TRABAJO DE FÍN DE TÍTULO

GRADO EN INGENIERÍA INFORMÁTICA – TECNOLOGÍAS DE LA INFORMACIÓN

ESTUDIO DE MEDIDAS Y HERRAMIENTAS DE SEGURIDAD Y SU CONFIGURACIÓN EN WINDOWS 10

Autor: Omaro Efraín Vega González

Tutor: Francisco Alayón Hernández

Septiembre 2020

ULPGC Universidad de Las Palmas de Gran Canaria | Escuela de Ingeniería Informática

AGRADECIMIENTOS

Primero, a mi madre, hermanos y familia al completo. Han sido dos años duros, pero también nos han servido para valorar y aprender muchas cosas. Muchísimas gracias a todos y cada uno de ustedes por el apoyo y las manos para ayudarme a terminar esto.

Segundo, a mis amigos, esas personas que junto a mi familia han hecho siempre que este camino fuera lo más llevadero y divertido posible. Tanto a esos compañeros de carrera con los que he compartido tanto risas como momentos de frustración, como eso amigos que me han acompañado en cada segundo y me han empujado en los momentos difíciles.

Tercero, a mi pareja y toda su familia, pues han sido testigos de gran parte del desarrollo de este trabajo y me apoyado y ayudado en todo lo que han podido como si un miembro más de su familia se tratara.

Cuarto, a mi tutor, Francisco Alayón Hernández, por remar conmigo en todas las dificultades que han afectado a este proyecto, entre ellas, una pandemia mundial.

Quinto, y esta vez más importante, a ti papá. Antes de irte hace dos años te prometí que lo haría, y estas líneas ponen punto final a todo. Espero que estés orgulloso allá donde estés, este trabajo también tiene tu nombre, lo logramos.

RESUMEN

Cada vez existen más cantidad de usuarios que hacen uso de sistemas informáticos como los ordenadores. Además, haciendo uso de estos para gestiones delicadas como puedan ser pagos con tarjetas, transacciones bancarias, correo electrónico, etc.

Esto supone un amplio vector de ataque para cibercriminales que quieran aprovecharse de la posible falta de conocimientos del usuario medio.

Se ha realizado un trabajo de investigación para averiguar posibles ataques comunes y las diferentes opciones de configuración que nos ofrece Windows 10 en su sistema operativo para defender los ordenadores de estos.

Se propone como un manual explicativo para todo tipo de usuarios, a fin de concienciar y ayudar a la hora de que el mayor número de personas tengan sistemas un poco más seguros.

ABSTRACT

There are more and more users who use computer systems such as computers. In addition, making use of these for delicate procedures such as card payments, bank transactions, email, etc.

This is a broad vector of attack for cybercriminals who want to take advantage of the possible lack of knowledge of the average user.

A research work has been carried out to find out possible common attacks and the different configuration options that Windows 10 offers us in its operating system to defend computers from them.

It is proposed as an explanatory manual for all types of users, in order to raise awareness and help when the greatest number of people have slightly safer systems.

CONTENIDO

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

1. INTRODUCCIÓN

1.1. ESTADO DEL ARTE

En la actualidad, nos encontramos con un escenario en el que el porcentaje de hogares con al menos un ordenador personal según nos indica Statista[1] es de 49.7% a nivel mundial, pero si, además, nos centramos únicamente en países desarrollados esa cifra asciende a un 82.3% en 2019[2]. Si queremos contextualizar un poco más estos datos a un entorno más cercano, en España esta cifra es del 49.7%.

Además, el porcentaje de uso de sistemas operativos lo ocupa en su gran mayoría Windows con un 77.1% seguido por OS X con un 18.34%[3]. Si a estos datos le añadimos que además el uso de sistemas Windows 10 con respecto al resto de SO de Microsoft es del 70.98% hace que sea bastante representativo la existencia de este documento sobre seguridad en el mismo.

La cantidad de personas conectadas a la red es cada vez mayor. Esta afirmación tiene, como todo, su connotación buena y mala. Pero vamos a centrarnos en la mala o, al menos, peligrosa y delicada para el usuario. Y es que cada vez existen más usuarios con ordenadores personales y acceso a Internet que comparten sus datos, realizan transacciones bancarias, compras y realizan muchas acciones de carácter comprometido en un entorno que muchas veces creen seguro y se ha visto comprometido.

Este documento recoge, a modo de manual, una serie de configuraciones para varios estadios posibles y diferentes opciones de configuraciones para los mismos para intentar conseguir el entorno más seguro posible para la realización de las funciones que necesiten.

