Auditoria de Seguridad en Windows
Práctica 11

1. Objetivo

En esta práctica el alumno debe aprender a utilizar las herramientas que permiten auditar la seguridad de un computador. Para ello, el alumno debe realizar 3 tareas:
1.-Activar y configurar los controles de seguridad.
2.-Activar y configurar la auditoría de seguridad, para controlar los eventos que se generan.
3.-Analizar los registros de eventos de seguridad, para evaluar problemas con la seguridad.

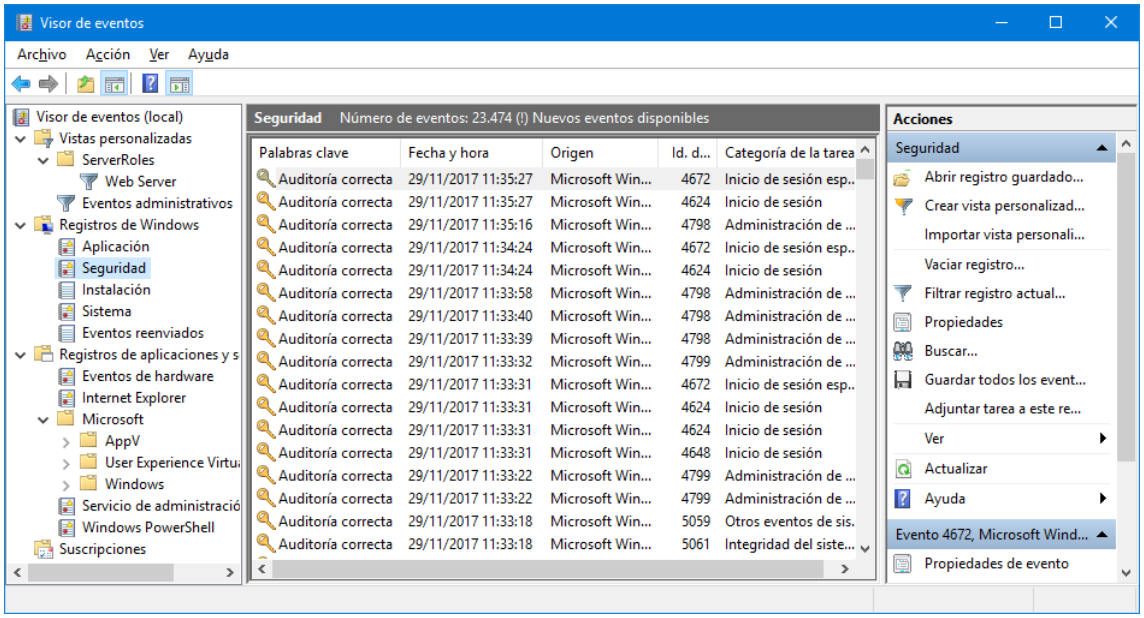
2. El visor de eventos de Windows

Permite analizar registros de eventos. Para arrancar el visor de eventos hacer:

Inicio > Panel de control > Herramientas administrativas > Visor de eventos

O teclear **eventvwr** (*event viewer*) en la consola.

Desplegar el árbol del visor en el panel izquierdo y al seleccionar "Seguridad" aparece:



El uso del visor es totalmente intuitivo. La parte interesante para la asignatura se centra en los Registros de Windows, y en particular en el Registro de Seguridad de Windows.

También pueden ser de interés algunos "Registros de aplicaciones y servicios". Por ejemplo en:

Reg app y serv > Microsoft > Windows > Windows Firewall With Advanced Security > Firewall

Observar los eventos que hay en el registro con las directivas de auditoría que tiene activadas el sistema por defecto. Buscar información en Internet sobre los códigos numéricos que aparecen.

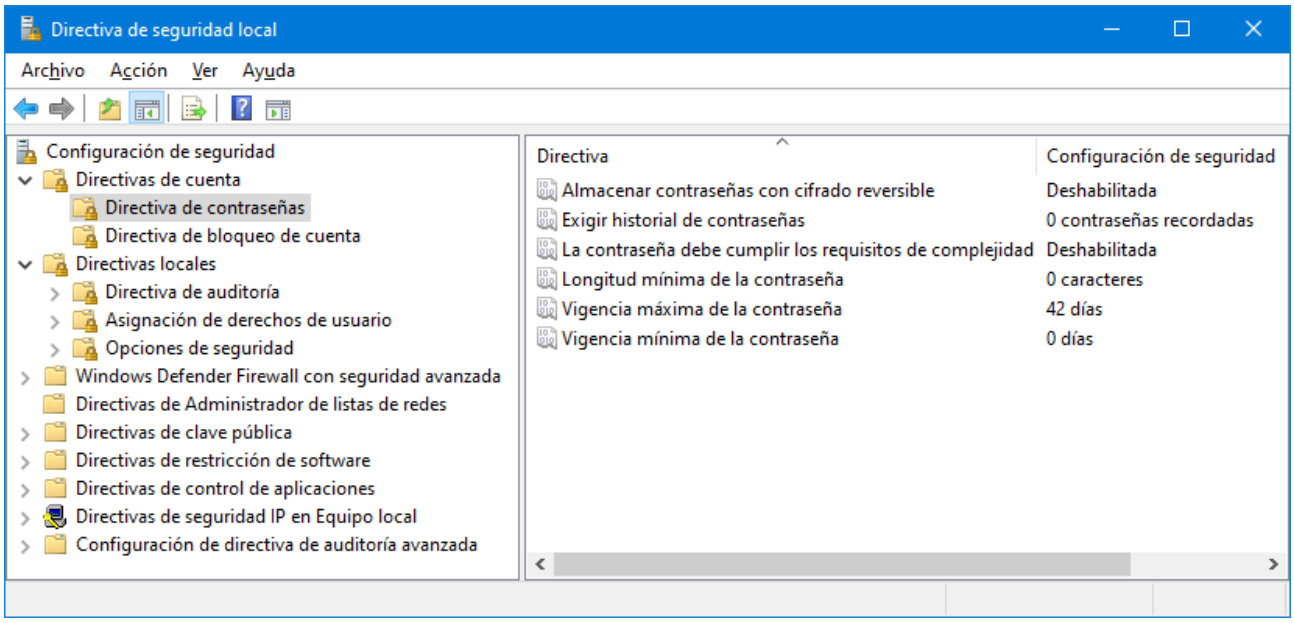
Luego, realizar tareas como Buscar, Filtrar, Guardar, etc.

