



Las guías CCN-STIC para entornos Windows se centran en exclusividad en este popular sistema operativo que representa casi el 90% de los clientes instalados en el entorno empresarial y doméstico. En cuanto a los servidores dicho predominio pertenece a otras opciones Unix dada la gratuidad de los mismos, frente a las costosas licencias de servidor Windows. Aun así cualquier administrador del sistema prefiere un entorno gráfico a uno basado en líneas de comandos que conlleva mayor dominio del sistema, si bien Microsoft está empezando a evaluar el uso de este tipo de sistemas por comandos en sus series Core de 2008 y 2012 Server por la descarga de recursos hardware que supone y la versatilidad de dicho sistema de administración.

En cuanto a la securización de los sistemas operativos de Microsoft, debemos siempre tener en cuenta los siguientes criterios antes de realizar el *bastionado* de un sistema. El Director de seguridad no debe realizar dichas funciones, pero si supervisar su realización para permitir que su labor sea más efectiva en cuanto al control de los sistemas. Hoy día centrales de CCTV, alarmas, terminales de usuario, etc, representan un sistema heterogeneo de recursos de hardware que complican la labor de control y seguridad, pero ello no es óbice para que no se intente realizar el mayor número de procedimientos que permitan lograr el objetivo de la securización de nuestros sistemas.

Como norma general nunca deberemos implementar los scripts (cadena de comandos y sentencias que automatizan el procedimiento de securización) sin el conocimiento previo de nuestra arquitectura de sistema, ya que corremos el riesgo de dejarla inservible, ya que avanzar disponiendo de todos los privilegios a nivel administrador en los sistemas es facil. Retomar el control y escalar privilegios para volver a controlar el sistema desde un usuario restringido es una tarea ardua y a veces imposible por una mala planificación de la ejecución de los scripts.

Para proceder a la securización siempre debemos contar con personal cualificado y con el administrador del sistema, es imposible realizar dicha labor sin los apoyos del personal de soporte de nuestra red, salvo que al hacerlo deseemos excluirlos de su labor de administración. Normalmente en los sistemas informáticos existen varios responsables entre los que cabe destacar el Administrador del Sistema, el Administrador de Seguridad y la Autoridad del Sistema, todas ellas preferentemente desempeñadas por personas distintas y que ayudaran a consensuar las decisiones necesarias a tomar, que van desde la implementación de medidas de seguridad de cifrado de discos duros, borrado seguro de datos, instalación de herramientas de comunicaciones, apertura y cierre de puertos, medidas complementarias de control de acceso a determinados terminales clientes o simplemente personal con credenciales de acceso al

sistema a nivel administrador. Todas esas decisiones se deben tener claras antes de la implementación del sistema. La CCN-STIC-204 CO-DRS-POS Pequeñas Redes detalla dichos requisitos a cumplimentar con anterioridad a la securización del sistema ya que detallarlos ayuda a tener una idea clara sobre nuestro sistema informático. Si bien no todas las CCN-STIC son clasificadas, algunas si lo son para impedir que su uso público suponga un conocimiento previo por parte de delincuentes que deseen acceder al sistema y conozcan los procedimientos descritos en el mismo, pero cualquier ciudadano puede registrarse en el CERT Nacional y obtener acceso a dichas guías, con el simple requisito de exponer en su solicitud la necesidad que tiene de conocer dicha información.

Como norma general si debemos ser conscientes de que a pesar de que exista una guía de securización del CCN-STIC para un determinado sistema operativo, si éste carece de soporte por parte del fabricante como es el caso de los betustos Windows 2000 (CCN-STIC 508), Windows XP (CCN-STIC 501 A o B), Windows Vista (CCN-STIC 517) y Windows 2003 Server SP3 (CCN-STIC 503 A o B), debemos promover su actualización ya que el soporte garantiza que existan parches que impidan ejecutar vulnerabilidades conocidas en el sistema operativo que por otro lado el fabricante se habrá preocupado de filtrar a los fines de forzar la actualización y adquisición de nuevas licencias.

Los sistemas operativos que nos ocupan por su amplia generalización y existencia de soporte son:

- CCN-STIC 521A Configuración segura de Windows Server 2008 R2: Instalación completa, controlador dominio o miembro ( no core , no independiente)
- CCN-STIC 521B Configuración segura de Windows Server 2008 R2: Instalación completa e independiente (no core, no miembro de dominio)
- CCN-STIC 521C Configuración segura de Windows Server 2008 R2: Instalación Core, controlador de dominio o miembro ( no completa, no independiente)
- CCN-STIC 521D Configuración segura de Windows Server 2008 R2: Instalación Core e independiente
- CCN-STIC 522A Seguridad en Windows 7 (cliente en dominio)
- CCN-STIC 522B Seguridad en Windows 7 (cliente independiente)
- CCN-STIC 523 Configuración segura de Windows Server 2008 R2 como servidor de ficheros

Además de securizar los sistemas operativos deberemos estar atentos a otros productos de Microsoft instalados en nuestros sistemas y que pueden disponer de guías de securización propias que nos permitan alcanzar un mayor grado de bastionado de las mismas, como pueden ser:

- CCN-STIC 520 Internet Explorer 11 para cliente MS Windows 7 como miembro de dominio e independiente
- CCN-STIC 524 Implementación de IIS 7.5 sobre Windows Server 2008 R2 en servidor miembro de dominio
- CCN-STIC 528 Implementación de Hyper-V en Microsoft Windows 2008 R2 Core
- CCN-STIC 529 Microsoft Office 2013
- CCN-STIC 530 Microsoft Office 2010
- Etc.

Dado el gran espectro de software disponible y la amplia variedad de arquitecturas conviene siempre echar un vistazo a las guías por si se han creado nuevas o por si han dejado de tener vigencia algunas de ellas. En cualquier caso el esfuerzo de creación de dichas guías no solo se circunscribe al personal del CERT Nacional sino también a los miembros de empresas colaboradoras como SIDERTIA que desarrollan dichas guías en conjunción con el CERT.