1.2. MOTIVACIÓN

Como estudiante de la mención de Tecnologías de la información recibo cierta formación en seguridad con dos asignaturas dedicadas explícitamente a ello, aunque, la segunda no sea a efectos prácticos dedicada a seguridad sino enfocada desde el punto de vista legal de la seguridad informática.

También se nos forma en otras asignaturas como puede ser SSR o "servicios y seguridad en red", pero, todos los enfoques se realizan siguiendo la política de uso de software libre que se sigue como tónica general en todo el grado y centrando el conocimiento casi en su totalidad en distribuciones del sistema operativo Linux.

Eso nos lleva al punto de querer investigar sobre las diferentes herramientas y opciones de seguridad que nos proporciona el sistema operativo que lidera la cuota de mercado a nivel mundial y que a su vez es la que recibe mayor número de ataques por motivos obvios, como es Windows 10.

1.3. OBJETIVOS

Partiendo de la base que la seguridad máxima es un estado utópico o al menos muy costoso en comparación con el rendimiento que obtenemos. Se pretende seguir una investigación sobre diferentes medidas que nos permite configurar Microsoft en su sistema operativo Windows 10 para conseguir la mejor configuración de seguridad en los siguientes estadios posibles:

- **Maquina blindada**

  Esta máquina se considera en un utópico estado de máxima seguridad, siempre entendiendo que no podemos lograr el 100%.

  Máquina completamente aislada, sin acceso a Internet, ni ningún uso para usuarios. La información alojada en esta máquina solo debe ser accesible para un administrador.

  Esta máquina se usará como base para el resto, es decir, se creará esta configuración, y luego se comenzarán a abrir puertas para el uso determinado en cada caso.

- **Máquina para uso regular de un usuario con acceso ofimático e Internet.**

  Esta máquina simulará el estado de un sistema usado regularmente por un usuario estándar que hace uso de paquetes ofimáticos, acceso a Internet, uso de correo electrónico, y si se encuentra en un entorno profesional, acceder a recursos compartidos.

- **Máquina para uso regular accesible en remoto por un administrador.**

  Esta máquina se considera similar a la anterior, es decir, tendrá acceso a Internet, uso de correo electrónico y acceder a recursos compartidos. Pero con las facilidades para que un administrador pueda acceder de manera remota a la máquina.

  Podría entenderse, como una posible configuración para una estación en un puesto de trabajo donde un administrador de sistemas deba acceder de manera remota a algún equipo para resolver incidencias. Desde la misma red o desde otra red haciendo uso de VPN.

- **Máquina para el uso de un desarrollador.**

  Esta máquina contempla un estadio donde un sistema deba tener ciertos servicios disponibles para hacer pruebas. Como pueda ser, tener un servidor Apache o NPM server.

  Además, debe tener la posibilidad de hacer uso control de versiones, tanto en un servidor local con Git, como una versión online como pueda ser Git+Github o Bitbucket.

Se entiende esta máquina como un entorno con las accesibilidades básicas para un posible entorno de trabajo. Entonces, también deberá tener acceso a recursos en Internet, acceso a correo electrónico y a posibles recursos compartidos en red como impresoras o archivos.

Todo esto, desde un punto de vista y lenguaje entendible por el mayor número de personas posibles, ya sean entendidas en la materia o no. Con el objetivo de concienciar a las mismas de lo importante que es la seguridad informática en sus equipos y como aplicar las diferentes configuraciones de la manera más accesible posible.

2. JUSTIFICACIÓN DE LAS COMPETENCIAS ESPECÍFICAS CUBIERTAS

Finalizar el Grado en Ingeniería informática conlleva una serie de competencias generales recogidas en el RD 1393/2007, así como unas competencias nucleares recogidas por la Universidad de Las Palmas de Gran Canaria (ULPGC) y las competencias propias del título recogidas en el Anexo II de la Resolución de 8 de junio de 2009, de la Secretaría General de Universidades (BOE de 4 de agosto de 2009), entre las que se encuentran las competencias básicas comunes a la Ingeniería Informática y las competencias específicas de las intensificaciones.

2.1. CII01

"Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente."

Para el desarrollo de los diferentes estadios de los que consta el trabajo, se han estudiado y seleccionado una serie de técnicas y recursos, que nos llevaran a crear diferentes configuraciones de sistemas informáticos fiables, seguros y que cumplen unos mínimos de calidad aceptables.

