

Suscríbete a DeepL Pro para poder editar este documento.  
Entra en www.DeepL.com/pro para más información.



**Prueba de fuego de CIS Microsoft SQL Server 2019**

v1.2.0

-

04

-

30

-

2021

# Condiciones de uso

Consulte en el siguiente enlace nuestras condiciones de uso actuales:

*https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/*

Tabla de contenidos

[Condiciones de uso 1](#_Toc150388)

[Resumen 5](#_Toc150389)

[Público al que va dirigido 5](#_Toc150390)

[Orientación de consenso 5](#_Toc150391)

[Convenciones tipográficas 6](#_Toc150392)

[Estado de la evaluación 6](#_Toc150393)

[Definiciones de los perfiles 7](#_Toc150394)

[Agradecimientos 8](#_Toc150395)

[Recomendaciones 9](#_Toc150396)

[1 Instalación, actualizaciones y parches 9](#_Toc150397)

[1.1 Asegúrese de instalar las últimas actualizaciones acumulativas y de seguridad de SQL Server](#_Toc150398)

[(Manual) 9](#_Toc150399)

[1.2 Garantizar el uso de servidores de miembros de una sola función (manual) 11](#_Toc150400)

[2 Reducción de la superficie 13](#_Toc150401)

[2.1 Asegúrese de que la opción de configuración del servidor de "consultas distribuidas ad hoc" esté en "0" (automatizado) 13](#_Toc150402)

[2.2 Asegúrese de que la opción de configuración del servidor "CLR Enabled" esté ajustada a "0" (automatizado) 15](#_Toc150403)

[2.3 Asegúrese de que la opción de configuración del servidor "Cross DB Ownership Chaining" esté establecida en "0" (automatizada) 18](#_Toc150404)

[2.4 Asegúrese de que la opción de configuración del servidor "Database Mail XPs" esté establecida en "0".](#_Toc150405)

[(Automatizado) 20](#_Toc150406)

[2.5 Asegúrese de que la opción de configuración del servidor "Procedimientos de automatización de Ole" esté establecida en "0" (automatizado) 22](#_Toc150407)

[2.6 Asegúrese de que la opción de configuración del servidor de "acceso remoto" esté ajustada a "0" (automatizado) 24](#_Toc150408)

[2.7 Asegúrese de que la opción de configuración del servidor "Conexiones de administración remota" esté establecida en "0" (automatizada) 26](#_Toc150409)

[2.8 Asegúrese de que la opción de configuración del servidor "Scan For Startup Procs" esté establecida en "0".](#_Toc150410)

[(Automatizado) 28](#_Toc150411)

[2.9 Asegúrese de que la propiedad de la base de datos 'Trustworthy' esté desactivada (automatizada) 30](#_Toc150412)

[2.10 Asegúrese de que los protocolos innecesarios de SQL Server estén configurados como 'Desactivados' (Manual) 32](#_Toc150413)

[2.11 Asegúrese de que SQL Server está configurado para utilizar puertos no estándar (Automatizado) 34](#_Toc150414)

[2.12 Asegúrese de que la opción "Ocultar Instancia" esté establecida en "Sí" para el Servidor SQL de Producción](#_Toc150415)

[instancias (automatizadas) 36](#_Toc150416)

[2.13 Asegúrese de que la cuenta de inicio de sesión "sa" esté configurada como "Desactivada" (Automática) 39](#_Toc150417)

[2.14 Asegúrese de que la cuenta de inicio de sesión "sa" ha sido renombrada (automatizada) 41](#_Toc150418)

[2.15 Asegúrese de que "AUTO\_CLOSE" esté en "OFF" en las bases de datos contenidas (automatizadas) 43](#_Toc150419)

[2.16 Asegúrese de que no existe ningún inicio de sesión con el nombre "sa" (automatizado) 45](#_Toc150420)

[2.17 Asegúrese de que la opción de configuración del servidor "clr strict security" esté establecida en "1".](#_Toc150421)

[(Automatizado) 47](#_Toc150422)

[3 Autenticación y autorización 49](#_Toc150423)

[3.1 Asegúrese de que la propiedad "Autenticación del servidor" esté configurada como "Autenticación de Windows".](#_Toc150424)

[Modo" (automatizado) 49](#_Toc150425)

[3.2 Asegúrese de que los permisos de CONEXIÓN del usuario "invitado" están revocados en todas las bases de datos de SQL Server, excepto en la maestra, la msdb y la tempdb (automatizada) 51](#_Toc150426)

[3.3 Asegurarse de que los "usuarios huérfanos" son eliminados de las bases de datos de SQL Server](#_Toc150427)

[(Automatizado) 53](#_Toc150428)

[3.4 Asegurarse de que la autenticación SQL no se utiliza en las bases de datos contenidas (automatizado) 55](#_Toc150429)

[3.5 Asegúrese de que la cuenta de servicio MSSQL del servidor SQL no es un administrador](#_Toc150430)

[(Manual) 57](#_Toc150431)

[3.6 Asegúrese de que la cuenta de servicio SQLAgent del servidor SQL no es un administrador](#_Toc150432)

[(Manual) 59](#_Toc150433)

[3.7 Asegúrese de que la cuenta de servicio de texto completo de SQL Server no es un administrador](#_Toc150434)

[(Manual) 61](#_Toc150435)

[3.8 Asegúrese de que sólo se conceden los permisos por defecto especificados por Microsoft al rol de servidor público (automatizado) 63](#_Toc150436)

[3.9 Asegúrese de que los grupos BUILTIN de Windows no son inicios de sesión SQL (automatizados) 65](#_Toc150437)

[3.10 Asegurarse de que los grupos locales de Windows no son inicios de sesión de SQL (automatizados) 67](#_Toc150438)

[3.11 Asegúrese de que el rol público en la base de datos msdb no tiene acceso a los proxies de SQL Agent (automatizado) 69](#_Toc150439)

[4 Políticas de contraseñas 71](#_Toc150440)

[4.1 Asegúrese de que la opción "MUST\_CHANGE" esté activada para todos los inicios de sesión autenticados por SQL (manual) 71](#_Toc150441)

[4.2 Asegúrese de que la opción "CHECK\_EXPIRATION" esté activada para todos los autenticados de SQL](#_Toc150442)

[Logins dentro del rol de Sysadmin (automatizado) 73](#_Toc150443)

[4.3 Asegúrese de que la opción "CHECK\_POLICY" esté activada para todos los inicios de sesión autenticados de SQL (automatizados) 75](#_Toc150444)

[5 Auditoría y registro 77](#_Toc150445)

[5.1 Asegúrese de que el "Número máximo de archivos de registro de errores" sea mayor o igual a "12" (automatizado) 77](#_Toc150446)

[5.2 Asegúrese de que la opción de configuración del servidor "Trace Enabled" (rastreo activado por defecto) esté establecida en "1".](#_Toc150447)

[(Automatizado) 80](#_Toc150448)

[5.3 Asegúrese de que la "Auditoría de inicio de sesión" esté configurada como "inicios de sesión fallidos" (automatizado) 82](#_Toc150449)

[5.4 Asegúrese de que la "Auditoría del Servidor SQL" está configurada para capturar tanto los "inicios de sesión fallidos" como los "exitosos" (Automatizado) 85](#_Toc150450)

[6 Desarrollo de aplicaciones 88](#_Toc150451)

[6.1 Asegurarse de que la entrada de usuarios de la base de datos y de la aplicación está desinfectada (manual) 88](#_Toc150452)

[6.2 Asegúrese de que el "Conjunto de permisos del ensamblaje del CLR" esté establecido en "SAFE\_ACCESS" para todos los CLR](#_Toc150453)

[Montajes (automatizados) 90](#_Toc150454)

[7 Cifrado 92](#_Toc150455)

[7.1 Asegúrese de que el "Algoritmo de cifrado de clave simétrica" esté configurado como "AES\_128" o superior en las bases de datos que no sean del sistema (automatizadas) 92](#_Toc150456)

[7.2 Asegúrese de que el tamaño de la clave asimétrica está configurado como "mayor o igual a 2048" en las bases de datos que no son del sistema (automatizado) 94](#_Toc150457)

[8 Apéndice: Consideraciones adicionales 96](#_Toc150458)

[8.1 Asegúrese de que el "Servicio de Navegador del Servidor SQL" está configurado correctamente (Manual) 96](#_Toc150459)

[Apéndice: Cuadro resumen de recomendaciones 98](#_Toc150460)

[Apéndice: Historial de cambios 101](#_Toc150461)

# Resumen

Este documento proporciona una guía prescriptiva para establecer una postura de configuración segura para Microsoft SQL Server 2019 .

2019. Para obtener la última versión de esta guía , visite http://benchmarks.cisecurity.org. Si tiene preguntas , comentarios o ha identificado formas de mejorar esta guía , escríbanos a feedback@cisecurity.org.

## Público al que va dirigido

Esta prueba está dirigida a administradores de sistemas y aplicaciones , especialistas en seguridad , auditores, personal de asistencia técnica y personal de implantación de plataformas que deseen desarrollar , implantar, evaluar o solucionar el problema de Microsoft SQL Server 2019 en la plataforma de Microsoft Windows .

## Orientación de consenso

Este banco de pruebas se creó mediante un proceso de revisión por consenso compuesto por expertos en la materia . Los participantes en el consenso aportan su perspectiva desde diversos ámbitos, como la consultoría , el desarrollo de programas informáticos , el cumplimiento de las normas de auditoría , la investigación en seguridad, las operaciones, la administración y el ámbito jurídico .

Cada parámetro del SIC pasa por dos fases de revisión de consenso . La primera fase tiene lugar durante el desarrollo inicial del parámetro . Durante esta fase , los expertos en la materia se reúnen para debatir , crear y poner a prueba los proyectos de trabajo del parámetro . Este debate se lleva a cabo hasta que se llega a un consenso sobre las recomendaciones del parámetro . Esta segunda fase comienza después de la publicación del punto de referencia . Durante esta fase , el equipo de consenso revisa toda la información proporcionada por la comunidad de Internet para incorporarla al punto de referencia . Si está interesado en participar en el proceso de consenso , visite https://workbench.cisecurity.org/.

## Convenciones tipográficas

En esta guía se utilizan las siguientes convenciones tipográficas :

|  |  |  |
| --- | --- | --- |
| Convención | | Significado |
|  | Fuente Monospace estilizada | Se utiliza para bloques de código , comandos y ejemplos de secuencias de comandos . Los textos deben interpretarse exactamente como se presentan . |
|  |
| Fuente Monospace | | Se utiliza para el código en línea , los comandos o los ejemplos . Los textos deben interpretarse exactamente como se presentan . |
| *<continuación itálica>* | | Los textos en cursiva entre paréntesis indican una variable que requiere una sustitución por un valor real . |
| *Italicfont* | | Se utiliza para indicar el título de un libro , artículo u otra publicación . |
| **Nota** | | Información adicional o advertencias |

## Estado de la evaluación

Se incluye un estado de evaluación para cada recomendación . El estado de la evaluación indica si la recomendación puede ser aplicada o si requiere medidas manuales para su puesta en práctica . Ambos estados son igualmente importantes y se determinan y apoyan como se define a continuación :

**Automatizado**

Representa las recomendaciones para las que la evaluación del control técnico puede ser automatizada y validada para su aprobación . Las recomendaciones incluyen la información necesaria para aplicar la automatización .

**Manual**

Representa las recomendaciones para las que la evaluación del control técnico no puede ser automatizada y requiere todos o algunos pasos manuales para confirmar que el estado configurado es el esperado . El estado esperado puede variar en función del entorno .

## Definiciones de los perfiles

Los siguientes perfiles de configuración están definidos por este Benchmark :

* **Nivel1-Motor de la base de datos**

Los elementos de este perfil se aplican a Microsoft SQL Server 2019 y pretenden :

* + ser práctico y prudente ; o proporcionar un beneficio de seguridad ordinario ; y o no inhibir la utilidad de la tecnología más allá de lo aceptable .
* **Nivel1-AWSRDS**

Los elementos de este perfil son aplicables a Microsoft SQL Server 2019 en AWSRDS y pretenden :

* + ser práctico y prudente ; o proporcionar un beneficio de seguridad ordinario ; y o no inhibir la utilidad de la tecnología más allá de lo aceptable .
* **Nivel2-Motor de la base de datos**

Este perfil amplía el perfil "Level1-DatabaseEngine " . Los elementos de este perfil se aplican a Microsoft SQL Server 2019 y presentan una o más de las siguientes características :

* + están pensados para entornos o casos en los que la seguridad es importante ; o actúan como medida de defensa en profundidad ; y o pueden afectar a la utilidad o al rendimiento de la tecnología .
* **Nivel2-AWSRDS**

Este perfil amplía el perfil "Level1-AWSRDS " . Los elementos de este perfil se aplican a Microsoft SQL Server 2019 en AWSRDS y presentan una o más de las siguientes características :

* + están pensados para entornos o casos en los que la seguridad es importante ; o actúan como medida de defensa en profundidad ; y o pueden afectar a la utilidad o al rendimiento de la tecnología .

## Agradecimientos

Este punto de referencia ejemplifica las grandes cosas que una comunidad de usuarios, proveedores y expertos en la materia puede lograr a través de la colaboración consensuada. La comunidad de CIS agradece a todo el equipo de consenso, con un reconocimiento especial a las siguientes personas que contribuyeron en gran medida a la creación de esta guía:

**Colaborador**

MichalHoran

DeanLackey

MatthewWoods

RobKraft

EmadAl-Mousa

**Editor**

BrianKelleyMCSE , CISA, Security+, MicrosoftMVP-SQLServer

TimHarrison , CentrodeSeguridaddeInternetSeanMcCown

# Recomendaciones

## 1 Instalación, actualizaciones y parches

Esta sección contiene recomendaciones relacionadas con la instalación y los parches de SQLServer .

#### 1.1 Asegúrese de que las últimas actualizaciones acumulativas y de seguridad de SQL Server están

#### Instalado (manual)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

Los parches de SQLServer contienen actualizaciones de programas que solucionan problemas de seguridad y funcionalidad del producto encontrados en el software . Estos parches pueden instalarse con una actualización de seguridad , que es un único parche , o con una actualización acumulativa, que es un conjunto de parches. La versión del servidor SQL y los niveles de parches deben ser los más compatibles con las necesidades operativas de la organización .

**Justificación:**

El uso del software de SQL Server más reciente , junto con los parches aplicables, puede limitar las posibilidades de vulnerabilidad del software . La versión de la instalación y/o los paquetes aplicados durante la configuración deben establecerse de acuerdo con las necesidades de la organización .

**Auditoría:**

Para determinar el nivel de parche del servidor SQL , ejecute el siguiente código .

SELECT SERVERPROPERTY('ProductLevel') como SP\_installed, SERVERPROPERTY('ProductVersion') como Version;

**Remediación:**

Identifique la versión actual y el nivel de parche de sus instancias de SQLServer y asegúrese de que contienen los últimos parches de seguridad . Asegúrese de que estos parches en los entornos de prueba antes de actualizar las instancias de producción .

Los últimos paquetes de servidores SQL se pueden encontrar aquí : https://docs.microsoft.com/en-us/sql/database-engine/install-windows/latest-updatesfor-microsoft-sql-server?view=sql-server-ver15

**Valor por defecto :**

Las actualizaciones acumulativas y de seguridad no se instalan por defecto .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/install-windows/latestupdates-for-microsoft-sql-server?view=sql-server-ver15
2. https://support.microsoft.com/en-us/help/4041553/sql-server-service-packs-arediscontinued-starting-from-sql-server

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 2.2 Asegúrese de que el software es compatible con el proveedor  Asegúrese de que sólo las aplicaciones de software o los sistemas operativos actualmente admitidos por el proveedor de software se añaden al inventario de software autorizado de la organización . El software no soportado debe ser etiquetado como no soportado en el sistema de inventario . | ● | ● | ● |
| v6 | 4 Evaluación y reparación continua de vulnerabilidades  Evaluación y reparación continua de vulnerabilidades |  |  |  |

#### 1.2 Garantizar el uso de servidores miembros de una sola función (manual)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1- AWSRDS

**Descripción:**

Se recomienda instalar el software SQLServers en un servidor dedicado . Esta consideración arquitectónica ofrece flexibilidad en materia de seguridad, ya que el servidor de la base de datos puede colocarse en una subred separada que permita el acceso sólo a determinados hosts y a determinados protocolos . Los grados de disponibilidad son más fáciles de alcanzar, ya que, con el tiempo , una empresa puede pasar de un servidor de bases de datos combinado a otro en forma de clúster, utilizando el equilibrio de la carga o una combinación de los mismos .

**Justificación:**

Se trata de no gestionar (es decir, reducir) la superficie de ataque del servidor que aloja el software SQLServers, ya que las únicas superficies a tener en cuenta son el sistema operativo subyacente , el propio SQLServer y cualquier herramienta de seguridad/operativa que pueda instalarse adicionalmente. Como se indica en la descripción , la disponibilidad puede ser más fácil si la base de datos es un servidor dedicado .