3. Configurar controles de seguridad

En un sistema operativo, como Windows, hay muchos controles de seguridad que se pueden activar/desactivar y configurar. Una de las herramientas que permite configurar varios controles de seguridad es la "Directiva de seguridad local" (secpol). Para usar esta herramienta hacer:

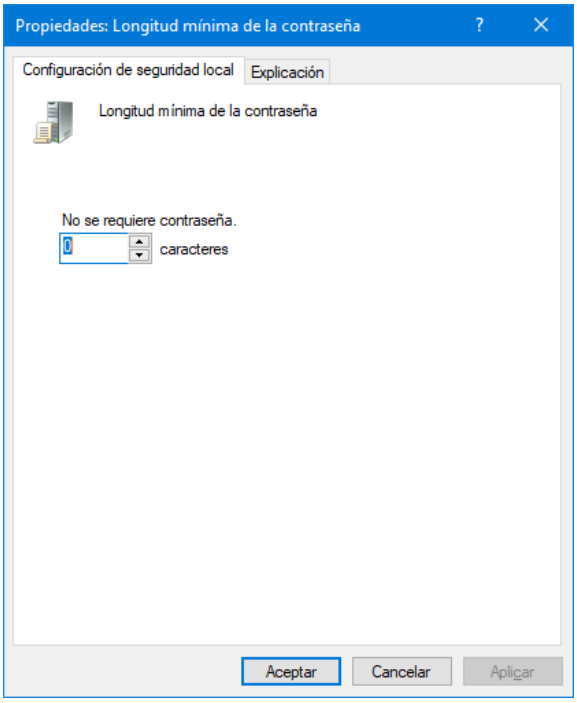
Panel de control > Herramientas administrativas > Directiva de seguridad local

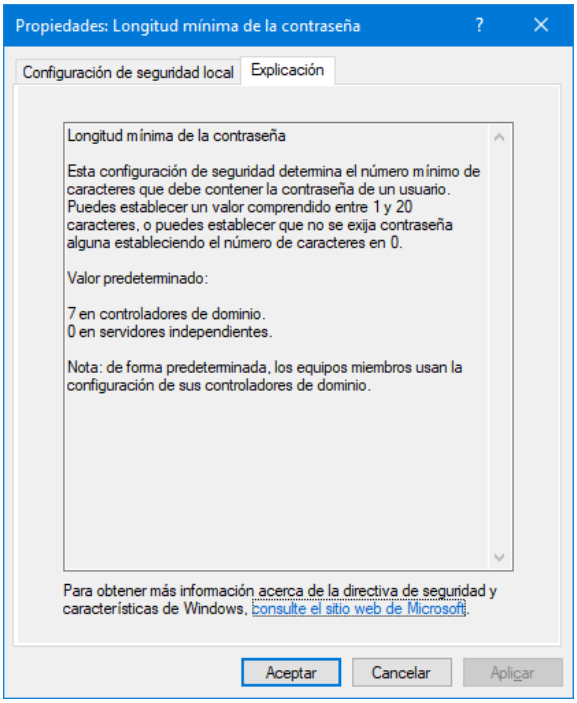
O teclear **secpol** (*security policy*) en la consola. Se despliega la siguiente ventana:



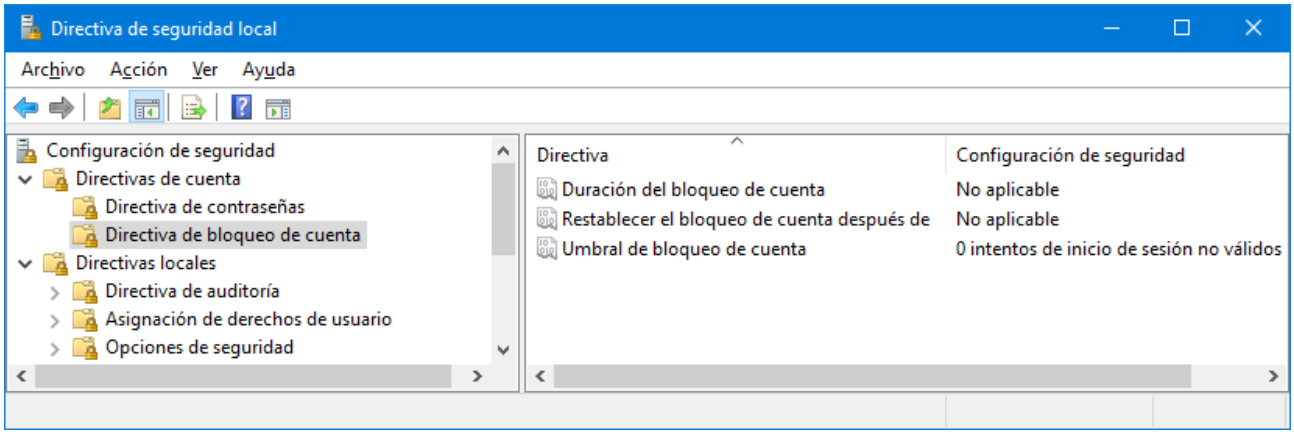
El panel de la izquierda contiene múltiples opciones de "Configuración de seguridad". En la ventana anterior se ha seleccionado la opción "Directivas de cuenta > Directiva de contraseñas". En el panel derecho se puede observar las directivas y su configuración.

Por ejemplo la directiva "Longitud mínima de la contraseña" está configurada a 0 caracteres. Haz doble clic en la directiva para cambiar su configuración. Aparecen estas ventanas:





Observar la “Directiva de bloquea de cuenta”:



Observar las opciones que ofrece y aprender a configurar el bloqueo. Comprobar que las opciones configuradas funcionan realmente.

