Best Practices and Recommendations

Security Guidelines

Sage 200

Sage Murano

Sage Despachos Connected

Sage

Buenas prácticas en materia de **Seguridad**

La seguridad es un aspecto fundamental en el diseño y desarrollo de nuestras soluciones. Nuestros productos Sage Murano, Sage 200 y Sage Despachos Connected son constantemente revisados, utilizando distintas herramientas de seguridad para comprobar nuestro código. Adicionalmente contamos con análisis de seguridad por parte de empresas independientes.

Es esencial seguir las directrices y recomendaciones de seguridad aplicables a los distintos productos y sistemas involucrados, ya que en ocasiones las políticas de seguridad son vulnerables a través del eslabón más débil de la cadena. Este documento proporciona recomendaciones para la instalación y configuración de Sage Murano, Sage 200 y Sage Despachos Connected.

Tabla de Contenidos

Directrices generales de seguridad

Garantizar la seguridad de la infraestructura local de las aplicaciones es esencial.

Datos de clientes, información financiera, asientos contables… vas a terminar almacenando ésta y otra información sensible utilizando nuestros productos de gestión. Esta información puede almacenarse en tus servidores si utilizas una solución on-premise, o bien fuera de la infraestructura de tu empresa en el caso de utilizar nuestras versiones en la nube. Recuerda que siempre obtendrás una mayor Seguridad, de una manera más sencilla, si optas por alguna de nuestras versiones en la nube.

Tendrás un mayor nivel de seguridad sin ningún esfuerzo adicional por tu parte si decides utilizar ”Sage 200 cloud”, “Sage Despachos en la nube” o nuestras versiones del programa Partner Cloud. Sin embargo, si decides continuar utilizando alguna de las versiones locales de estos productos o incluso si alojas estos productos por medio de algún proveedor de almacenamiento no recomendado por Sage, estas recomendaciones de seguridad te resultarán de utilidad.

Independientemente de donde hayas decidido finalmente alojar los datos gestionados por el programa, es importante adoptar un enfoque de seguridad a varios niveles alineado con los distintos estándares de la industria en este sentido, de forma que los datos permanezcan siempre con el mayor nivel de seguridad posible. Este documento cubre muchos de los controles que deberán implementarse para asegurar sus datos.

Recomendaciones generales

Sage recomienda seguir las siguientes pautas para garantizar la seguridad de su propia instalación de Sage Murano, Sage 200 y Sage Despachos Connected.

Mantén tus sistemas siempre actualizados.

Asegúrate de instalar siempre las últimas actualizaciones del software y del sistema operativo, de modo que siempre utilices las últimas versiones compatibles de Microsoft Windows. Este aspecto es igualmente aplicable a nuestros productos: por favor, instala siempre las últimas actualizaciones de Sage Murano, Sage 200 y Sage Despachos Connected. Nuestras actualizaciones de producto suelen incluir mejoras en la seguridad, el rendimiento y la funcionalidad.

Seguridad en la base de datos

Utiliza identificadores de usuario únicos en Microsoft SQL Server

De acuerdo con el Principio de Mínimo Privilegio, debes asegurarte de que cada una de las bases de datos de Sage Murano, Sage 200 o Sage Despachos Connected (en caso de tener más de una) estén configuradas de modo que utilicen un identificador único de inicio de sesión cada una de ellas, de forma que cada uno de ellos sólo sirva para acceder a una de las bases de datos, pero no al resto. Otra forma de cumplir con este principio, en caso de que tengas más de una base de datos por cualquier motivo, es separarlas en servidores o instancias diferentes, de forma que, una vez más, cada inicio de sesión sólo de acceso a una de ellas.

Asegura el servidor otorgando al usuario de base de datos el nivel de permiso adecuado.

Es altamente recomendable evitar que el usuario de la base de datos ("logic") esté configurado como System Administrator (sa). En su lugar, configura simplemente esta cuenta de usuario en la base de datos como db_owner.

Configura la base de datos para que todas las conexiones hacia ella sean encriptadas.

Debes activar el protocolo TLS y configurarlo utilizando un certificado válido para la conexión con la base de datos, de manera que se pueda garantizar la seguridad y la integridad de los datos durante su envío entre el programa y la base de datos.

Para obtener más información a este respecto, puedes consultar el artículo "Configuración de las opciones de cifrado en SQL Server" para asegurarte de configurar de manera segura la conexión con la base de datos.

Como medida de seguridad adicional, y dependiendo de la versión de SQL Server que estés utilizando, puedes activar también el protocolo de flujo TDS (Tabular Data Stream) y utilizarlo junto con los protocolos TLS 1.2 y/o TLS 1.3 ("Compatibilidad con TDS 8.0 y TLS 1.3").

Restringe el acceso al servidor de base de datos a través de la red.

