



LABORATORIO 2

Investigación Digital y Forense

Daniel Alejandro Olarte Ávila

Universidad Sergio Arboleda

Universidad Sergio Arboleda Cl. 74 #14-14

Bogotá, Colombia

Correo: daniel.olarte01@correo.usa.edu.co

Escuela de Ciencias Exactas e Ingeniería

Profesor: Juan Carlos Galindo Piraquive

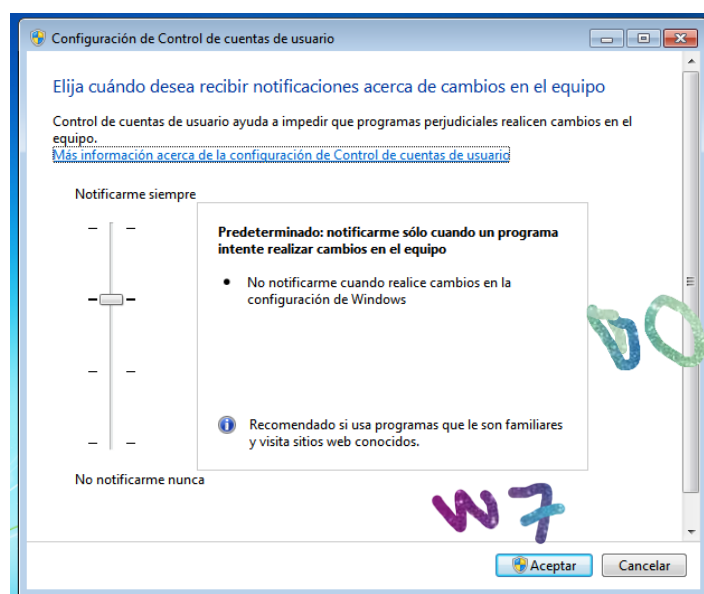
11/04/2023

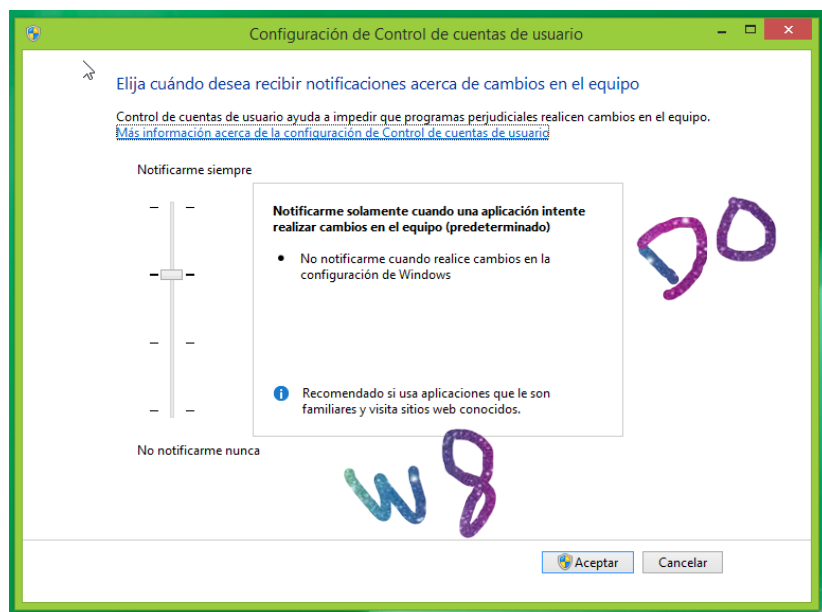
1) INTRODUCCION

En el siguiente laboratorio se explorarán y aplicarán medidas de seguridad para proteger los recursos y datos de una organización de accesos no autorizados. En este laboratorio, nos enfocaremos en el control de acceso de usuarios, gestión de dispositivos de seguridad y seguridad de red, para garantizar la integridad y confidencialidad de la información de la organización. Aprenderás sobre medidas de seguridad importantes, como autenticación, autorización y auditoría, y cómo implementar funciones de seguridad como Windows Biometric Framework (WBF), BitLocker, AppLocker, firewall y DirectAccess. Además, te enseñaremos cómo utilizar PowerShell para realizar tareas de administración y automatización de forma más eficiente. Prepárate para aprender y aplicar medidas de seguridad informática esenciales en este laboratorio.