2.2. CII05

"Conocimiento, administración y mantenimiento sistemas, servicios y aplicaciones informáticas."

Durante el desarrollo de este trabajo se han adquirido conocimientos, así como reforzado otros sobre el mantenimiento de sistemas basados en el sistema operativo Windows 10. Esto se debe principalmente al profundo estudio que se ha tenido que realizar en las opciones que nos ofrece Microsoft en su sistema operativo de cara a la seguridad.

2.3. CII10

"Conocimiento de las características, funcionalidades y estructura de los Sistemas Operativos y diseñar e Implementar aplicaciones basadas en sus servicios."

El profundo estudio que se ha realizado para llevar a cabo este proyecto, así como las pruebas de ataques y defensas y la implementación de medidas de seguridad que ofrece Microsoft en su sistema operativo Windows 10. Ha llevado a un mejor conocimiento de muchas de sus características y funcionalidades y como usar las mismas para ofrecer mejores opciones de seguridad.

2.4. TI01

"Capacidad para comprender el entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones."

Si bien es cierto que este trabajo se presenta en su mayoría como un documento orientado a un entorno personal, se ha estudiado y planteado opciones que pueden ser aplicables en entornos empresariales. Además, se han adaptado medidas que se aplican en un entorno empresarial para aplicarlas en sistemas que no dependan de una gestión centralizada.

2.5. TI03

"Capacidad para emplear metodologías centradas en el usuario y la organización para el desarrollo, evaluación y gestión de aplicaciones y sistemas basados en tecnologías de la información que aseguren la accesibilidad, ergonomía y usabilidad de los sistemas."

En el desarrollo de este proyecto, no solo se ha pensado en obtener la seguridad máxima disponible o aceptable. También se ha pensado en qué aplicar a cada escenario para que la experiencia de usuario en el uso del sistema sea la mejor posible dentro de las capas de seguridad añadidas.

2.6. TI07

"Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos."

Durante el desarrollo de este proyecto, se ha indagado en innumerables opciones, herramientas y posibilidades de las que disponemos en los sistemas informáticos Windows 10. Esto ha permitido comprenderlo en profundidad para lograr los estados de seguridad esperados en la definición de los estadios.

2.7. TFG01

"Ejercicio original a realizar individualmente y presentar y defender ante un tribunal universitario, consistente en un proyecto en el ámbito de las tecnologías específicas de la Ingeniería en Informática de naturaleza profesional en el que se sinteticen e integren las competencias adquiridas en las enseñanzas."

Teniendo en cuenta el gran marco teórico e investigativo que posee este proyecto, engloba una buena parte de aprendizaje, así como síntesis de información para luego poder aplicarla. Pero esta no podrá haber sido entendida ni aplicada sin todos los conocimientos previos adquiridos en el grado. Además de enfoques que se tomaron en la investigación están basados en los conocimientos adquiridos gracias a asignaturas impartidas en el grado.

3. APORTACIONES

Desde un punto de vista personal indiscutiblemente me ha aportado conocimientos nuevos sobre el sistema operativo Windows 10 de Microsoft y también algunos conocimientos aplicables a versiones previas a este sistema operativo como pueden ser Windows 8.1, 8 o 7.

Como efecto colateral, se han adquirido conocimientos asociados a Windows Server y Active Directory, pues mucha información que se encuentra está destinado a redes empresariales con control centralizado y se han tenido que adaptar a las configuraciones disponibles en Windows 10 de manera local.

Además, ha generado inquietudes fuera del nivel técnico. Estas inquietudes se refieren a la manera en la que uso mis equipos personales que usan Windows 10 como sistema operativo. No lo considero inquietudes técnicas, aunque comprendan medidas técnicas para solucionarlas. Estas se refieren a cosas que no tenía en cuenta a la hora de usar mi sistema operativo Windows 10 que he visto interesantes como puede ser el uso del cifrado BitLocker para cifrar el disco duro de mi equipo portátil personal o la desactivación de la opción para compartir mis datos de navegación para la publicidad personalizada.

Por otro lado, como estudiante de una carrera técnica, es bien sabido que la redacción no es el fuerte de las personas de nuestro perfil. La realización de la memoria correspondiente a este proyecto y la adaptación del lenguaje y la redacción a un lenguaje más neutro y menos técnico ha permitido mejorar esas habilidades no tan desarrolladas en mí.

