

---

# ET-SEGURIDAD SQL

## INSTRUCCIONES DE USO

### IMPORTANTE

Este software puede ser bloqueado por software antivirus. Asegúrese de añadir la excepción correspondiente si fuese necesario. Se recomienda deshabilitar el antivirus durante el proceso de instalación.

Para entornos con más de un equipo conectados en red es necesario que el programa de firewall conceda paso a los servicios de Microsoft SQL Server.

Necesitaremos tener instalada una instancia de Microsoft SQL Server. Compatible con las versiones 2005 en adelante ya sean Completas (de pago, capacidad ilimitada) o Express (gratuito, máximo 4GB de ocupación). No se incluyen con la instalación del programa. Puede encontrar las diferentes versiones en el propio sitio web de Microsoft o para una instalación automática tiene disponibles los siguientes instaladores:

[Instalador Microsoft SQL Express 2005](#)

[Instalador Microsoft SQL Express 2012](#)

### PASO 1

Después de completar la instalación tendremos a nuestra disposición dos programas. En primer lugar inicializaremos ET-Seguridad



## PASO 2

Aparecerá a continuación una ventaba de bienvenida. Pulse “Empezar a configurar”



## PASO 3

A continuación nos aparecerá la siguiente ventana de inicio de sesión y configuración donde tendremos de introducir la información de conexión a nuestra instancia del servicio de SQL Server.

Las credenciales de SQL Server, si se ha utilizado nuestro instalador automático, serán las siguientes:

**Nombre del servidor:** Nombre del equipo que alberga la instancia de SQL \ LOPD. Por ejemplo: “servidor\lopd” donde servidor es el nombre del equipo que contiene la instancia lopd de SqlServer.

Pueden utilizarse direcciones IP, como por ejemplo:127.0.0.1\lopd en caso que no esté disponible el DNS para la red local y si son direcciones IP estáticas.

**Autenticación:** Autenticación de SQL Server

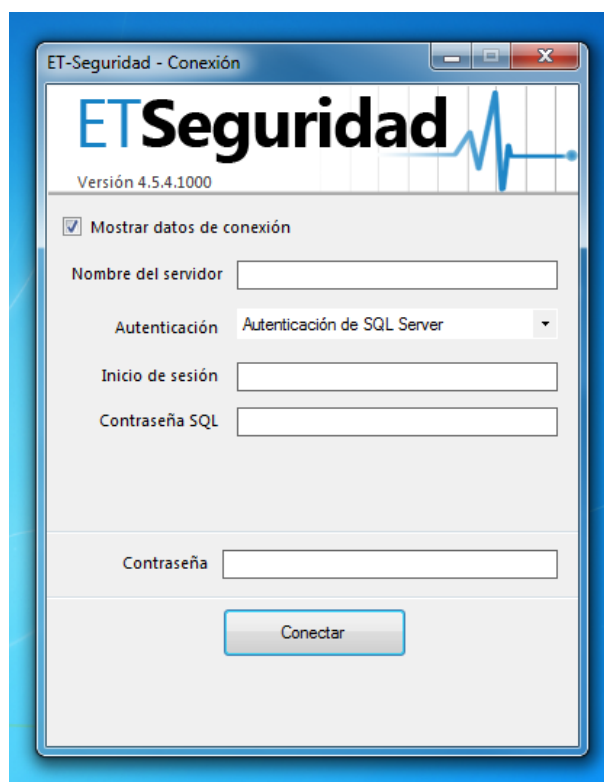
**Inicio de sesión:** sa

**Contraseña SQL:** Sqladmin1

**Contraseña:** Por defecto es ‘5555’, necesario para poder acceder a la aplicación

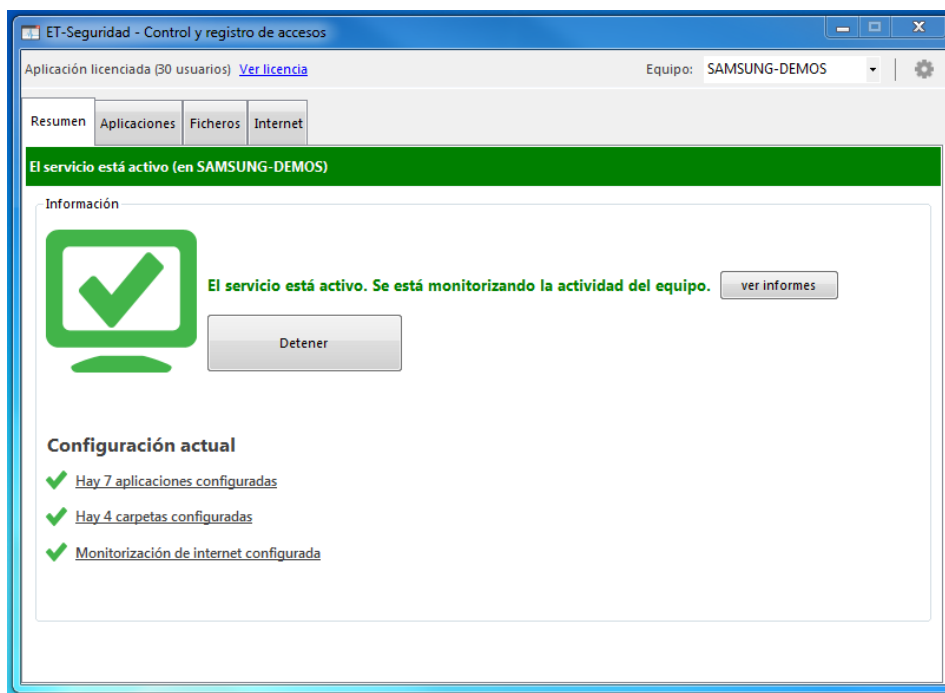
Puede consultar el documento:

