Sociedad Andaluza para el Desarrollo de las Telecomunicaciones
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

seguridad+ Y CONFIANZA DIGITAL | AndalucíaCERT CENTRO DE SEGURIDAD TIC

Informe de divulgación
Fin del soporte de Windows Server 2003

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-9014-151013*
Edición:	*0*
Categoría	*Uso Interno*
Fecha de elaboración:	*13/10/2015*
N° de Páginas	*1 de 11*

1 TABLA DE CONTENIDOS

2 OBJETO

El objetivo de este documento es recordar la finalización del soporte para Windows Server 2003, de las vulnerabilidades actuales del sistema y como plantear las implicaciones que pueden derivarse de un sistema operativo obsoleto y sin soporte.

Por último se plantea una serie de recomendaciones que deben tenerse en cuenta para la migración, y consejos que pueden ayudar a mitigar los riesgos mientras se planifica y realiza la migración de los sistemas.

3 ALCANCE

Este documento va destinado al personal técnico de la Junta de Andalucía. En él se describe la problemática actual debida al fin del soporte de Windows Server 2003, sus implicaciones y algunas recomendaciones temporales de seguridad.

4 SITUACIÓN.

Windows Server 2003 ha sido uno de los sistemas operativos más ampliamente usado de entre la plataforma de servidores de Microsoft, con cerca de 30 millones licencias vendidas a nivel mundial.

Ilustración 1: Pantalla de Windows Server 2003.

Como consecuencia del final del ciclo de vida del sistema operativo Windows Server 2003, desde el 14 de Julio de 2015, Microsoft ha dejado de prestar servicios de soporte extendido para este sistema operativo.

A partir de ese momento, dicho sistema operativo ha dejado de recibir actualizaciones, incluyendo parches de seguridad, soporte para incidencias o actualizaciones de contenidos técnicos online.

Microsoft prevé la aparición de vulnerabilidades críticas de forma continuada y que ponen en riesgo a los usuarios que todavía usan este sistema.

La siguiente tabla muestra el ciclo de vida de las distintas versiones de Windows Server 2003.

Producto	Fecha de inicio del ciclo de vida	Fecha de fin del soporte técnico principal	Fecha de fin del soporte técnico extendido	Fecha de fin de soporte de Service Pack	Notas
Windows Server 2003 R2 Datacenter Edition (32-Bit x86)	05/03/2006	13/07/2010	14/07/2015	14/04/2009	
Windows Server 2003 R2 Datacenter Edition with Service Pack 2	13/03/2007	Nota de revisión	Nota de revisión		El Soporte Técnico será retirado en cuanto se produzca cualquiera de estas dos situaciones, o 24 meses después del lanzamiento del siguiente service pack o al final del ciclo de vida de soporte técnico del producto. Para más información consulte la directiva de Service Packs en http://support.microsoft.com/lifecycle/#ServicePackSupport.
Windows Server 2003 R2 Datacenter x64 Edition	05/03/2006	13/07/2010	14/07/2015	14/04/2009	
Windows Server 2003 R2 Datacenter x64 Edition with Service Pack 2	13/03/2007	Nota de revisión	Nota de revisión		El Soporte Técnico será retirado en cuanto se produzca cualquiera de estas dos situaciones, o 24 meses después del lanzamiento del siguiente service pack o al final del ciclo de vida de soporte técnico del producto. Para más información consulte la directiva de Service Packs en http://support.microsoft.com/lifecycle/#ServicePackSupport.
Windows Server 2003 R2 Enterprise Edition (32-Bit x86)	05/03/2006	13/07/2010	14/07/2015	14/04/2009	
Windows Server 2003 R2 Enterprise x64 Edition	05/03/2006	13/07/2010	14/07/2015	14/04/2009	
Windows Server 2003 R2 Standard Edition (32-bit x86)	05/03/2006	13/07/2010	14/07/2015	14/04/2009	
Windows Server 2003 R2 Standard x64 Edition	05/03/2006	13/07/2010	14/07/2015	14/04/2009	

Ilustración 2: Ciclo de vida del soporte de Windows Server 2003.

