

# informatizate

<http://www.informatizate.net>

## Seguridad en SQL Server 2000

**Robert G. Ancajima Rojas**

Area de Desarrollo e Inteligencia de  
Negocios

GRUPO [GESFOR OSMOS](#) PERU S.A.

Microsoft Certified System Engineer

Microsoft Certified Systems Administrator

Microsoft Certified DataBase Administrator

[robertancajima\(at\)](mailto:robertancajima(at)informatizate(dot)net)

[informatizate\(dot\)net](mailto:informatizate(dot)net)

Mayo 30 del 2004.



Asegurar nuestra base de datos puede ser una ardua tarea, pero muy gratificante. Nada puede hacernos sentir mas orgullosos que tener nuestro servidor con un optimo nivel de seguridad. El presente artículo propone una serie de consideraciones de seguridad de SQL Server 2000 que pueden ser aplicados de acuerdo a la naturaleza del ambiente de trabajo en el que nos desarrollamos.

### SEGURIDAD FISICA DEL SERVIDOR

Restringir el acceso físico al servidor SQL Server únicamente al personal autorizado. Además, también debemos tener en cuenta la seguridad física del lugar donde está almacenado o dispuesto el servidor, es decir, en un lugar ventilado adecuadamente, un lugar con los dispositivos ante alguna contingencia, como por ejemplo:

- Extintores, antes los incendios o corto circuitos.
- Ubicación adecuada del servidor, por ejemplo si existen riesgos de inundación, tal vez podríamos ubicarlo en un lugar elevado.
- El cableado debe estar adecuado al lugar para evitar problemas con el fluido eléctrico.
- UPS o sistema de alimentación continua de energía.

### AUTENTICACION DE USUARIO DE SQL SERVER

La autenticación ocurre de 2 formas:

- a) Autenticación de Modo Mixto
- b) Autenticación Windows

El problema con la autenticación de Modo Mixto es que las combinaciones de nombre de usuario y contraseña son pasados como un texto libre al SQL Server. En la Autenticación Windows, la parte de autenticación es manejada por el sistema operativo de red y por lo tanto es mucho mas seguro. Siempre que fuera posible elegir Autenticación de Windows en lugar de Autenticación de Modo Mixto. Si es inevitable utilizar la Autenticación de Modo Mixto por razones de compatibilidad con versiones anteriores de SQL u otro motivo, utilizar contraseñas complejas para el login SA y todos los demás logins.

## **ROL DE SERVIDOR SYSTEM ADMINISTRATOR**

Elegir cuidadosamente los miembros del rol de servidor "System Administrator", por el hecho de que este rol permite realizar cualquier acción dentro del servidor SQL Server. Por defecto, el grupo de administradores locales de Windows NT o 2000 BUILTIN\ADMINISTRATORS forman parte del rol de servidor "sysadmin".

## **REMOVER CUENTA BUILTIN\ADMINISTRATORS**

Por lo general, los administradores de red no necesitan tener derechos de System Administrator en nuestro servidor de base de datos. En el caso de que existiera esta necesidad por parte de alguno de ellos, crear un nuevo grupo NT e incluir solo a los usuarios que necesiten tener derecho de System Administrator.

## **CUENTAS Y CONTRASEÑAS**

- Nunca usar contraseñas en blanco o escribir las contraseñas en alguna aplicación. Para detectar los usuarios de SQL Server que tienen contraseñas en blanco podemos utilizar el siguiente script:

```
USE MASTER
GO
SELECT NAME, PASSWORD FROM SYSLOGINS WHERE PASSWORD IS NULL AND NAME IS
NOT NULL
```

- Es recomendable tener contraseñas mixtas que comiencen con uno o varios números seguido por una combinación de letras y caracteres especiales para contrarrestar los ataques producidos por los hackers.
- Renombrar la cuenta Administrator del servidor SQL Server para evitar que personas malintencionadas intenten adivinar la contraseña del Administrador.
- Deshabilitar la cuenta de usuario de Windows "Invitado". Quitar el usuario Invitado de las Bases de Datos de producción.

## **SEGURIDAD DE CARPETAS Y ARCHIVOS DE DATOS**

- Instalar siempre SQL Server en una partición NTFS, para poder establecer seguridad principalmente a la carpeta "Microsoft SQL Server" y a los archivos de base de datos \*.mdf, \*.ndf y \*.ldf.
- Asegurar todos las carpetas compartidas en el servidor de SQL Server con el permiso de únicamente lectura. En caso de tener acceso a carpetas compartidas de lectura y escritura, asegurarnos que únicamente las personas correctas tienen acceso a estas carpetas compartidas.
- Encriptar los archivos de copia de seguridad y base de datos. Esta es una nueva opción que puede ser realizada desde la versión de Windows 2000 Server únicamente en particiones NTFS, el cual facilita la encriptación del archivo utilizando las características de la Arquitectura de Encriptación de Windows y la Infraestructura de Claves Publicas.