4. PLANIFICACIÓN

4.1. PLANIFICACIÓN DEL PROYECTO

El tiempo de desarrollo estimado de este proyecto que se propuso se vio notoriamente afectado principalmente por dos factores. El primero, la pandemia mundial, Covid-19, que provocó grandes retrasos durante el proceso debido a que se tuvo que modificar la infraestructura de virtualización y tuvo que crearse un servidor ftpes para que el tutor de este proyecto pudiera tener acceso a las máquinas. Además, psicológicamente afecto al rendimiento general y en consecuencia a su avance.

Por otro lado, la estimación del tiempo de realización de la memoria no fue el adecuado, pues, conforme se fue realizando el enfoque fue cambiando hacia un manual de usuario accesible para todo tipo de usuarios, con el objetivo de ayudar al mayor número de personas.

Fases	Duración estimada (horas)	Tareas
Estudio previo / Análisis	40	Tarea 1.1: Estudio de los manuales ofrecidos por Microsoft
		Tarea 1.2: Búsqueda y estudio de recursos externos como libros, foros, artículos, etc.
Diseño / Desarrollo / Implementación	135	Tarea 2.1: Localización de las vulnerabilidades que queremos cubrir
		Tarea 2.2: Configuración de las diferentes medidas en Windows para cubrir las vulnerabilidades
Evaluación / Validación / Prueba	95	Tarea 3.1: Realización de los diferentes ataques para comprobar la integridad
		Tarea 3.2: Mejoras y cambios deducidos tras las pruebas de ataques
Documentación / Presentación	30	Tarea 4.1: Elaboración de la memoria
		Tarea 4.2: Preparación de la presentación del TFT

Tabla 1. Planificación inicial

Fases	Duración real aproximada (horas)	Tareas
Estudio previo / Análisis	60	Tarea 1.1: Estudio de los manuales ofrecidos por Microsoft
		Tarea 1.2: Búsqueda y estudio de recursos externos como libros, foros, artículos, etc.
Diseño / Desarrollo / Implementación	180	Tarea 2.1: Localización de las vulnerabilidades que queremos cubrir
		Tarea 2.2: Creación de máquinas virtuales
		Tarea 2.3: Configuración de las diferentes medidas en Windows para cubrir las vulnerabilidades
		Tarea 2.4: Creación y configuración de servidor ftpes
Evaluación / Validación / Prueba	120	Tarea 3.1: Realización de los diferentes ataques para comprobar la integridad
		Tarea 3.2: Mejoras y cambios deducidos tras las pruebas de ataques
Documentación / Presentación	70	Tarea 4.1: Elaboración de la memoria
		Tarea 4.2: Preparación de la presentación del TFT

Tabla 2. Planificación real

4.2. ESTRUCTURA DEL DOCUMENTO

Este documento se presenta como memoria para el trabajo de fin de grado realizado y está dividido en siete capítulos, cuyo contenido se resume a continuación:

- El primero de ellos es la introducción, donde se pone en contexto la situación en la que se crea este proyecto. Además, se explica la motivación por crear el mismo y se indican los objetivos que se quieren alcanzar en el proyecto.
- El segundo capítulo engloba las competencias cubiertas y la justificación.
- El tercer capítulo se centra en las aportaciones personales que ha generado la realización de este proyecto.
- En el cuarto capítulo se presenta las tablas con la correspondiente planificación inicial, así como una tabla con los tiempos reales corregidos con respecto a los estimados iniciales.
- El quinto capítulo se centra en englobar los recursos que se usaron para la realización de este proyecto, desde los recursos físicos como los equipos informáticos usados, como los servicios que se usaron para alcanzar los objetivos.
- En el sexto punto se incluye el grueso de este proyecto, por un lado, se definen las opciones y servicios ofrecidos por Windows para ayudarnos a crear un sistema más seguro. Por otro lado, se explican ciertos ataques que puede recibir un sistema y como crear defensas ante ellos, y configuraciones extras que añaden más seguridad preventiva.

- En el séptimo punto se expresan las conclusiones a las que se ha llegado tras la finalización del proyecto, así como futuras mejoras que pueda tener el mismo en otras líneas de trabajo en el futuro.

A este contenido, se le añade un punto final que engloba toda la bibliografía consultada para la realización de este proyecto.

5. RECURSOS UTILIZADOS

5.1. SISTEMA UTILIZADO

Durante el desarrollo de este proyecto se usaron dos ordenadores como hosts de las máquinas virtuales. Esto sucedió porque en primera instancia, se quiso usar un ordenador portátil con Ubuntu para trabajar con el hipervisor KVM y para que fuera más accesible a la hora de trabajar con el tutor y poder enseñarle el trabajo en persona. Posteriormente, y con la situación provocada por el Covid-19, se optó por usar un equipo sobremesa con sistema operativo Windows 10 haciendo uso de VirtualBox para que existiera mayor compatibilidad entre el equipo del tutor y los que yo tenía disponibles.