5 RIESGOS

En general no es recomendable mantenernos en un entorno obsoleto. Esto tiene una serie de implicaciones importantes que es necesario conocer para poder tomar las decisiones adecuadas, ser conscientes de la situación y poder actuar en consecuencia.

Al no haber más actualizaciones, los sistemas son susceptibles de ser explotados aprovechando las vulnerabilidades que tienen a su favor los atacantes. Pero también existen otras implicaciones, que resumimos en:

- **Carencia de mantenimiento software:** No se contará con parches, actualizaciones, ni reparaciones funcionales ni de seguridad de Windows Server 2003; lo que aumenta la responsabilidad y el esfuerzo para mantener la funcionalidad y seguridad de los sistemas por parte de los departamentos técnicos.
- **Carencia de soporte técnico:** Microsoft no prestará soporte técnico en la resolución de problemas.
- **Problemas con software de aplicación:** Programas nuevos y actualizaciones de los actuales pueden dejar de funcionar en Windows Server 2003, ya que los fabricantes no desarrollarán actualizaciones para este sistema.
- **Problemas con el hardware:** Los nuevos equipos, los ya existentes y/o nuevos componentes no estarán certificados para funcionar con Windows Server 2003. También pueden aparecer problemas de drivers e incompatibilidades en componentes físicos.
- **Incumplimiento de políticas de seguridad e incumplimientos legales:** El Esquema Nacional de Seguridad (ENS) deja bien claro la necesidad de gestionar las vulnerabilidades existentes en los equipos, algo que con Windows Server 2003 ya no sería posible. Concretamente nos encontramos con los siguientes apartados:
  - **Artículo 20 del RD 3/2010 (Integridad y actualización del sistema):** Indica que *"Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad delos mismos".*
  - **Anexo II del RD 3/2010, apartado 4.3.4 Mantenimiento [op.exp.4]:** Indica que *"Para mantener el equipamiento físico y lógico que constituye el sistema,[...]*

    a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas.

    b) Se efectuará un seguimiento continuo de los anuncios de defectos.

    c) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización".

6 VULNERABILIDADES

Windows Server 2003 cuenta con cerca de 900 vulnerabilidades reconocidas. La evolución histórica se puede apreciar en la siguiente gráfica.