**Impacto:**

Es difícil ver un impacto razonablemente adverso en este cambio arquitectónico , ya que los costes de este cambio se han pagado . Es posible que haya que modificar las aplicaciones personalizadas para que se adapten a las conexiones de base de datos a través de la red en lugar de en el host (es decir, utilizando TCP/IP en lugar de NamedPipes ). Es posible que se requieran licencias de hardware adicionales para realizar los cambios en la arquitectura de la investigación .

**Auditoría:**

Asegúrese de que no hay otras funciones habilitadas para el sistema operativo subyacente y de que no se instala ninguna herramienta de exceso , por la política de la empresa .

**Remediación:**

Desinstalar la herramienta de proceso y/o eliminar los roles necesarios del sistema operativo subyacente .

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 2.10 Segregar física o lógicamente el riesgo Aplicaciones  Los sistemas segregados física o lógicamente deben utilizarse para aislar y ejecutar los programas necesarios para las operaciones comerciales, pero que suponen un gran riesgo para la organización . |  |  | ● |
| v6 | 9.5 OperarServiciosCríticosEnHostsDedicados (esdecir, DNS, correo, web, base de datos)  Operar servicios críticos en máquinas de host físicas o lógicas separadas , como servidores de DNS , archivos, correo, web y bases de datos . |  |  |  |

## 2 Reducción de la superficie

SQLServer ofrece varias opciones de configuración , algunas de las cuales pueden controlarse mediante el procedimiento sp\_configurestoredprocedimiento . Esta sección contiene la lista de las recomendaciones correspondientes .

#### 2.1 Asegúrese de que la opción de configuración del servidor de "consultas distribuidas ad hoc" esté en "0" (automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

La activación de AdHocDistributedQueries permite a los usuarios consultar datos y ejecutar declaraciones de fuentes de datos externas . Esta función debe estar desactivada .

**Justificación:**

Esta función puede utilizarse para acceder de forma remota y explotar vulnerabilidades en instancias remotas del servidor SQL y para ejecutar funciones visuales básicas para aplicaciones .

**Auditoría:**

Ejecute el siguiente comando T-SQL :

SELECT name, CAST(value as int) as value\_configured, CAST(value\_in\_use as int) as value\_in\_use FROM sys.configurations

WHERE name = 'Ad Hoc Distributed Queries';

Las dos columnas de valor deben mostrar 0.

**Remediación:**

Ejecute el siguiente comando T-SQL :

EXECUTE sp\_configure 'show advanced options', 1;

RECONFIGURAR;

EXECUTE sp\_configure 'Ad Hoc Distributed Queries', 0;

RECONFIGURAR;

IR A

EXECUTE sp\_configure 'show advanced options', 0; RECONFIGURE;

**Valor por defecto :**

0 (desactivado)

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/adhoc-distributed-queries-server-configuration-option

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 9.2 Asegúrese de que sólo se ejecuten los puertos , protocolos y servicios aprobados se ejecutan en  Asegúrese de que todos los puertos de red , protocolos y servicios de un sistema con necesidades empresariales validadas estén funcionando en cada sistema . |  | ● | ● |
| v6 | 9.1 Limitar los puertos , protocolos y servicios abiertos  Asegúrese de que todos los puertos , protocolos y servicios con necesidades empresariales validadas se ejecutan en cada sistema . |  |  |  |

#### 2.2 Asegúrese de que la opción de configuración del servidor "CLR Enabled" esté ajustada a "0" (automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

El clr habilitado especifica si los conjuntos de usuarios pueden ser ejecutados por el servidor SQL .

**Justificación:**

Permitir el uso de los ensamblajesCLR agrava la superficie de ataque de SQLServer y supone un riesgo tanto para los ensamblajes involuntarios como para los maliciosos .

**Impacto:**

Si se utilizan conjuntosCLR, es posible que las aplicaciones deban diseñarse para eliminar el riesgo de que se habilite este ajuste . Como alternativa, algunas organizaciones pueden permitir que se habilite este ajuste 1para los conjuntos creados con el SAFE , pero no permiten que los conjuntos creados con los sistemas UNSAFEy EXTERNAL\_ACCESS . Para encontrar conjuntos creados por el usuario , ejecute la siguiente consulta en las bases de datos , sustituyendo *<nombre de la base de datos> por el nombre de cada base de datos* :

USE [<nombre de la base de datos>]

IR A

SELECT name AS Assembly\_Name, permission\_set\_desc

FROM sys.assemblies

WHERE is\_user\_defined = 1;

IR A

**Auditoría:**

Ejecute el siguiente comando T-SQL :

SELECCIONE el nombre,

CAST(valor como int) como valor\_configurado,

CAST(valor\_en\_uso como int) como valor\_en\_uso

FROM sys.configurations

WHERE name = 'clr strict security';

Si ambos valores son 1, esta recomendación no es aplicable . En caso contrario, ejecute el siguiente comando TSQL :

SELECCIONE el nombre,

CAST(valor como int) como valor\_configurado,

CAST(valor\_en\_uso como int) como valor\_en\_uso

FROM sys.configurations

WHERE name = 'clr enabled';

Ambas columnas de valor deben mostrar 0 para que sean conformes .

**Remediación:**

Ejecute el siguiente comando T-SQL :

EXECUTE sp\_configure 'clr enabled', 0; RECONFIGURE;

**Valor por defecto :**

Por defecto , esta opción está desactivada (0).

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/t-sql/statements/create-assembly-transactsql

**Información adicional :**

Si clr estricta seguridadissetto 1esta recomendación no es aplicable . Por defecto , la seguridad estricta está activada y trata SAFEy EXTERNAL\_ACCESS como si estuvieran marcados como INSEGURO. Aunque no se recomienda , la opción clr strict securityoptionpuede estar activada para la compatibilidad con la versión anterior . Esta recomendación se ha mantenido para los entornos configurados para la compatibilidad hacia atrás .

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 18.11 Utilizar plantillas de configuración estándar para Bases de datos  En el caso de las aplicaciones que sólo utilizan una base de datos , utilice una configuración de endurecimiento estándar. |  | ● | ● |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
|  | plantillas. Todos los sistemas que forman parte de los procesos empresariales críticos deben ser probados . |  |  |  |
| v6 | 18.9 SanitizeDeployedSoftwareOfDevelopmentArtifacts  En el caso de las aplicaciones desarrolladas dentro de la empresa , asegúrese de que los artefactos de desarrollo (datos y secuencias de comandos de muestra , bibliotecas , componentes, código de depuración y herramientas no utilizados) no se incluyan en el software desplegado ni sean accesibles en el entorno de producción . |  |  |  |

#### 2.3 Asegúrese de que la opción de configuración del servidor "Cross DB Ownership Chaining" esté establecida en "0" (automatizada)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

La opción controla el encadenamiento de la propiedad de todas las bases de datos a nivel de instancia (o servidor ) .

**Justificación:**

Cuando está activada , esta opción permite a un miembro del db\_ownerodeunabasededatosobtengaaccesoalosobjetosdepropiedaddecualquier otra base de datos , lo que provoca una revelación de información innecesaria . Cuando se requiera , las cadenas de propiedad entre bases de datos sólo deben habilitarse para las bases de datos específicas que lo requieran, en lugar de hacerlo en el nivel de instancia de todas las bases de datos, utilizando el comando ALTER DATABASE<nombre\_de\_base> *SET DB\_CHAINING* ON . Esta opción de base de datos no puede modificarse en maestro, modelo, o bases de datos del sistema temporal .

**Auditoría:**

Ejecute el siguiente comando T-SQL :

SELECCIONE el nombre,

CAST(valor como int) como valor\_configurado,

CAST(valor\_en\_uso como int) como valor\_en\_uso

FROM sys.configurations

WHERE name = 'cross db ownership chaining';

Ambas columnas de valor deben mostrar 0 para que sean conformes .

**Remediación:**

Ejecute el siguiente comando T-SQL :

|  |
| --- |
| EXECUTE sp\_configure 'cross db ownership chaining', 0;  RECONFIGURAR; IR |

**Valor por defecto :**

Por defecto , esta opción está desactivada (0).

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/crossdb-ownership-chaining-server-configuration-option

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 14.6 ProtectInformationthroughAccessControlLists  Proteger toda la información almacenada en los sistemas con controles de acceso específicos para sistemas de archivos , redes, reclamaciones, aplicaciones y bases de datos . Estos controles se basarán en el principio de que sólo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a ella como parte de sus responsabilidades . | ● | ● | ● |
| v6 | 14.4 ProtectInformationWithAccessControlLists  Toda la información almacenada en los sistemas se protegerá con controles de acceso específicos del sistema de archivos , redes compartidas, reclamaciones, aplicaciones y bases de datos . Estos controles se basarán en el principio de que sólo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a ella como parte de sus responsabilidades . |  |  |  |

#### 2.4 Asegúrese de que la opción de configuración del servidor "Database Mail XPs" esté establecida en "0".

#### (Automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1- AWSRDS

**Descripción:**

La opción Database Mail XPsoption controla la capacidad de generar y transmitir mensajes de correo electrónico desde SQL Server .

**Justificación:**

Desactivando el La opción Database Mail XP reduce la superficie de los servidores SQL , elimina un vector de ataque del DoS y un canal para la filtración de datos desde el servidor de bases de datos a un host remoto .

**Auditoría:**

Ejecute el siguiente comando T-SQL :

SELECCIONE el nombre,

CAST(valor como int) como valor\_configurado,

CAST(valor\_en\_uso como int) como valor\_en\_uso

FROM sys.configurations

WHERE name = 'Database Mail XPs';

Ambas columnas de valor deben mostrar 0 para que sean conformes .

**Remediación:**

Ejecute el siguiente comando T-SQL :

EXECUTE sp\_configure 'show advanced options', 1;

RECONFIGURAR;

EXECUTE sp\_configure 'Database Mail XPs', 0;

RECONFIGURAR;

IR A

EXECUTE sp\_configure 'show advanced options', 0; RECONFIGURE;

**Valor por defecto :**

Por defecto , esta opción está desactivada (0).

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/relational-databases/databasemail/database-mail

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 9.2 Asegúrese de que sólo hay puertos , protocolos y servicios aprobados  EstánCorriendo  Asegúrese de que todos los puertos de red , protocolos y servicios de un sistema con necesidades empresariales validadas estén funcionando en cada sistema . |  | ● | ● |
| v6 | 18 AplicaciónSoftwareSeguridad  AplicaciónSoftwareSeguridad |  |  |  |

#### 2.5 Asegúrese de que la opción de configuración del servidor "Procedimientos de automatización de Ole" esté establecida en "0" (automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

El Procedimientos de automatización Ole controla si los objetos de automatización Ole pueden ser iniciados dentro de los lotes Transact-SQL . Estos son procedimientos almacenados extendidos que permiten a los usuarios de SQL Server ejecutar funciones externas a SQL Server .

**Justificación:**

La activación de esta opción aumentará la superficie de ataque de SQL Server y permitirá a los usuarios ejecutar funciones en el contexto de seguridad de SQL Server .

**Auditoría:**

Ejecute el siguiente comando T-SQL :

SELECCIONE el nombre,

CAST(valor como int) como valor\_configurado,

CAST(valor\_en\_uso como int) como valor\_en\_uso

FROM sys.configurations

WHERE name = 'Procedimientos de automatización de Ole';

Ambas columnas de valor deben mostrar 0 para que sean conformes .

**Remediación:**

Ejecute el siguiente comando T-SQL :

EXECUTE sp\_configure 'show advanced options', 1;

RECONFIGURAR;

EXECUTE sp\_configure 'Procedimientos de automatización Ole', 0;

RECONFIGURAR;

IR A

EXECUTE sp\_configure 'show advanced options', 0; RECONFIGURE;

**Valor por defecto :**

Por defecto , esta opción está desactivada (0).

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/oleautomation-procedures-server-configuration-option

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 5.1 EstablecerConfiguracionesSeguras  Mantener documentados los estándares de configuración de seguridad para todos los sistemas y programas operativos autorizados . | ● | ● | ● |
| v6 | 18 AplicaciónSoftwareSeguridad  AplicaciónSoftwareSeguridad |  |  |  |

#### 2.6 Asegúrese de que la opción de configuración del servidor de "acceso remoto" esté establecida en "0" (automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

La opción controla la ejecución de los procedimientos almacenados localmente en los servidores remotos o de los procedimientos almacenados remotamente en el servidor local .

**Justificación:**

La funcionalidad puede ser utilizada para lanzar un ataque de denegación de servicio (DoS) en servidores remotos mediante la descarga del procesamiento de consultas en el objetivo .

**Impacto:**

Según Microsoft : Esta función se eliminará en la próxima versión de Microsoft SQL Server . No utilice esta función en los nuevos trabajos de desarrollo y modifique las aplicaciones que la utilizan actualmente en la medida de lo posible . Utilice sp\_addlinkedserver .

**Auditoría:**

Ejecute el siguiente comando T-SQL :

SELECCIONE el nombre,

CAST(valor como int) como valor\_configurado,

CAST(valor\_en\_uso como int) como valor\_en\_uso

FROM sys.configurations WHERE name = 'remote access';

Las dos columnas de valor deben mostrar 0.

**Remediación:**

Ejecute el siguiente comando T-SQL :

EXECUTE sp\_configure 'show advanced options', 1;

RECONFIGURAR;

EXECUTE sp\_configure 'acceso remoto', 0;

RECONFIGURAR;

IR A

EXECUTE sp\_configure 'show advanced options', 0; RECONFIGURE;

Reinicia el motor de la base de datos .

**Valor por defecto :**

Por defecto , esta opción está activada (1).

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configurewindows/configure-the-remote-access-server-configuration-option

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 9.2 Asegúrese de que sólo se ejecuten los puertos , protocolos y servicios aprobados se ejecutan en  Asegúrese de que todos los puertos de red , protocolos y servicios de un sistema con necesidades empresariales validadas estén funcionando en cada sistema . |  | ● | ● |
| v6 | 9.1 Limitar los puertos , protocolos y servicios abiertos  Asegúrese de que todos los puertos , protocolos y servicios con necesidades empresariales validadas se ejecutan en cada sistema . |  |  |  |

#### 2.7 Asegúrese de que la opción de configuración del servidor "Conexiones de administración remota" esté establecida en "0" (automatizada)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

La página web conexiones de administración remota controla si una aplicación de cliente en un ordenador remoto puede utilizar la conexión de administrador dedicada (DAC).

**Justificación:**

La conexión dedicada del administrador (DAC) permite a un administrador acceder a un servidor en funcionamiento para ejecutar funciones de diagnóstico o declaraciones de Transact-SQL , o para solucionar problemas en el servidor , incluso cuando el servidor está bloqueado o funcionando en un estado normal y no responde a una conexión del motor de base de datos de SQLServer . En un escenario de clústeres , es posible que el administrador no esté registrado en el mismo modo que aloja actualmente la instancia de SQLServer y, por lo tanto, se considere "remoto". Por lo tanto, esta configuración debe estar normalmente habilitada (1) para los clústeres de SQLServer que fallan ; de lo contrario, debe estar habilitada (0) , que es el valor predeterminado .

**Auditoría:**

Ejecute el siguiente comando T-SQL :

Utiliza el maestro;

IR A

SELECCIONE el nombre,

CAST(valor como int) como valor\_configurado,

CAST(valor\_en\_uso como int) como valor\_en\_uso

FROM sys.configurations

WHERE name = 'conexiones de administración remota'

AND SERVERPROPERTY('IsClustered') = 0;

Si no se devuelven datos , la instancia es un grupo y esta recomendación no es aplicable . Si se devuelven datos, las dos columnas de evaluación deben indicar 0 para que se cumpla .

**Remediación:**

Ejecute el siguiente comando T-SQL en instalaciones agrupadas :

|  |
| --- |
| EXECUTE sp\_configure 'remote admin connections', 0;  RECONFIGURAR; IR |

**Valor por defecto :**

Por defecto , esta opción está deshabilitada (0), sólo las conexiones locales pueden utilizar el DAC .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configurewindows/remote-admin-connections-server-configuration-option

**Información adicional :**

Si se trata de una instalación en clúster , esta opción debe estar activada, ya que, de lo contrario, el servidor SQL en clúster no podrá enlazar con el local y el DAC no estará disponible . Habilítelo para instalaciones agrupadas . Desactívela para instalaciones independientes que no sean necesarias .

