Smith & Nephew, Inc.
2905 Northwest Blvd, Suite 40
Plymouth, MN 55441
EE. UU.

T +1 763 452 4950
F +1 763 452 4980
www.smith-nephew.com

Sistema quirúrgico RI.HIP NAVIGATION sobre CORI◊

ACTUALIZACIONES DEL SISTEMA OPERATIVO Y DEL SOFTWARE DE SEGURIDAD

Información de carácter general

Para asegurar que el sistema quirúrgico RI.HIP NAVIGATION sobre CORI siga funcionando de la manera deseada, Smith+Nephew recomienda seguir estas pautas para las actualizaciones de Windows y del software antivirus. Estas pautas se actualizarán continuamente a través de este sitio web. Asegúrese de consultar con el equipo de seguridad informática de su organización sobre el uso de RI.HIP NAVIGATION y de estas pautas.

Actualizaciones de Windows

RI.HIP NAVIGATION se configura a través de la configuración predeterminada de la «Group Policy» (Directiva de grupo) local. Si su organización utiliza la configuración de la «Group Policy» (Directiva de grupo) de Windows en alguno de los servidores en los que está instalado el software RI.HIP NAVIGATION, no cambie los ajustes.

Instale solamente las actualizaciones de seguridad de Microsoft; tanto los **paquetes acumulativos mensuales** como las **actualizaciones solo de seguridad** están permitidos. No instale Service Packs ni actualizaciones opcionales. Las normas sobre productos sanitarios requieren que los Service Packs sean probados y publicados por el fabricante del producto sanitario. Si se añade RI.HIP NAVIGATION al dominio del hospital, se recomienda la guía suministrada en este documento.

Aunque las **actualizaciones de seguridad de Microsoft** pueden instalarse inmediatamente después de que Microsoft las publique, Smith+Nephew recomienda posponer cinco días la instalación. Este documento se actualizará en ese plazo de cinco días, si es necesario, después de que Smith+Nephew evalúe las actualizaciones de seguridad.

A continuación se ofrece información sobre la realización de configuraciones de directivas informáticas:

Para Windows 10 y posterior:

- Deshabilite «**Activar actualizaciones recomendadas**» mediante Actualizaciones automáticas.
- Deshabilite «**Permitir la instalación inmediata de Actualizaciones automáticas**».
- Habilite «**No reiniciar automáticamente con usuarios que hayan iniciado sesión**» en instalaciones de actualizaciones automáticas.
- Ajuste «**Configurar Actualizaciones automáticas**» a «**Deshabilitado**».

No instale actualizaciones durante el tratamiento de pacientes.

Las siguientes actualizaciones de seguridad no pueden instalarse:

- **KB2823324**: Vulnerabilidades en el controlador modo kernel podrían permitir la elevación de privilegios (2829996): MS13-036
- **KB2984615**: Vulnerabilidades en el controlador modo kernel podrían permitir la elevación de privilegios (2984615) MS14-045
- **KB4577051**: 2020-09 Actualización acumulativa de calidad mensual de seguridad para Windows Embedded Standard 7 para sistemas basados en x64

Actualizaciones de controladores

No actualice los controladores en RI.HIP NAVIGATION.

No utilice la configuración manual ni las actualizaciones de Windows para actualizar controladores en RI.HIP NAVIGATION. Esta directiva está asegurada por la configuración de «Group Policy» (Directiva de grupo), que no debe cambiarse.

Para Windows 10:

- Ajuste «**Especificar el orden de búsqueda de controladores de dispositivos en ubicaciones de origen**» a «**Habilitado**» y compruebe la casilla «**No buscar en Windows Update**».
- En el editor de Group Policy (Directiva de grupo) local, ajuste «**No incluyas controladores con las actualizaciones de Windows**» a «**Habilitado**».

Configuración de la Group Policy (Directiva de grupo) aplicable

Si su organización utiliza la configuración de la «Group Policy» (Directiva de grupo) de Windows en alguno de los servidores en los que está instalado software de Smith+Nephew, no cambie los ajustes de las directivas siguientes.

- Computer ConfigurationPoliciesAdministrative TemplatesWindows ComponentsRemote Desktop Services*
- Computer ConfigurationPoliciesAdministrative TemplatesWindows ComponentsWindows PowerShell*
- Computer ConfigurationPoliciesWindows SettingsSecurity SettingsSoftware Restriction Policies*
- User ConfigurationPoliciesAdministrative TemplatesWindows ComponentsRemote Desktop Services*
- User ConfigurationPoliciesAdministrative TemplatesWindows ComponentsWindows PowerShell*
- User ConfigurationPoliciesWindows SettingsSecurity SettingsSoftware Restriction Policies*

Software antivirus

Smith+Nephew recomienda proteger el sistema con software antivirus de última generación. Un representante de Smith+Nephew deberá verificar el funcionamiento del sistema después de la primera instalación del software antivirus. Tenga en cuenta que la configuración de algunos programas de software de protección contra malware (p. ej., el detector de virus) pueden afectar negativamente al funcionamiento del sistema. Por ejemplo, si se llevan a cabo detecciones en tiempo real y se monitoriza el acceso a cada archivo, el acceso a los datos de pacientes puede verse restringido. Para obtener resultados óptimos:

- Deshabilite todas las funciones adicionales del software antivirus (p. ej., los detectores de exploradores o de correo electrónico y el firewall adicional).
- Deshabilite los mensajes emergentes del software antivirus.

Configure el software antivirus (p. ej., añadiendo elementos a las excepciones de carpetas) de forma que no explore ni modifique los siguientes directorios:

- C:\Brainlab, D:\Brainlab y F:\Brainlab, etc.
- C:\PatientData, D:\PatientData y F:\PatientData, etc.

Software de terceros

Con la excepción del antivirus y de las actualizaciones de seguridad de Microsoft, no instale ningún software de terceros sin la aprobación de Smith+Nephew. Si se instala software de terceros, la seguridad y la eficacia del producto sanitario ya no puede asegurarse, y es posible que queden anuladas algunas garantías.

Prácticas óptimas

Para obtener los mejores resultados, Smith+Nephew recomienda lo siguiente:

- Lleve a cabo análisis de seguridad de los dispositivos y medios de almacenamiento (p. ej., CD-ROM, DVD-ROM, discos duros USB y unidades de memoria Flash USB) para detectar y eliminar el malware que pueda haber antes de utilizar el dispositivo o el medio.
- Habilite «**System Restore**» **(Restauración del sistema)** para la unidad **C:** a fin de que el sistema pueda restaurarse a un estado anterior, en caso necesario.
- Programe la descarga e instalación de Windows y de actualizaciones del antivirus al apagar el sistema. Preste especial atención a los servidores y a las máquinas virtuales y asegúrese de que los sistemas se reinicien por completo posteriormente.
- Si no está activado un análisis tras el acceso/en tiempo real, programe un análisis a petición/programado al apagar el sistema.

Más información

Esta directiva sustituye a toda la documentación pasada y presente de los productos. Para obtener más información o ayuda, póngase en contacto con el servicio de atención al cliente de Smith+Nephew.

- +1 833 766 2846 (teléfono)
- ri.support@smith-nephew.com