[Solución de problemas de Microsoft Sql Server para ET-Seguridad](#)



## PASO 4

Se nos presentará la ventana principal de la aplicación. En esta ventana usted podrá configurar la aplicación de control de accesos. Podrá configurar que aplicaciones se ejecutan, que tratamiento tienen los ficheros y las páginas web visitadas por los usuarios tanto locales como de cualquier equipo que se haya unido a la red de ET-Seguridad (disponible solo en versión SQL Server). Se encuentra al lado del icono de configuración (arriba a la derecha). También podrá activar y desactivar el servicio de control de accesos de forma remota.



Detalle de las cuatro pestañas:

### “Resumen”

En esta pestaña usted puede iniciar y parar el servicio de control de accesos con el botón “Iniciar/Detener”. A demás puede ver los informes de accesos pulsando el botón de “Ver informes”. También podrá ver un resumen del estado de la configuración de los controles de acceso en la parte inferior de la ventana.

## “Aplicaciones”

En la pestaña de Aplicaciones puede añadir las aplicaciones que quiere controlar sus accesos. Para ello debe pulsar el botón añadir y elegir “buscar aplicación” para navegar y buscar la aplicación deseada. Por el contrario puede elegir la opción “Escribir el nombre manualmente” para introducir el nombre del ejecutable .exe que desea controlar.

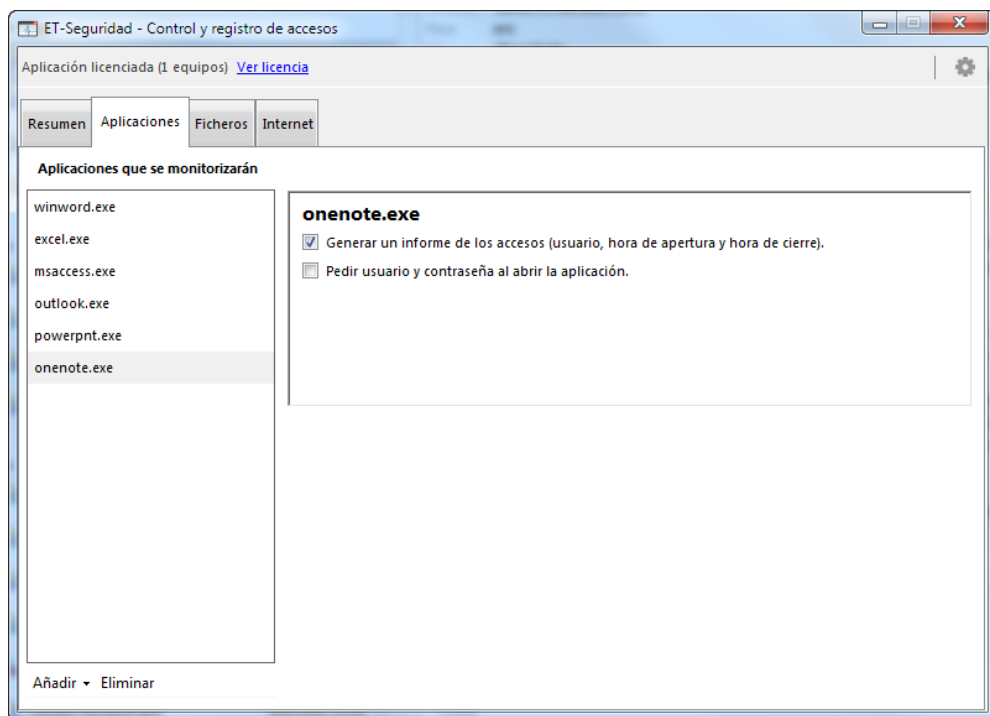
En la lista que aparece a su izquierda podremos observar las aplicaciones añadidas para ser controladas y a la derecha observaremos las diferentes opciones que podremos aplicar a la aplicación seleccionada de la lista de ejecutables.