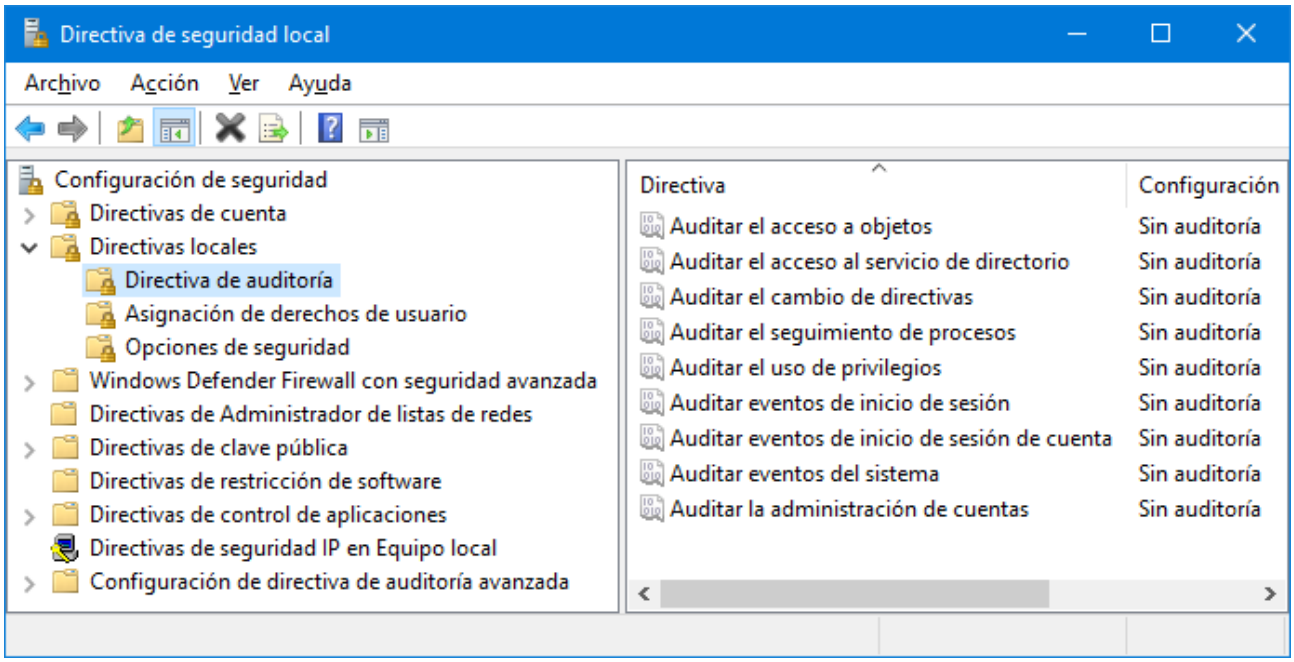
En la opción del panel izquierdo “Directivas locales” observar las directivas que se pueden configurar en “Asignación de derechos de usuario” y en “Opciones de seguridad”.

Comprueba que en la opción “Windows Defender Firewall con seguridad avanzada” da acceso a la configuración de Firewall de Windows, pero la configuración se puede hacer en el propio Firewall.

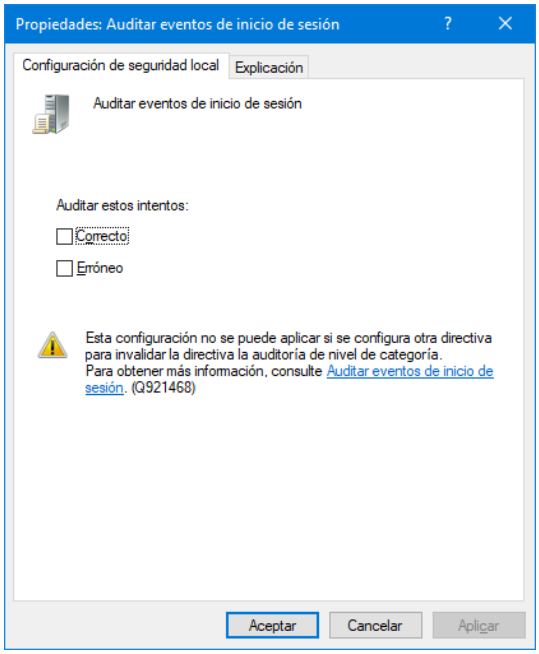
Observa el resto de tipos de Directivas que permite configurar la herramienta, para tener una idea de lo que permite configurar la herramienta secpol. Para usarlas correctamente, primero hay que conocer la tecnología con la trabajan.

4. Configurar los eventos de auditoría que se deben registrar

Una forma de establecer los eventos de auditoría a registrar es mediante la herramienta secpol. Para la auditoría es interesante, dentro de **Directivas locales**, la opción "**Directiva de auditoría**". También es interesante el último grupo "**Configuración de directiva de auditoría avanzada**".



Observar en la figura anterior que la "Directiva de auditoría" permite auditar las categorías que se muestran en el panel derecho. Si se selecciona una directiva cualquiera del panel derecho aparece una ventana como la siguiente:



Observar que tenemos 4 opciones:

1) No auditar los inicios de sesión, dejando sin seleccionar ambas casillas.

2) Auditar solo los inicios de sesión correctos, seleccionando solo la casilla "Correcto".

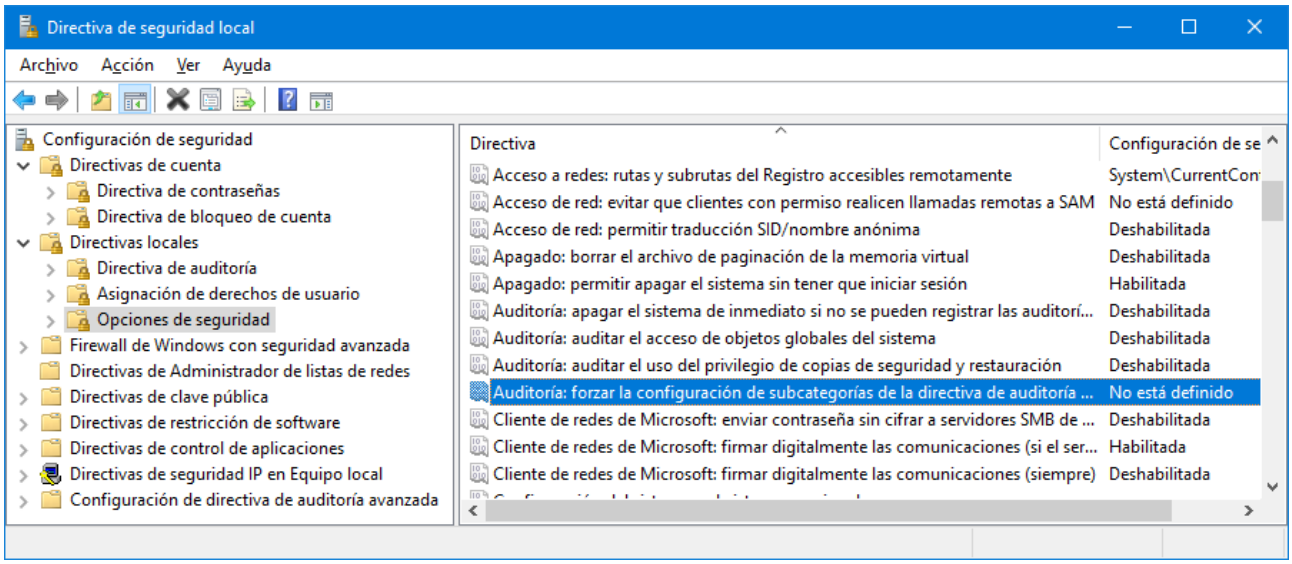
3) Auditar solo los inicios de sesión erróneos, seleccionando solo la casilla "Erróneo".

4) Auditar los inicios de sesión correctos y los erróneos, seleccionando ambas casillas.

Para las nueve directivas de auditoría se puede seleccionar las cuatro opciones anteriores. Para disponer de mayor detalle en la selección de los eventos a auditar es necesario utilizar la "Configuración de directiva de auditoría avanzada".