La encriptación puede realizarse vía línea de comandos (comando cipher.exe) o vía GUI. En la siguiente pagina podemos encontrar información acerca de encriptación de archivos:

<http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q273856>

## **SEGURIDAD DE CLAVES DE REGISTRO DE SQL SERVER**

Verificar que el grupo TODOS esta restringido a tener solo el permiso de Lectura en las siguientes claves de registro:

1. HKLM\Software\Microsoft\Microsoft SQL Server
2. HKLM\System\CurrentControlset\Services\MSSQLServer
3. HKLM\Software\Microsoft\MSSQLServer

Si existiera mas de una instancia de SQL Server, revisar la seguridad de sus claves de registro.

## **HABILITAR NIVEL DE AUDITORIA**

Esta consideración es importante, por ejemplo cuando se requiere saber quienes y cuantas veces han intentado conectarse en forma correcta y errónea al servidor de Base de Datos.

## **CONTROLAR ACCESO A TRAVES DE PROCEDIMIENTOS ALMACENADOS**

Establecer permisos a nivel de procedimientos almacenados para poder acceder a la información de la base de datos. En otras palabras, no permitir ejecutar consultas desde aplicaciones y manipular la Base de Datos directamente usando las sentencias SELECT/INSERT/UPDATED/DELETE.

## **EVITAR TENER SERVIDOR SQL SERVER Y SERVIDOR WEB INSTALADOS EN UNA MISMA COMPUTADORA**

En este caso, mantener el servidor SQL Server en una computadora diferente que tenga instalado el Servicio Web. Debido a que el Servidor web es uno de los componentes físicos mas vulnerables a ataques realizados por Hackers, es recomendable, aislarlo de cualquier componente de la red que maneje data importante. Así de esta manera si es atacado el Servidor Web, entonces los datos no se verían afectados.

## **SEGURIDAD EN LAS APLICACIONES**

En las aplicaciones no permitir la ejecución de comandos SQL de los usuarios. Esto podría ser muy peligroso (conocido como SQL Injection), por ejemplo un usuario con ciertos conocimientos podría ejecutar comandos que puede destruir los datos o ganar acceso no autorizado a información sensitiva.

## **OCULTAR LA INSTANCIA DE SQL SERVER**

Al ocultar una instancia de SQL Server, se deshabilitan las respuestas de las operaciones de difusión de los clientes que intenten enumerar esas instancias de SQL Server presentes en la red.

Para ocultar una instancia de SQL Server realizar lo siguiente:

Abrir HERRAMIENTA DE RED DE SQL SERVER

En el TAB GENERAL, verificar TCP en la lista de Protocolos "Disponibles".

Seleccionar TCP, clic en Propiedades. En la siguiente ventana seleccionar habilitar "Ocultar Servidor"



### **BLOQUEO DE PUERTOS**

Si el servidor de Base de Datos esta detrás de un Firewall, bloquear los puertos UDP 1434 y el puerto TCP 1433. La versión de Windows Server 2003 tiene incorporado su propio Firewall, aunque no es muy completo puede ser utilizado para realizar el bloqueo de estos puertos.

### **MODIFICAR PUERTO PREDETERMINADO**

Si fuera posible cambiar el puerto predeterminado de SQL Server. Debido a que el puerto TCP 1433 es ampliamente conocido, los intrusos que intenten ingresar al servidor de Base de Datos siempre iniciaran su ataque a través de este puerto.

### **ACTUALIZACION DE SERVICE PACKS Y PARCHES DE SEGURIDAD**

Estar actualizado con los últimos service packs y parches de seguridad proporcionados por Microsoft. Cuidadosamente evaluar los service packs y parches de seguridad antes de aplicarlos en el servidor SQL Server de producción. La siguiente URL es de Microsoft Security Alerts en el cual podremos subscribirnos para ser notificados de los últimos service packs:

<http://www.microsoft.com/technet/security/bulletin/notify.msp>

### **SOFTWARE ANTIVIRUS**

Instalar un Software Anti-virus en el servidor de SQL Server pero evitar que las carpetas que contienen las bases de datos sean escaneados regularmente. Además, este software debe estar siempre actualizado.

## **MICROSOFT BASELINE SECURITY ANALYZER**

Es un herramienta gratuita que permite analizar algunos aspectos comunes de seguridad como contraseñas, vulnerabilidades de SQL Server y otros aspectos, local o remotamente a computadoras con sistema operativo Windows Server 2003, Windows XP, Windows 2000 y Windows NT.

<http://www.microsoft.com/technet/security/tools/mbsahome.msp>

Implementar un adecuado nivel de seguridad es un gran desafío pero mantener este mismo nivel en el tiempo lo es aún mas. Es por ello que siempre debemos tener presente las diversas consideraciones de seguridad de SQL Server para estar listos y así enfrentar pro activamente cualquier amenaza de seguridad.