DESARROLLO

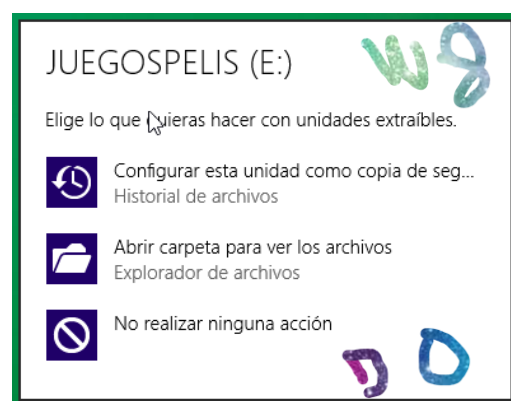
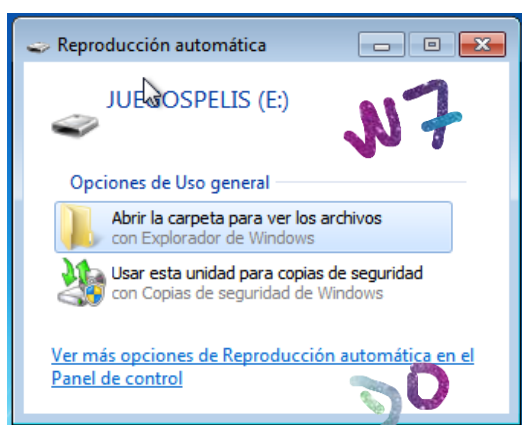
- a) En primer lugar, abordaremos el tema del control de acceso de usuarios (UAC), una medida de seguridad que está diseñada para alertarte y prevenir cambios no autorizados en tu equipo, garantizando que ninguna aplicación pueda modificar datos importantes por sí sola. Exploraremos el funcionamiento del UAC y su importancia en la protección de los recursos y datos de la organización.





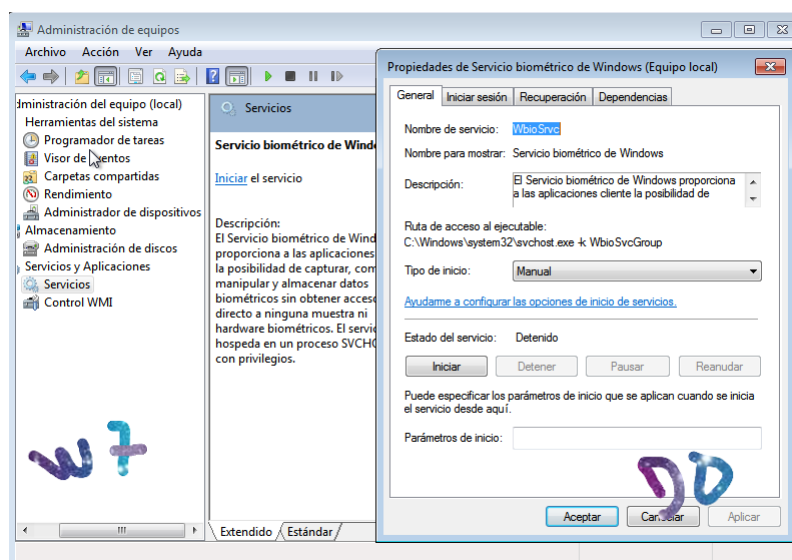
El Control de Cuentas de Usuario de Windows (UAC) tiene cuatro niveles de seguridad, cada uno más restrictivo que el anterior. El proceso de configuración es sencillo, solo se necesita acceder a la configuración de este parámetro y seleccionar el nivel de seguridad deseado mediante una barra deslizante. Cada nivel tiene sus propias características y tipos de avisos. Cuando se activa la ventana de aviso, no se puede realizar ninguna otra acción en Windows hasta que se tome una decisión. La ventana permanecerá en primer plano y no se puede minimizar ni interactuar con ninguna otra pantalla hasta que se resuelva la alerta.

