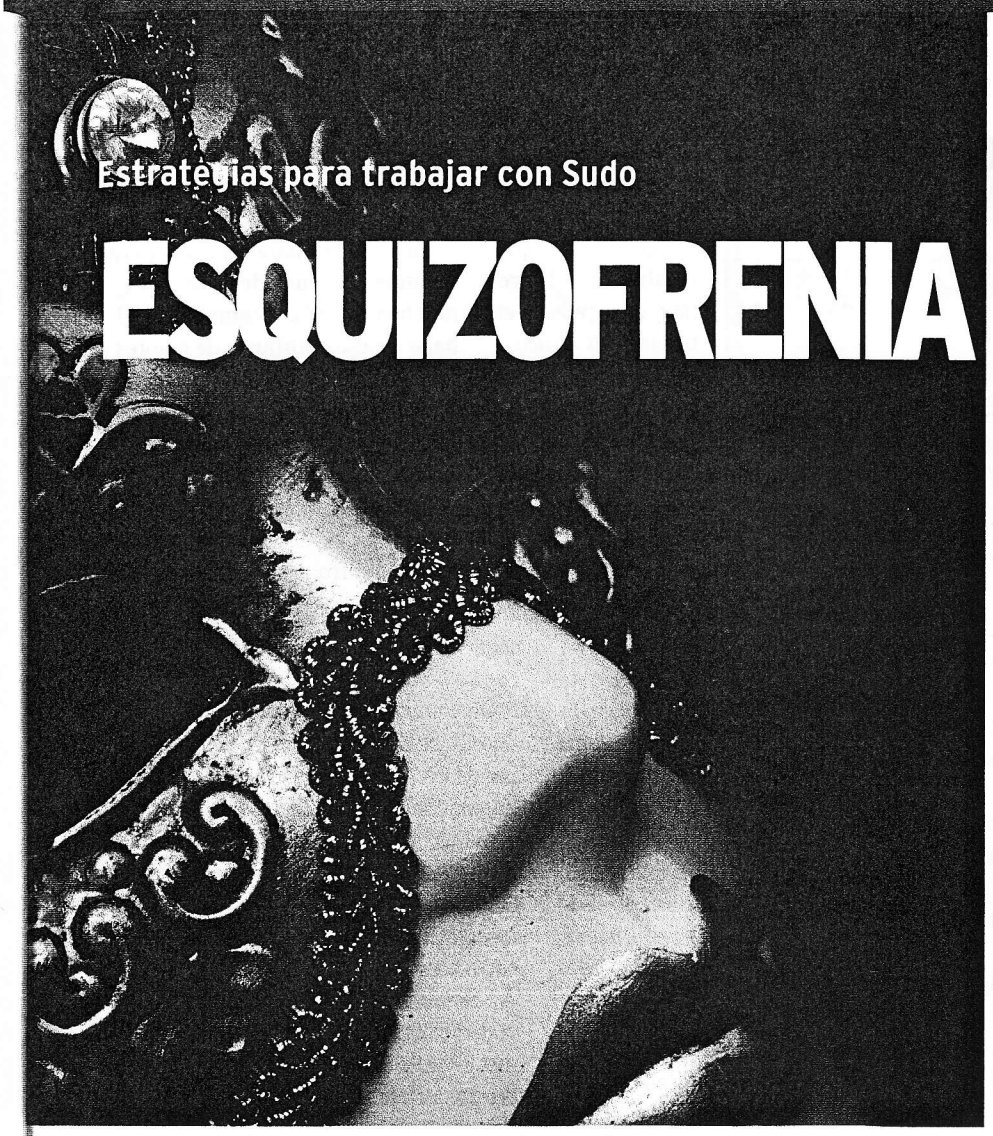

Estrategias para trabajar con Sudo

ESQUIZOFRENIA

El comando *sudo* nos ayuda a trabajar sin estar expuestos. Examinamos algunas técnicas para operar con él. **POR JAMES MOHR**

Antes que permitir a los usuarios registrarse directamente en la cuenta de root, los administradores de sistemas utilizan a menudo el comando *su*. *su* nos permite cambiar a un nuevo usuario y operar con los permisos de ese usuario. El inconveniente de este método es que el usuario *su* puede hacer cualquier cosa que pueda hacer el usuario destino.

