



Si sobre algo si disponen de competencia los Directores de Seguridad es sobre la supervisión de trabajos encaminados a garantizar que procedimientos, instalaciones y mantenimientos se realizan de la forma adecuada, delegar la competencia sobre la securización de nuestros sistemas en terceros puede provocar que a causa de una ineficiente instalación o configuración nuestra empresa sufra perdidas de información o intromisión en el sistema por no saber exactamente que están realizando en el mismo. Delegar no es inhibirse, es confiar en la labor de terceros para el desarrollo del trabajo encomendado y supervisar el cumplimiento de sus instrucciones.

El CCN-CNI no posibilita a cualquier ciudadano o empresa acceso a sus guías o procedimientos, si bien cualquier español tiene la posibilidad de registrarse en dicho portal y mediante previa acreditación de sus fines solicitar acceso a una determinada guía o script de configuración que haga a su sistema más seguro y eficiente. Si bien el acceso a dicha información está vetado para todas las guías como detallamos en el tema 1 existen algunas de acceso publico sin necesidad de registro previo, y ello es posible gracias a que una red mas segura contribuye a la seguridad de todos. Por ello debemos trabajar por disponer de redes informáticas más seguras con la ayuda del CCN-CNI.

Habitualmente las guías de mayor utilidad son aquellas que están encaminadas a la securización de los servidores más que de las estaciones de trabajo, ello es debido a que una estación comprometida es un problema para el cliente o usuario, pero un servidor es un problema para todos los usuarios, no solo para uno. Por ello daremos unas pautas de securización a nivel servidor que son realmente el objetivo natural de aquellos de desean acceder al sistema, ya sea a servidores de correo electrónico, paginas web, documentos en la nube o mensajería, un servidor independientemente de su destino es un objetivo prioritario para los "crackers".

Debido a las restricciones de acceso ya descritas anteriormente solo podemos acceder a la guía de securización de correo electrónico (Exchange 2010, bajo Microsoft Windows 2008) y su anexo es un script que nos automatizará el proceso de securización de dicho servidor.

Bajo ningún concepto debe ejecutarse el script sin haber verificado con el personal de soporte técnico las características de nuestro servidor o corremos el riesgo de dejar inservible la instalación y la información, motivo por el cual siempre leeremos con antelación la guía (documento en PDF) para evitar que

nuestra securización sea tan efectiva que haga a nuestro servidor un inmenso "*posavasos*".