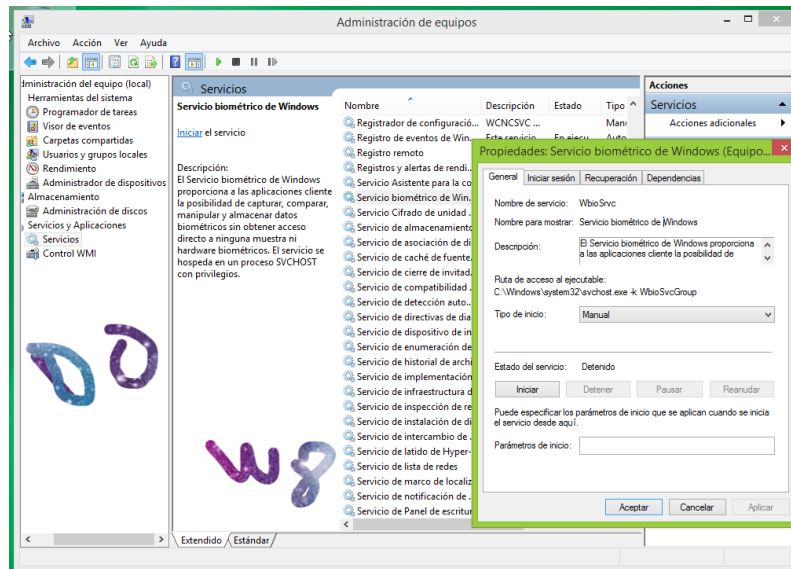
- b) Otra función importante para analizar y garantizar la seguridad es la de Reproducción Automática, la cual funciona como una herramienta útil para los usuarios al momento de conectar o insertar un nuevo dispositivo, como unidades flash USB, discos duros, CDs, entre otros. La función de Reproducción Automática permite que se ejecuten automáticamente las acciones adecuadas para el dispositivo en cuestión, pero también puede ser un riesgo de seguridad si se ejecutan acciones maliciosas de forma automática. Exploraremos cómo configurar la función de Reproducción Automática de manera segura y efectiva, para minimizar los riesgos de seguridad al conectar nuevos dispositivos.



La función de Reproducción Automática se introdujo en Windows XP y se ha mantenido en versiones posteriores, incluyendo Windows 7 y posteriores. En Windows 7, la función de Reproducción Automática permite que el sistema operativo detecte y abra automáticamente el contenido de un dispositivo externo, como una unidad flash USB, un CD o un DVD, tan pronto como se conecta al equipo. Esta función puede ser conveniente para los usuarios, pero también puede presentar riesgos de seguridad si se ejecutan acciones maliciosas de forma automática. Es importante comprender cómo configurar la función de Reproducción Automática de manera segura para minimizar estos riesgos.

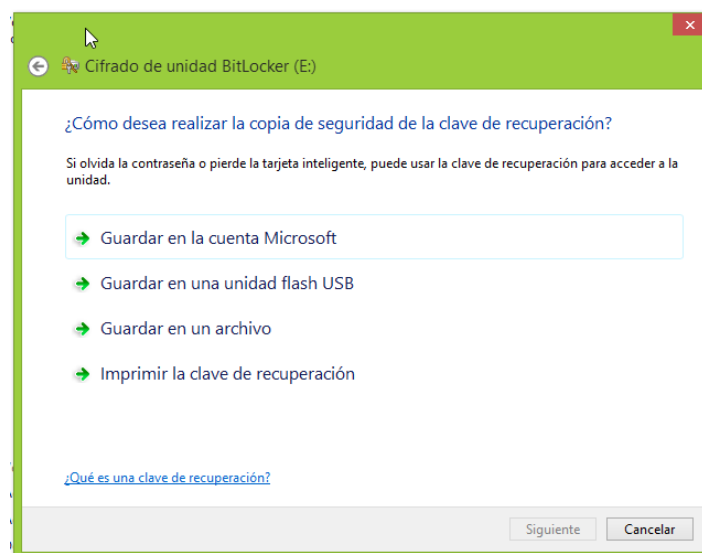
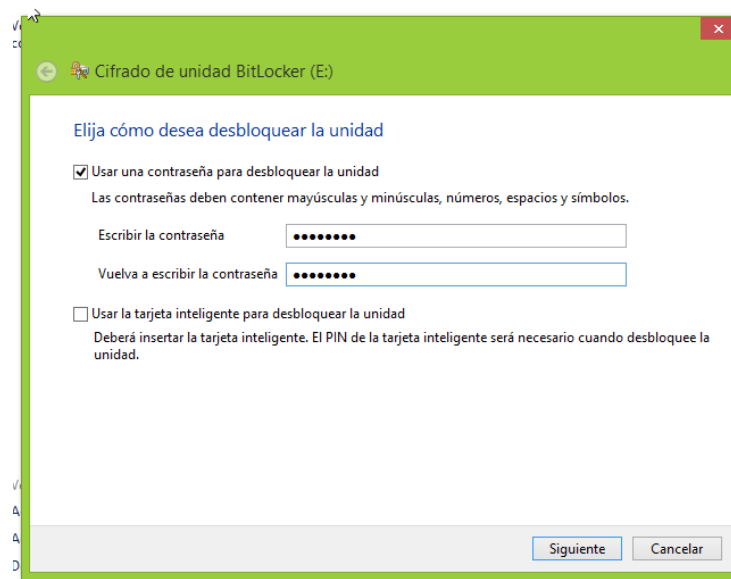
- c) La plataforma Windows Biometric Framework (WBF) es una herramienta importante para la seguridad en Windows. WBF proporciona una API estándar y un conjunto de servicios para que los proveedores de hardware y software de dispositivos biométricos puedan desarrollar controladores y aplicaciones que se integren con el sistema operativo de Windows. Con WBF, los usuarios pueden configurar, administrar y utilizar dispositivos biométricos compatibles con Windows 7 para autenticación y otras aplicaciones de seguridad. La autenticación biométrica es una forma segura y conveniente de verificar la identidad de los usuarios y puede ser utilizada en lugar o en combinación con contraseñas tradicionales para proteger los recursos y datos de la organización. En este laboratorio, se explorará cómo utilizar y configurar WBF para la autenticación biométrica en Windows.