El ordenador portátil, se trata de un HP Omen modelo 15-ce005ns, que consta de las siguientes especificaciones:

- CPU: Intel Core i7-7700HQ (4 núcleos (8 hilos), frecuencia 2.8-3.8 GHz, 6MB de caché)
- RAM: SDRAM de 2x8GB DDR4-2400
- HDD: SATA de 1TB a 7200rpm + SSD de 128GB PCIe NVMe M.2
- Tarjeta gráfica: NVIDIA GeForce GTX 1050 4GB GDDR5

El ordenador sobremesa, se trata de un ordenador clónico montado por piezas, que consta de las siguientes especificaciones:

- CPU: Intel Core i5-4670K (4 núcleos (8 hilos), frecuencia 3.4-3.8 GHz, 6MB de caché)
- RAM: 4x4GB DDR3-1600
- HDD: SATA de 1TB a 7200rpm + SSD de 250GB SATA
- Tarjeta gráfica: AMD Radeon R9 200 Series 3GB GDDR5

5.2. VIRTUALIZACIÓN

Para la realización de este proyecto de investigación y para que fuese un trabajo efectivo, se construyó un entorno basado en la virtualización, en el que trabajar y realizar todas las pruebas para comprobar las diferentes configuraciones para los estadios que queríamos construir.

Esto fue necesario debido a la necesidad de disponer de varias configuraciones o simulaciones de ordenadores reales para los cuales no había medios físicos ni económicos para poseerlos. Se optó por hacer uso de la virtualización para recrear los diferentes estados previstos, además de poseer un entorno donde poder realizar todo tipo de pruebas e investigación sin riesgo de estropear una máquina física.

5.2.1. ¿QUÉ ES LA VIRTUALIZACIÓN?

Si nos referimos a virtualización en el contexto de la informática, según VMware[4], podríamos entender la virtualización como una abstracción de recursos (ordenadores personales, servidores, redes, almacenamiento, etc.) basada en software. Es decir, emular la existencia de ciertos recursos que, durante su uso, no genere diferencias aparentes si se compara con un recurso real. Se puede entender por virtualización también, cosas tan simples como una partición de disco duro que genera dos discos duros virtuales o más, partiendo de uno físico.

La virtualización en nuestro caso tiene sentido porque nos permite crear varios entornos de pruebas aislados en los que recrear las diferentes configuraciones sin que unas se vean afectadas por otras. Pero, la principal ventaja en este proyecto es las posibilidades de recreación de diferentes sistemas que no serían posibles adquirir de manera física.

5.2.2. VENTAJAS DE LA VIRTUALIZACIÓN

Si se mira desde el punto de vista de los servidores, hay análisis que demuestran que, junto con los equipos de escritorio, tan solo se usan entre un 8-15% del tiempo que están encendidos[5]. Haciendo uso de la virtualización se podría llegar a cargas superiores al 50% de uso, virtualizando varios servidores en una misma máquina para aprovechar su potencia.

Permite una mayor facilidad para la creación de entornos de pruebas. Por ejemplo, para emular distintos tipos de configuraciones hardware y probar software sin disponer físicamente de esos recursos.

Además, proporciona aislamiento. En el caso que compete a este trabajo, permite tener entornos de pruebas aislados para que posibles fallos o problemas de seguridad no hagan que se vean afectados entre ellos.

Si se ve desde un punto de vista económico, permite tener a disposición del usuario, simulaciones de diferentes maquinas simultaneas o hardware específico del que no se pueda disponer por accesibilidad o economía. Además, permite reducir costes en software comercial que limite su uso por CPU. Se puede pagar una única licencia que se instala en una máquina física pero que aloja varias máquinas virtuales.

5.2.3. DESVENTAJAS DE LA VIRTUALIZACIÓN

Si se puntualizan ciertos aspectos negativos que se pueden observar en los sistemas virtualizados, se puede indicar que el sistema operativo virtualizado tiene un rendimiento inferior si comparamos el mismo sistema operativo instalado directamente en una máquina física. Además, el rendimiento gráfico está limitado en sistemas virtualizados.

El hardware que se puede utilizar está limitado por el que sea soportado y que permita la gestión de este por parte del software de virtualización que se vaya a utilizar.