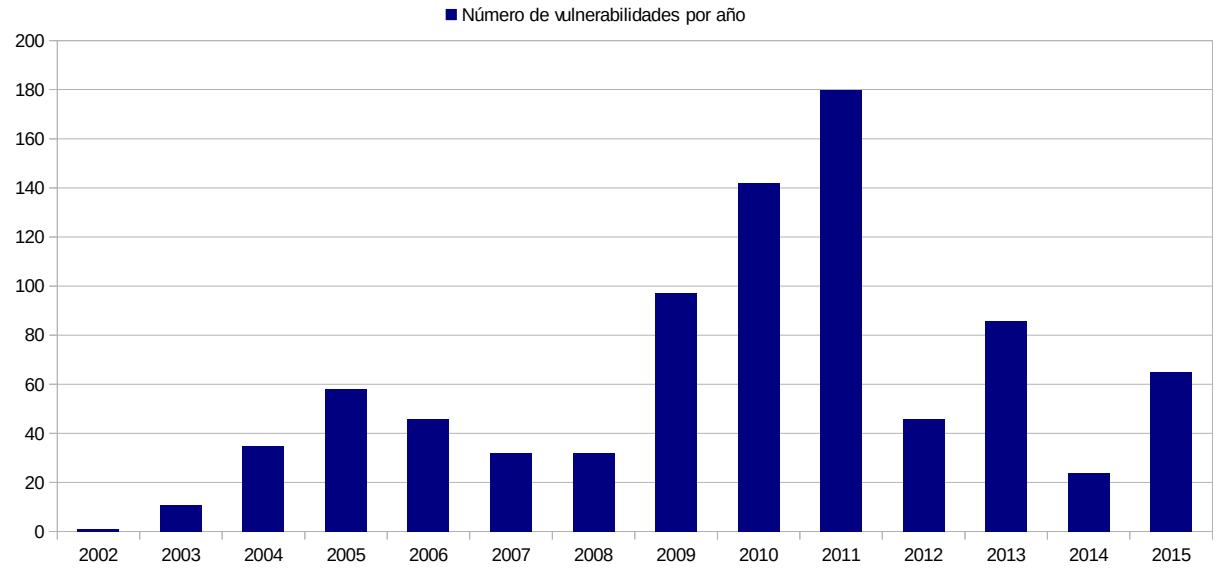

Ilustración 3: Vulnerabilidades de Windows Server 2003.

Atendiendo al nivel de criticidad CVSS de las vulnerabilidades, más del 30 % de las vulnerabilidades son de la máxima severidad. A lo largo del año 2015 se detectaron 9 vulnerabilidades de la máxima severidad.

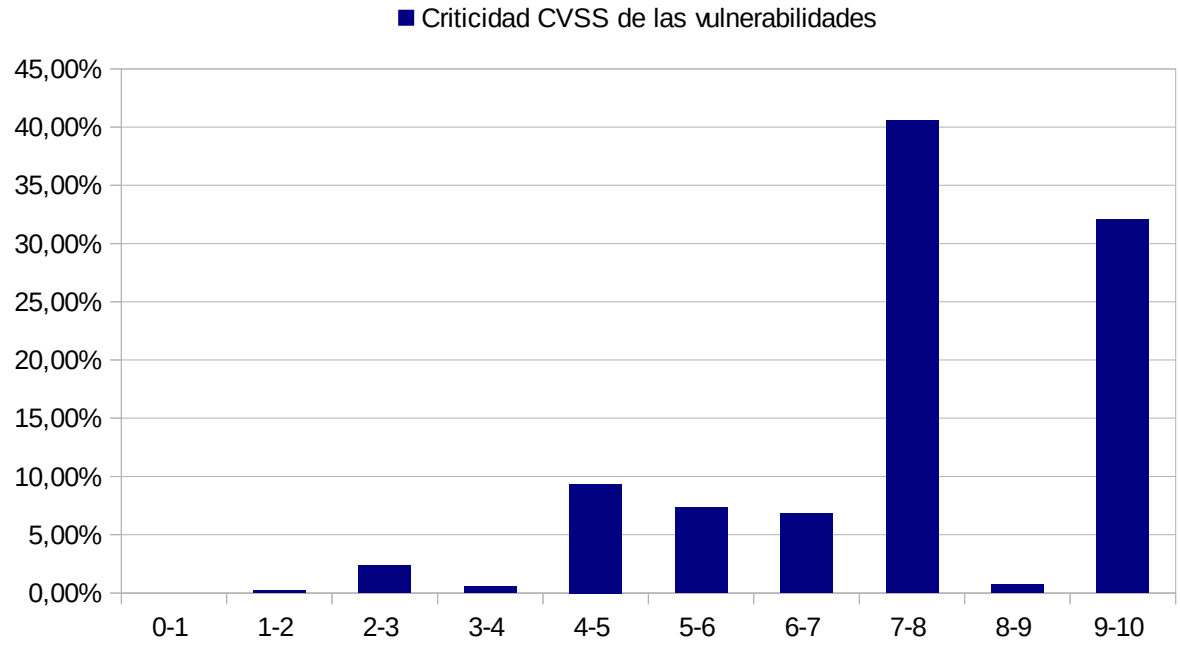

Ilustración 4: Criticidad de las vulnerabilidades de Windows Server 2003.

El mismo martes 14 de Julio de 2015 que finalizó el servicio de soporte técnico de Microsoft para Windows Server 2003, se publicaron boletines de seguridad con nivel de severidad crítica.

Desde la fecha del fin de soporte de Windows Server 2003 se han detectado múltiples fallos de seguridad en otros productos de la plataforma Microsoft Windows Server, para los cuales Microsoft ha publicado parches para solventarlos. Previsiblemente, tales vulnerabilidades también son aplicables a Windows Server 2003. Hay que insistir en que Windows Server 2003 ya no cuenta con tales parches.