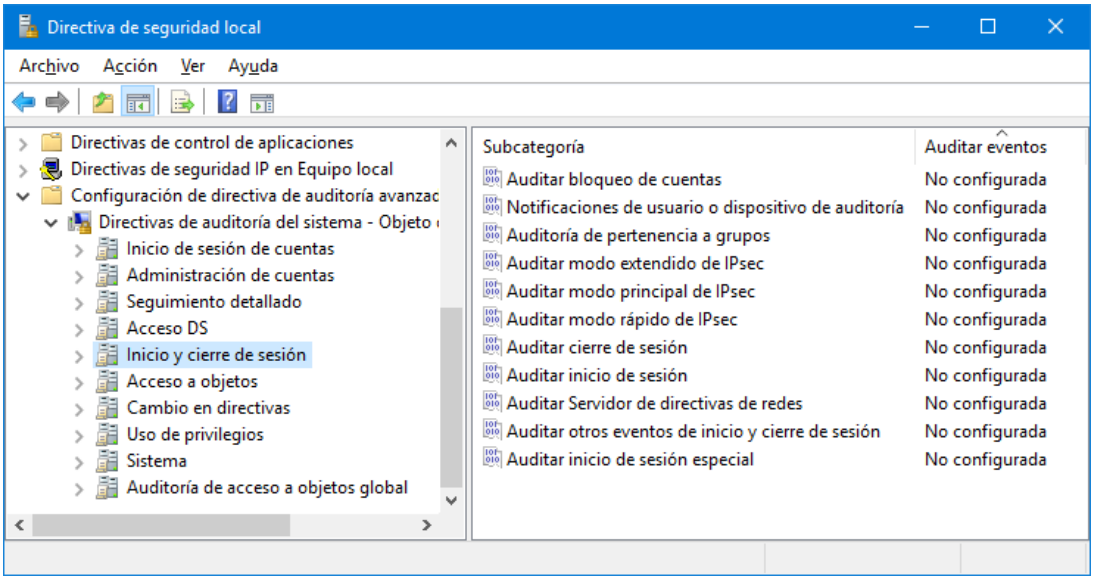
En las prácticas y trabajos de la asignatura de seguridad usar la Auditoría Avanzada.

Para activarla hay que ir primero a "Opciones de seguridad" en el panel izquierdo y luego en el panel derecho seleccionar la directiva "Auditoría: forzar la configuración de subcategorías ..." como muestra la figura siguiente:

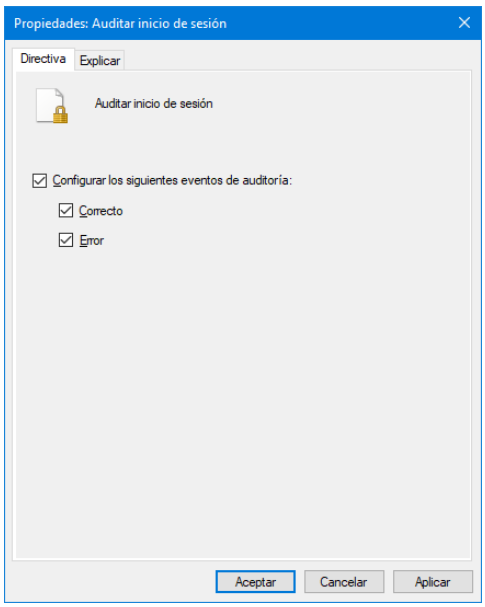


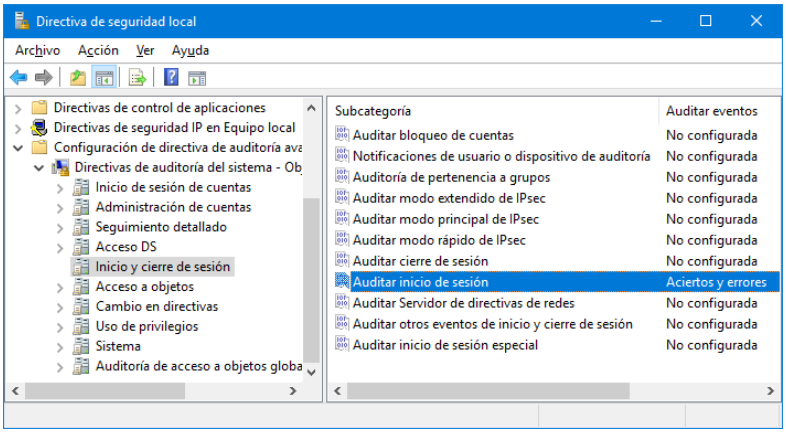
Hacer doble clic sobre la directiva y en la ventana que se muestra, habilitarla.

Después desplegamos la última opción del panel izquierdo. Observar que en el panel izquierdo tenemos las mismas directivas (o categorías) de auditoría que aparecían antes en el panel derecho. Pero ahora al seleccionar una en el panel izquierdo aparecen en el panel derecho sus subcategorías.



Ahora, el Inicio y cierre de sesión permite auditar nueve eventos independientes. Por ejemplo, seleccionar en el panel derecho "Auditar inicio de sesión" y auditar tanto los inicios correctos como los intentos de inicio que generan un error.