Posiblemente el factor más crítico sería, que si existe una avería en la máquina física que hace de sistema de virtualización afectará a todas las máquinas virtuales que este aloje, pudiendo ser estado nefasto debido a la cantidad de servicios que podrían quedar inutilizados.

5.2.4. TIPOS DE VIRTUALIZACIÓN

Los tipos de virtualización se pueden englobar en dos grandes campos que son la virtualización de recursos, y la posiblemente más conocida, virtualización de plataforma.

5.2.4.1. VIRTUALIZACIÓN DE RECURSOS

- **Memoria virtual:**

Se trata de una técnica usada por los sistemas operativos gracias a la cual se genera una memoria de trabajo contigua para las aplicaciones, cuando en realidad esta está fragmentada e incluso alojada en el disco duro en lugar de en la memoria RAM.

- **Virtualización de almacenamiento:**

Se considera virtualización de almacenamiento a la abstracción del almacenamiento, como ocurre con las particiones de disco duro donde podemos emular varios discos a partir de uno solo. O incluso, un sistema RAID donde varios discos duros se representan como uno sólo.

- **Virtualización de red:**

Se da en situaciones enfocadas a la seguridad en las que los recursos de red a nivel de hardware o software se abstraen del recurso físico. Bien porque se quiera agrupar los recursos físicos haciendo uso de una unidad lógica virtual o porque se quiera dividir los recursos físico de red.

Dos ejemplos claros serían las conexiones VPN que usa una red virtual basada en una red física. Y las redes VLAN que se tratan de subredes virtuales basadas en una red física.

- **Unión de canales de Ethernet:**

Configuración mediante la cual, varias interfaces de red Ethernet que se encuentren en una máquina, se usan como una sola para obtener redundancia o aumentar la velocidad.

5.2.4.2. VIRTUALIZACIÓN DE PLATAFORMA

- **Parcial:**

En este tipo de virtualización se virtualiza la mayoría del Hardware. Permite compartir recursos y aislar procesos, pero al no hacer posible la existencia de varias instancias simultaneas de SO (sistema operativo) invitados, no se identifica realmente como MV.

- **Nativa:**

El software de virtualización llamado hipervisor virtualiza el hardware suficiente para permitir que un SO invitado que ha sido diseñado para la misma CPU, o al menos comparte el mismo repertorio de instrucciones que tiene el host, se pueda ejecutar de forma aislada. Permite la ejecución de varias instancias al mismo tiempo.

- **Emulación o simulación:**

En estos dos casos, se trata de virtualizar un sistema con una CPU muy diferente a la del sistema host. Permite, por ejemplo, crear software para nuevos procesadores antes de que estos se encuentren disponibles físicamente, y naturalmente, no permite hacer uso de la virtualización por hardware.

- **Virtualización a nivel de sistema operativo:**

Las máquinas virtuales comparten sistema operativo con el host, siendo el propio kernel el que implemente las funciones del hipervisor. Las aplicaciones que corren en el interior de la máquina virtual siguen viéndola como un sistema autónomo.

- **Paravirtualización:**

El hipervisor ofrece una API especial (hypercalls), usable en sistemas operativos invitados que han de ser modificables para poder introducirle el paso de instrucciones.

Esto permite que el hipervisor sea menos complejo, y hace posible que el sistema operativo invitado se optimice para la virtualización, al éste ser de algún modo

consciente de que es una máquina virtual. Suele ser un tipo de virtualización muy rápida.

5.2.5. ¿POR QUÉ KVM?

Todos los posibles estadios se implementaron en máquinas virtuales alojadas en KVM (Kernel-based Virtual Machine) que se trata de un módulo de virtualización en el kernel de Linux que le permite funcionar como hipervisor de tipo 1 o nativo.

Para suplir las necesidades que existen para la realización de este proyecto, se decidió escoger KVM como hipervisor para alojar las máquinas virtuales.

KVM[6] es una solución de virtualización completa en la que se usa el kernel de Linux como hipervisor, esto quiere decir, que tanto el control de dispositivos reales como la planificación de tareas y la gestión de memoria del sistema host las hace el núcleo de Linux. Al tratarse de un hipervisor de tipo nativo, su ejecución se realiza directamente en el hardware del equipo pues forma parte del núcleo de Linux desde la versión 2.6.20.

5.2.6. ¿POR QUÉ VIRTUALBOX?