Para hacernos una idea del riesgo, veamos el caso del Windows Server 2008. En la siguiente tabla se puede apreciar la evolución de vulnerabilidades durante el año, desde agosto a octubre se han descubierto 45 vulnerabilidades.

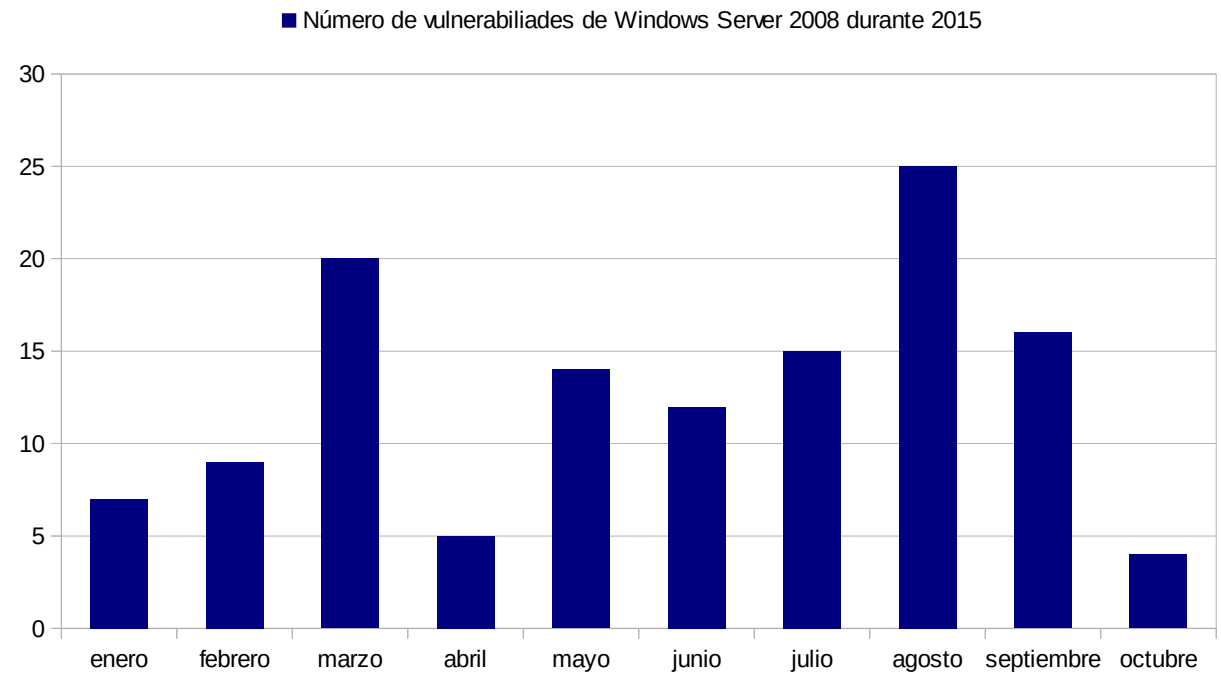

Ilustración 5: Vulnerabilidades de Windows Server 2008.

7 PLAN DE MIGRACIÓN

Para llevar a cabo la migración del sistema es necesario seguir las recomendaciones de los fabricantes de los sistemas y productos afectados, así como adoptar unas buenas prácticas de gestión de proyectos y de gestión de las TI. Como en cualquier proyecto de migración de sistemas se debe previamente evaluar, analizar y planificar los pasos a seguir. A continuación exponemos brevemente una serie de consideraciones a tener en cuenta:

- Contar con un inventariado actualizado de los sistemas. Lógicamente, es crucial identificar los servidores Windows Server 2003 y descubrir que servicios prestan directa o indirectamente. Es

esencial realizar un análisis de riesgos que oriente la decisión a tomar. Se deben considerar aspectos como la infraestructura en la que están desplegados los servidores, la carga de trabajo que soportan y cuales son los requerimientos de la organización respecto al servicio. Finalmente se debe definir la nueva arquitectura, que dará respuesta a cuestiones tales como si se replataforma la infraestructura, si se migra el servicio a otra tecnología, o si se consolida el servicio en un entorno físico o virtual, entre otras cuestiones.