“Generar un informe de los accesos” generará un registro de los de los accesos a las aplicaciones cuando se acceda a ellas.

Al habilitar la opción de “Pedir usuario y contraseña al abrir la aplicación” haremos que cuando se proceda a acceder a la aplicación con esta opción habilitada, nos muestre una ventana de identificación de usuario.

Esto es útil para proporcionar un sistema de autenticación en aplicaciones que no dispongan de un sistema propio para ello. Si habilita esta opción, deberá pulsar a continuación “Ver los usuarios que pueden acceder a la aplicación” para poder establecer usuarios para que puedan acceder a las aplicaciones controladas con este sistema.

Si deseamos que una aplicación no pueda ser accedida, será tan sencillo como marcar la opción de “Pedir usuario y contraseña” y a continuación en la opción “Ver los usuarios que pueden acceder a la aplicación”. Si tenemos usuarios creados nos tendremos que asegurar que tengan desmarcada la opción “Tiene permiso para abrir [nombre del ejecutable]”.



## “Ficheros”

En esta sección puede añadir las carpetas o directorios que contengan los ficheros que desee controlar. Para ello usted debe pulsar sobre “Añadir” y elegir “Buscar carpeta” para localizar la carpeta deseada, o “Escribir la ruta manualmente” si desea escribir la ruta manualmente. Además puede añadir las ubicaciones típicas mediante la opción de “Añadir carpetas típicas”.

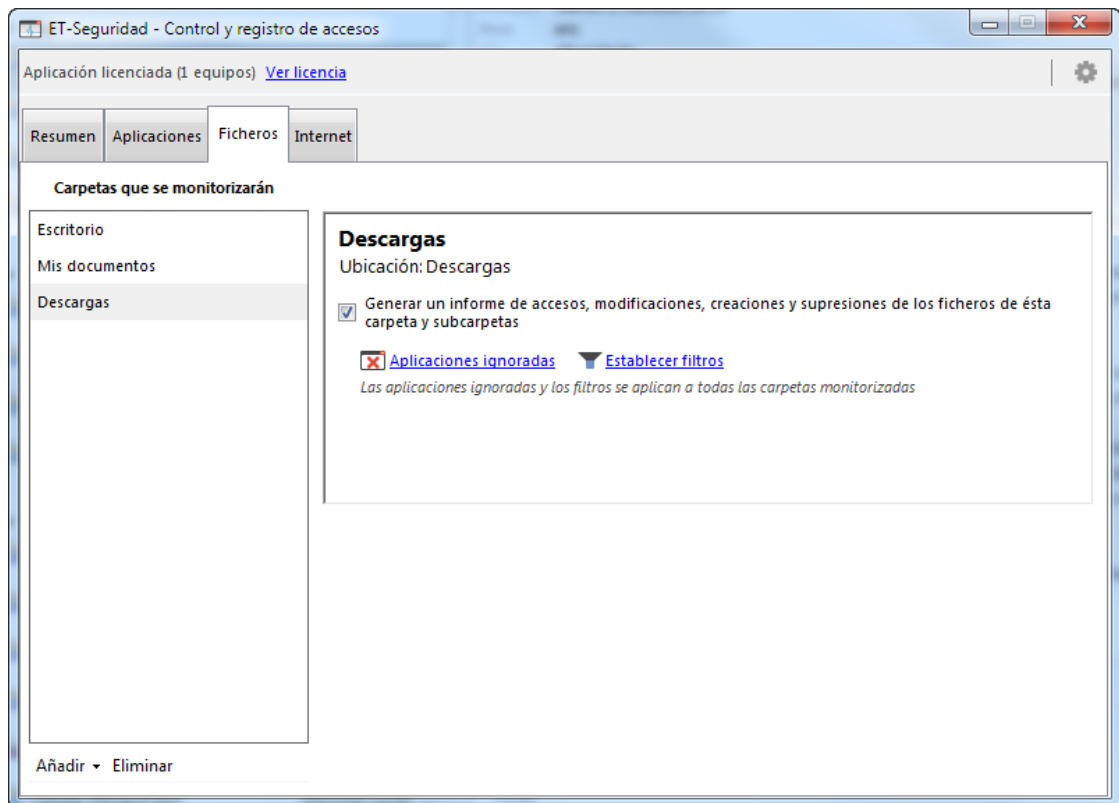
En la parte izquierda está presente la lista de directorios configurados. En la parte derecha podremos observar las opciones que podremos aplicar a la ubicación seleccionada a la izquierda.

“Generar un informe [...]” generará un registro cuando un usuario realice una acción de acceso, creación, modificación o eliminación.