Además de todas las medidas de seguridad comentadas hasta ahora, Sage recomienda también hacer que Sage Murano, Sage 200 o Sage Despachos Connected funcionen en una VLAN separada del resto, o bien implementar un control de acceso a la red estricto (Network Access Control, NAC) mediante "MAC pinning" (puedes configurarlo en Microsoft Windows de forma que sólo se permita el tráfico de ciertas direcciones MAC con otros dispositivos de tu red).

Si deseas obtener información más detallada con respecto a la configuración del cortafuegos y a los puertos que deberás mantener abiertos, puedes consultar el artículo "Configuración de Firewall de Windows para permitir el acceso a SQL Server" de Microsoft.

No utilices las contraseñas por defecto.

La instalación de Sage Murano, Sage 200 y Sage Despachos Connected permite definir una contraseña personalizada que será utilizada por el usuario de la base de datos. Sin embargo, durante el asistente de instalación y configuración, no es obligatorio definir tu propia contraseña. Si no has definido tu propia contraseña para el usuario de la base de datos, y aun sigues utilizando alguna de las contraseñas por defecto que el programa te ha facilitado, te recomendamos que cambies tu contraseña y establezcas una nueva que sea suficientemente segura.

Consulta el artículo "Directiva de contraseñas" si necesitas más información al respecto de cómo establecer una política de contraseñas seguras con respecto al acceso a la base de datos.

Seguridad de Sage Murano, Sage 200 y Sage Despachos Connected.

Evita que los usuarios puedan instalar programas de terceros.

Como ya sabes, Sage Murano, Sage 200 y Sage Despachos Connected son productos que, en sus versiones de escritorio, se ejecutan en Microsoft Windows y pueden ser instaladas de forma que sólo utilicen un único ordenador, o de forma que se puedan utilizar desde distintos ordenadores dentro de tu propia red interna de trabajo.

Dado que estos productos almacenan y procesan multitud de datos e información sensible, es muy importante que se pueda garantizar su seguridad e integridad.

En este sentido, Sage te recomienda que configures tus ordenadores donde vayas a ejecutar nuestras soluciones de manera que sea el único software que se pueda ejecutar en tus máquinas de trabajo. Sin embargo, la realidad es que los usuarios a menudo necesitan de otros programas para poder llevar a cabo su trabajo. Por ello, deberías considerar la implementación de algunas medidas de seguridad adicionales para garantizar que sólo los programas que tú necesites se puedan instalar y ejecutar en tus ordenadores.

Ten en cuenta que Microsoft Windows ofrece una serie políticas (más conocidas por sus siglas en inglés, GPO o Group Policy Objects) que pueden ser configuradas en tus sistemas de forma que puedas evitar la descarga e instalación de programas no deseados o que simplemente no sean necesarios en tu propia instalación.

Permisos de las cuentas de usuario de tus sistemas.

Es muy importante que los usuarios de Windows que se utilicen para acceder a nuestros productos no tengan privilegios de administración.

Configurar todos los usuarios como estándar y restringir su capacidad para ejecutar otros procesos con elevación de permiso es una de las principales recomendaciones para tu instalación, y que además está considerado uno de los principales estándares en la industria.

Puedes tomar como referencia el artículo “Implementación de modelos administrativos de menor privilegio” de la página web de documentación de Microsoft.

Activar la aleatorización de imágenes (ASLR).

Asegúrate de tener activas las opciones de “Protección contra vulnerabilidades de seguridad” en tus equipos (tanto en el/los servidor/es como en los puestos de trabajo). Básicamente, consiste en la

activación de forma obligatoria de la aleatorización de imágenes (o ASLR en inglés, Address Space Layout Randomization) y la Prevención de ejecución de datos (o DEP, del inglés Data Execution Prevention). Ambas son medidas altamente efectivas que evitarán la posible ejecución de algunos ataques y diferentes exploits en tus sistemas).

Desde Sage, te recomendamos activar ambas medidas de seguridad en tus ordenadores, aunque el más importante de los dos es el ASLR.

Puedes encontrar más información en los artículos "Turn on mandatory ASLR in Windows Security" y "Mitigar las amenazas mediante el uso de las funciones de seguridad de Windows 10" con respecto a estas medidas de seguridad.

No expongas tu solución a Internet mediante el protocolo Remote Desktop Protocol (RDP)

Si accedes a Sage 200 o Sage Despachos desde más de un puesto de trabajo, y utilizas Terminal Server para acceder a estas soluciones desde fuera de tu sitio habitual de trabajo a través de Internet, debes plantearte tunelizar el tráfico RDP a través de una conexión HTTPS, de manera que puedas utilizar el programa directamente en un navegador web.

Consulta el siguiente artículo en inglés ("Security guidance for remote desktop adoption") para obtener más información sobre este tema.

Desactiva el Modo Seguro en todos los puestos de trabajo.