- Planificar el despliegue. Diseñar la planificación de la migración del servicio y de los datos. Identificar las herramientas que faciliten y automaticen la migración de los datos. Hay que tener en cuenta las necesidades operaciones del servicio.
- Llevar a cabo la migración. En este fase final se lleva a cabo el despliegue, la migración de datos, y las pruebas de validación final. También se debe considerar las necesidades formativas.

8 BASTIONADO DE MICROSOFT WINDOWS SERVER.

En el caso excepcional de que el plan de migración se extienda en el tiempo, se recomiendan unas medidas paliativas para reducir las vulnerabilidades.

Para mejorar la seguridad del sistema se pueden emplear técnicas de seguridad de red, habilitación de controles de seguridad en el sistema y mediante el bastionado del sistema. En este apartado nos centraremos en este último.

La técnica de bastionado en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo. Esto se logra eliminando software, servicios, usuarios, etc... innecesarios en el sistema, así como cerrando puertos que no estén en uso así como otros métodos y técnicas que se destacan de manera resumida a continuación.

Entre las actividades propias de un proceso de bastionado se pueden contar las siguientes:

- **Configuraciones necesarias para protegerse de posibles ataques físicos o de hardware de la máquina**. Entre otras actividades, destacan el upgrade de firmware, el establecimiento de contraseñas complejas para el arranque del equipo y la configuración de la BIOS, la deshabilitación de inicio de sistema para cualquier unidad que no sea el disco duro principal, y en casos de servidores, la deshabilitación de dispositivos ópticos, usb o similares, para evitar cualquier entrada de malware desde un medio de almacenamiento externo.
- **Activación y/o configuración adecuada de servicios de actualizaciones.** Instalar los parches pendiente de aplicar al servidor Windows Server 2003. Por ejemplo, una de las vulnerabilidades más peligrosas se resolvió con el boletín MS12-020 "Vulnerabilities in Remote Desktop Could

Allow Remote Code Execution (2671387)" en marzo de 2012, no obstante aún en día se sigue explotando. También es necesario aplicar regularmente los parches de terceras aplicaciones instaladas en el sistema, prestando especial atención a las vulnerabilidades de productos Java y Adobe.

- **Instalación, configuración y mantenimiento de programas de seguridad** tales como antivirus con firmas actualizadas y listas blancas de aplicaciones.
- **Configuración de la política local del sistema**, considerando varios puntos relevantes:
  - Política de contraseñas robusta, con claves temporales, almacenamiento histórico de contraseñas (para no usar contraseñas cíclicas), bloqueos de cuentas por intentos erróneos y requisitos de complejidad de contraseñas.
  - Renombrado y deshabilitación de cuentas estándar del sistema, como administrador e invitado.
  - Asignación correcta de derechos de usuario, de tal manera que se pueda reducir las posibilidades de elevación de privilegios, y tratando siempre de limitar al mínimo los privilegios y/o derechos de los usuarios activos.
  - Configuración de opciones de seguridad generales, como aquellas relacionadas con rutas de acceso compartido, apagado de sistema, inicio y cierre de sesión y opciones de seguridad de red.
  - Activación de auditorías de sistema, claves para tener un registro de algunos intentos de ataques característicos como ataques por fuerza bruta.
- **Configuración de servicios de sistema**. En este punto es necesario tratar siempre de deshabilitar todos aquellos servicios que no vayan a prestar una funcionalidad necesaria para el funcionamiento del sistema. Por ejemplo, si su equipo no posee tarjetas de red inalámbricas, el servicio de redes inalámbricas debería estar deshabilitado. Especialmente, se deben eliminar los siguientes servicios, siempre que no sean imprescindibles para el buen funcionamiento del sistema: HTTP/HTTPS, NetBIOS, WINS, herramientas de administración web, servidores de correo, servidores de base de datos, servidores DNS/DHCP y servicios SIP.
- **Configuración de los protocolos de red**. Es muy recomendable que las aplicaciones y protocolos usen configuraciones robustas. Se deben tomar medidas como deshabilitar el SSL 2.0/3.0, deshabilitar cifradores débiles tales como RC4 y DES, o usar TLS 1.2 siempre que sea posible.
- **Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema**. En la medida de lo posible, denegar explícitamente cualquier permiso de archivo a las cuentas de acceso anónimos o que no tengan contraseña. Un correcta asignación de permisos a nivel de carpetas y archivos es clave para evitar acceso no deseado al contenido de los mismos.
- **Configuración de opciones de seguridad de los distintos programas**, como clientes de correo electrónico, navegadores de internet y en general de cualquier tipo de programa que tenga interacción con la red.

