PRÁCTICA 7

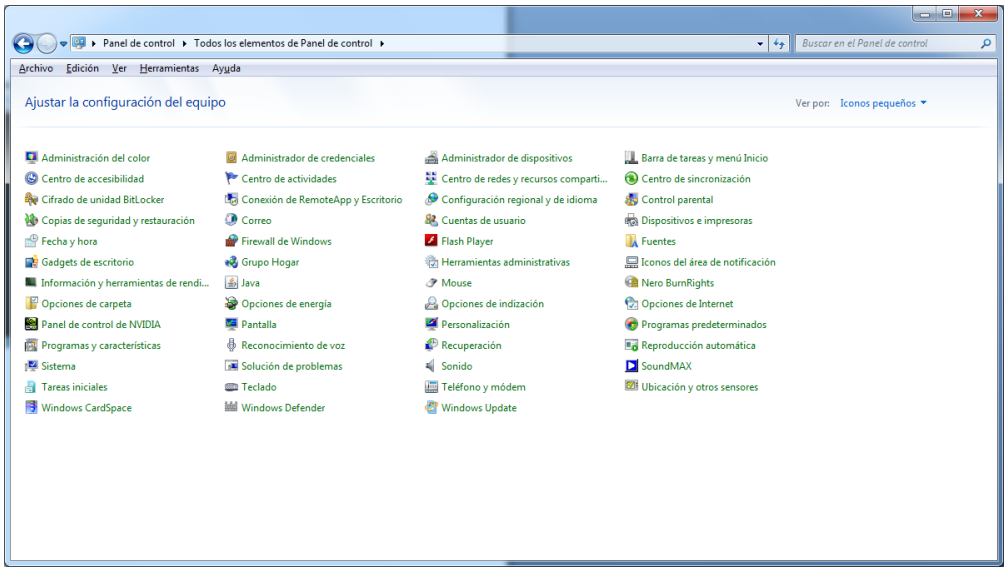
H- Verifica la auditoria de control de acceso “Visor de sucesos” de dicho usuario en Windows y Linux.

- **<u>Windows</u>**

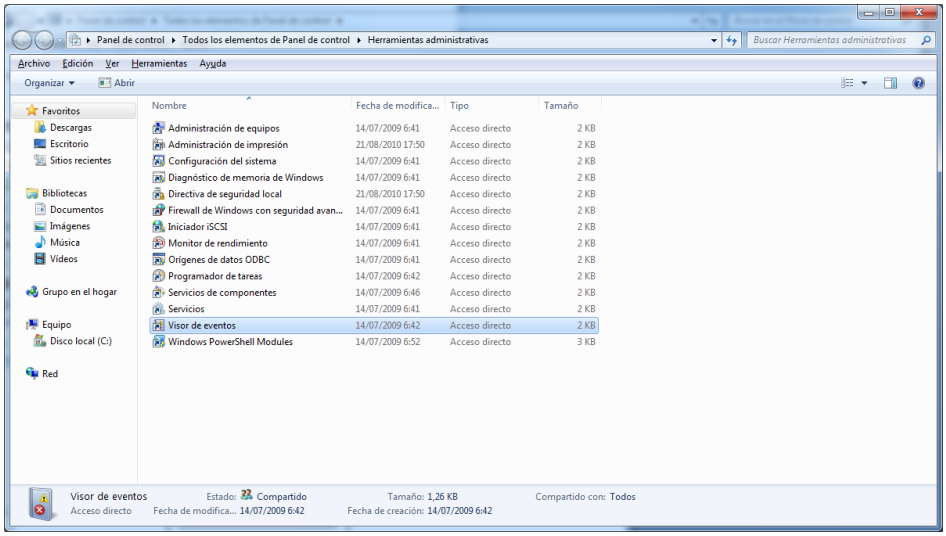
Si un controlador no funciona o lo hace de forma defectuosa Windows incorpora el Visor de sucesos, que nos permite analizar qué es lo que ha ocurrido con el controlador que está causando problemas.

Si un controlador no funciona y quieres saber que ha pasado abre el visor de sucesos de la siguiente forma:

Haz clic sobre el botón Inicio y a continuación sobre Panel de Control.