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 9.2 Asegúrese de que sólo se ejecuten los puertos , protocolos y servicios aprobados se ejecutan en  Asegúrese de que todos los puertos de red , protocolos y servicios de un sistema con necesidades empresariales validadas estén funcionando en cada sistema . |  | ● | ● |
| v6 | 9.1 Limitar los puertos , protocolos y servicios abiertos  Asegúrese de que todos los puertos , protocolos y servicios con necesidades empresariales validadas se ejecutan en cada sistema . |  |  |  |

#### 2.8 Asegúrese de que la opción de configuración del servidor 'Scan For Startup Procs' esté establecida en

#### 0" (automatizado)

**PerfilAplicabilidad :**

* Nivel1- Base de datosEngine
* Nivel1-AWSRDS

**Descripción:**

La opción escanear los procesos de inicio , si está activada , hace que SQLServer escanee y ejecute automáticamente todos los procedimientos almacenados que se ejecutan al iniciar el servicio .

**Justificación:**

La aplicación de este control reduce la amenaza de que una entidad aproveche estas instalaciones para fines ilícitos .

**Impacto:**

Configurar el escaneo de los procedimientos de inicio en 0evitará que ciertas trazas de auditoría y otros procedimientos almacenados de monitorización de uso común se reinicien en el arranque . Además, la replicación requiere que esta configuración esté habilitada (1) y se cambiará automáticamente si es necesario .

**Auditoría:**

Ejecute el siguiente comando T-SQL :

SELECCIONE el nombre,

CAST(valor como int) como valor\_configurado,

CAST(valor\_en\_uso como int) como valor\_en\_uso

FROM sys.configurations

WHERE name = 'scan for startup procs';

Las dos columnas de valor deben mostrar 0.

**Remediación:**

Ejecute el siguiente comando T-SQL :

EXECUTE sp\_configure 'show advanced options', 1;

RECONFIGURAR;

EXECUTE sp\_configure 'scan for startup procs', 0; RECONFIGURE;

IR A

EXECUTE sp\_configure 'show advanced options', 0; RECONFIGURE;

Reinicia el motor de la base de datos .

**Valor por defecto :**

Por defecto , esta opción está desactivada (0).

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configurewindows/configure-the-scan-for-startup-procs-server-configuration-option

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 5.1 EstablecerConfiguracionesSeguras  Mantener documentados los estándares de configuración de seguridad para todos los sistemas y programas operativos autorizados . | ● | ● | ● |
| v6 | 18 AplicaciónSoftwareSeguridad  AplicaciónSoftwareSeguridad |  |  |  |

#### 2.9 Asegúrese de que la propiedad de la base de datos 'Trustworthy' esté desactivada (automatizada)

**PerfilAplicabilidad :**

- • Nivel1-Motor de la base de datos

**Descripción:**

El TRUSTWORTHY permite a los objetos de la base de datos acceder a objetos de otras bases de datos en determinadas circunstancias .

**Justificación:**

Proporciona protección contra los ensamblajesCLR maliciosos o los procedimientos extendidos .

**Auditoría:**

Ejecute la siguiente consulta T-SQL en las bases de datos con un valor de base de datos de confianza de ON:

SELECCIONE el nombre

FROM sys.databases

WHERE is\_trustworthy\_on = 1 AND name != 'msdb';

Los norows deben ser devueltos .

**Remediación:**

Ejecute la siguiente sentencia T-SQL contra las bases de datos (sustituya *<nombre\_de\_la\_base\_de\_datos> a continuación* ) devuelta por el procedimiento de auditoría :

ALTER DATABASE [<nombre\_de\_base\_de\_datos>] SET TRUSTWORTHY OFF;

**Valor por defecto :**

Por defecto , esta propiedad de la base de datos es OFF (is\_trustworthy\_on = 0), excepto para la base de datos base de datos msdbd en la que se requiere que sea ON.

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/relational-databases/security/trustworthydatabase-property
2. https://support.microsoft.com/it-it/help/2183687/guidelines-for-using-thetrustworthy-database-setting-in-sql-server

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 14.6 ProtectInformationthroughAccessControlLists  Proteger toda la información almacenada en los sistemas con controles de acceso específicos para sistemas de archivos , redes, reclamaciones, aplicaciones y bases de datos . Estos controles se basarán en el principio de que sólo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a ella como parte de sus responsabilidades . | ● | ● | ● |
| v6 | 14.4 ProtectInformationWithAccessControlLists  Toda la información almacenada en los sistemas se protegerá con controles de acceso específicos del sistema de archivos , redes compartidas, reclamaciones, aplicaciones y bases de datos . Estos controles se basarán en el principio de que sólo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a ella como parte de sus responsabilidades . |  |  |  |

#### 2.10 Asegúrese de que los protocolos innecesarios de SQL Server estén configurados como "Desactivados" (Manual)

**PerfilAplicabilidad :**

- • Nivel1-Motor de la base de datos

**Descripción:**

SQLServers admite los protocolos de memoria compartida , NamedPipes y TCP/IP . Sin embargo, SQLServers debe configurarse para que acoja el mínimo necesario en función de las necesidades de la organización .

**Justificación:**

El uso de menos protocolos minimiza la superficie de ataque del servidor SQL y , en algunos casos , puede protegerlo de ataques remotos .

**Impacto:**

Los servicios del motor de la base de datos (MSSQL y SQLAgent ) deben detenerse y reiniciarse para que el cambio surta efecto .

**Auditoría:**

Abrir **SQLServerConfigurationManager**; gotothe **SQLServerNetworkConfiguration**.

Asegúrese de que los protocolos requeridos estén activados .

**Remediación:**

Abrir **SQLServerConfigurationManager**; gotothe **SQLServerNetworkConfiguration**.

Asegúrese de que los protocolos necesarios estén activados . Desactive los protocolos que no sean necesarios .

**Valor por defecto:**

Por defecto , los protocolos TCP/IP y de memoria compartida están habilitados en todas las ediciones comerciales .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configurewindows/enable-or-disable-a-server-network-protocol

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 9.2 Asegúrese de que sólo se ejecuten los puertos , protocolos y servicios aprobados se ejecutan en  Asegúrese de que todos los puertos de red , protocolos y servicios de un sistema con necesidades empresariales validadas estén funcionando en cada sistema . |  | ● | ● |
| v6 | 9.1 Limitar los puertos , protocolos y servicios abiertos  Asegúrese de que todos los puertos , protocolos y servicios con necesidades empresariales validadas se ejecutan en cada sistema . |  |  |  |

### 2.11 Asegúrese de que SQL Server está configurado para utilizar puertos no estándar (automatizados)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

Si se instala , una instancia de SQLServer por defecto tendrá asignado un puerto por defecto de TCP:1433 para la comunicación TCP/IP . Los administradores pueden configurar manualmente la instancia nombrada para utilizar TCP:1433 para la comunicación . TCP:1433esunpuertoServidorSQLconocidoydeberíacambiarestaasignacióndepuertos . En un escenario de múltiples instancias , cada una de ellas debe tener asignado su propio puerto TCP/IP .

**Justificación:**

El uso de un puerto no predeterminado ayuda a proteger la base de datos de ataques dirigidos al puerto predeterminado .

**Impacto:**

El cambio del puerto por defecto hará que el DAC (DedicatedAdministratorConnection ) escuche en un puerto cualquiera . Además, puede hacer que algunas aplicaciones importantes , como los cortafuegos de aplicaciones , requieran una configuración especial . En general, debes establecer un puerto estático para un uso consistente de las aplicaciones , incluyendo los firewalls , en lugar de utilizar puertos dinámicos que se elegirán aleatoriamente en cada inicio del SQL Server .

**Auditoría:**

Ejecuta el siguiente script T-SQL :

SELECT TOP(1) local\_tcp\_port FROM sys.dm\_exec\_connections

WHERE local\_tcp\_port IS NOT NULL;

O

SELECT local\_tcp\_port

FROM sys.dm\_exec\_connections WHERE session\_id = @@SPID

Si se devuelve un valor de 1433 se devuelve, es un error .

**Remediación:**

1. En **SQLServerConfigurationManager**, en el panel de control , expanda **SQLServer**

**Configuración de la red**, expanda Protocolos para *<nombredeinstancia>, y haga doble clic en el protocolo TCP/IP*

1. En el **cuadro de diálogo de propiedades TCP/IP** , en el apartado **Dirección IPA** , aparecen varias direcciones IP en el formato IP1, IP2, hasta IPAll. Una de ellas es la dirección IP del adaptador de bucle invertido , 127.0.0.1. Para cada dirección IP del ordenador aparecen otras direcciones IP .
2. En IPAll, cambie el campo **TCPPortfield de** 1433a un puerto no estándar o deje el campo **TCPPortfieldvacío y establezca el valor de** **TCPDynamicPortsen** 0 para habilitar la asignación de puertos dinámicos y, a continuación, haga clic en **OK**.
3. En el panel de control , haga clic en **SQLServerServices**.
4. En el panel de detalles , haga clic con el botón derecho del ratón en **SQLServer (*<Nombredeinstancia> ) y luego haga clic en*** **Reiniciar**, para detener y reiniciar SQLServer .

**Valor por defecto :**

Por defecto , las instancias del servidor SQL escuchan el tráfico TCP/IP en el puerto TCP 1433 y las instancias con nombre utilizan puertos dinámicos .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configurewindows/configure-a-server-to-listen-on-a-specific-tcp-port

**Información adicional :**

En el caso de AWSRDS , esto sólo se configura durante el proceso de construcción .

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 9.2 Asegúrese de que sólo hay puertos , protocolos y servicios aprobados  EstánCorriendo  Asegúrese de que todos los puertos de red , protocolos y servicios de un sistema con necesidades empresariales validadas estén funcionando en cada sistema . |  | ● | ● |
| v6 | 9 Limitación y control de puertos , protocolos y servicios de red Servicios  Limitación y control de puertos , protocolos y servicios de red |  |  |  |

### 2.12 Asegúrese de que la opción "Ocultar Instancia" esté establecida en "Sí" para el SQL de producción

### Instancias del servidor (automatizadas)

**PerfilAplicabilidad :**

- • Nivel1-Motor de la base de datos

**Descripción:**

Las instancias de SQLServer no agrupadas que se encuentren en entornos de producción deben ser designadas como "olvidadas" para evitar que el servicio de navegación de SQLServer las anuncie .

**Justificación:**

La designación de las instancias del servidor SQL de producción como ocultas conduce a una instalación más segura porque no se pueden enumerar . Sin embargo, las instancias agrupadas pueden romperse si se selecciona esta opción .

**Impacto:**

Este método sólo impide que la instancia se incluya en la red . Si la instancia está oculta ( nota expuesta por SQLBrowser ), las conexiones tendrán que especificar el servidor y el puerto para poder conectarse . Esto no impide que los usuarios se conecten al servidor si conocen el nombre de la instancia y el puerto .

Si oculta una instancia con nombre propio , es posible que el servicio de cluster no pueda conectarse a SQL Server. Server. Consulte la referencia de la documentación de Microsoft .

**Auditoría:**

Realice el métodoGUI o T-SQL mostrado :

***1.1.1.1 Método GU***

1. En **SQLServerConfigurationManager**, expanda **SQLServerConfiguración de red**, haga clic con el botón derecho del ratón en **Protocolos para *<nombredeinstancia> y seleccione*** **Propiedades**.
2. En la página web **ficha de banderas** , en la casilla **HideInstance** , si se selecciona Si se selecciona "Sí" , se cumple .

***1.1.1.2 Método T-SQL***

Ejecute el siguiente T-SQL .

DECLARE @getValue INT;

EXEC master.sys.xp\_instance\_regread

@rootkey = N'HKEY\_LOCAL\_MACHINE',

@key = N'SOFTWARE\Microsoft\Microsoft SQL

Server\MSSQLServer\SuperSocketNetLib',

@value\_name = N'HideInstance',

@value = @getValue OUTPUT; SELECT @getValue;

El valor de 1deberá ser devuelto a la conformidad .

**Remediación:**

Realice el métodoGUI o T-SQL mostrado :

***1.1.1.3 Método GUIM***

1. En **SQLServerConfigurationManager**, expanda **SQLServerConfiguración de red**, haga clic con el botón derecho del ratón en **Protocolos para *<nombredeinstancia> y seleccione*** **Propiedades**.
2. En la página web **ficha Banderas** , en la casilla **HideInstance** , seleccione Sí, y luego haga clic en **Aceptar para cerrar el cuadro de diálogo** . El cambio surtirá efecto inmediatamente en las nuevas conexiones .

***1.1.1.4 Método T-SQL***

Ejecute el siguiente T-SQL para remediarlo :

EXEC master.sys.xp\_instance\_regwrite

@rootkey = N'HKEY\_LOCAL\_MACHINE',

@key = N'SOFTWARE\Microsoft\Microsoft SQL

Server\MSSQLServer\SuperSocketNetLib',

@value\_name = N'HideInstance',

@type = N'REG\_DWORD', @value = 1;

**Valor por defecto :**

Por defecto , las instancias de SQLServer están ocultas .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/hidean-instance-of-sql-server-database-engine

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 9.2 Asegúrese de que sólo hay puertos , protocolos y servicios aprobados  EstánCorriendo  Asegúrese de que todos los puertos de red , protocolos y servicios de un sistema con necesidades empresariales validadas estén funcionando en cada sistema . |  | ● | ● |
| v6 | 9 Limitación y control de puertos , protocolos y servicios de red Servicios  Limitación y control de puertos , protocolos y servicios de red |  |  |  |

### 2.13 Asegúrese de que la cuenta de inicio de sesión "sa" esté configurada como "Desactivada" (Automática)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

El sa es una cuenta conocida y a menudo utilizada por todo el servidor SQL con privilegios de administrador del sistema . Esta es la cuenta de origen creada durante la instalación y siempre tiene el principal\_id=1y sid=0x01.

**Justificación:**

La aplicación de este control reduce la probabilidad de que un atacante ejecute ataques de fuerza bruta de nuevo contra un director bien conocido .

**Impacto:**

No es una buena práctica de seguridad codificar aplicaciones o guiones en en esta cuenta . Sin embargo, si se ha hecho esto , la desactivación de la cuenta impedirá que los scripts y las aplicaciones se autentiquen en el servidor de la base de datos y ejecuten las tareas y funciones necesarias .

**Auditoría:**

Utilice la siguiente sintaxis para determinar si el cuenta deshabilitada . Comprobación de sid=0x01 asegura que la cuenta saaccounty se está comprobando en caso de que se haya renunciado a la misma por malas prácticas .

SELECT nombre, is\_disabled

FROM sys.server\_principals

WHERE sid = 0x01

AND is\_disabled = 0;

Los noruegos deben volver a cumplir la normativa .

Un is\_disabledvalueof 0 indica que el registro está actualmente habilitado y, por lo tanto, necesita ser corregido .

**Remediación:**

Ejecute la siguiente consulta T-SQL :

USO [maestro]

IR A

DECLARE @tsql nvarchar(max)

SET @tsql = 'ALTER LOGIN ' + SUSER\_NAME(0x01) + ' DISABLE'

EXEC (@tsql) GO

**Valor por defecto :**

Por defecto , la cuenta de cuenta salogin está deshabilitada en el momento de la instalación cuando se selecciona el modo de autenticación de Windows . Si se selecciona el modo mixto (SQLServer y autenticación de Windows ) en la instalación , la opción predeterminada para el salogin está activada .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/relational-databases/system-catalogviews/sys-server-principals-transact-sql
2. https://docs.microsoft.com/en-us/sql/t-sql/statements/alter-login-transact-sql
3. https://docs.microsoft.com/en-us/sql/relational-databases/security/choose-anauthentication-mode

**Información adicional :**

En el caso de la AWSRDS, el nombre por defecto de esta cuenta es rdsen lugar de sa.

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 16.8 DisableAnyUnassociatedAccounts  Desactivar cualquier cuenta que no pueda ser asociada a un proceso de negocio o a un propietario de negocio . | ● | ● | ● |
| v6 | 5.1 MinimizarYUsarEscasamenteLosPrivilegiosAdministrativos  Reduzca al mínimo los privilegios administrativos y utilice las cuentas administrativas sólo cuando sean necesarias . Implementar una auditoría centrada en el uso de las funciones administrativas privilegiadas y supervisar los comportamientos anómalos . |  |  |  |

### 2.14 Asegúrese de que la cuenta de inicio de sesión "sa" ha sido renombrada (automatizada)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

La cuenta saaccountyesunaconocimientoconfundidoy,a menudo, utilizado por el servidor SQL con privilegios de administrador del sistema . El salogin es el inicio de sesión creado durante la instalación y siempre tiene principal\_id=1y sid=0x01.

**Justificación:**

Es muy difícil lanzar ataques con palabras clave y de fuerza bruta contra salogin si no se conoce su nombre .

**Impacto:**

No es una buena práctica de seguridad codificar aplicaciones o guiones en la dirección salogin. Sin embargo, si se ha hecho esto , cambiar el nombre del impedirá que los scripts y las aplicaciones se autentifiquen en el servidor de la base de datos y ejecuten las tareas y funciones requeridas .

**Auditoría:**

Utilice la siguiente sintaxis para determinar si el salogin (principal) esnombre .