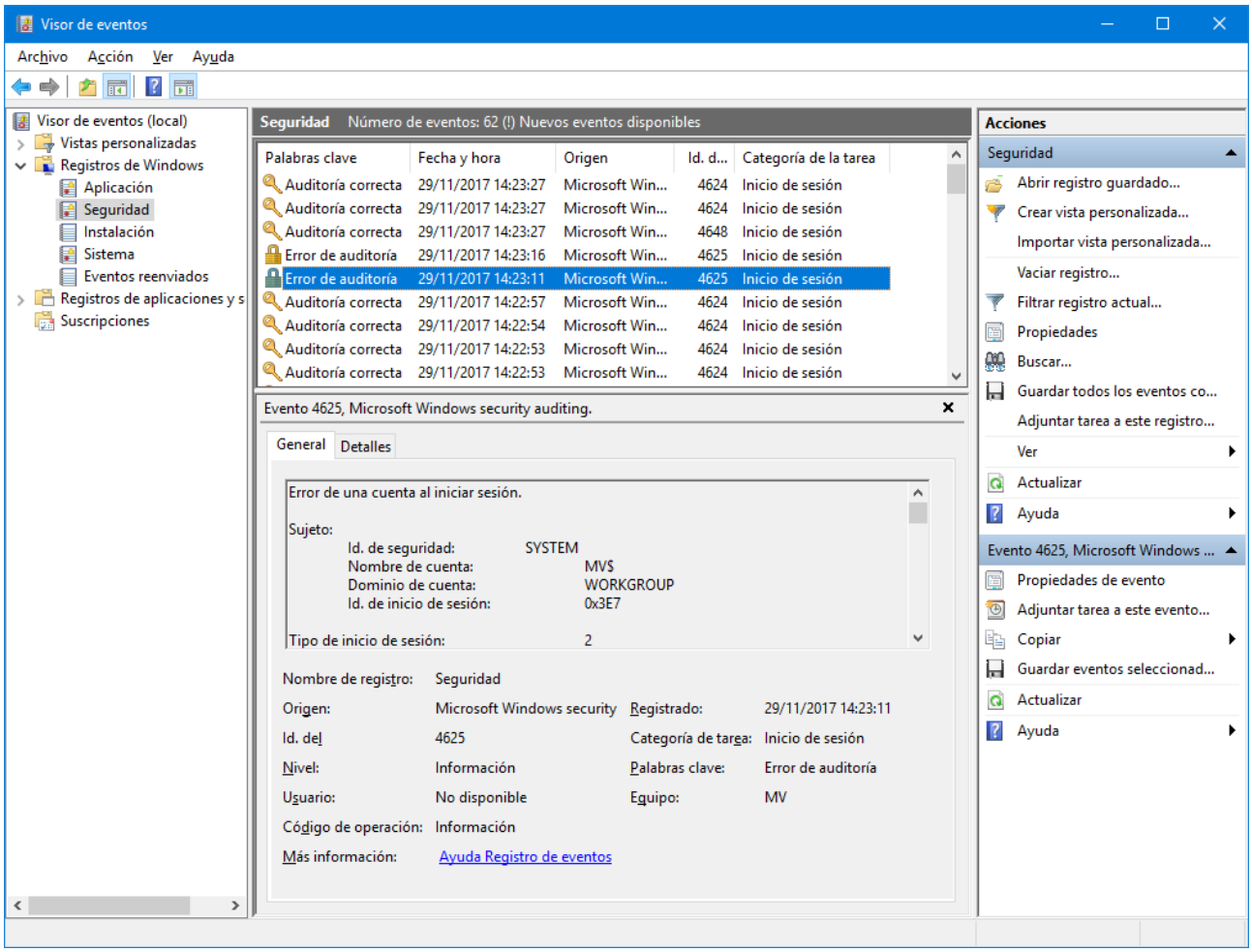


Comprobar que el SO está realizando la captura de eventos de auditoría del inicio de sesión.

En el Visor de eventos Vaciar el registro de eventos de seguridad.

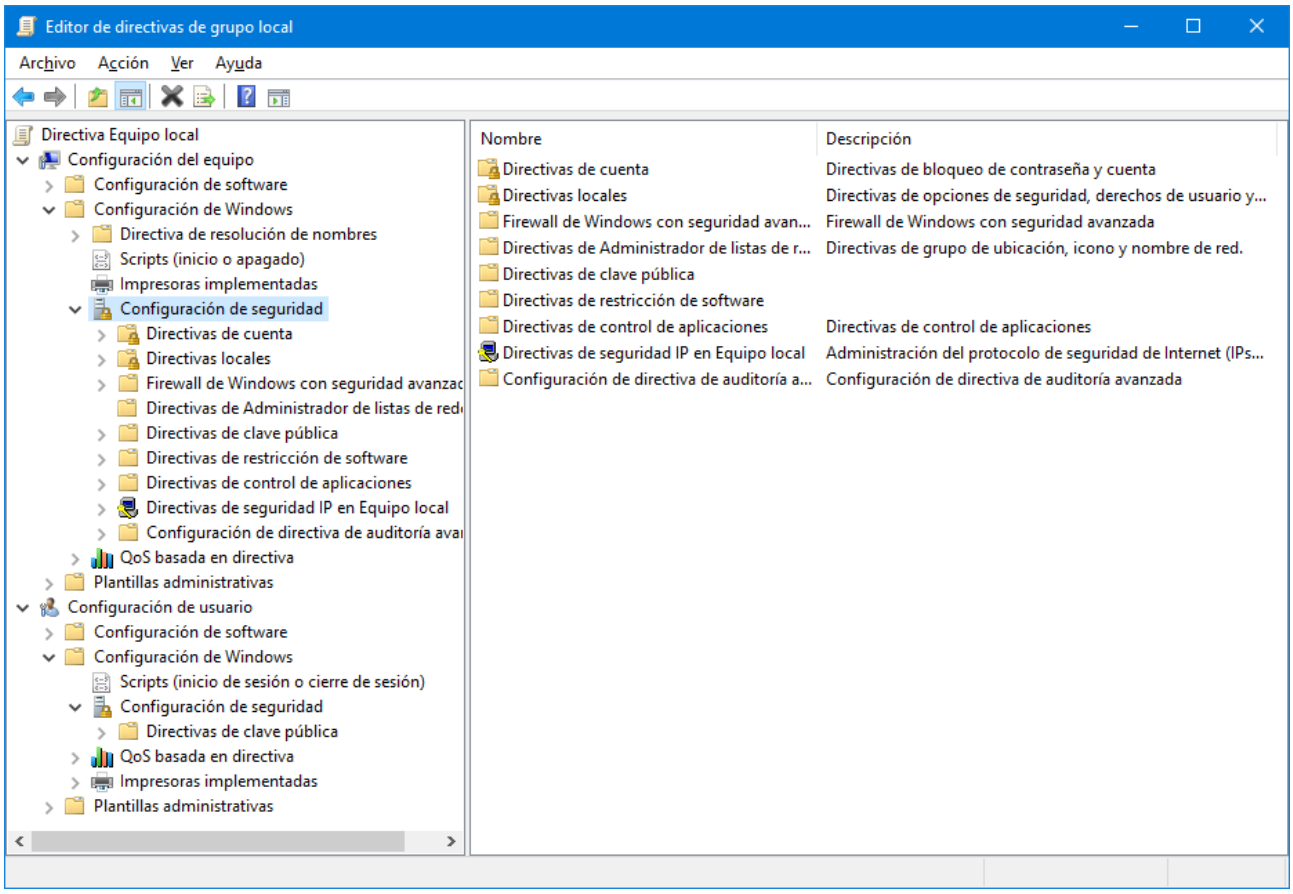
Cerrar la sesión en Windows, y hacer dos intentos de logon con contraseña incorrecta. Al tercer intento usar la contraseña correcta para a acceder nuevamente al sistema.

Usar el Visor de eventos para ver lo que ha ocurrido:



Otra forma de acceder a esta funcionalidad es usando el Editor de directivas de grupo local.