- **Configuración de acceso remoto**. En caso de no ser estrictamente necesario, es bueno deshabilitar el acceso remoto. Sin embargo, cuando es necesario tener control remoto de la máquina, es preciso configurarlo de manera adecuada, restringiendo el acceso a un número muy limitado de usuario, restringiendo al mínimo las conexiones concurrentes, tomando cuidado en la desconexión y cierre de sesión y estableciendo un canal cifrado de comunicaciones para tales propósitos, como SSH.
- **Configuración adecuada de cuentas de usuario**, tratando de trabajar la mayor parte del tiempo con cuentas de acceso limitado y deshabilitando las cuentas de administrador.
- **Cifrado de archivos o unidades según las necesidades del sistema**, considerando un almacenamiento externo para las llaves de descifrado. Considerar además la opción de trabajar con sistemas de cifrado de mensajería instantánea y correo electrónico.
- **Realizar y programar un sistema de respaldos frecuente a los archivos y al estado de sistema**. En la medida de lo posible, administrar los respaldos vía red o llevar los respaldos a unidades físicas que estén alejadas del equipo que las origina.

Para una adecuada configuración del sistema se recomienda seguir las buenas prácticas definidas en las guías CCN-STIC del Centro Criptológico Nacional.

- CCN-STIC-503A Seguridad en Windows 2003 Server (controlador de dominio)
- CCN-STIC-503B Seguridad en Windows 2003 Server (servidor independiente)

9 CONCLUSIONES

Es importante entender las amenazas que implican el permanecer con un sistema operativo servidor obsoleto y valorar la necesidad de contar con un análisis de riesgos. Cada organización debería plantearse, si no se ha hecho ya, la migración del servicio a una versión de sistema operativo soportado.

Se prevé que tras el fin del soporte de Windows Server 2003 el número y la sofisticación de amenazas se incremente de manera significativa.

En cualquier caso, el fin del ciclo de vida de Windows Server 2003 supone un riesgo que debe de ser tomado en cuenta y gestionado de forma adecuada.

Por tanto, AndalucíaCERT recomienda la elaboración de un plan de migración de los servicios a una infraestructura con sistema operativo soportado. Con dicha migración se rebajaría sustancialmente el impacto de las potenciales amenazas y se consolidaría una infraestructura de sistemas más eficiente, más segura, con mejoras en su administración y con una menor tasa de fallos.

10 GLOSARIO

Antivirus: Los antivirus son programas cuya función es detectar y eliminar Virus informáticos y otros programas maliciosos (a veces denominados malware). Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos (también conocidos como firmas o vacunas) de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado.

CVSS (Common Vulnerability Scoring System): Estándar de valoración de la severidad de las vulnerabilidades de la seguridad de los sistemas informáticos.

Vulnerabilidades: Una vulnerabilidad en seguridad informática hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

11 DOCUMENTACION DE REFERENCIA

Finalización del soporte para Windows Server 2003
Microsoft publica 14 boletines de seguridad para Windows Server 2003
Boletines de Seguridad de Microsoft
Boletines de Seguridad Septiembre 2015
Microsoft lanza un parche de seguridad de emergencia
Guía de bastionado de Microsoft Windows Server
Windows Server 2003 Security Baseline
Introducción al Hardening de Sistemas