SELECCIONE el nombre

FROM sys.server\_principals WHERE sid = 0x01;

Anameof sa indica que la cuenta no ha sido renombrada y, por lo tanto, necesita ser remediada . **Remediación:**

Sustituya el valor *<usuario\_diferente> con la siguiente sintaxis y ejecute el nombre del* salogin.

ALTER LOGIN sa WITH NAME = <different\_user>;

**Valor por defecto :**

Por defecto , el nombre nombre de la salog es 'sa'.

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/relational-databases/security/choose-anauthentication-mode

**Información adicional :**

En el caso de la AWSRDS, el nombre por defecto de esta cuenta es rdsen lugar de sa.

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 5.1 EstablecerConfiguracionesSeguras  Mantener documentados los estándares de configuración de seguridad para todos los sistemas y programas operativos autorizados . | ● | ● | ● |
| v6 | 5 Uso controlado de los privilegios de administración  Uso controlado de los privilegios de administración |  |  |  |

### 2.15 Asegúrese de que "AUTO\_CLOSE" esté en "OFF" en las bases de datos contenidas (automatizadas)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

AUTO\_CLOSE determina si la base de datosivendose cierra una vez finalizada la conexión . Si se habilita , las siguientes conexiones a la base de datosivend requerirán la apertura de la base de datos y la creación de una caché de procedimientos relevantes .

**Justificación:**

Dado que la autenticación de los usuarios para las bases de datos contenidas se realiza dentro de la base de datos y no en el nivel de instancia del servidor , la base de datos debe abrirse cada vez que se autentifica un usuario . La apertura/cierre frecuente de la base de datos consume recursos adicionales del servidor y puede contribuir a la interrupción del servicio .

**Auditoría:**

Realice lo siguiente para encontrar bases de datos contenidas que no estén configuradas como se indica :

SELECT name, containment, containment\_desc, is\_auto\_close\_on

FROM sys.databases

WHERE contención <> 0 y is\_auto\_close\_on = 1;

Los norows deben ser devueltos .

**Remediación:**

Ejecute el siguiente T-SQL , sustituyendo *<nombre\_de\_base\_de\_datos> por cada nombre de base de datos encontrado por el procedimiento de auditoría* :

ALTER DATABASE <nombre de la base de datos> SET AUTO\_CLOSE OFF;

**Valor por defecto :**

Por defecto , la propiedad de la base de datos AUTO\_CLOSE es OFF, lo que equivale a is\_auto\_close\_on = 0.

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/relational-databases/databases/securitybest-practices-with-contained-databases

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 5.1 EstablecerConfiguracionesSeguras  Mantener documentados los estándares de configuración de seguridad para todos los sistemas y programas operativos autorizados . | ● | ● | ● |
| v6 | 18 AplicaciónSoftwareSeguridad  AplicaciónSoftwareSeguridad |  |  |  |

### 2.16 Asegúrese de que no existe ningún inicio de sesión con el nombre "sa" (automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

El salogin (porejemplo, eldirector) esunacuentaconocidayampliamenteutilizadaenSQLServer . Por lo tanto, no debe haber unalogro llamado saeincluso cuando el original salogin (principal\_id = 1) ha sido renombrado .

**Justificación:**

La aplicación de este control reduce la probabilidad de que un atacante ejecute ataques de fuerza bruta contra un nombre principal bien conocido .

**Impacto:**

No es una buena práctica de seguridad codificar aplicaciones o guiones en sa cuenta . Dado que la mejor práctica es nombrar y desactivar la cuenta cuenta sa , alguna aplicación de tercera parte comprobará la existencia de un nombre sa y, si no existe, crea una . La eliminación de impedirá que los scripts y las aplicaciones se autentifiquen en el servidor de la base de datos y ejecuten las tareas o funciones requeridas .

**Auditoría:**

Utilice la siguiente sintaxis para determinar si existe una cuenta denominada sa.

SELECT principal\_id, name

FROM sys.server\_principals WHERE name = 'sa';

Los norows deben ser devueltos .

**Remediación:**

Ejecute la página web ALTER o DROP basándose en el principal\_id devuelto para el registro llamado sa. Sustituya el valor *<nombre\_diferente> con la siguiente sintaxis y ejecute el nombre del* salogin.

USO [maestro]

IR A

|  |
| --- |
| -- Si principal\_id = 1 o el inicio de sesión posee objetos de la base de datos, renombre el inicio de sesión sa  ALTERAR LOGIN [sa] CON NOMBRE = <nombre\_diferente>;  IR A  -- Si el inicio de sesión no posee ningún objeto de la base de datos, entonces elimínalo  -- NO elimine el inicio de sesión si es principal\_id = 1 DROP LOGIN sa |

**Valor por defecto :**

El acceso con principal\_id = 1 se llama sabydefault .

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 5.1 EstablecerConfiguracionesSeguras  Mantener documentados los estándares de configuración de seguridad para todos los sistemas y programas operativos autorizados . | ● | ● | ● |
| v6 | 5.1 MinimizarYUsarEscasamenteLosPrivilegiosAdministrativos  Reduzca al mínimo los privilegios administrativos y utilice las cuentas administrativas sólo cuando sean necesarias . Implementar una auditoría centrada en el uso de las funciones administrativas privilegiadas y supervisar los comportamientos anómalos . |  |  |  |

### 2.17 Asegúrese de que la opción de configuración del servidor "clr strict security" esté establecida en "1".

### (Automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

El clr seguridad estricta especifica si el motor aplica el PERMISSION\_SETen los conjuntos .

**Justificación:**

Permitir el uso de los ensamblajesCLR agrava la superficie de ataque de SQLServer y supone un riesgo tanto para los ensamblajes involuntarios como para los maliciosos .

**Impacto:**

Si se utilizan ensamblajesCLR , es posible que las aplicaciones deban ser diseñadas para eliminar el virus antes de activar este ajuste . Para encontrar conjuntos creados por el usuario , ejecute la siguiente consulta en todas las bases de datos , sustituyendo <nombre de la base de datos> por el nombre de cada base de datos :

USE [<nombre de la base de datos>]

IR A

SELECT name AS Assembly\_Name, permission\_set\_desc

FROM sys.assemblies

WHERE is\_user\_defined = 1;

IR A

**Auditoría:**

Ejecute el siguiente comando T-SQL :

SELECCIONE el nombre,

CAST(valor como int) como valor\_configurado,

CAST(valor\_en\_uso como int) como valor\_en\_uso

FROM sys.configurations

WHERE name = 'clr strict security';

Las dos columnas de valoración deben indicar 1 para ser conformes .

**Remediación:**

Ejecute el siguiente comando T-SQL :

EXECUTE sp\_configure 'show advanced options', 1;

RECONFIGURAR;

EXECUTE sp\_configure 'clr strict security', 1;

RECONFIGURAR;

IR A

EXECUTE sp\_configure 'show advanced options', 0; RECONFIGURE;

**Valor por defecto :**

Por defecto , esta opción está activada (1).

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/clrstrict-security?view=sql-server-ver15&viewFallbackFrom=sql-server-2019

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 18.9 Separación de los sistemas de producción y no producción  Mantener entornos separados para los sistemas de producción y de no producción .  Los promotores no deben tener entornos de acceso a la producción no controlados . |  | ● | ● |
| v7 | 18.11 Utilizar plantillas de configuración estándar para Bases de datos  En el caso de las aplicaciones que se basan únicamente en una base de datos , se deben utilizar plantillas de configuración de endurecimiento estándar . Todos los sistemas que formen parte de procesos empresariales críticos deben probarse . |  | ● | ● |

# *3 Autenticación y autorización*

Esta sección contiene recomendaciones relacionadas con los mecanismos de autenticación y autorización de SQLServer .

### 3.1 Asegúrese de que la propiedad "Autenticación del servidor" esté configurada como "Windows".

### Modo de autenticación" (automatizado)

**PerfilAplicabilidad :**

* Nivel1- Base de datosEngine
* Nivel1-AWSRDS

**Descripción:**

Utiliza **WindowsAuthentication para validar los intentos de conexión** .

**Justificación:**

Windows ofrece un mecanismo de autenticación más robusto que la autenticación del servidor SQL .

**Impacto:**

Para cambiar la configuración del modo de acceso es necesario reiniciar el servicio .

**Auditoría:**

Ejecuta la siguiente sintaxis :

SELECT SERVERPROPERTY('IsIntegratedSecurityOnly') como [login\_mode];

A modo\_de\_inicio\_de\_la\_contraseña\_de\_la\_familia 1 indica que la propiedad **ServidordeAutenticaciónestáen** **WindowsAuthenticationMode**. A modo de inicio de sesión 0 indica un modo de autenticación mixto .

**Remediación:**

Realice el métodoGUI o T-SQL mostrado :

***1.1.1.5 Método GUIM***

1. Abrir **SQLServerManagementStudio**.
2. Openthe **ObjectExplorer** y conéctese a la instancia de la base de datos de destino .
3. Haga clic con el botón derecho del ratón en el nombre del establecimiento y seleccione **Propiedades**.
4. Seleccione la página **Página de seguridad en el menú de la izquierda** .
5. Establezca el **autenticación del servidor en** **Modo de autenticación de Windows**.

***1.1.1.6 Método T-SQL***

Ejecute el siguiente T-SQL en una ventana de consulta :

USO [maestro]

IR A

EXEC xp\_instance\_regwrite N'HKEY\_LOCAL\_MACHINE',

N'Software\Microsoft\MSSQLServer\MSSQLServer', N'LoginMode', REG\_DWORD, 1 GO

Reinicie el servicio SQLServers para que el cambio surta efecto .

**Valor por defecto :**

WindowsAuthenticationMode

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configurewindows/server-properties-security-page

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 16.2 ConfigureCentralizedPointofAuthentication  Configure el acceso a todas las cuentas a través de los menos puntos de autenticación centralizados posibles , incluidos los sistemas de red , de seguridad y de nube . |  | ● | ● |
| v6 | 16.9 ConfigureAccountAccessCentrally  Configure el acceso para todas las cuentas a través de un punto de autenticación centralizado , por ejemplo, Directorio activo o LDAP . Configure también los dispositivos de red y de seguridad para la autenticación centralizada . |  |  |  |

### 3.2 Asegúrese de que los permisos de CONEXIÓN del usuario "invitado" están revocados en todas las bases de datos de SQL Server, excluyendo la maestra, la msdb y la tempdb (automatizada)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

Retire la parte superior de guestusertoconnect toSQLServerdatabases , except for maestra, msdb, y tempdb.

**Justificación:**

Alogin asume la identidad del invitado cuando el usuario alogin tiene acceso al servidor SQL pero no tiene acceso a la base de datos a través de su propia cuenta y la base de datos es cuenta de usuario invitado . Revocación del permiso de CONNECT para el usuarioinvitadoaseguraráqueelcatalogenopuedaaccederalabasede datos información de la base de datos con un acceso no explícito .

**Impacto:**

Cuando CONNECT en se revoca el permiso para el usuario invitado , se debe asignar un registro de inicio de sesión de SQL Server a un uso de la base de datos de forma explícita para tener acceso a la base de datos .

**Auditoría:**

Ejecute el siguiente fragmento de código para cada base de datos (sustituyendo *<nombre de la base de datos> según corresponda* ) en la instalación para determinar si el usuario invitado tiene CONNECT . Tampoco se devolverán los permisos .

USE <nombre de la base de datos>;

IR A

SELECT DB\_NAME() AS DatabaseName, 'guest' AS Database\_User,

[permission\_name], [state\_desc]

FROM sys.database\_permissions

WHERE [grantee\_principal\_id] = DATABASE\_PRINCIPAL\_ID('guest')

AND [state\_desc] LIKE 'GRANT%'

AND [permission\_name] = 'CONNECT'

AND DB\_NAME() NOT IN ('master','tempdb','msdb');

**Remediación:**

El siguiente fragmento de código hace referencia a CONECTARpermisosdela usuario invitado en la base de datos . Sustituya *<nombre de la base de datos> como corresponda* :

USE <nombre de la base de datos>;

IR A

REVOCAR LA CONEXIÓN DEL INVITADO;

**Valor por defecto :**

El invitado se añade a todas las bases de datos nuevas, pero sin CONNECT por defecto .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/relational-databases/policy-basedmanagement/guest-permissions-on-user-databases

**Información adicional :**

El guestus no puede hacer que se revoque el permiso de CONNECT en maestro, msdband tempdb, pero este permiso debe ser revocado en todas las demás bases de datos de la instancia de SQLServer .

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 14.6 ProtectInformationthroughAccessControlLists  Proteger toda la información almacenada en los sistemas con controles de acceso específicos para sistemas de archivos , redes, reclamaciones, aplicaciones y bases de datos . Estos controles se basarán en el principio de que sólo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a ella como parte de sus responsabilidades . | ● | ● | ● |
| v6 | 16 Seguimiento y control de cuentas  Seguimiento y control de cuentas |  |  |  |

### 3.3 Asegurarse de que los "usuarios huérfanos" son eliminados de las bases de datos de SQL Server

### (Automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

Un usuario de la base de datos para el que el servidor SQL correspondiente no está definido o está mal definido en la instancia del servidor no puede registrarse en la instancia y se le considera huérfano y debe ser eliminado .

**Justificación:**

Los usuarios huérfanos deben ser eliminados para evitar el posible mal uso de esos usuarios rotos de cualquier manera .

**Auditoría:**

Ejecute la siguiente consulta T-SQL en cada base de datos para identificar a los usuarios huérfanos . Tampoco se devolverán los resultados .

USE <nombre de la base de datos>;

IR A

EXEC sp\_change\_users\_login @Action='Report';

**Remediación:**

Si el usuario huérfano no puede coincidir con un inicio de sesión existente mediante el proceso documentado de Microsoft al que se hace referencia a continuación , ejecute la siguiente consulta T-SQL en la base de datos correspondiente para eliminar un usuario huérfano :

USE <nombre de la base de datos>;

IR A

DROP USER <nombre de usuario>;

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/sql-server/failover-clusters/troubleshootorphaned-users-sql-server

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 16.8 DisableAnyUnassociatedAccounts  Desactivar cualquier cuenta que no pueda ser asociada a un proceso de negocio o a un propietario de negocio . | ● | ● | ● |
| v6 | 16 Seguimiento y control de cuentas  Seguimiento y control de cuentas |  |  |  |

### 3.4 Asegurarse de que la autenticación SQL no se utiliza en las bases de datos contenidas (automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

Las bases de datos contenidas no aceptan las reglas de finalización de la contraseña para los usuarios autenticados de SQL .

**Justificación:**

La ausencia de una política de contraseñas reforzada puede aumentar la probabilidad de que se establezca una credencial débil en una base de datos conservada .

**Impacto:**

Si bien las bases de datos contenidas ofrecen flexibilidad para la reubicación de las bases de datos en diferentes circunstancias y entornos , esto debe equilibrarse con la consideración de que no existe ningún mecanismo de política de contraseñas para los usuarios autenticados de SQLA en las bases de datos contenidas .

**Auditoría:**

Ejecute la siguiente línea T-SQL en cada base de datos que contenga usuarios de la base de datos que utilicen autenticación SQL :

|  |
| --- |
| SELECT nombre como DBUser  FROM sys.database\_principals  WHERE name NOT IN ('dbo','Information\_Schema','sys','guest')  AND type IN ('U','S','G')  AND authentication\_type = 2; GO |

**Remediación:**

Aprovechar los usuarios autentificados de Windows en las bases de datos contenidas .

**Valor por defecto :**

Los usuarios autentificados SQLA (autentificación USER CON CONTRASEÑA ) están permitidos en las bases de datos contenidas .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/relational-databases/databases/securitybest-practices-with-contained-databases

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 16.2 ConfigureCentralizedPointofAuthentication  Configure el acceso a todas las cuentas a través de los menos puntos de autenticación centralizados posibles , incluidos los sistemas de red , de seguridad y de nube . |  | ● | ● |
| v6 | 16.12 UseLongPasswordsForAllUserAccounts  Cuando no se admita la autenticación multifactorial , se exigirá a las cuentas de usuario que tengan una contraseña larga en el sistema (de más de 14 caracteres ). |  |  |  |

### 3.5 Asegúrese de que la cuenta de servicio MSSQL del servidor SQL no es un

### Administrador (manual)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

La cuenta de servicio y/o el SID de servicio utilizados por el servicio MSSQLSERVER para una instancia por defecto o *<NombredeInstancia>*  para una instancia con nombre no debe ser miembro del grupo de administradores de Windows, ya sea directamente o indirectamente (a través de un grupo ) . Esto significa que la cuenta conocida como Sistema local (también conocida como NT AUTHORITYSYSTEM) no debe utilizarse para el servicio MSSQL ya que esta cuenta tiene más privilegios que los que requiere elSQLServerservicio .