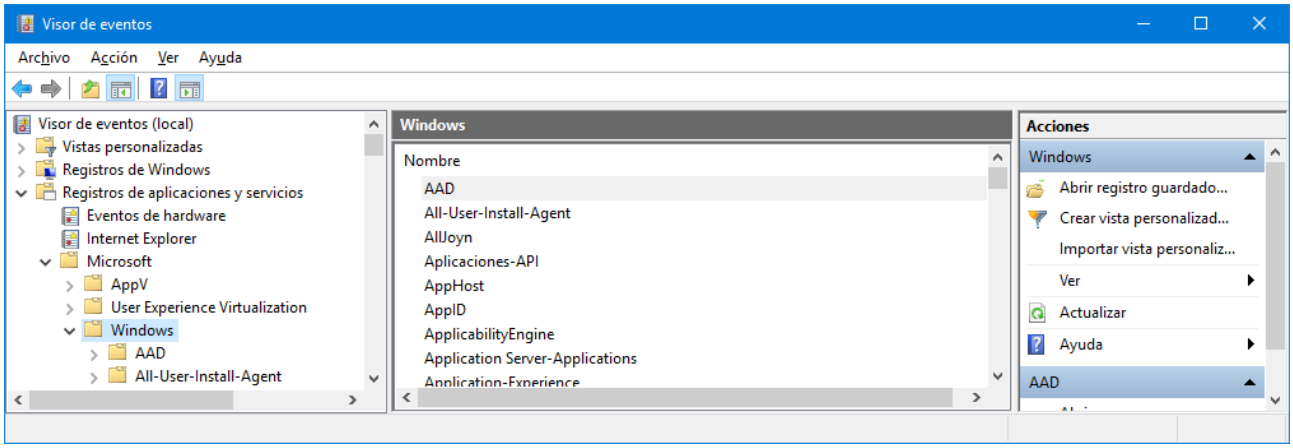
Ejecutar gpedit.msc en una consola y aparece la ventana siguiente:



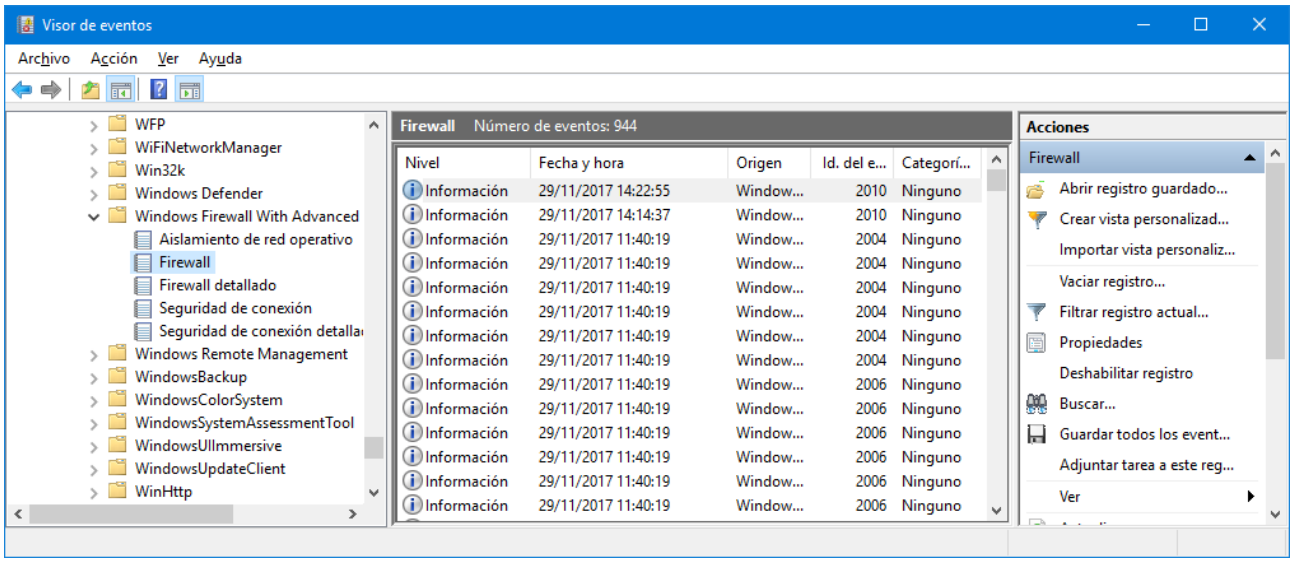
Como se puede comprobar dentro de toda la "Configuración del equipo" tenemos una sección dedicada a la "Configuración de seguridad".

5. Auditar el cortafuegos

Para ver los eventos que genera el Firewall en el Visor de Eventos hay que navegar en el panel izquierdo del visor: Registros de aplicaciones y servicios > Microsoft > Windows >



Y seguimos ... > Windows Firewall With Advanced Security

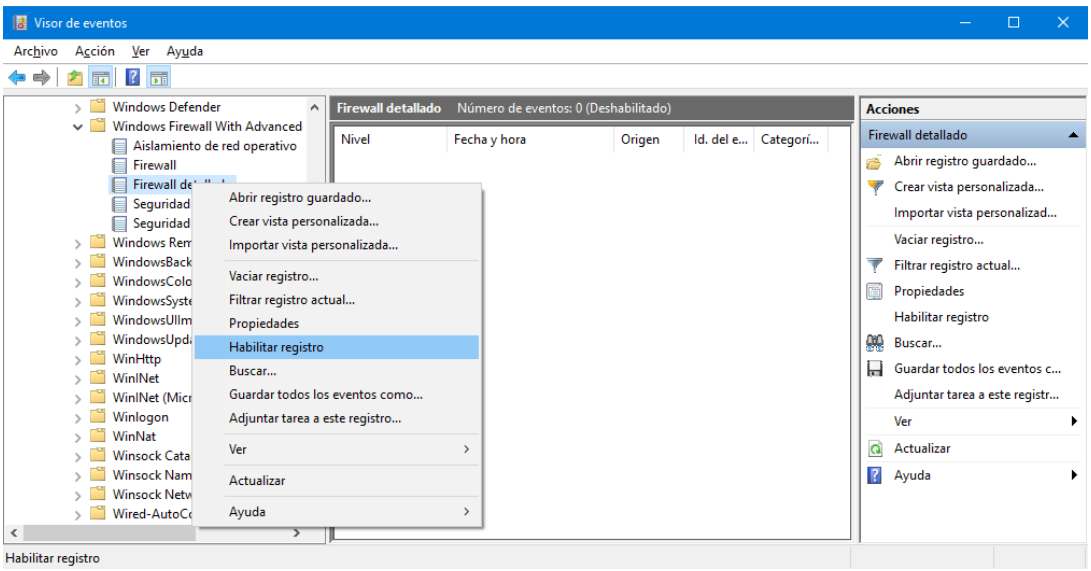


Se puede ver que hay 5 registros de eventos disponibles.