VirtualBox o Oracle VM VirtualBox es un hipervisor propiedad de Oracle Corporation. Dispone de dos versiones, una open source llamada VirtualBox OSE (Open Source Edition) bajo licencia GPLv2 y una versión privativa gratuita sujeta a la "VirtualBox Personal Use and Evaluation License" o PUEL.

Se trata de un hipervisor de tipo 2 o no nativo que se caracterizan por ejecutarse sobre el sistema operativo de la máquina que lo aloja.

Ante la situación vivida por la pandemia COVID-19 en el presente del desarrollo de este proyecto, se generó cierta dificultad que tuvo que ser solventada haciendo uso de virtualización en un sistema operativo Windows en lugar de en uno Linux como se planteó en inicio.

Esto se debió a que en primera instancia se iban a generar las máquinas en un entorno Linux bajo un hipervisor de tipo 1 como KVM pues ofrece un mejor aprovechamiento de recursos. Pero, ante la imposibilidad de hacer reuniones en persona al estar en un confinamiento, se decidió crear nuevamente las máquinas virtuales haciendo uso de VirtualBox, pues se consideró que era la herramienta que mejor se adaptaba a las posibilidades que tenía tanto el alumno como el tutor para ambos poder ejecutar las máquinas virtuales de cara a seguimiento y comprobaciones.

5.3. FTPES

Partiendo de la premisa que el protocolo de transferencia de archivos FTP realiza tanto la transmisión de las credenciales de acceso como la transferencia de datos sin ningún tipo de cifrado. Se añadió una nueva capa de seguridad haciendo uso de SSL/TLS sobre el protocolo FTP para crear FTPS y FTPES, también conocido este conjunto

como FTP over TLS/SSL. Esta capa extra soluciona el problema de confidencialidad en la autenticación y en la transferencia de datos que existe en FTP.

FTPS es conocido como FTPS implícito y se trata de una mejora antigua aplicada sobre FTP para proporcionar seguridad y privacidad al mismo. FTPS hace uso de un puerto diferente al 21 estándar en FTP para realizar la conexión. En este caso, usa el puerto 990 TCP para la conexión y el 989 para el canal de datos. Antes de que se haga ningún intercambio de información con el servidor FTP, se realiza la negociación TLS/SSL asegurando todo el canal de comunicación, que implica la autenticación y la transferencia de archivos asegurada por TLS.

FTPES también conocido como FTPS explícito, se trata de una mejora más moderna y es el protocolo que se usa actualmente cuando se quiere activar la seguridad en FTP. Como su propio nombre indica, el cliente FTPS solicita explícitamente seguridad en el servidor. En primera instancia, si el cliente está configurado para requerir obligatoriamente seguridad, el cliente FTPES se conecta al servidor FTP a través del puerto 21, establecerá una comunicación cifrada con TLS antes de realizar la autenticación y transferir ninguna información. El protocolo FTPES no requiere ningún puerto adicional abierto, ni en el servidor ni en el cliente, FTPES hace uso del puerto TCP 21 para el control y un puerto aleatorio entre cierto rango configurado para transferir la información.

6. DESARROLLO

En este apartado se engloba todo el grueso del proyecto, determinado por el planteamiento y la organización de este desde el punto de vista metodológico, así como las opciones que nos proporciona Windows. Por otro lado, se encuentran definidas y explicadas todas las configuraciones a usar y como aplicarlas.

6.1. METODOLOGÍA

La metodología seguida para la realización de este proyecto es la llamada metodología Waterfall. Se trata de un proyecto de investigación que no tiene entregas parciales a corto plazo, y, en el cual no se puede paralelizar el trabajo dividiéndolo en tareas al realizarlo una sola persona, como podría suceder con la metodología Agile.

En este proyecto se recopilaron una serie de requisitos al inicio de este que dejaron claro el flujo de trabajo que había que seguir para poder desarrollarlo de la mejor manera posible. Esto hace que el progreso se mida con facilidad debido a que se conoce de antemano las fases y el alcance de estas.

El trabajo se completó siguiendo unas fases que se tendrían que completar antes de seguir con las siguientes, haciendo del progreso del proyecto entregas de tareas completadas secuencialmente.

Las pruebas del proyecto fue la fase realizada en última instancia tras todas las fases previas de creación de escenarios, investigación y selección de recursos lo cual encaja con la metodología Waterfall.

La metodología Waterfall es una metodología buena para proyectos que tengan un alcance fijo y se posea un tiempo y un presupuesto inalterable. Esto encaja con este proyecto, ya que, aunque el tiempo no era inalterable si se construyó la organización del proyecto pensando en encajarlo en un número de horas predefinido y fijo.