**Justificación:**

Siguiendo el principio de los privilegios de la administración , las cuentas de servicio deben tener menos privilegios que los necesarios para realizar su trabajo . En el caso de los servicios SQL Server, la configuración del servidor SQL Server asignará los permisos necesarios directamente al SID del servicio. SID. No deberían ser necesarios permisos o privilegios adicionales .

**Impacto:**

La herramienta **La herramienta SQLServerConfigurationManager debe utilizarse siempre para cambiar la**  cuenta de servicio **del servidor SQL** . Esto garantizará que la cuenta tenga los privilegios necesarios . Si el servicio necesita acceder a otros recursos que no sean los directorios y el registro estándar definidos por Microsoft , es posible que haya que conceder permisos adicionales por separado a esos recursos .

**Auditoría:**

Compruebe que la cuenta de servicio ( en el caso de una cuenta local o AD ) y el SID de servicio SID no sean miembros del grupo de administradores de Windows .

**Remediación:**

En el caso de que se utilice sistema local , utilice el **SQLServerConfigurationManager para cambiar a una cuenta con privilegios** . De lo contrario, elimine el SID del servicio de cuentas SID del grupo de administradores . Es posible que tenga que salir de la página web **SQLServerConfigurationManager si se han cambiado los permisos subyacentes o si** **SQLServerConfigurationManager no se utilizó originalmente para establecer la cuenta de servicio** .

**Valor por defecto :**

Por defecto , la cuenta de servicio (o SID de servicio) no es miembro del grupo de administradores. SID) no es miembro del grupo de administradores .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configurewindows/configure-windows-service-accounts-and-permissions

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 4.3 Garantizar el uso de las cuentas administrativas dedicadas  Asegúrese de que todos los usuarios con acceso a una cuenta administrativa utilicen una cuenta dedicada o secundaria para las actividades más importantes . Estas cuentas sólo deben utilizarse para actividades administrativas y no para navegar por Internet , correo electrónico o actividades similares . | ● | ● | ● |
| v6 | 5.1 MinimizarYUsarEscasamenteLosPrivilegiosAdministrativos  Reduzca al mínimo los privilegios administrativos y utilice las cuentas administrativas sólo cuando sean necesarias . Implementar una auditoría centrada en el uso de las funciones administrativas privilegiadas y supervisar los comportamientos anómalos . |  |  |  |

### 3.6 Asegúrese de que la cuenta de servicio SQLAgent del servidor SQL no es un

### Administrador (manual)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

La cuenta de servicio y/o el servicio SID utilizados por el SQLSERVERAGENT para una instancia por defecto o SQLAGENT$<NombredeInstancia> para una instancia con nombre no debe ser miembro del grupo de administradores de Windows, ya sea directamente o indirectamente (a través de un grupo ). Esto significa que la cuenta conocida como SistemaLocal (AKA NT AUTHORITYSYSTEM) no debe utilizarse para el servicio servicio SQLAGENT ya que esta cuenta tiene más privilegios que los que requiere el servicio SQLServers .

**Justificación:**

Siguiendo el principio de los privilegios de la administración , las cuentas de servicio deben tener menos privilegios que los necesarios para realizar su trabajo . En el caso de los servicios SQL Server , la configuración del servidor SQL Server asignará los permisos necesarios directamente al SID del servicio. SID. No deberían ser necesarios permisos o privilegios adicionales .

**Impacto:**

La herramienta **La herramienta SQLServerConfigurationManager debe utilizarse siempre para cambiar la**  cuenta de servicio **del servidor SQL** . Esto garantizará que la cuenta tenga los privilegios necesarios . Si el servicio necesita acceder a otros recursos que no sean los directorios y el registro estándar definidos por Microsoft , es posible que haya que conceder permisos adicionales por separado a esos recursos .

Si utiliza la función de inicio automático , el servicio SQLAGENTdebe serAdministrador .

**Auditoría:**

Compruebe que la cuenta de servicio ( en el caso de una cuenta local o AD ) y el SID de servicio SID no sean miembros del grupo de administradores de Windows .

**Remediación:**

En el caso de que se utilice sistema local , utilice el **SQLServerConfigurationManager para cambiar a una cuenta con privilegios** . De lo contrario, elimine el SID del servicio de cuentas SID del grupo de administradores . Es posible que tenga que salir de la página web **SQLServerConfigurationManager si se han modificado los permisos subyacentes o si** **SQLServerConfigurationManager no se utilizó originalmente para establecer la cuenta de servicio** .

**Valor por defecto :**

Por defecto , la cuenta de servicio (o SID de servicio) no es miembro del grupo de administradores. SID) no es miembro del grupo de administradores .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configurewindows/configure-windows-service-accounts-and-permissions

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 4.3 Garantizar el uso de las cuentas administrativas dedicadas  Asegúrese de que todos los usuarios con acceso a una cuenta administrativa utilicen una cuenta dedicada o secundaria para las actividades más importantes . Estas cuentas sólo deben utilizarse para actividades administrativas y no para navegar por Internet , correo electrónico o actividades similares . | ● | ● | ● |
| v6 | 5.1 MinimizarYUsarEscasamenteLosPrivilegiosAdministrativos  Reduzca al mínimo los privilegios administrativos y utilice las cuentas administrativas sólo cuando sean necesarias . Implementar una auditoría centrada en el uso de las funciones administrativas privilegiadas y supervisar los comportamientos anómalos . |  |  |  |

### 3.7 Asegúrese de que la cuenta de servicio de texto completo de SQL Server no es una

### Administrador (manual)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

La cuenta de servicio y/o el servicio SID utilizados por MSSQLFDLaunchers para una instancia por defecto o El servicio MSSQLFDLauncher$<NombreDeInstancia> para una instancia con nombre no debe ser miembro del grupo AdministradorDeVentanas, ni directa ni indirectamente (a través de un grupo). grupo). Esto significa que la cuenta conocida como Sistema local (también conocida como NT AUTHORITYSYSTEM) no debe utilizarse para el servicio de texto completo, ya que esta cuenta tiene más privilegios que los que requiere el servicio SQLServers .

**Justificación:**

Siguiendo el principio de los privilegios de la administración, las cuentas de servicio deben tener menos privilegios que los necesarios para realizar su trabajo . En el caso de los servicios SQL Server , la configuración del servidor SQL Server asignará los permisos necesarios directamente al SID del servicio. SID. No deberían ser necesarios permisos o privilegios adicionales .

**Impacto:**

La herramienta **La herramienta SQLServerConfigurationManager debe utilizarse siempre para cambiar la**  cuenta de servicio **del servidor SQL** . Esto garantizará que la cuenta tenga los privilegios necesarios . Si el servicio necesita acceder a otros recursos que no sean los directorios y el registro estándar definidos por Microsoft , es posible que haya que conceder permisos adicionales por separado a esos recursos .

**Auditoría:**

Compruebe que la cuenta de servicio ( en el caso de una cuenta local o AD ) y el SID de servicio SID no sean miembros del grupo de administradores de Windows .

**Remediación:**

En el caso de que se utilice sistema local , utilice el **SQLServerConfigurationManager para cambiar a una cuenta con privilegios** . De lo contrario, elimine el SID del servicio de cuentas SID del grupo de administradores . Es posible que tenga que salir de la página web **SQLServerConfigurationManager si se han modificado los permisos subyacentes o si** **SQLServerConfigurationManager no se utilizó originalmente para establecer la cuenta de servicio** .

**Valor por defecto :**

Por defecto , la cuenta de servicio (o SID de servicio) no es miembro del grupo de administradores. SID) no es miembro del grupo de administradores .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configurewindows/configure-windows-service-accounts-and-permissions

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 4.3 Garantizar el uso de las cuentas administrativas dedicadas  Asegúrese de que todos los usuarios con acceso a una cuenta administrativa utilicen una cuenta dedicada o secundaria para las actividades más importantes . Estas cuentas sólo deben utilizarse para actividades administrativas y no para navegar por Internet , correo electrónico o actividades similares . | ● | ● | ● |
| v6 | 5.1 MinimizarYUsarEscasamenteLosPrivilegiosAdministrativos  Reduzca al mínimo los privilegios administrativos y utilice las cuentas administrativas sólo cuando sean necesarias . Implementar una auditoría centrada en el uso de las funciones administrativas privilegiadas y supervisar los comportamientos anómalos . |  |  |  |

### 3.8 Asegúrese de que sólo se conceden los permisos por defecto especificados por Microsoft al rol de servidor público (automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

público es un rol de servidor fijo especial que contiene todos los registros . A diferencia de otros roles de servidor fijo , los permisos pueden cambiarse para el rol rol público . De acuerdo con el principio de los privilegios de la administración , los servidor público no debe utilizarse para otorgar permisos en el ámbito del servidor ya que todos los usuarios los heredarían .

**Justificación:**

Todos los accesos al servidor SQL pertenecen a público no puede ser eliminado de este rol . Por lo tanto, cualquier permiso otorgado a este rol estará disponible para todos los inicios de sesión, a menos que se les haya negado explícitamente para inicios de sesión específicos o roles de servidor definidos por el usuario .

**Impacto:**

Cuando se revocan los permisos extraños de el acceso puede ser cancelado sin que se concedan los permisos a los usuarios explícitos o a los roles de servidor más definidos que contengan los accesos requeridos .

**Auditoría:**

Utilice la siguiente sintaxis para determinar si se han concedido permisos adicionales a función de servidor público .

SELECT \*

FROM master.sys.server\_permissions

WHERE (grantee\_principal\_id = SUSER\_SID(N'public') y state\_desc LIKE

'GRANT%')

AND NOT (state\_desc = 'GRANT' y [permission\_name] = 'VIEW ANY DATABASE' y class\_desc = 'SERVER')

AND NOT (state\_desc = 'GRANT' y [permission\_name] = 'CONNECT' y class\_desc = 'ENDPOINT' y major\_id = 2)

AND NOT (state\_desc = 'GRANT' y [permission\_name] = 'CONNECT' y class\_desc = 'ENDPOINT' y major\_id = 3)

AND NOT (state\_desc = 'GRANT' y [permission\_name] = 'CONNECT' y class\_desc = 'ENDPOINT' y major\_id = 4)

AND NOT (state\_desc = 'GRANT' y [permission\_name] = 'CONNECT' y class\_desc = 'ENDPOINT' y major\_id = 5);

Esta consulta no debe devolver ninguna filas.

**Remediación:**

1. Añade los permisos extraños encontrados en los resultados de la consulta de auditoría a los roles de servidor específicos definidos por el usuario que requieren el acceso .
2. Revocar el *<nombre\_de\_permiso> de la* rol públicocomo se muestra a continuación

USO [maestro]

IR A

REVOKE <nombre\_de\_permiso> FROM public; GO

**Valor por defecto :**

Por defecto , el servidor público se otorga Ver cualquier base de datos y el

CONNECTpermissiononthedefaultendpoints (TSQL Local Machine, TSQL Named Pipes, TSQL Default TCP, TSQL Default VIA). El VISTA DE CUALQUIER BASE DE DATOS permite el acceso a los datos de la base de datos , a menos que se deniegue explícitamente . **Referencias:**

1. https://docs.microsoft.com/en-us/sql/relationaldatabases/security/authentication-access/server-level-roles
2. https://docs.microsoft.com/en-us/sql/relationaldatabases/security/authentication-access/server-level-roles#permissions-of-fixedserver-roles

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 14.6 ProtectInformationthroughAccessControlLists  Proteger toda la información almacenada en los sistemas con controles de acceso específicos para sistemas de archivos , redes, reclamaciones, aplicaciones y bases de datos . Estos controles se basarán en el principio de que sólo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a ella como parte de sus responsabilidades . | ● | ● | ● |
| v6 | 5.1 MinimizarYUsarEscasamenteLosPrivilegiosAdministrativos  Reduzca al mínimo los privilegios administrativos y utilice las cuentas administrativas sólo cuando sean necesarias . Implementar una auditoría centrada en el uso de las funciones administrativas privilegiadas y supervisar los comportamientos anómalos . |  |  |  |

### 3.9 Asegúrese de que los grupos BUILTIN de Windows no son inicios de sesión SQL (automatizados)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

Antes de SQLServer2008 , el grupo El grupo de administradores BUILTIN se añadía como inicio de sesión de SQLServer con privilegios de administrador del sistema durante la instalación por defecto . Las mejores prácticas promueven la creación de un grupo de nivel de directorio activo que contenga cuentas de personal de administración de empresas aprobadas y el uso de este grupo AD controlado como inicio de sesión con privilegios de administrador del sistema . Los gruposAD deben especificarse durante la instalación de SQLServer y en BUILTINAdministratorsgroupseríadebidoalogar .

**Justificación:**

Los grupos Los grupos BUILTIN (Administradores, Todos, Usuarios Autenticados , Invitados, etc.) generalmente contienen miembros muy amplios que no se ajustan a la mejor práctica de garantizar que sólo los usuarios necesarios tengan acceso a una instancia de SQLServer . Estos grupos no deben utilizarse para ningún nivel de acceso a una instancia de motor de base de datos SQLServer .

**Impacto:**

Antes de cerrar la página BUILTINgroups , asegúrese de que se han añadido los grupos AD alternativos o los registros de Windows con los permisos correspondientes . De lo contrario, la instancia de SQLServer puede resultar totalmente inaccesible .

**Auditoría:**

Utilice la siguiente sintaxis para determinar si algún BUILTIN se ha añadido algún grupo o cuenta como inicio de sesión en el servidor SQL .

SELECT pr.[nombre], pe.[nombre\_permiso], pe.[estado\_desc]

FROM sys.server\_principals pr

JOIN sys.server\_permissions pe

ON pr.principal\_id = pe.grantee\_principal\_id WHERE pr.name like 'BUILTIN%';

Esta consulta no debe devolver ninguna línea .

**Remediación:**

1. Para cada BUILTIN , si es necesario, cree un grupo AD más restrictivo que contenga sólo las cuentas de usuario requeridas .
2. Añada la dirección o cuentas individuales de Windows como inicio de sesión del servidor SQL y conceder los permisos necesarios .
3. Deje caer el BUILTIN en la sintaxis después de reemplazar *<nombre> en* [BUILTIN<nombre> *].*

USO [maestro]

IR A

DROP LOGIN [BUILTIN<nombre>] GO

**Valor por defecto :**

Por defecto , no se añaden grupos grupos BUILTIN se añaden como registros SQL .

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 14.6 ProtectInformationthroughAccessControlLists  Proteger toda la información almacenada en los sistemas con controles de acceso específicos para sistemas de archivos , redes, reclamaciones, aplicaciones y bases de datos . Estos controles se basarán en el principio de que sólo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a ella como parte de sus responsabilidades . | ● | ● | ● |
| v6 | 14.4 ProtectInformationWithAccessControlLists  Toda la información almacenada en los sistemas se protegerá con controles de acceso específicos del sistema de archivos , redes compartidas, reclamaciones, aplicaciones y bases de datos . Estos controles se basarán en el principio de que sólo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a ella como parte de sus responsabilidades . |  |  |  |

### 3.10 Asegúrese de que los grupos locales de Windows no son inicios de sesión de SQL (automatizados)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

Los grupos locales de Windows no deben usarse como inicio de sesión para las instancias del servidor SQL .

**Justificación:**

Permitir que los grupos locales de Windows sean el inicio de sesión de SQL proporciona una brecha en la que cualquier persona con derechos de administrador de nivel de SO (y sin derechos de SQL Server ) podría añadir usuarios a los grupos locales de Windows y, por lo tanto, permitirse a sí mismos o a otros el acceso a la instancia de SQL Server .

**Impacto:**

Antes de eliminar los inicios de sesión del grupo local , asegúrate de que se han añadido los inicios de sesión alternativos de ADGroups o Windows con los permisos correspondientes . De lo contrario, la instancia de SQLServer puede resultar totalmente inaccesible .

**Auditoría:**

Utilice la siguiente sintaxis para determinar si se han añadido grupos locales como inicios de sesión del servidor SQL .

|  |
| --- |
| USE [master] GO  SELECT pr.[name] AS LocalGroupName, pe.[permission\_name], pe.[state\_desc]  FROM sys.server\_principals pr  JOIN sys.server\_permissions pe  ON pr.[principal\_id] = pe.[grantee\_principal\_id]  WHERE pr.[type\_desc] = 'WINDOWS\_GROUP'  AND pr.[name] like CAST(SERVERPROPERTY('MachineName') AS nvarchar) + '%'; |

Esta consulta no debe devolver ninguna línea .

**Remediación:**

1. Para cada LocalGroupName si es necesario, cree un grupo AD equivalente que contenga sólo las cuentas de usuario requeridas .
2. Añada el grupo de AD o las cuentas individuales de Windows como inicio de sesión de SQL Server y conceda los permisos necesarios .
3. Deje caer el LocalGroupNameloginusing the syntaxbelow afterreplacement *<nombre>.*

USO [maestro]

IR A

DROP LOGIN [<nombre>] GO

**Valor por defecto :**

Por defecto , no se añaden grupos locales como registros SQL .