El registro "Firewall" contiene los eventos relacionados con la configuración del Firewall. Se añade un evento cada vez que se añade, quita o modifica una regla, o cuando se cambia el perfil de una interfaz de red. Compruébalo analizando unos cuantos eventos que aparecen en el panel central del visor de eventos.

El registro "Firewall detallado" contiene los eventos relacionados con el estado operativo del Firewall. Por defecto este registro esta deshabilitado. Para activarlo hacer clic en el botón derecho del ratón y seleccionar "Habilitar registro" en el menú contextual que aparece. También se puede habilitar en el panel derecho de acciones. Observar que el menú contextual que aparece contiene exactamente las mismas opciones que el panel derecho de acciones.

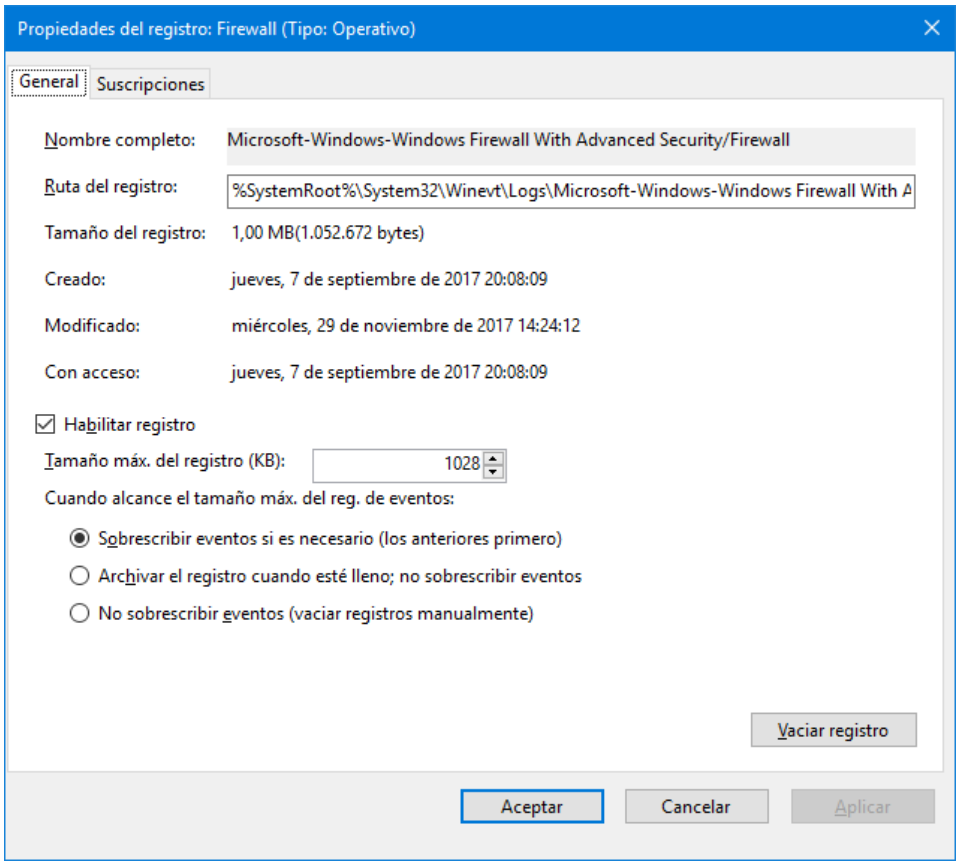
Parece que este registro no es muy útil, pues casi todos los cambios relativos al funcionamiento del Firewall se almacenan en el registro "Firewall".



El registro "Seguridad de conexión" contiene los eventos relacionados con la configuración de las reglas y los parámetros de IPsec.

El registro "Seguridad de conexión detallada" contiene los eventos relacionados con el funcionamiento de IPsec.

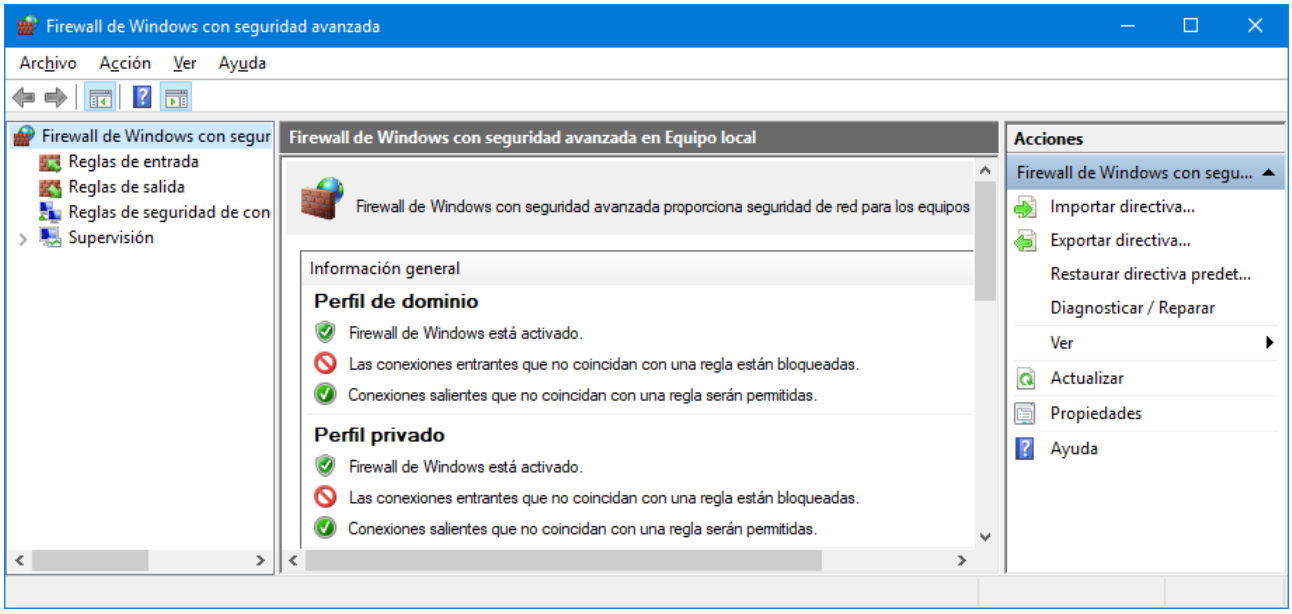
Selecciona el registro "Firewall" en el panel izquierdo. En el panel derecho de acciones selecciona la opción "Propiedades" y aparece la ventana siguiente:



