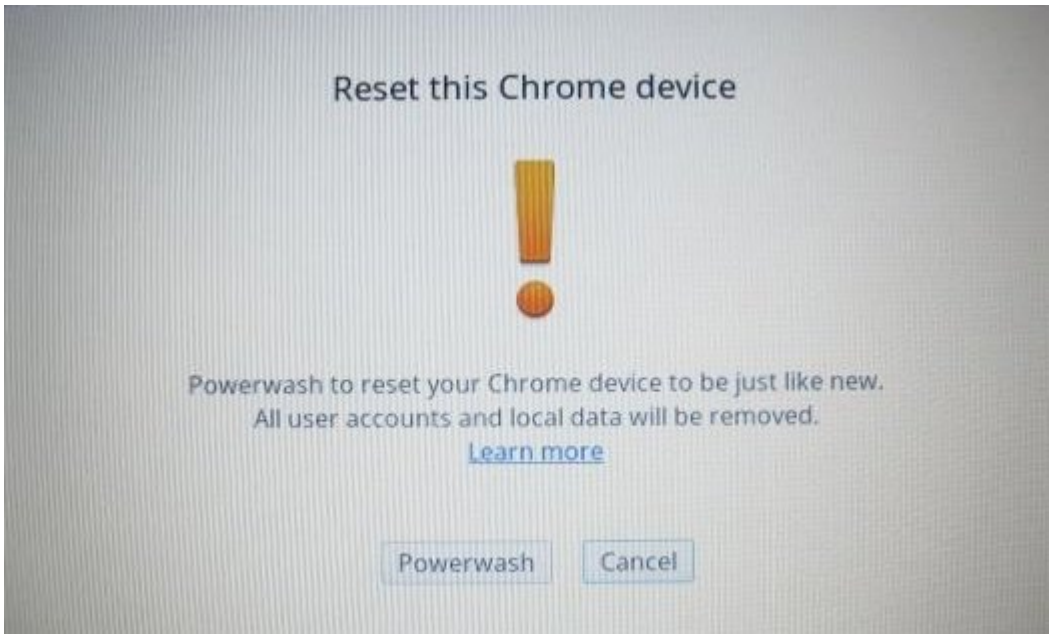
Para evitar que la contraseña de su Mac sea restablecida, puede habilitar el cifrado de disco en tu Mac con **FileVault**, establecer una contraseña de firmware dentro del modo de recuperación, o ambos métodos.

Bonificación

Bastante interesante los métodos, ¿no? Desafortunadamente todo sistema es inseguro, y no solo los computadores ó portátiles con los anteriores Sistemas Operativos pueden ser accesados, vulnerando la seguridad con contraseña. A continuación mostraremos que esto también podrá se aplicado en dispositivos móviles, como tablets ó SmartPhones.

Chrome OS

Como en todos los productos de Google, la cuenta de Google (Gmail) es usada para dar acceso a dispositivos y servicios. Supongamos que tiene un **Chromebook** que desea usar, pero no se puede iniciar sesión. Tal vez has olvidado la contraseña de Google asociada con el dispositivo. En este escenario, puede arrancar el Chromebook y presionar **Ctrl + Shift + Alt + R** al mismo tiempo. Se le pedirá si desea reestablecer al estado de fabrica el dispositivo. Después de restablecerlo, puedes iniciar sesión con otra cuenta de Google y de ahora en adelante esta sera la cuenta propietaria del dispositivo. Esto borrará todos los datos en el dispositivo.