Cabe tener en cuenta que el objetivo de esta sección es monitorizar la actividad de los documentos tipo ofimáticos (documentos de texto, hojas de cálculo, bases de datos sencillas como Access...) monitorizar la actividad de los ficheros de una aplicación tiende a tener una utilidad nula.

La opción de establecer filtros nos permitirá filtrar por lista blanca o lista negra el tipo de extensiones que queremos controlar

La opción de “Aplicaciones ignoradas” se utilizará para que aplicaciones del tipo antivirus, sistemas de backup... nos saturen la base de datos con información no relevante y confusa ya que también nos estaría generando información de acceso cuando estén realizando sus respectivas tareas con los ficheros.

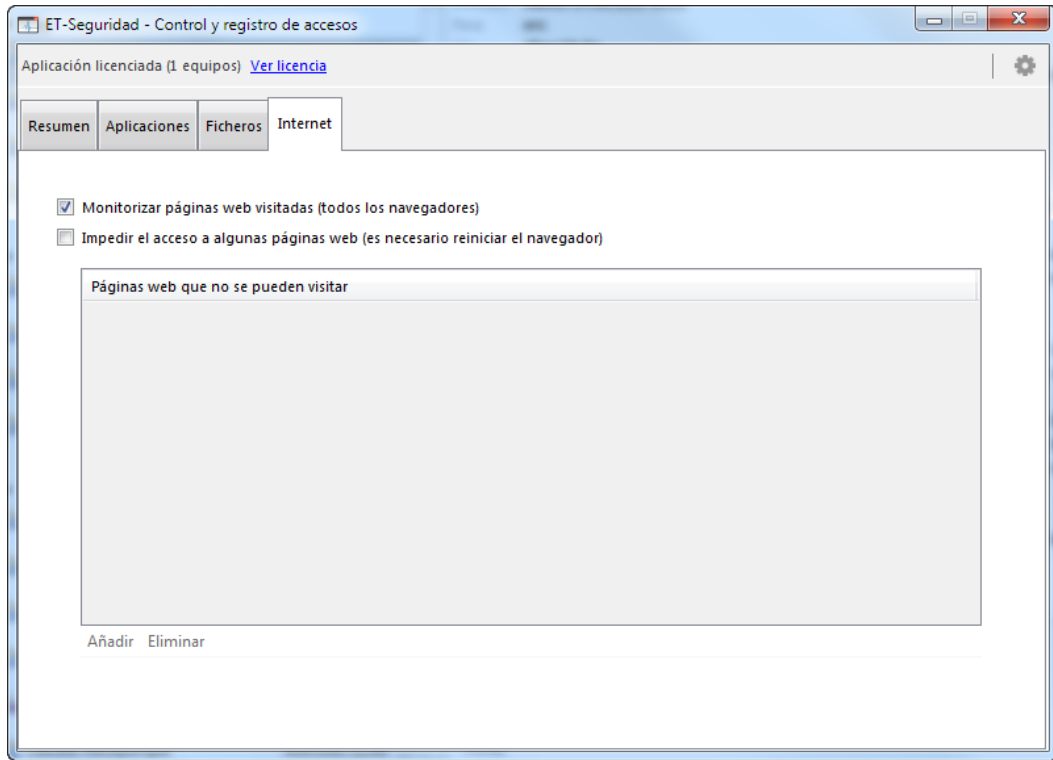


## “Internet”

“Monitorizar páginas web visitadas” genera un registro de accesos cuando un usuario visita sitios web (funciona con todos los navegadores). No podemos monitorizar accesos a páginas https debido a que este tipo de comunicaciones se realiza de forma cifrada, siéndonos imposible descifrar estos valores.

“Impedir el acceso [...]” bloquea los sitios web que se especifiquen. Para poder añadir direcciones restringidas pulse “Añadir” e introduzca la URL del sitio web. Debemos tener en cuenta que los cambios solo se aplicarán cuando se reinicie el navegador web.

Des de los informes de accesos que se generan también podremos añadir reglas a la lista presente.



## Licencia del programa

Et-Seguridad SQL gestiona las licencias por equipos. El equipo que hace la función de servidor, habitualmente, quién también aloja el servicio de SQL, será donde se deberá activar el código de licencia. Todos los equipos que se conecten a la misma instancia de SQL Server, que el equipo registrado, serán activados automáticamente.

En Opciones >> Gestionar Licencia, podremos asignar y desasignar licencias a equipos para contemplar casos donde se sustituyen o retiran equipos que ya no hayan de hacer uso del sistema de control de accesos.

El código de licencia puede ser proporcionado por los mismos miembros de EdorTeam Soft o puede ser adquirida a través de internet con el enlace que le aparecerá en pantalla. Consulte el siguiente documento para obtener más detalles acerca de las licencias disponibles: [Versiones y Licencias ET-Seguridad](#)