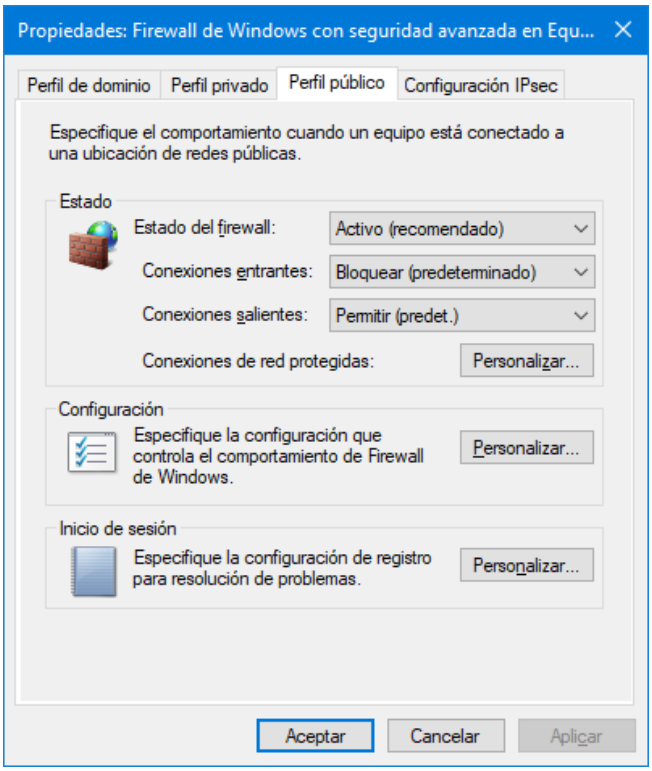
Observar el nombre del registro y su ubicación en el sistema de ficheros.

Analizar el trafico interceptado por el Firewall

La primera tarea a realizar es indicar al Firewall que genere registros del trafico que controla. Para ello hay que abrir la consola de gestión del "Firewall de Windows con seguridad avanzada" y seleccionar la raíz del panel izquierdo.

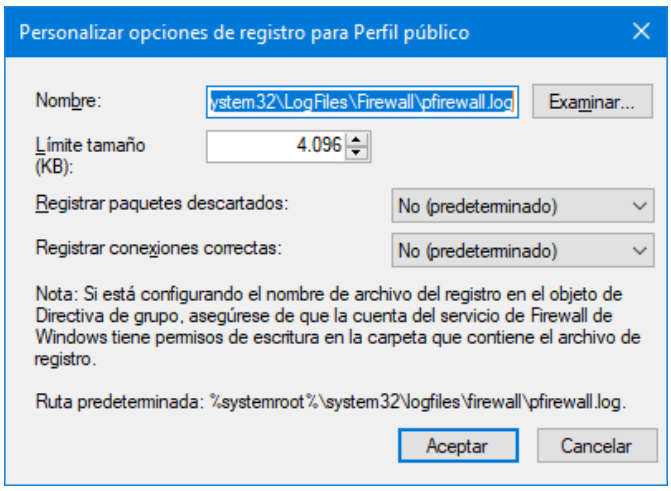


En el panel derecho de acciones seleccionar "Propiedades" y aparece esta ventana:



Comprobar que hay tres perfiles de utilización del Firewall: dominio, privado y público. Si se está trabajando en el perfil público, seleccionar su pestaña, y luego pulsar el botón "Personalizar..." en el cuadro inferior de Inicio de sesión.

Aparece la ventana siguiente:



Activar el Registro de paquetes descartados y el de conexiones correctas. Si no se activa al menos una de estas dos opciones, el Firewall no registra nada. Ahora se puede abrir el fichero pfirewall.log con cualquier editor de ficheros de texto.

Acceso rápido al Firewall: Teclear wf en una consola de texto para abrir la consola de gestión del Firewall. También se puede teclear wf.msc en el cuadro de búsqueda de programas y archivos del botón Inicio.

6. Realización de ejercicios de auditoría

Los aspectos mostrados en esta práctica son solo un ejemplo introductorio de las posibilidades de auditoría disponibles en el sistema operativo Windows 10. Las posibilidades reales deben ser exploradas con más detalle por cada equipo de prácticas realizando ejercicios de auditoría.

Los ejercicios deben realizarse en la Máquina Virtual utilizada en las prácticas y los pasos que se van realizando se deben documentar imprimiendo ventanas (Alt+ImprPant) y copiándolas en un documento abierto en la MV con el programa WordPad, junto con un mínimo texto explicativo. Es muy conveniente guardar frecuentemente el documento en el formato "Documento XML abierto de Office (*.docx)".

Si se pide un ejercicio de auditoría en el examen de prácticas habrá que entregar un documento de este tipo en el Campus Virtual.

Generalmente, en los ejercicios de auditoría hay que realizar 4 tareas secuenciales:

1.-Activar y configurar los controles de seguridad.
Utilizar la herramienta secpol, el Firewall, o incluso propiedades del sistema de ficheros, como la concesión de permisos de acceso. Muchos de los controles que se pueden utilizar ya estarán activados y tendrán una configuración por defecto que aplica el propio sistema.

2.-Activar y configurar la auditoría de seguridad, para controlar los eventos que se generan.
El objetivo suele ser recopilar información sobre cuatro aspectos:

- Cuando se activa y se desactiva un control, por ejemplo el Firewall.
- Cuando se cambia la configuración de un control, por ejemplo las reglas del Firewall.
- Cuando el control detecta una violación de seguridad y cual, por ejemplo una denegación de acceso. Esto permite analizar los ataques que han fracasado.
- También se puede recabar información de la ausencia de violaciones de seguridad, por ejemplo todos los accesos que permite el Firewall. El volumen de información a tratar aumenta muchísimo. Pero esto permite analizar los ataques que han tenido éxito.

La herramienta fundamental para realizar esta tarea es secpol, usando la "Configuración de directiva de auditoría avanzada".

3.-Realizar pruebas para generar eventos.
En esta tarea los alumnos deben realizar algunas pruebas para generar eventos de auditoría. Por ejemplo, acceder al sistema dando contraseñas erróneas varias veces y finamente volviendo a entrar con la contraseña correcta. También pueden acceder a archivos cuyo acceso este auditado. Y por supuesto, pueden intentar escanear el computador usando cualquier herramienta de red, como por ejemplo Nmap.

4.-Analizar los registros de eventos de seguridad, para evaluar problemas con la seguridad.
Utilizar el Visor de eventos para analizar los eventos capturados. Se puede vaciar el registro para tener unos pocos eventos y localizarlos rápidamente, pero **es más realista no hacerlo**. Diseñar algún filtro o alguna consulta para localizar algún tipo de evento en particular y documentarlo. Finalmente y de modo opcional, volcar los archivos de eventos para su análisis, utilizando alguna herramienta de análisis de registros o realizando algún tipo de programa que procese XML.