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 14.6 ProtectInformationthroughAccessControlLists  Proteger toda la información almacenada en los sistemas con controles de acceso específicos para sistemas de archivos , redes, reclamaciones, aplicaciones y bases de datos . Estos controles se basarán en el principio de que sólo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a ella como parte de sus responsabilidades . | ● | ● | ● |
| v6 | 14.4 ProtectInformationWithAccessControlLists  Toda la información almacenada en los sistemas se protegerá con controles de acceso específicos del sistema de archivos , redes compartidas, reclamaciones, aplicaciones y bases de datos . Estos controles se basarán en el principio de que sólo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a ella como parte de sus responsabilidades . |  |  |  |

### 3.11 Asegúrese de que el rol público de la base de datos msdb no tiene acceso a los proxies de SQL Agent (automatizado)

**PerfilAplicabilidad :**

- • Nivel1-Motor de la base de datos

**Descripción:**

El sitio web base de datos pública contiene todos los usuarios de la base de datos base de datos msdb . Los proxies de SQLAgent definen un contexto de seguridad en el que se puede ejecutar un paso de trabajo .

**Justificación:**

La concesión de acceso a los proxies de SQLAgent para el permitiría a todos los usuarios utilizar el apoderado que puede tener altos privilegios . Esto probablemente rompería el principio de los privilegios de la playa.

**Impacto:**

Antes de volver a activar el del proxy , asegúrese de que se han añadido los inicios de sesión alternativos o las funciones de base de datos definidas por el usuario con los permisos correspondientes .

De lo contrario, los pasos de trabajo de SQLAgent dependientes de este acceso fallarán .

**Auditoría:**

Utilice la siguiente sintaxis para determinar si se ha concedido el acceso a los datos de la base de datos base de datos msdbd función pública .

USE [msdb]

IR A

SELECT sp.name AS proxyname

FROM dbo.sysproxylogin spl

JOIN sys.database\_principals dp

ON dp.sid = spl.sid

JOIN sysproxies sp

ON sp.proxy\_id = spl.proxy\_id

WHERE principal\_id = USER\_ID('public'); GO

Esta consulta no debe devolver ninguna línea .

**Remediación:**

1. Asegúrese de que los principales de seguridad requeridos tengan acceso explícito al proxy (utilice sp\_grant\_login\_to\_proxy).
2. Revocar el acceso a *<nombre de usuario> del* rol público .

|  |
| --- |
| USE [msdb] GO  EXEC dbo.sp\_revoke\_login\_from\_proxy @name = N'public', @proxy\_name = N'<proxyname>';  IR A |

**Valor por defecto :**

Por defecto , el msdb no tiene acceso a ningún proxy .

**Referencias:**

1. https://support.microsoft.com/en-us/help/2160741/best-practices-in-configuringsql-server-agent-proxy-account

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 14.6 ProtectInformationthroughAccessControlLists  Proteger toda la información almacenada en los sistemas con controles de acceso específicos para sistemas de archivos , redes, reclamaciones, aplicaciones y bases de datos . Estos controles se basarán en el principio de que sólo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a ella como parte de sus responsabilidades . | ● | ● | ● |
| v6 | 14.4 ProtectInformationWithAccessControlLists  Toda la información almacenada en los sistemas se protegerá con controles de acceso específicos del sistema de archivos , redes compartidas, reclamaciones, aplicaciones y bases de datos . Estos controles se basarán en el principio de que sólo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a ella como parte de sus responsabilidades . |  |  |  |

# *4 Políticas de contraseñas*

Esta sección contiene recomendaciones relacionadas con las políticas de contraseñas de SQLServer .

### 4.1 Asegúrese de que la opción "MUST\_CHANGE" esté activada para todos los inicios de sesión autenticados por SQL (manual)

**PerfilAplicabilidad :**

- • Nivel1-Motor de la base de datos

**Descripción:**

Siempre que se seleccione esta opción ON, SQLServer solicitará una contraseña actualizada la primera vez que se utilice el nuevo registro oral .

**Justificación:**

La imposición de un cambio de contraseña después de la creación de un nuevo registro evitará que los administradores de la cuenta o cualquier persona que acceda a contraseña inicial para el uso de la entrada SQL creada sin ser advertida .

**Impacto:**

CHECK\_EXPIRATIONy CHECK\_POLICY deben estar activadas. ON. Finalizar Los usuarios finales deben disponer de los medios (aplicación ) para cambiar la contraseña cuando se les obliga a ello .

**Auditoría:**

1. Abrir **SQLServerManagementStudio**.
2. Abrir **Explorar objetos y conectarse a la instancia de destino** .
3. Navegue hasta **Ficha de inicio de sesión** **Explorar el objeto y expandirlo** . Haga clic con el botón derecho del ratón en la página deseado y seleccione **Propiedades**.
4. Compruebe que la casilla "Debe cambiar la contraseña en el siguiente inicio de sesión" está marcada .

**Nota:** Este procedimiento de auditoría sólo es aplicable inmediatamente después de que se haya creado o modificado la entrada para el cambio de contraseña . Cuando se cambia la contraseña , se puede saber específicamente que esta opción fue el mecanismo de refuerzo para el cambio de contraseña.

**Remediación:**

Establezca la opción MUST\_CHANGE para los inicios de sesión autenticados de SQLA cuando se crea el diálogo inicialmente :

CREAR LOGIN <nombre\_de\_usuario> CON CONTRASEÑA = '<valor\_contraseña>' MUST\_CHANGE, CHECK\_EXPIRATION = ON, CHECK\_POLICY = ON;

Establezca la opción MUST\_CHANGE para los inicios de sesión autenticados de SQLA al restablecer la contraseña :

ALTER LOGIN <nombre\_de\_usuario> CON CONTRASEÑA = '<nueva\_contraseña\_valor>' MUST\_CHANGE;

**Valor por defecto :**

ON cuando se crea un nuevo acceso a través de la interfaz de usuario de SSMS . OFF cuando se crea un nuevo acceso utilizando T-SQL CREATE LOGINa menos que la opción MUST\_CHANGE se incluye explícitamente junto con CHECK\_EXPIRATION = ON.

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/t-sql/statements/alter-login-transact-sql
2. https://docs.microsoft.com/en-us/sql/t-sql/statements/create-login-transact-sql

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 4.2 ChangeDefaultPasswords  Antes de desplegar un nuevo conjunto , cambie todas las contraseñas por defecto para que los valores coincidan con las cuentas de nivel administrativo . | ● | ● | ● |
| v6 | 16 Seguimiento y control de cuentas  Seguimiento y control de cuentas |  |  |  |

#### 4.2 Asegúrese de que la opción "CHECK\_EXPIRATION" esté activada para todos los SQL

#### Logins autentificados dentro del rol de administrador del sistema (automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

Aplique la misma política de caducidad de las contraseñas utilizada en Windows Stop a las contraseñas utilizadas en el servidor SQL .

**Justificación:**

Garantizar que los inicios de sesión de SQL cumplan con la política de contraseñas seguras aplicada por Windows Server Benchmark permitirá que las contraseñas de los inicios de sesión de SQL con con privilegios de administrador del sistema se cambien con frecuencia para evitar el compromiso de un ataque de fuerza bruta . CONTROL SERVER es un permiso equivalente para sysadmin y los inicios de sesión con ese permiso también deben tener contraseñas que caduquen .

**Impacto:**

Se trata de una recomendación de mitigación para los sistemas que no pueden seguir la recomendación de utilizar únicamente los inicios de sesión autenticados de Windows .

En cuanto a la limitación de esta regla, sólo se puede iniciar sesión con sysadmin y CONTROL SERVER , hay muchos casos de aplicaciones que se ejecutan sin privilegios de administrador del sistema que tienen contraseñas codificadas con precisión o contraseñas codificadas con precisión (lo que ocurre la primera vez es casi imposible de cambiar ). Hay muchas aplicaciones empresariales que se consideran las mejores de raza que tienen este fallo .

Además, tenga en cuenta que la política de contraseñas se toma de la política local del ordenador , que se toma de la configuración de la política de dominio por defecto . Muchas organizaciones tienen una política de contraseñas diferente para las cuentas de servicio. Éstas se gestionan enADb estableciendo la contraseña de la cuenta para que no caduque y realizando algún otro proceso cuando sea necesario cambiar la contraseña . Con el control de la cuenta , esto es perfectamente aceptable desde el punto de vista de la auditoría . Si no hay un gran unSQLServidoresunacuentadeservicio , entoncestienesquehacerlomismo . Esto garantiza que el cambio de contraseña se produzca durante la ventana de tiempo de inactividad comunicada y no de forma arbitraria .

**Auditoría:**

Ejecute la siguiente sentencia T-SQL para encontrar sysadminorequivalentecon CHECK\_EXPIRATION = OFF. Tampoco se devolverán los registros .

SELECT l.[name], 'sysadmin membership' AS 'Access\_Method'

FROM sys.sql\_logins AS l

WHERE IS\_SRVROLEMEMBER('sysadmin',name) = 1

AND l.is\_expiration\_checked <> 1

UNIÓN DE TODOS

SELECT l.[name], 'CONTROL SERVER' AS 'Access\_Method'

FROM sys.sql\_logins AS l

JOIN sys.server\_permissions AS p

ON l.principal\_id = p.grantee\_principal\_id

WHERE p.type = 'CL' AND p.state IN ('G', 'W') AND l.is\_expiration\_checked <> 1;

**Remediación:**

Para cada *<nombre\_de\_usuario> encontrado por el procedimiento de auditoría* , ejecute la siguiente sentencia T-SQL :

ALTER LOGIN [<nombre\_de\_usuario>] WITH CHECK\_EXPIRATION = ON;

**Valor por defecto :**

CHECK\_EXPIRATIONes ON por defecto cuando se utiliza el SSMS para crear un inicio de sesión autenticado en SQL .

CHECK\_EXPIRATION es OFF por defecto cuando se utiliza T-SQL CREATE LOGIN sin especificar la opción CHECK\_EXPIRATION .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/relational-databases/security/passwordpolicy?view=sql-server-ver15

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 16.10 AsegurarQueTodasLasCuentasTienenFechaDeCaducidad  Garantizar que todas las cuentas tengan una fecha de caducidad que se controle y se aplique . |  | ● | ● |
| v6 | 16.2 AllAccountsHaveAMonitoredExpirationDate  Garantizar que todas las cuentas tengan una fecha de caducidad que se controle y se aplique . |  |  |  |

#### 4.3 Asegúrese de que la opción "CHECK\_POLICY" esté activada para todos los inicios de sesión autenticados de SQL (automatizados)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

Aplique la misma política de finalización de contraseña que se utiliza en Windows Stop a las contraseñas utilizadas en dentro de SQLServer .

**Justificación:**

Asegúrese de que las contraseñas de inicio de sesión autenticadas en SQL cumplan con la política de contraseñas seguras aplicada por los Puntos de Referencia de Windows Server para que no puedan ser comprometidas fácilmente mediante un ataque de fuerza bruta .

**Impacto:**

Se trata de una recomendación de mitigación para los sistemas que no pueden seguir la recomendación de utilizar únicamente los inicios de sesión autenticados de Windows .

Las contraseñas débiles pueden conducir a sistemas comprometidos . Los inicios de sesión autenticados de SQLServera utilizarán la política de contraseñas establecida en la política local del ordenador , que normalmente se establece en la política de dominio predeterminada .

Esta configuración se aplica únicamente cuando se modifica la contraseña . Esta configuración no obliga a cambiar las contraseñas débiles existentes .

**Auditoría:**

Utilice el siguiente formulario de códigos para determinar el estado de los registros SQL y si se ha impuesto su complejidad de paso .

SELECT nombre, is\_disabled

FROM sys.sql\_logins

WHERE is\_policy\_checked = 0;

El is\_policy\_checkedvalueof 0 indica que la opción CHECK\_POLICY es OFF; el valor de 1 es ON. Si valor\_desactivado es 1, este registro está desactivado y no se puede utilizar . Si no se devuelve, existe un acceso autenticado de SQLA y todos tienen CHECK\_POLICY ON.

**Remediación:**

Para cada *<nombre\_de\_usuario> encontrado por el procedimiento de auditoría* , ejecute la siguiente sentencia T-SQL :

ALTER LOGIN [<nombre\_de\_usuario>] WITH CHECK\_POLICY = ON;

**Nota:**  En el caso de AWSRDS, no realice esta corrección para la cuenta principal .

**Valor por defecto :**

CHECK\_POLICYis ON **Referencias:**

1. https://docs.microsoft.com/en-us/sql/relational-databases/security/passwordpolicy

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 4.4 UseUniquePasswords  Cuando no se admita la autenticación multifactorial (como administrador local , root o cuentas de servicio ), las cuentas utilizarán contraseñas que se ajusten a ese sistema . |  | ● | ● |
| v6 | 16 Seguimiento y control de cuentas  Seguimiento y control de cuentas |  |  |  |

## 5 Auditoría y registro

Esta sección contiene recomendaciones relacionadas con los mecanismos de registro de datos de SQLServer .

#### 5.1 Asegúrese de que el "Número máximo de archivos de registro de errores" sea mayor o igual a "12" (automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

Los archivos de registro de errores de SQLServer deben estar protegidos contra pérdidas . Los archivos de registro deben tener una copia de seguridad antes de que se reescriban . Conservar más registros de errores ayuda a evitar la pérdida de un reciclaje frecuente antes de que puedan producirse las copias de seguridad .

**Justificación:**

El registro de errores de SQLServer contiene información importante sobre eventos de servidor principal e información sobre intentos de inicio de sesión .

**Impacto:**

Cuando se alcanza el número máximo de registros de error , el archivo de registro de error más antiguo se elimina cada vez que se reinicia el servidor SQL o se ejecuta el sp\_cycle\_errorlogseejecuta .

**Auditoría:**

Realice el métodoGUI o T-SQL mostrado :

***1.1.1.7 Método GUIM***

1. Abrir **SQLServerManagementStudio**.
2. Abrir **Explorar objetos y conectarse a la instancia de destino** .
3. Navegue hasta la página web **Gestión en** **Explorador de objetos** y expanda . Haga clic con el botón derecho en el archivo **SQLServerLogsy seleccione** **Configurar**.
4. Verifique el **La casilla "Limitar el número de archivos de error antes de su reciclaje" está marcada**
5. Verifique el **El número máximo de archivos de error es superior o igual a** 12

***1.1.1.8 Método T-SQL***

Ejecutar el siguiente T-SQL . El Número de archivos de registro devueltos debe ser mayor o igual que 12.

DECLARE @NumErrorLogs int;

EXEC master.sys.xp\_instance\_regread

N'HKEY\_LOCAL\_MACHINE',

N'Software\Microsoft\MSSQLServer\MSSQLServer',

N'NumErrorLogs',

@NumErrorLogs OUTPUT;

SELECT ISNULL(@NumErrorLogs, -1) AS [NumberOfLogFiles];

**Remediación:**

Ajustar el número de registros que se han evitado . El valor por defecto de 6 puede ser insuficiente para un entorno de producción . Realice el métodoGUI o T-SQL que se muestra :

***1.1.1.9 Método GUIM***

1. Abrir **SQLServerManagementStudio**.
2. Abrir **Explorar objetos y conectarse a la instancia de destino** .
3. Navegue hasta la página web **Gestión en** **Explorar objetos y expandirlos** . Haga clic con el botón derecho en el archivo **SQLServerLogsy seleccione** **Configurar**
4. Compruebe la página web **Limitar el número de archivos de error antes de reciclarlos**
5. Configure el **El número máximo de errores de registro es superior o igual a** 12

***1.1.1.10 Método T-SQL***

Ejecute el siguiente T-SQL para cambiar el número de archivos de registro de errores , sustituya *<NúmeroSobre12> por el número de archivos de error que desee* :

EXEC master.sys.xp\_instance\_regwrite

N'HKEY\_LOCAL\_MACHINE',

N'Software\Microsoft\MSSQLServer\MSSQLServer',

N'NumErrorLogs',

REG\_DWORD, <NúmeroSuperior a 12>;

**Valor por defecto :**

6Los archivos de registro de errores de SQL Server, además del archivo de registro de errores actual, se conservan por defecto .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/scmservices-configure-sql-server-error-logs

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 6.4 Garantizar un almacenamiento adecuado de los registros  Asegúrese de que todos los sistemas que tienen registros tienen un espacio de almacenamiento adecuado para los registros generados . |  | ● | ● |
| v6 | 6.3 EnsureAuditLoggingSystemsAreNotSubjectToLoss (es decir, rotación/archivo)  Asegúrese de que todos los sistemas que tienen un espacio de almacenamiento adecuado para los registros generados de forma regular , de modo que los archivos de los registros no se llenen entre los intervalos de rotación . Los registros deben archivarse y firmarse digitalmente de forma periódica . |  |  |  |

#### 5.2 Asegúrese de que la opción de configuración del servidor "Trace Enabled" (rastreo habilitado por defecto) esté establecida en

#### "1" (Automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

La pista predeterminada proporciona un registro de auditoría de la actividad de la base de datos, incluida la creación de cuentas en creaciones de cuentas, la elevación de privilegios y la ejecución de comandos DCC .