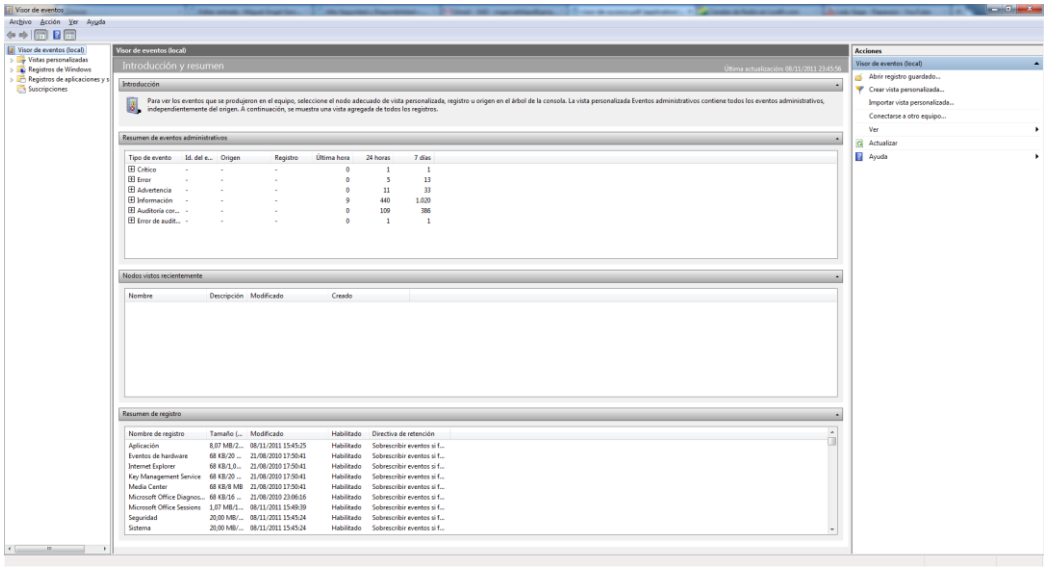


Ahora debes hacer doble clic sobre el icono de Herramientas Administrativas y luego nuevamente doble clic sobre el icono Visor de Sucesos.

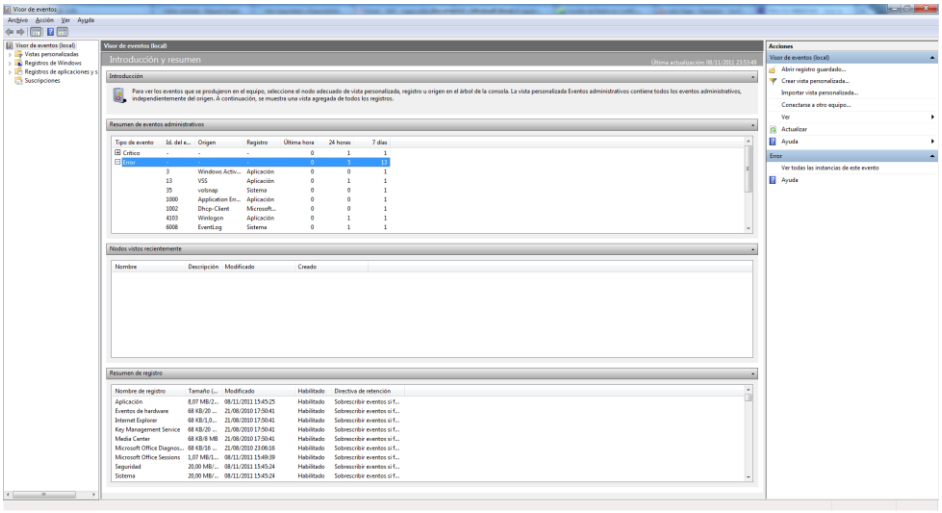


A continuación verás una ventana en la se registran todos los sucesos de Windows, y también verás si alguno de ellos está fallando.

Ahora si haces doble clic sobre el controlador que marca el error, accederás a otra ventana en la muestra la causa del error.