El Modo Seguro hace que Windows se inicie mediante un estado básico de su configuración, y está especialmente indicado para solucionar algunos problemas con los drivers del sistema y algunos otros aspectos de la configuración. Sin embargo, un usuario malicioso podría hacer uso de esta característica para, por ejemplo, crear nuevos usuarios en el sistema, reactivar usuarios que hayan sido previamente desactivados y algunas otras cuestiones que podrían poner en riesgo la seguridad del sistema.

Para evitar esta situación, la recomendación principal es desactivar la posibilidad de arrancar en Modo Seguro. Este cambio puede realizarlo de manera muy sencilla alguno de los administradores utilizando la herramienta MSConfig ("Como abrir MSConfig en Windows 10") o bien modificando las opciones de arranque de Windows ("Información general sobre las opciones de arranque en Windows").

Recuerda además que, como ya se ha comentado antes, las cuentas con privilegios de administración deben ser utilizadas exclusivamente para tareas administrativas, y nunca se deben utilizar en el día a día de los usuarios estándar.

Criterios de referencia del CIS.

Las recomendaciones del CIS (más conocidos CIS Benchmark, en inglés) son consideradas como un estándar de la industria a la hora de configurar de manera segura los servidores y los puestos de trabajo, de forma que se pueda garantizar su integridad y seguridad.
Estas recomendaciones abarcan medidas como la desactivación de la consola (CMD) o del Powershell en Microsoft Windows.
Para más información y una lista complete de estas recomendaciones, puedes visitar la página "CIS Benchmark".

Bloqueo de los programas / Modo quiosco

De forma adicional a todas las recomendaciones anteriores, quizás puedas considerar la posibilidad de ejecutar Sage Murano, Sage 200 o Sage Despachos Connected en modo quiosco.

Esta forma de ejecutar las soluciones te permitirá obtener el mayor nivel de seguridad en los puestos de trabajo, de forma que puedas configurarlos para que sólo permitan la ejecución de uno de estos programas, o incluso optar por el modo multi aplicación, que permite ejecutar un número reducido de ellos si fuera necesario.

El equipo de seguridad de Sage ha recopilado una guía paso a paso, para que puedas hacer uso de esta característica en Microsoft Windows. Puedes llevar a cabo los siguientes pasos una vez hayas instalado y configurado Sage Murano, Sage 200 o Sage Despachos Connected en tu sistema.

Shell Launcher y AppLocker

1. Abre la opción "Programas y características" en el "Panel de control", y selecciona "Activar o desactivar las características de Windows". Expande la entrada "Bloqueo de dispositivo" y selecciona "Selector de Shell". Pulsa el botón "Aceptar".

2. Añade o configura una cuenta de usuario estándar en tu sistema, en caso de que no tuvieras ya una.

3. Descarga el código Fuente que encontrarás en Selector de shell y modifícalo, de manera que arranque Sage Murano, Sage 200 o Sage Despachos Connected utilizando la cuenta de usuario estándar del paso anterior.

4. Aplica la configuración de AppLocker que encontrarás en este enlace.

5. Asegúrate de añadir la consola de comandos (CMD) y el PowerShell a la lista de exclusión de ejecutables (puede ser que no estén incluídos por defecto).

6. Utiliza el Editor de Políticas de Grupo para desactivar la combinación de teclas CTRL + ALT + DEL. Lo encontrarás en la opción “Configuración de usuario > Plantillas administrativas > Sistema > Opciones Ctrl+Alt+Del”. Marca todas las opciones para activar esta política.

7. Puedes encontrar más opciones de configuración adicionales para blindar aún más tu quiosco en caso de que necesites ejecutar varias aplicaciones, en el artículo “Utilizar ApLocker para crear un quiosco de Windows 10 que ejecute varias aplicaciones”.

8. Establece el inicio de sesión automático para el usuario del paso 2 y tendrás todo listo.

Apéndice: Vulnerabilidades conocidas y medidas de mitigación recomendadas

En este apéndice puedes encontrar una lista de todas las vulnerabilidades conocidas de Sage Murano, Sage 200 y Sage Despachos Connected que están disponibles de manera pública como parte del CVE (Common Vulnerabilities and Exposures) del MITRE.

Te recomendamos encarecidamente seguir todas las recomendaciones de seguridad que se dan en este documento. A continuación, se dan recomendaciones específicas para cada una de las vulnerabilidades conocidas:

Número CVE	Descripción	Mitigaciones
CVE-2023-2809	*The use of hardcoded, plaintext MS SQL database credentials in the application code (a DLL) makes it possible to read all databases from the MS SQL database server. This could be linked to known techniques to gain remote execution of MS SQL commands and escalate privileges on Windows systems. In addition to having the credentials hardcoded in the system DLL, the NO use of an encrypted communication channel between the database and the Sage 200 system, makes it possible to extract the credentials in plain text by performing a dump of the process.*	Actualiza tu solución a la versión 2023.75 o superior. Sigue todas las recomendaciones de seguridad de este documento que te sean posibles

sage.com