**Justificación:**

La pista predeterminada proporciona información de auditoría valiosa sobre las actividades relacionadas con la seguridad en el servidor .

**Auditoría:**

Ejecute el siguiente comando T-SQL :

SELECCIONE el nombre,

CAST(valor como int) como valor\_configurado,

CAST(valor\_en\_uso como int) como valor\_en\_uso

FROM sys.configurations

WHERE name = 'default trace enabled';

Las dos columnas de valoración deben mostrar 1.

**Remediación:**

Ejecute el siguiente comando T-SQL :

EXECUTE sp\_configure 'show advanced options', 1;

RECONFIGURAR;

EXECUTE sp\_configure 'default trace enabled', 1;

RECONFIGURAR;

IR A

EXECUTE sp\_configure 'show advanced options', 0; RECONFIGURE;

**Valor por defecto :**

1 (on)

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configurewindows/default-trace-enabled-server-configuration-option

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 6.2 Activar el registro de auditoría  Asegúrese de que el registro de la ubicación se ha activado en todos los sistemas y dispositivos de red . | ● | ● | ● |
| v7 | 6.3 EnableDetailedLogging  Permite que el registro del sistema incluya información detallada como la fuente de los eventos , la fecha, el usuario, la marca de tiempo, las direcciones de origen , las direcciones de destino y otros elementos de uso . |  | ● | ● |
| v6 | 6.2 EnsureAuditLogSettingsSupportAppropriateLogEntry Formato  Validar la configuración de los registros de auditoría para cada dispositivo de red dura y el software instalado en él , asegurándose de que los registros incluyan la fecha , la marca de tiempo, las direcciones de origen , las direcciones de destino y otros elementos de uso para cada paquete o transacción . Los sistemas deben registrar los registros en un formato estandarizado, como los registros de los eventos comunes . Si los sistemas no pueden generar registros en un formato estandarizado , se pueden utilizar herramientas de normalización para convertir los registros en dicho formato . |  |  |  |

#### 5.3 Asegúrese de que la "Auditoría de inicio de sesión" esté configurada como "inicios de sesión fallidos" (automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

Este ajuste registrará los intentos de autenticación fallidos para el inicio de sesión de SQLServer en el **SQLServerErrorlog**. Esta es la configuración por defecto para SQLServer .

Históricamente, esta configuración ha estado disponible en todas las versiones y ediciones de SQLServer . Antes de la disponibilidad de **SQLServerAudit**, este era el único mecanismo proporcionado para capturar los inicios de sesión (exitosos o fallidos ).

**Justificación:**

La captura de inicios de sesión fallidos proporciona información clave que puede utilizarse para detectar ataques de adivinación de contraseñas . La captura de los intentos de inicio de sesión exitosos puede utilizarse para confirmar el acceso al servidor durante las investigaciones forenses , pero el uso de esta configuración de nivel de riesgo para la captura de los inicios de sesión exitosos crea un ruido excesivo en el **SQLServerErrorlog,quepuedeconvertirseenunDBAqueintenta resolver problemas**. En otra parte de la comparativa , se recomienda utilizar la nueva función de auditoría de SQLServer, más ligera, para capturar tanto los inicios de sesión exitosos como los fallidos .

**Impacto:**

Como mínimo , queremos asegurarnos de que los inicios de sesión fallidos sean capturados para detectar si un adversario está tratando de robar contraseñas o de otra manera de acceder a un servidor SQL correctamente .

El cambio de la configuración requiere el restablecimiento del servicio SQLServers.

**Auditoría:**

EXEC xp\_loginconfig 'nivel de auditoría';

A valor\_de\_configuración fracaso indica que el servidor de auditoría está configurado en **Failedlogly**. Si un valor\_de\_configuración\_de todos aparece, se registran tanto los inicios de sesión fallidos como los exitosos . Ambas configuraciones deberían considerarse válidas , pero la captura de los inicios de sesión correctos mediante este método crea mucho ruido en el registro de errores de **SQLServerErrorlog**.

**Remediación:**

Realice cualquiera de los dos métodos el métodoGUIoT-SQL mostrado :

***1.1.1.11 Método GU***

1. Abrir **SQLServerManagementStudio**.
2. Haga clic con el botón derecho del ratón en la instancia de destino y seleccione **Propiedades y navegue hasta** **Ficha de seguridad** .
3. Seleccione la opción **Fracaso en el registro en** **LoginAuditing** y haga clic en **ACEPTAR**.
4. Reinicie la instancia del servidor SQL .

***1.1.1.12 Método T-SQL***

1. Corre:

EXEC xp\_instance\_regwrite N'HKEY\_LOCAL\_MACHINE',

N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG\_DWORD, 2

1. Reinicie la instancia del servidor SQL .

**Valor por defecto :**

Por defecto , sólo se capturan los intentos de acceso fallidos .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configurewindows/server-properties-security-page

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 16.13 AlertonAccountLoginBehaviorDeviation  Alerta cuando los usuarios se desvían del comportamiento habitual de inicio de sesión , como la hora del día , la ubicación del puesto de trabajo y la duración . |  |  | ● |
| v6 | 16.10 PerfilUserAccountUsageAndMonitorForAnomalies  Perfilar el uso de la cuenta típica de los usuarios determinando el horario de acceso y la duración de acceso normales . Deben generarse informes que indiquen los usuarios que se han conectado durante horas inusuales o que han superado su duración normal de conexión . Esto incluye |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
|  | marcar el uso de las credenciales del usuario desde un ordenador distinto al que trabaja generalmente . |  |  |  |

#### 5.4 Asegúrese de que la "Auditoría del Servidor SQL" está configurada para capturar tanto los "inicios de sesión fallidos" como los "exitosos" (Automatizado)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

SQLServerAuditis es capaz de capturar tanto los inicios de sesión fallidos como los exitosos y escribirlos en tres lugares : el registro de eventos de la aplicación , el registro de eventos de seguridad o el sistema de archivos . Lo utilizaremos para capturar cualquier intento de inicio de sesión en SQLServer , así como cualquier intento de cambiar la política de auditoría . Esto también servirá como segunda fuente para registrar los intentos de inicio de sesión fallidos .

**Justificación:**

Al utilizar Auditoría en lugar de la configuración tradicional en la pestaña Seguridad para capturar los registros exitosos , se redujo el ruido en el ERRORLOG. Esto lo mantiene más pequeño y más fácil de leer para los administradores de bases de datos que intentan resolver problemas con el servidor SQL . Además, el objeto Auditoría puede escribir en el registro de eventos de seguridad , aunque esto requiere una configuración del sistema operativo . Esto ofrece una opción adicional para almacenar los eventos de inicio de sesión , especialmente en conjunción con un SIEM .

**Impacto:**

Con la recomendación anterior , sólo se capturan los inicios de sesión fallidos . Si el objeto de auditoría no se implementa con la configuración adecuada , SQLServer no capturará los inicios de sesión correctos , lo que podría resultar útil para los forenses .

**Auditoría:**

SELECCIONE

S.name AS 'Nombre de la auditoría'

, CASE S.is\_state\_enabled

CUANDO 1 ENTONCES 'Y'

WHEN 0 THEN 'N' END AS 'Audit Enabled'

, S.type\_desc AS 'Write Location'

SA.name AS 'Nombre de la especificación de auditoría'

CASE SA.is\_state\_enabled

CUANDO 1 ENTONCES 'Y'

WHEN 0 THEN 'N' END AS 'Especificación de auditoría habilitada'

, SAD.audit\_action\_name

, SAD.audited\_result

FROM sys.server\_audit\_specification\_details AS SAD

JOIN sys.server\_audit\_specifications AS SA

ON SAD.server\_specification\_id = SA.server\_specification\_id

JOIN sys.server\_audits AS S

ON SA.audit\_guid = S.audit\_guid

WHERE SAD.audit\_action\_id IN ('CNAU', 'LGFL', 'LGSD');

El conjunto de resultados debe contener 3 filas , una antes de cada una de las siguientes nombres\_de\_acción\_de\_auditoría:

- •

GRUPO\_DE\_CAMBIO\_DE\_AUDITORÍA

- •

FAILED\_LOGIN\_GROUP - •

GRUPO\_DE\_INGRESO\_CON ÉXITO

Tanto la especificación de Auditoría como la de Auditoría deben estar habilitadas y resultados\_de\_auditoría\_deben incluir tanto el éxito como el fracaso .

**Remediación:**

Realice el métodoGUI o T-SQL mostrado :

***1.1.1.13 Método GUIM***

1. Ampliar la página web **SQLServer en** **ObjectExplorer**.
2. Amplíe la página web **Carpeta de seguridad**
3. Haga clic con el botón derecho en la carpeta **Auditorías y elija** **NuevaAuditoría ...**
4. Especifique un nombre para el **Auditoría del servidor**.
5. Especifique los detalles del destino de la auditoría y haga clic en **OKpara guardar el** **Auditoría del servidor**.
6. Haga clic con el botón derecho del ratón en **ServerAuditSpecificationsy elija** **NuevaEspecificaciónDeAuditoríaDelServidor ...**
7. Nombre del **ServerAuditSpecification**
8. Seleccione la página web recién creada **Auditoría del servidor en el sitio web** **Auditoría en el menú desplegable** .
9. Haga clic en el menú desplegable de **Tipo de acción de auditoría y seleccione** GRUPO\_DE\_CAMBIO\_DE\_AUDITORÍA.
10. Haga clic en el nuevo menú desplegable **AuditActionTypey seleccione** FAILED\_LOGIN\_GROUP.
11. Haga clic en el nuevo menú desplegable bajo **AuditActionType y seleccione** GRUPO\_DE\_INGRESO\_CON ÉXITO.
12. Haga clic en Aceptar para guardar la **Especificación de Auditoría del Servidor**.
13. Haga clic con el botón derecho del ratón en el nuevo **ServerAuditSpecification y seleccione** **HabilitarEspecificaciónDeAuditoríaDelServidor**.
14. Haga clic con el botón derecho del ratón en el nuevo **ServerAudit y seleccione** **HabilitarAuditoríaDelServidor**.

***1.1.1.14 Método T-SQL***

Ejecutar códigos similares :

CREAR AUDIT DEL SERVIDOR TrackLogins

A APPLICATION\_LOG;

IR A

CREAR ESPECIFICACIÓN DE AUDITORÍA DEL SERVIDOR TrackAllLogins

PARA LA AUDITORÍA DEL SERVIDOR TrackLogins

ADD (FAILED\_LOGIN\_GROUP),

ADD (SUCCESSFUL\_LOGIN\_GROUP),

ADD (AUDIT\_CHANGE\_GROUP)

CON (ESTADO = ON);

IR A

ALTER SERVER AUDIT TrackLogins

CON (ESTADO = ON);

IR A

**Nota:**  Si el destino escrito para el objeto de auditoría es el registro de eventos de seguridad , consulte el tema Libros en línea WriteSQLServerAuditEventos en el registro de seguridad y siga los pasos adecuados .

**Valor por defecto :**

Por defecto , no hay eventos de registro de seguimiento de objetos de auditoría .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/relationaldatabases/security/auditing/create-a-server-audit-and-server-audit-specification

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 4.9 LogandAlertonInsuficienteAdministración CuentaInicio de sesión  Configure los sistemas para que emitan un mensaje de entrada tras un inicio de sesión exitoso en una cuenta administrativa . |  | ● | ● |
| v6 | 5.5 LogFailedAdministrativeLoginAttempts  Configure los sistemas para que emitan un mensaje de alarma cuando no se haya iniciado la sesión en una cuenta administrativa . |  |  |  |

## 6 Desarrollo de aplicaciones

Esta sección contiene recomendaciones relacionadas con el desarrollo de aplicaciones que interactúan con SQLServer .

#### 6.1 Asegurarse de que la entrada de usuarios de la base de datos y de la aplicación está desinfectada (manual)

**PerfilAplicabilidad :**

- • Nivel1-Motor de la base de datos

**Descripción:**

Valide siempre las entradas de usuario recibidas del cliente de la base de datos o de la aplicación comprobando el tipo , la longitud, el formato y el rango antes de transmitirlas al servidor de la base de datos .

**Justificación:**

La desinfección de las entradas de los usuarios minimiza drásticamente el riesgo de inyección SQL .

**Impacto:**

La limpieza de la entrada del usuario puede requerir cambios en el código de la aplicación y en la sintaxis de los objetos de la base de datos . Estos cambios pueden requerir que las aplicaciones y las bases de datos se desvíen temporalmente de la línea . Cualquier cambio en el código TSQL o en el código de la aplicación debe probarse a fondo en un entorno de pruebas antes de la implementación de la producción .

**Auditoría:**

Compruebe con los equipos de aplicación que la interacción con la base de datos se realiza mediante el uso de procedimientos almacenados y no de SQL dinámico . Revocar cualquier INSERT, UPDATE o DELETE para que las modificaciones de los datos se realicen mediante procedimientos almacenados . Compruebe que no hay ninguna consulta SQL en el código de la aplicación producida por la concatenación de cadenas .

**Remediación:**

Los siguientes pasos pueden ser tomados para remediar la inyección SQL de inyección SQL:

* RevisiónTSQLy código de aplicación paraSQLInjection
* Sólo se permite a las cuentas con privilegios mínimos enviar datos de usuario al servidor
* Minimizar el riesgo de ataque de inyección SQL utilizando comandos parametrizados y procedimientos almacenados
* Rechazar la entrada del usuario que contenga datos binarios , secuencias de escape y caracteres de comentario
* Valide siempre las entradas de los usuarios y no las utilice directamente para crear declaraciones SQL

**Referencias:**

1. https://owasp.org/www-community/attacks/SQL\_Injection

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 18.2 Garantizar la comprobación explícita de errores para todo el software desarrollado por la empresa  En el caso de los programas informáticos desarrollados dentro de la empresa , asegúrese de que se realiza una comprobación de errores explícita y se documenta para todas las entradas , incluyendo el tamaño , el tipo de datos y los cambios o formatos aceptados . |  | ● | ● |
| v6 | 18.3 SanitizeInputForIn-houseSoftware  En el caso de los programas informáticos desarrollados dentro de la empresa , asegúrese de que se realiza una comprobación de errores explícita y se documenta para todas las entradas , incluyendo el tamaño , el tipo de datos y los cambios o formatos aceptados . |  |  |  |

#### 6.2 Asegúrese de que el "Conjunto de permisos del ensamblaje de CLR" esté establecido en "SAFE\_ACCESS" para todos

#### Montajes CLR (automatizados)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

La configuración de los permisos de ensamblaje de CLRA en SAFE\_ACCESS impedirá que los ensamblajes accedan a recursos externos del sistema, como archivos , la red, variables de entorno o el registro .

**Justificación:**

Conjuntos con ACCESO\_EXTERNO o UNSAFEpermissionsets pueden utilizarse para acceder a áreas sensibles del sistema operativo , robar y/o transmitir datos y alterar el estado y otras medidas de protección del sistema operativo Windows subyacente .

Los ensamblados creados por Microsoft (is\_user\_defined = 0) se excluyen de esta comprobación, ya que son necesarios para el funcionamiento general del sistema .

**Impacto:**

Las medidas de mediación deben probarse primero con el entorno más moderno antes de la producción para asegurarse de que el conjunto sigue funcionando tal y como se ha diseñado con SAFEpermissionsetting.

**Auditoría:**

Ejecute la siguiente sentencia SQL :

USE <nombre de la base de datos>;

IR A

SELECCIONE el nombre,

permission\_set\_desc FROM sys.assemblies

WHERE is\_user\_defined = 1;

Todos los conjuntos girados deben mostrar SAFE\_ACCESS en la columna permission\_set\_desccolumna .

**Remediación:**

USE <nombre de la base de datos>;

IR A

ALTER ASSEMBLY <nombre\_de\_ensamblaje> CON PERMISSION\_SET = SAFE;

**Valor por defecto :**

El permiso SAFE se establece por defecto .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/relational-databases/clrintegration/security/clr-integration-code-access-security
2. https://docs.microsoft.com/en-us/sql/relational-databases/system-catalogviews/sys-assemblies-transact-sql
3. https://docs.microsoft.com/en-us/sql/t-sql/statements/alter-assembly-transactsql

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 5.1 EstablecerConfiguracionesSeguras  Mantener documentados los estándares de configuración de seguridad para todos los sistemas y programas operativos autorizados . | ● | ● | ● |
| v6 | 18 AplicaciónSoftwareSeguridad  AplicaciónSoftwareSeguridad |  |  |  |

## 7 Cifrado

Estas recomendaciones se refieren a los aspectos relacionados con el cifrado de SQL Server .