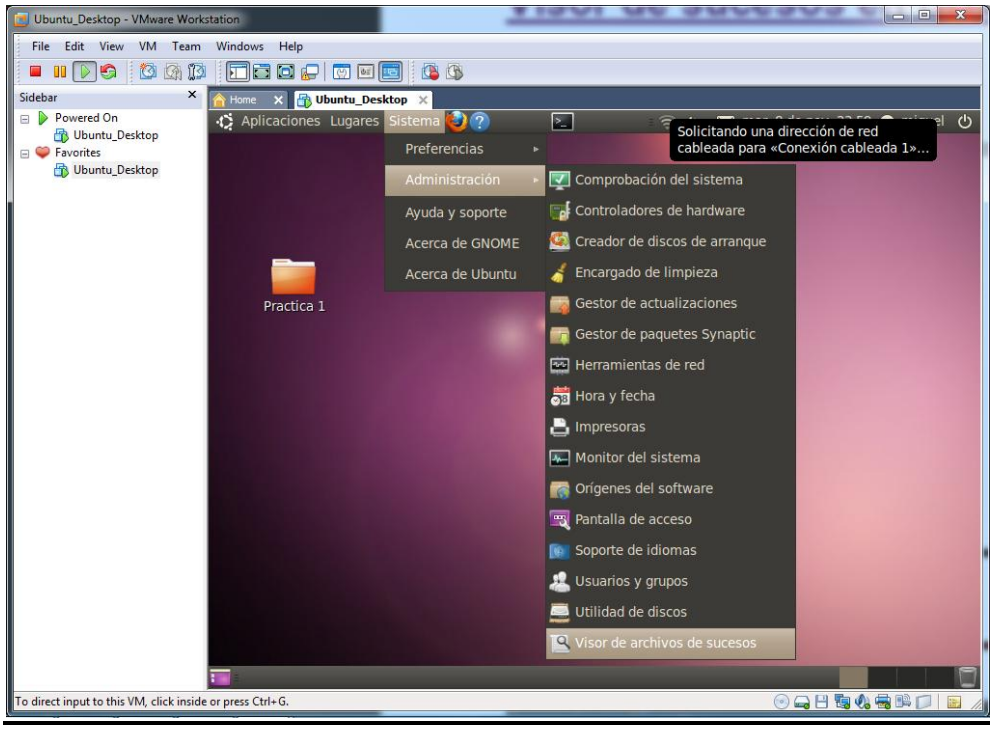


Por ejemplo si un usuario intenta tener acceso a una unidad de red y se produce un error, ese intento se registra como Acceso Erróneo Auditado.


Visor de eventos
Archivo Acción Ver Ayuda
Visor de eventos (local)
Vistas personalizadas
Registros de Windows
Registros de aplicaciones y s
Suscripciones
Visor de eventos (local)
Introducción y resumen
Última actualización: 08/11/2011 23:53:49
Introducción
Para ver los eventos que se produjeron en el equipo, seleccione el nodo adecuado de vista personalizada, registro u origen en el árbol de la consola. La vista personalizada Eventos administrativos contiene todos los eventos administrativos, independientemente del origen. A continuación, se muestra una vista agregada de todos los registros.
Resumen de eventos administrativos
Tipo de evento Id. del e... Origen Registro Última hora 24 horas 7 días
Crítico - - - 0 1 1
Error - - - 0 3 13
3 Windows Activ... Aplicación 0 0 1
13 VSS Aplicación 0 1 1
25 volsnap Sistema 0 0 1
1000 Application Er... Aplicación 0 0 1
1002 Dhcp-Client Microsoft... 0 0 1
4103 Winlogon Aplicación 0 1 1
6008 EventLog Sistema 0 1 1
Nodos vistos recientemente
Nombre Descripción Modificado Creado
Resumen de registro
Nombre de registro Tamaño (... Modificado Habilitado Directiva de retención
Aplicación 8,07 MB/2... 08/11/2011 15:45:25 Habilitado Sobrescribir eventos si f...
Eventos de hardware 68 KB/20 ... 21/08/2010 17:50:41 Habilitado Sobrescribir eventos si f...
Internet Explorer 68 KB/1,0... 21/08/2010 17:50:41 Habilitado Sobrescribir eventos si f...
Key Management Service 68 KB/20 ... 21/08/2010 17:50:41 Habilitado Sobrescribir eventos si f...
Media Center 68 KB/8 MB 21/08/2010 17:50:41 Habilitado Sobrescribir eventos si f...
Microsoft Office Diagnos... 68 KB/16 ... 21/08/2010 23:06:18 Habilitado Sobrescribir eventos si f...
Microsoft Office Sessions 1,07 MB/1... 08/11/2011 15:49:39 Habilitado Sobrescribir eventos si f...
Seguridad 20,00 MB/... 08/11/2011 15:45:24 Habilitado Sobrescribir eventos si f...
Sistema 20,00 MB/... 08/11/2011 15:45:24 Habilitado Sobrescribir eventos si f...
Acciones
Visor de eventos (local)
Abrir registro guardado...
Crear vista personalizada...
Importar vista personalizada...
Conectarse a otro equipo...
Ver
Actualizar
Ayuda
Error
Ver todas las instancias de este evento
Ayuda

- **Ubuntu**

Para acceder al visor de sucesos en Ubuntu, nos situamos en Administración, Visor de archivos de sucesos.



En **auth.log1** podemos ver los accesos de los usuarios en diferentes días, con esta técnica podemos controlar todo tipo de accesos y posibles ataques a nuestro sistema de gente que no teníamos prevista su acceso.