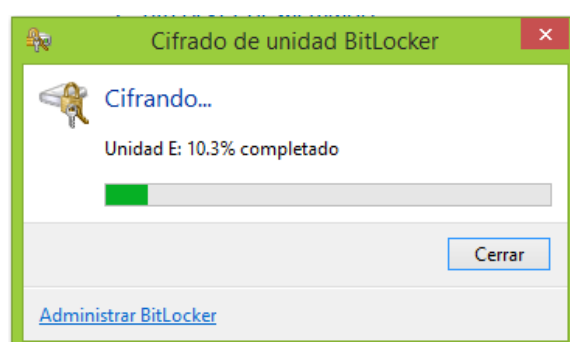
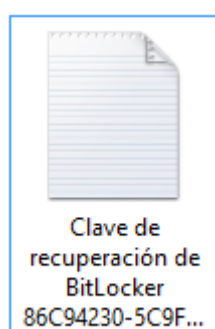


Además, es importante mencionar que el uso de dispositivos biométricos para autenticación puede mejorar significativamente la seguridad de un sistema, ya que la biometría es un método de autenticación más seguro y conveniente que las contraseñas tradicionales. Sin embargo, también es importante tener en cuenta que la implementación y uso adecuado de estos dispositivos es crucial para garantizar su efectividad en la protección de los recursos y datos de una organización.

- d) BitLocker es una herramienta muy importante para la seguridad de los datos almacenados en un equipo con Windows. Al utilizar el cifrado de disco completo, se asegura la protección de la información almacenada en la unidad de disco duro, incluso en caso de que el equipo sea robado o perdido. Es importante tener en cuenta que, como se mencionó anteriormente, para poder utilizar esta función se requiere una versión de Windows Pro o superior. En el caso de que se esté utilizando una versión Home, existen otras opciones de software de cifrado disponibles en el mercado que pueden proporcionar una funcionalidad similar.



Para el laboratorio se guardo la recuperación en formato archivo .txt (imagen 9) y cuando se procede a continuar BitLocker comenzara a encriptar el disco como se observa en la imagen 10.



Cuando allá finalizado el proceso de encriptación se observarán cambios en los iconos de los discos seleccionados para encriptar (imagen 11).