Muchas empresas creen que es una salvaguarda suficiente requerir que los usuarios se logueen en sus propias cuentas, y luego hagan *su* a la cuenta del administrador para llevar a cabo las tareas requeridas. Esta solución es práctica porque sólo necesitamos asegurar que todo el mundo tiene acceso a la contraseña de administrador, pero tiene el problema de seguridad añadido de que cualquiera con una contraseña de administrador se convierte en administrador y puede hacer *todo* lo que quiera.

Una buena alternativa es el comando *sudo*. Al igual que *su*, *sudo* nos permite ejecutar un comando como el usuario requerido, pero una vez que se haya completado, nos devuelve al contexto del usuario original. En realidad, podemos ejecutar *su* de forma que sólo se ejecute un comando, pero *sudo* nos permite restringir el acceso con posibilidades más potentes.

Debemos tener precaución al usarlo: si *sudo* está configurado de manera incorrecta, puede dejarnos en una situación igual de vulnerable que si no lo utilizáramos. Vamos a repasar algunas técnicas para trabajar con *sudo*.

Límites sin Restricción

He observado que muchos administradores usan *sudo* simplemente como una versión modificada de *su*, ejecutando todos los comandos como administrador. Aunque el acto de volver a invocar el comando con cada instrucción proporciona un recordatorio extra sobre la necesidad de tener precaución, sólo es necesario usar *sudo* para iniciar *bash*, por ejemplo, y la sesión es básicamente la misma que si hubiéramos ejecutado *su*. Algunos administradores extreman un poco el cuidado y limitan qué comandos pueden ejecutarse, pero incluso eso sólo toca superficialmente las posibilidades de *sudo*.

La configuración por defecto de muchas distribuciones Linux permiten al usuario ejecutar cualquier comando como administrador vía *sudo*, suponiendo que conozcan la contraseña de administrador. Si se trata de nuestro equipo de escritorio y tenemos la contraseña de administrador de todas formas, es un buen hábito usar *sudo* en lugar de *su*. Muchas tareas administrativas iniciadas mediante la interfaz gráfica KDE se inician en realidad con *kdesu*, que nos solicita la contraseña de administrador antes de continuar (véase la Figura 1).

Con *sudo*, no sólo basta con tener la contraseña del usuario destino: estamos limitados por los comandos definidos en la configuración de *sudo* en el archivo */etc/sudoers*. Para editar este archivo podemos utilizar *visudo*, que hace primero una copia y luego reemplaza el original al finalizar. Antes de guardar el archivo, se efectúa una verificación de sintaxis, y en caso de encontrar algún error, se muestra un mensaje por pantalla indicando el número de línea y el tipo de error, lo que nos da la oportunidad de volver a editar el archivo. Podemos salir sin guardar, o guardar los cambios en cualquier caso, lo que genera un aviso del sistema (véase la Figura 2).

Configurar Sudo

En el archivo *sudoers* por defecto, generalmente sólo se definen unas cuantas opciones. Estas opciones se dividen en tres tipos de directivas. El primer tipo define ciertos comportamientos por defecto. Las configuraciones pueden ser booleanas (on/off), enteros y cadenas. Generalmente sólo hay una directiva por línea, pero si es demasiado larga, podemos continuar de la manera habitual en Linux terminando la línea con una barra invertida (\).

Cuando se definen los valores por defecto, la línea tiene el formato general:

```
Defaults option
```

Por ejemplo:

```
Defaults env_reset
```

Esta entrada la indica a *sudo* que resetee las variables de entorno a las del usuario des-