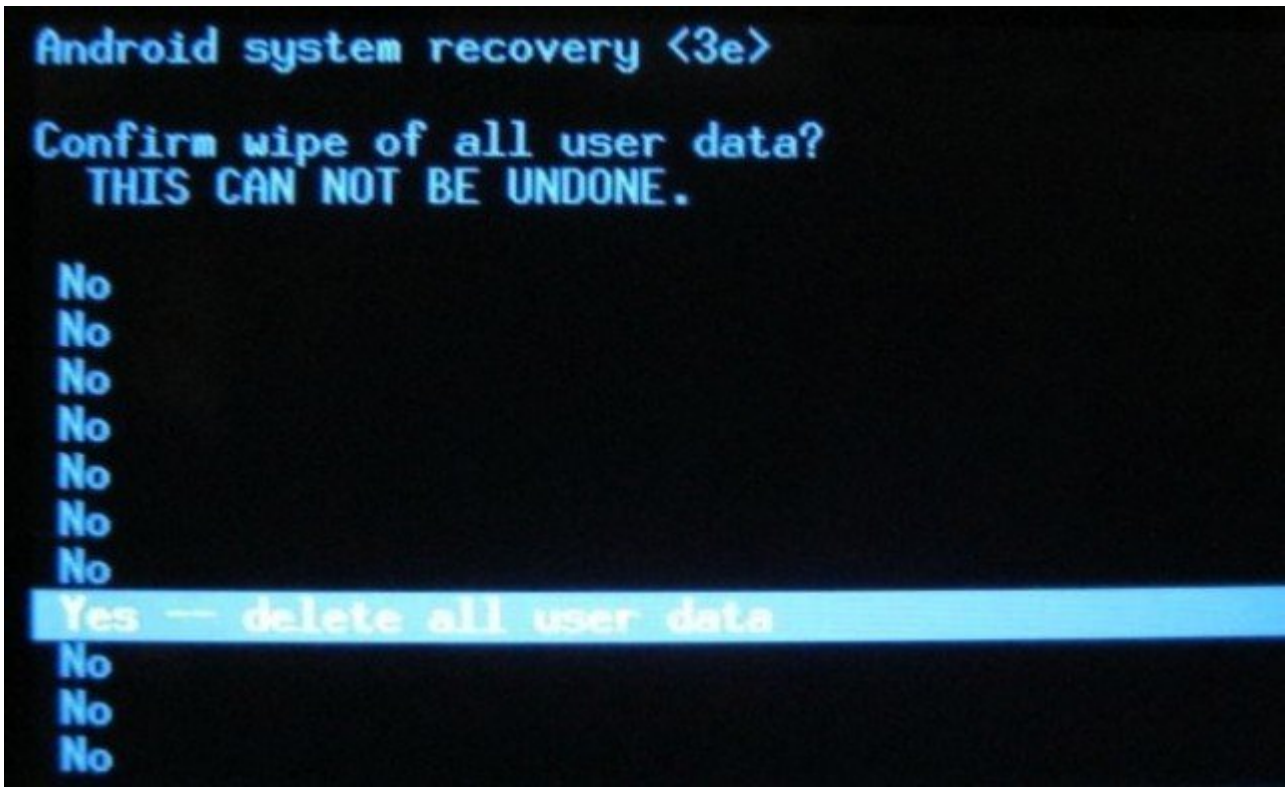
¿Como Protegernos?

No hay forma de obtener acceso a los archivos de un usuario sin su contraseña en un Chromebook – esos archivos están encriptados por defecto.

Android

Al igual que con Chromebook, la cuenta de Google esta asociada con el dispositivo, y cuando se ha intentado desbloquear varias veces sin éxito el dispositivo, terminaremos bloqueandolo, y solo podrá ser usado nuevamente ingresado los datos correctos de la cuenta de Google. Si no tiene esta información, puede ser fácil omitir el paso de desbloqueo en el dispositivo con otros métodos. Esto debería ser fácil en un dispositivo cuando la depuración USB está activado, ya que se podría manipular usando adb desde la terminal de la computadora, pero, es por eso que la depuración USB está desactivada por defecto.

Se podrá realizar un restablecimiento de fábrica desde el modo de recuperación, esto hará que el dispositivo vuelva a su estado de fábrica, borrando los datos del dispositivo. A continuación, puede iniciar sesión y configurar el dispositivo con otra cuenta de Google.



¿Como Protegernos?

En realidad no necesitamos, ya que como se menciono, por defecto se ha des habilita el modo de depuración USB, cuando se restablece el dispositivo se borraran todos los datos, así que no serán capaces de ver los datos que habían.

iOS

Las terminales iPhones, iPads y iPod Touch también cuentan con una forma de restablecer su contraseña. A diferencia de Android, estos productos de Apple pueden ser restaurados usando los datos de usuario de esta empresa. Ademas de esto, se puede obtener una copia de seguridad de todos los datos del dispositivo gracias a la sincronizacion con iCloud.

Apesar de tener una alternativa para no perder sus datos, todavía puede reiniciar los valores de fabrica del dispositivo usando el modo de recuperación. Apague el dispositivo, mantenga pulsado el botón de inicio, y luego conecte el cable USB del dispositivo al ordenador. Si no se enciende automáticamente, enciéndala. iTunes te dirá que ha detectado un dispositivo en modo recuperación y permitirá restaurar la configuración predeterminada de fábrica.

¿Como Protegernos?

Si alguien tiene acceso físico a su dispositivo y desea eliminar la contraseña, no hay nada que puedas hacer para detenerlos. Incluso cifrar sus archivos sólo protegerá sus

datos personales, siempre se podrá borrar la información y empezar de nuevo.