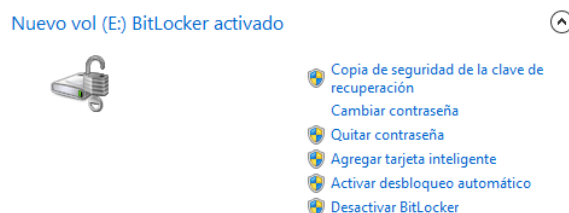
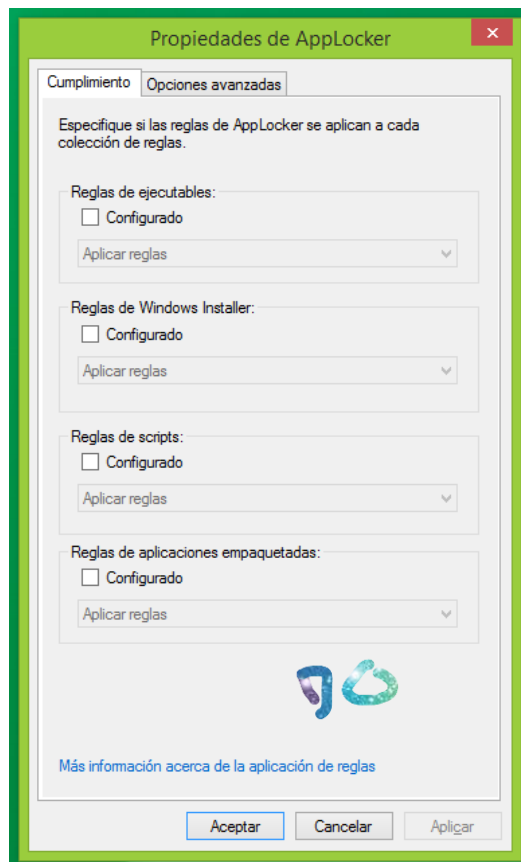
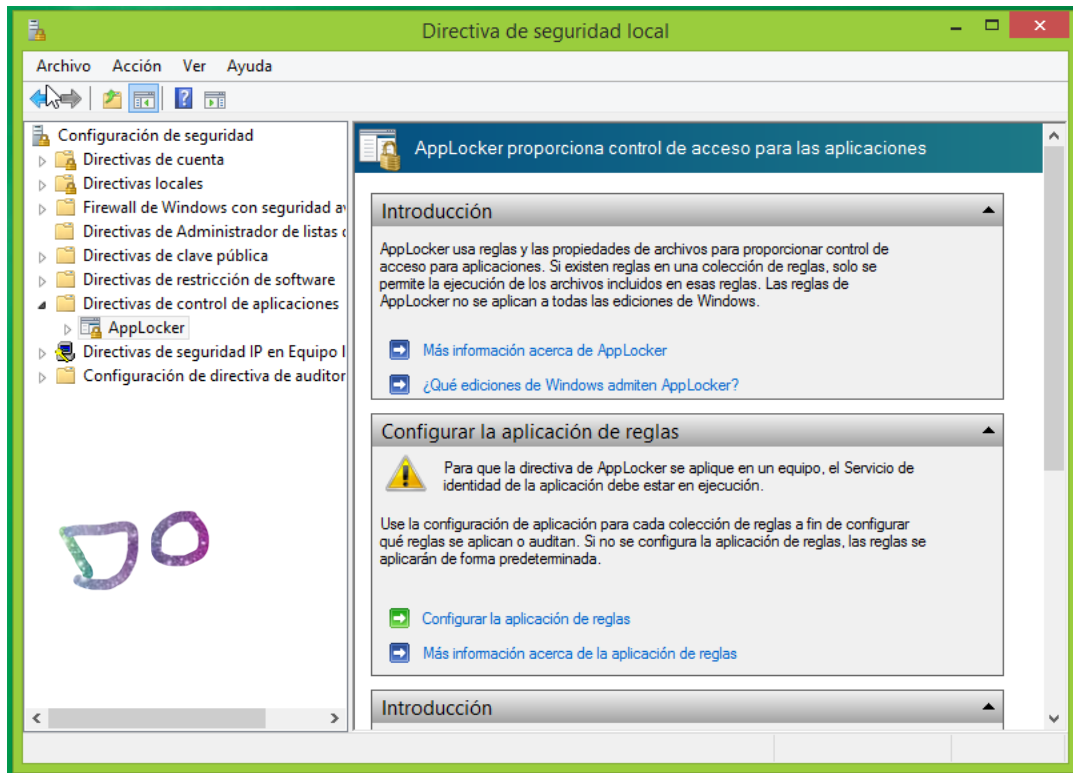


Imagen 1 Opciones de una unidad con encriptación BitLocker

Asimismo, BitLocker permite cifrar unidades extraíbles, como unidades flash USB o discos duros externos, lo que proporciona una forma segura de transportar información confidencial. También es posible configurar políticas de grupo para administrar y controlar el uso de BitLocker en una organización, lo que permite una implementación centralizada y consistente de la función de cifrado en toda la red de la empresa. En resumen, BitLocker es una herramienta útil y eficaz para proteger la información confidencial en sistemas operativos Windows.