#### 7.1 Asegúrese de que el "Algoritmo de cifrado de clave simétrica" esté configurado como "AES\_128" o superior en las bases de datos que no sean del sistema (automatizadas)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

Según las Mejores Prácticas de Microsoft , sólo las opciones del algoritmo AES de SQLServer , AES\_128, AES\_192, y AES\_256, deben utilizarse como algoritmo de cifrado de clave simétrica .

**Justificación:**

Los siguientes algoritmos (referidos por SQLServer ) se consideran débiles y obsoletos y no deberían seguir utilizándose en SQLServer : DES, DESX, RC2, RC4, RC4\_128.

Muchas organizaciones pueden aceptar los algoritmos TripleDES (TDEA) que utilizan las opciones de codificación 1 (3keyaka 3TDEA) o la opción de cifrado2( 2claves 2TDEA). EnSQLServer , estos se denominan TRIPLE\_DES\_3KEYy TRIPLE\_DESrespectivamente . Además, el algoritmo deSQLServer denominadoDESX es en realidad la misma implementación que el TRIPLE\_DES\_3KEY . Sin embargo, el uso del identificador DESX como tipo de algoritmo ha quedado obsoleto y ahora se desaconseja su uso .

**Impacto:**

Elimina el uso de algoritmos débiles y obsoletos que pueden poner el sistema en riesgo de que un atacante rompa la clave .

Los datos cifrados no pueden comprimirse , pero los datos comprimidos pueden cifrarse . Si utiliza la compresión , debe comprimir los datos antes de cifrarlos .

**Auditoría:**

Ejecute el siguiente código antes de cada base de datos de usuarios individuales :

USE <nombre de la base de datos>

IR A

SELECT db\_name() AS Database\_Name, name AS Key\_Name

FROM sys.symmetric\_keys

WHERE algorithm\_desc NOT IN ('AES\_128','AES\_192','AES\_256')

AND db\_id() > 4; GO

Para su cumplimiento , tampoco se deben devolver los votos .

**Remediación:**

Consulte la entrada de la clave de acceso de Microsoft SQL ServerBooksOnlineALTERSYMMETRIC : https://docs.microsoft.com/en-us/sql/t-sql/statements/alter-symmetric-key-transact-sql

**Valor por defecto :**

ninguno

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/t-sql/statements/alter-symmetric-keytransact-sql
2. http://support.microsoft.com/kb/2162020

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 14.4 EncryptAllSensitiveInformationinTransit  Cifrar la información sensible en tránsito . |  | ● | ● |
| v6 | 14.2 EncryptAllSensitiveInformationOverLess-trusted  Redes  Toda comunicación de información sensible a través de redes no confiables debe ser encriptada . Siempre que la información fluya a través de una red con un nivel de confianza bajo , la información debe estar cifrada . |  |  |  |

#### 7.2 Asegúrese de que el tamaño de la clave asimétrica esté configurado como "mayor o igual a 2048" en las bases de datos no pertenecientes al sistema (automatizadas)

**PerfilAplicabilidad :**

* Nivel1-Motor de la base de datos
* Nivel1-AWSRDS

**Descripción:**

Las mejores prácticas de Microsoft recomiendan utilizar un algoritmo de cifrado de 2048 bits para las claves asimétricas .

**Justificación:**

El El algoritmo de cifrado RSA\_2048 para las claves asimétricas en el servidor SQL es el nivel más alto que se ofrece y, por lo tanto, la opción más segura disponible (las otras opciones son RSA\_512 y RSA\_1024).

**Impacto:**

El nivel de bits más alto puede dar lugar a un menor rendimiento , pero reduce la probabilidad de que un atacante rompa la llave .

Los datos cifrados no pueden comprimirse , pero los datos comprimidos pueden cifrarse . Si utiliza la compresión , debe comprimir los datos antes de cifrarlos .

**Auditoría:**

Ejecute el siguiente código antes de cada base de datos de usuarios individuales :

USE <nombre de la base de datos>

IR A

SELECT db\_name() AS Database\_Name, name AS Key\_Name

FROM sys.asymmetric\_keys

WHERE longitud\_de\_clave < 2048

AND db\_id() > 4; GO

Para su cumplimiento , tampoco se deben devolver los votos .

**Remediación:**

Consulte la entrada de la clave de acceso de Microsoft SQL ServerBooksOnlineALTERASYMMETRIC : https://docs.microsoft.com/en-us/sql/t-sql/statements/alter-asymmetric-key-transactsql

**Valor por defecto :**

Ninguno

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/t-sql/statements/alter-asymmetric-keytransact-sql
2. http://support.microsoft.com/kb/2162020

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 14.4 EncryptAllSensitiveInformationinTransit  Cifrar la información sensible en tránsito . |  | ● | ● |
| v6 | 14.2 EncryptAllSensitiveInformationOverLess-trusted  Redes  Toda comunicación de información sensible a través de redes no confiables debe ser encriptada . Siempre que la información fluya a través de una red con un nivel de confianza bajo , la información debe estar cifrada . |  |  |  |

## 8 Apéndice: Consideraciones adicionales

En este apéndice se discuten posibles opciones de configuración para las que no se ofrece ninguna recomendación .

#### 8.1 Asegúrese de que el "Servicio de navegador de SQL Server" está configurado correctamente (Manual)

**PerfilAplicabilidad :**

- • Nivel1-Motor de la base de datos

**Descripción:**

Tampoco se recomienda desactivar el servicio de navegación del servidor SQL .

**Justificación:**

En el caso de la instalación de una instancia por defecto , el servicio de navegación de SQLServer está deshabilitado por defecto . A menos que haya una instancia con nombre en el mismo servidor , normalmente no hay razón para que se ejecute el servicio de navegación de SQLServer . En este caso, se recomienda encarecidamente que el servicio de navegación de SQLServer permanezca deshabilitado .

Cuando se trata de estos casos , dado que como seguridad se puede hacer un seguimiento de la lista del servidor SQL en cualquier puerto , es de beneficio limitado deshabilitar el servicio del navegador del servidor SQL .

Sin embargo, si todas las conexiones a la instancia nombrada son a través de aplicaciones y no son visibles para los usuarios , la configuración de la instancia nombrada para escuchar en el puerto estático , la desactivación del servicio de navegador de SQL Server y la configuración de la aplicación para conectarse a los puertos especificados deben ser la dirección tomada . Esto sigue la práctica general de reducir el área de la superficie , especialmente para una función no necesaria .

Por otra parte , si los usuarios finales se conectan directamente a las bases de datos de la instancia , lo normal es que utilicen *NombreServidorNombreInstancia es lo mejor* . Para ello, es necesario que el servicio SQLServerBrowsers esté en funcionamiento . Desactivar el servicio de navegación de SQLServer significaría que los usuarios finales tendrían que recordar los números de puerto de las instancias . Cuando no lo hagan, se generarán llamadas de servicio al personal de TI . Dada la limitada ventaja de desactivar el servicio , probablemente no merezca la pena el cambio , por lo que es más rentable tener el servicio de navegador de SQL Server activado .

**Auditoría:**

Compruebe el estado de SQL Browser Service mediante services.mscorsimilarmethods .

**Remediación:**

Habilite el servicio según sea necesario para su entorno .

**Valor por defecto :**

El servicio de navegación de SQLServer se desactiva si sólo se instala una instancia por defecto en el servidor . Si se instala una instancia con nombre Si se instala una instancia con nombre, el valor predeterminado es que el servicio de navegador SQLServer se configure como automático para el inicio .

**Referencias:**

1. https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/sqlserver-browser-service-database-engine-and-ssas

**CISControls :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ControlesVersión** | **Controlar** | **IG1** | **IG2** | **IG3** |
| v7 | 9.2 Asegúrese de que sólo se ejecuten los puertos , protocolos y servicios aprobados se ejecutan en  Asegúrese de que todos los puertos de red , protocolos y servicios de un sistema con necesidades empresariales validadas estén funcionando en cada sistema . |  | ● | ● |
| v6 | 9.1 Limitar los puertos , protocolos y servicios abiertos  Asegúrese de que todos los puertos , protocolos y servicios con necesidades empresariales validadas se ejecutan en cada sistema . |  |  |  |

# Apéndice: Tabla de recomendaciones

|  |  |  |  |
| --- | --- | --- | --- |
| **Controlar** | | **SetCorrectly** | |
| Sí | No |
| **1** | **Instalación, actualizaciones y parches** | | |
| 1.1 | Asegúrese de que se han instalado las últimas actualizaciones acumulativas y de seguridad de SQL Server (manual) | o | o |
| 1.2 | Garantizar el uso de servidores de una sola función (manual) | o | o |
| **2** | **Reducción de la superficie** | | |
| 2.1 | Asegúrese de que la opción de configuración del servidor " AdHocDistributedQueries " sea "0" (automatizada) | o | o |
| 2.2 | Asegúrese de que la opción de configuración del servidor " CLREnabled" sea "0" (automatizada) | o | o |
| 2.3 | Asegúrese de que la opción de configuración del servidor ' CrossDBOwnershipChaining' sea '0' (automatizada) | o | o |
| 2.4 | Asegúrese de que la opción de configuración del servidor de 'DatabaseMailXPs ' sea '0' (automatizada) | o | o |
| 2.5 | Asegúrese de que la opción de configuración del servidor de OleAutomationProcedures sea '0' (automatizada) | o | o |
| 2.6 | Asegúrese de que la opción de configuración del servidor de acceso remoto sea '0' (automatizada) | o | o |
| 2.7 | Asegúrese de que 'RemoteAdminConnections ' ServerConfigurationOptionissetto '0' (Automated) | o | o |
| 2.8 | Asegúrese de que 'ScanForStartupProcs ' ServerConfigurationOptionissetto '0' (Automated) | o | o |
| 2.9 | Asegurar 'la'confianza'en' la'base'de'datos'en 'off' (automatizada) | o | o |
| 2.10 | Asegúrese de que los protocolos del servidor SQL innecesarios estén desactivados (manualmente) | o | o |
| 2.11 | Asegúrese de que el servidor SQL está configurado en varios puertos estándar (automatizados) | o | o |
| 2.12 | Asegúrese de que la opción 'HideInstance ' esté en 'Yes' para las instancias del servidor SQL de producción (automatizado) | o | o |
| 2.13 | Asegúrese de que su cuenta de inicio de sesión esté deshabilitada (automatizada) | o | o |
| 2.14 | Asegúrese de que la cuenta de inicio de sesión de 'sa' ha sido renombrada (Automated) | o | o |
| 2.15 | Asegúrese de que 'AUTO\_CLOSE' esté 'OFF' en las bases de datos contenidas (Automated) | o | o |

|  |  |  |  |
| --- | --- | --- | --- |
| 2.16 | Asegúrese de que la línea de productos existe con el nombre "sa" (automatizado) | o | o |
| 2.17 | Asegúrese de que la opción de configuración del servidor de "seguridad de las cadenas" sea "1" (automatizada). | o | o |
| **3** | **Autenticación y autorización** | | |
| 3.1 | Asegúrese de que la propiedad 'ServerAuthentication ' se ajusta al 'WindowsAuthenticationMode ' (Automated) | o | o |
| 3.2 | Asegúrese de que se revocan los permisos de conexión del usuario "invitado" en todas las bases de datos del servidor SQL, excluyendo la base de datos maestra , la base de datos del sistema de gestión de datos (automatizada). | o | o |
| 3.3 | Asegúrese de que los " usuarios huérfanos" sean eliminados de las bases de datos del servidor SQL (automatizado) | o | o |
| 3.4 | Asegúrese de que no se utiliza la autenticación SQL en las bases de datos contenidas (automatizada) | o | o |
| 3.5 | Asegúrese de que la cuenta de servicio MSSQL del servidor no sea un administrador (manual) | o | o |
| 3.6 | Asegúrese de que la cuenta de servicio SQLAgent del servidor no es un administrador (manual) | o | o |
| 3.7 | Asegúrese de que la cuenta de servicio de texto completo del servidor SQL no sea un administrador (manual) | o | o |
| 3.8 | Asegúrese de que sólo se conceden los permisos especificados por Microsoft para la función de servidor público (automatizado) | o | o |
| 3.9 | Asegúrese de que los grupos de WindowsBUILTIN no sean SQLLogins (automatizados) | o | o |
| 3.10 | Asegurarse de que los grupos locales de las ventanas no sean SQLLogins (automatizado) | o | o |
| 3.11 | Asegúrese de que el rol público en la base de datos deemsdb no tenga acceso a los proxies deSQLAgent (automatizado) | o | o |
| **4** | **Políticas de contraseñas** | | |
| 4.1 | Asegúrese de que la opción "MUST\_CHANGE" esté activada para todos los inicios de sesión autenticados de SQL (manual) | o | o |
| 4.2 | Asegúrese de que la opción' CHECK\_EXPIRATION' esté 'activada' para'todos  SQLAuthenticatedLoginsWithintheSysadminRole  (Automatizado) | o | o |
| 4.3 | Asegúrese de que la opción "CHECK\_POLICY" esté activada para todos los inicios de sesión autenticados de SQL (automatizados) | o | o |
| **5** | **Auditoría y registro** | | |
| 5.1 | Asegúrese de que el "Número máximo de archivos de error " sea superior o igual a "12" (automatizado). | o | o |
| 5.2 | Asegúrese de que la opción de configuración del servidor ' DefaultTraceEnabled' sea '1' (automatizada) | o | o |
| 5.3 | Asegúrese de que "LoginAuditing " esté en "failedlogins " (automatizado) | o | o |
| 5.4 | Asegúrese de que 'SQLServerAudit ' capture tanto los inicios de sesión fallidos como los exitosos (automatizados) | o | o |
| **6** | **Desarrollo de aplicaciones** | | |
| 6.1 | Garantizar la limpieza de la base de datos y de la aplicación (manual) | o | o |
| 6.2 | Asegúrese de que 'CLRAssemblyPermissionSet ' esté en  SAFE\_ACCESS' forAllCLRAssemblies (Automated) | o | o |
| **7** | **Codificación** |  |  |
| 7.1 | Asegúrese de que el algoritmo de cifrado de clave simétrica esté establecido en  AES\_128 o superior en las bases de datos del sistema (automatizado) | o | o |
| 7.2 | Garantizar que el tamaño de la clave asimétrica sea "mayor que 2048 " en las bases de datos del sistema (automatizadas) | o | o |
| **8** | **Apéndice: Consideraciones adicionales** |  |  |
| 8.1 | Asegúrese de que 'SQLServerBrowserService ' está configurado correctamente (Manual) | o | o |

# Apéndice: Historia de los cambios

|  |  |  |
| --- | --- | --- |
| Fecha | Versión | Cambios para esta versión |
| Nov27 , 2019 | 1.0.0 | Lanzamiento inicial |
| 15 de mayo de 2020 | 1.1.0 | El texto de las Declaraciones Justificativas debe ser de dos frases (Ticket 10655 ) |
| 19 de mayo de 2020 | 1.1.0 | La palabra "como" falta en una frase (Ticket 10664 ) |
| 19 de mayo de 2020 | 1.1.0 | Timo menor- la palabra "tiene" debería ser "tiene" (Ticket10672 ) |
| 19 de mayo de 2020 | 1.1.0 | Varios cambios en el texto de la declaración de impacto para mejorar la legibilidad (billete 10673 ) |
| 19 de mayo de 2020 | 1.1.0 | OWAS ha cambiado la URL en las referencias (Ticket 10678 ) |
| 21 de mayo de 2020 | 1.1.0 | A partir de SQLServer2017 , sólo se actualiza la unidad de control y la seguridad (billete 10631 ) |
| 30 de junio de 2020 | 1.1.0 | BugFixRelease |
| 10 de septiembre de 2020 | 1.2.0 | MSSQL2019Depreciación de  "xp\_cmdshell " disabledvalidation  (Ticket11171 ) |
| Mar2 , 2021 | 1.2.0 | Error con control7 .2Asegurarse de que  AsymmetricKeySize (Ticket12352 ) |
| Mar2 , 2021 | 1.2.0 | la base de datos normal puede seguir viendo la cuenta denominada "sa" (billete 10660 ) |
| 8 de abril de 2021 | 1.2.0 | La consulta utilizada para el CIS-CAT no funciona cuando se configuran los puertos dinámicos . (Ticket11918 ) |
| 12 de abril de 2021 | 1.2.0 | NuevaRecomendación : Asegurar 'CLR  StrictSecurity ' ServerConfiguration  Opción "0" (Ticket10840 ) |
| 12 de abril de 2021 | 1.2.0 | Error en la declaración de impacto debido a cambios en el servidor SQL - noSAFEassemblyoption (Ticket10656 ) |
| 12 de abril de 2021 | 1.2.0 | CISSQLL1Check6 .2 no comprueba todas las instancias de la base de datos (Ticket 12681 ) |