- e) AppLocker es una herramienta muy útil para restringir el acceso a aplicaciones no autorizadas en un sistema, lo que puede ayudar a prevenir la ejecución de malware y otras amenazas de seguridad. Además, puede ser especialmente útil en entornos empresariales donde se necesita controlar el acceso a ciertas aplicaciones por parte de los empleados.

AppLocker permite configurar políticas de acceso a aplicaciones a nivel de usuario y a nivel de equipo, lo que permite a los administradores de sistemas controlar el acceso a aplicaciones en múltiples dispositivos. También es compatible con varios tipos de archivos, incluyendo archivos ejecutables, scripts y archivos de instalación de Windows Installer (MSI), lo que lo hace muy versátil en términos de su uso en diferentes entornos.



AppLocker proporciona un alto nivel de control sobre las aplicaciones que pueden ser ejecutadas en los dispositivos de la organización, lo que ayuda a proteger la red y los datos empresariales.




- f) Además de controlar el tráfico de red, el firewall también puede ser configurado para proteger el dispositivo contra ataques de red, como los ataques de denegación de servicio (DDoS), y para evitar que aplicaciones maliciosas se comuniquen con redes externas sin el conocimiento del usuario. En Windows, el firewall se puede configurar a través del Panel de Control o a través de la Configuración de Seguridad de Windows Defender en Windows 10. También existen herramientas de terceros que proporcionan características adicionales para el firewall de Windows.




Ayude a proteger su equipo con Firewall de Windows

Firewall de Windows ayuda a impedir que hackers o software malintencionado obtengan acceso al equipo a través de Internet o de una red.

[¿Cómo me ayuda un firewall a proteger mi equipo?](#)

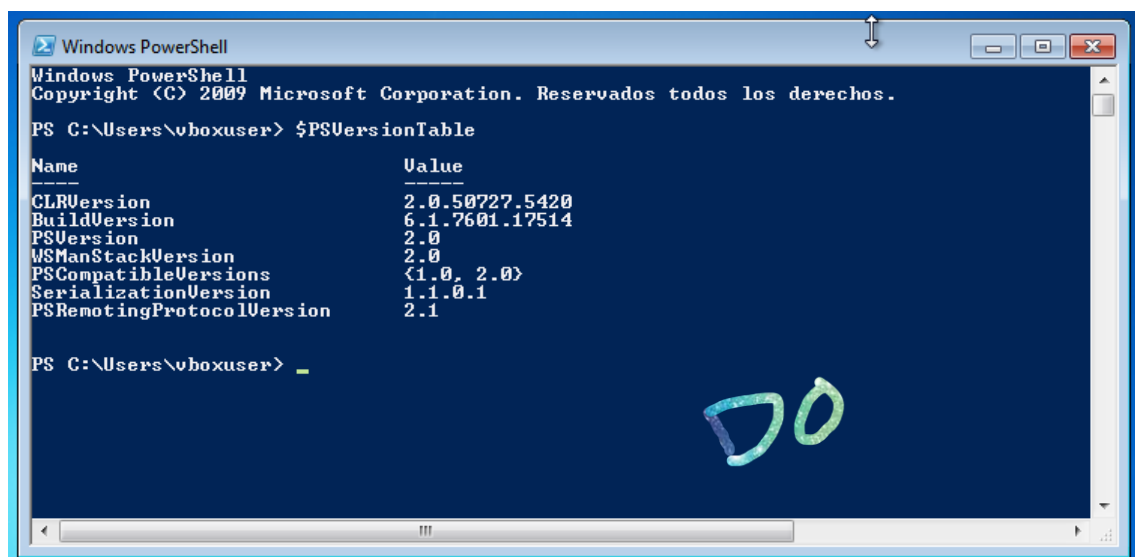
[¿Qué son las ubicaciones de red?](#)

	Redes domésticas o de trabajo (privadas)	No conectado ▼
	Redes públicas	Conectado ▲
Redes en lugares públicos como aeropuertos o cafeterías		
Estado de Firewall de Windows:		Activado
Conexiones entrantes:		Bloquear todas las conexiones a los programas que no estén en la lista de programas permitidos
Redes públicas activas:		 Red
Estado de notificación:		Notificarme cuando Firewall de Windows bloquee un nuevo programa

	Redes privadas	No conectado ▼
	Redes públicas o invitadas	Conectado ▲
Redes en lugares públicos como aeropuertos o cafeterías		
Estado de Firewall de Windows:		Activado
Conexiones entrantes:		Bloquear todas las conexiones a aplicaciones que no estén en la lista de aplicaciones permitidas
Redes públicas activas:		 Red
Estado de notificación:		Notificarme cuando Firewall de Windows bloquee una nueva aplicación

El Firewall de Windows también incluye opciones para configurar perfiles de red públicos y privados, lo que permite que las reglas del Firewall se adapten a diferentes entornos de red. Además, se pueden crear reglas personalizadas para permitir o bloquear el tráfico de red para aplicaciones específicas.

- g) DirectAccess es una función de red remota que permite a los usuarios remotos de una organización acceder de forma segura a los recursos de red internos sin necesidad de una VPN tradicional. DirectAccess establece una conexión segura y autenticada entre el dispositivo remoto y la red interna de la organización, lo que permite a los usuarios acceder a los recursos de la empresa de manera transparente y segura. DirectAccess utiliza tecnologías de cifrado y autenticación avanzadas para proteger la conexión y garantizar que solo los usuarios autorizados tengan acceso a los recursos de la red interna. Además, DirectAccess puede ser configurado para garantizar que los dispositivos remotos estén actualizados con las últimas políticas de seguridad antes de permitirles el acceso a los recursos de la red interna.
- h) PowerShell admite una amplia gama de comandos y funciones integrados, así como módulos adicionales que pueden ser agregados para ampliar su funcionalidad. También permite la comunicación con otros sistemas y herramientas, lo que lo convierte en una herramienta esencial para la administración de sistemas en un entorno empresarial.



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. Reservados todos los derechos.

PS C:\Users\vboxuser> $PSVersionTable

Name                           Value
----                           -
CLRVersion                     2.0.50727.5420
BuildVersion                    6.1.7601.17514
PSVersion                      2.0
WSManStackVersion              2.0
PSCompatibleVersions           {1.0, 2.0}
SerializationVersion          1.1.0.1
PSRemotingProtocolVersion      2.1
```

PS C:\Users\vboxuser> _

The screenshot shows a Windows PowerShell window with a dark blue background. The title bar reads 'Windows PowerShell'. The command prompt shows the user at 'PS C:\Users\vboxuser>'. The command '\$PSVersionTable' has been executed, resulting in a table of version information. The table has two columns: 'Name' and 'Value'. The rows include CLRVersion, BuildVersion, PSVersion, WSManStackVersion, PSCompatibleVersions, SerializationVersion, and PSRemotingProtocolVersion. There is a large, stylized 'DO' watermark in the bottom right corner of the window.

CONCLUSIONES

- La reproducción automática puede ser conveniente para algunos usuarios, pero también presenta un riesgo de seguridad si se conecta un dispositivo infectado con malware o virus.
- La integración de dispositivos biométricos a través de Windows Biometric Framework (WBF) puede mejorar la seguridad y la experiencia de usuario en aplicaciones que requieren autenticación biométrica.
- BitLocker proporciona una forma de cifrar completamente la unidad de disco duro para proteger la información almacenada en ella contra el acceso no autorizado.
- AppLocker permite a los administradores de sistemas crear políticas de seguridad que permiten o bloquean el acceso a las aplicaciones según reglas previamente configuradas para proteger la red y los datos empresariales.
- PowerShell es una herramienta poderosa que permite a los administradores de sistemas realizar tareas de administración y automatización de forma más rápida, eficiente y con menos errores.

En general, estas características de seguridad son herramientas valiosas para proteger la red y los datos empresariales contra amenazas conocidas y desconocidas. Sin embargo, es importante tener en cuenta que la implementación adecuada de estas herramientas es crucial para garantizar su eficacia. Además, los usuarios y administradores de sistemas deben estar capacitados para utilizar estas herramientas de manera efectiva para maximizar su potencial y minimizar los riesgos de seguridad.

REFERENCIAS

- <https://www.xataka.com/basics/uac-windows-que-como-funciona-como-se-configura-control-cuentas-usuario>
- https://www.muycomputer.com/2009/07/22/zona-practicapaso-a-pasoapplocker-bloquea-programas_we9erk2xxdc4vxtz8n8mtc4xrlqdlbmnsllcu4avq0twdhrxuy15cqegnyna7ahr
- <https://blog.soporteti.net/introduccion-a-directaccess>