6.1.1. DINÁMICA LLEVADA A CABO CON EL PROYECTO

Al tratarse de un proyecto de investigación, se comenzó con un fuerte proceso de búsqueda de información para establecer primero de qué se quería hablar y segundo qué ese iba a contar al respecto.

Posteriormente continuó el proceso de preparación de escenarios en los que se iba a trabajar. Esto consistió en crear una partición Ubuntu en mi ordenador personal y la instalación del paquete KVM. Una vez aquí y teniendo todo el entorno listo se procedió a crear todas las máquinas virtuales correspondientes a los escenarios haciendo uso de una ISO de Windows 10 pro en 64 bits.

A continuación, comenzó el proceso de investigación para hacer uso de las opciones de configuración que nos ofrece Microsoft en su sistema operativo.

En este momento, se procedió a experimentar en una máquina virtual auxiliar posibles ataques y soluciones a los mismos para ordenarlos y considerar si añadir dichas defensas a las máquinas finales.

Con las pruebas realizadas se procedió a configurar las defensas y correspondientes pruebas con las 4 máquinas que representan los 4 sistemas objetivo que se definen en el punto 1.3

Tras tener todo debidamente configurado, se procedió a crear la documentación centrada en la concienciación de las amenazas y aplicación de defensas contra las mismas.

En definitiva, la dinámica llevada a cabo se centró en un ciclo de investigación – aplicación – documentación que se repitió en tres iteraciones centradas respectivamente en ataques, seguridad adicional y protección contra Windows.

6.1.2. CREACIÓN DE ESCENARIOS

Para la creación de los diferentes escenarios se optó por hacer uso de máquinas virtuales que permitieran la flexibilidad suficiente para tener cuatro escenarios diferentes en un solo sistema físico.

Todas las máquinas se crearon partiendo de un disco ISO de Windows 10 en su versión PRO de 64 bits y todas fueron instaladas con la configuración por defecto y actualizadas a la última versión disponible en el momento de la instalación

Los cuatro escenarios se establecieron y crearon en base a ciertos perfiles que se creyeron interesantes en el momento de definir y comenzar este proyecto. Estos perfiles son:

- **Máquina blindada.**
- **Administrador de sistema.**
- **Usuario base.**
- **Programador.**

6.2. HERRAMIENTAS DE SEGURIDAD PROPORCIONADAS POR EL SISTEMA OPERATIVO WINDOWS 10

En este bloque, se clasifican y definen las diferentes herramientas que nos proporciona Windows para proteger su sistema y que han sido usadas en este proyecto para añadir seguridad añadida a la seguridad por defecto configurada por Microsoft en su sistema Windows 10.

6.2.1. FIREWALL DE WINDOWS DEFENDER

La definición de cortafuego o "firewall" en inglés, originariamente se refiere a una estructura que debe limitar la propagación del fuego en un espacio determinado y mitigar los posibles daños en los humanos y sus posesiones.

En el ámbito de la informática, un cortafuego se define como un sistema de seguridad de la red basado en software, o hardware que limita el acceso a través del propio cortafuego. Aporta seguridad en la puerta de acceso de comunicación entre redes de confianza y redes inseguras. Decide qué tráfico pasa a través de él en función a un conjunto de reglas configuradas en el mismo.

Los cortafuegos se pueden clasificar en dos grandes grupos, los cortafuegos basados en red y los cortafuegos basados en host.

Un cortafuego basado en red se trata de un sistema encargado de controlar el tráfico saliente y entrante de una red. Usualmente, se trata de un sistema dedicado con algún software adicional instalado que permita monitorizar, filtrar y hacer logs del tráfico. Un ejemplo de un cortafuego basado en red sería el cortafuego open source PFSense[7].

Un cortafuego basado en host se trata de un software instalado y ejecutado en el ordenador o dispositivo individual que controla el tráfico entrante y saliente de un ordenador en particular. Se usa como una medida granular para añadir una capa de seguridad en el ordenador final, o como una capa extra en un entorno empresarial donde ya existe un cortafuego basado en red. Un ejemplo de un cortafuego basado en host sería el cortafuego de Windows Defender[8].

Windows 10, dentro de su software de seguridad Windows Defender, que viene incluido en los sistemas operativos de Microsoft desde Windows XP, incluye un módulo de cortafuegos en el que nos apoyaremos para configurar qué comunicaciones estarán permitidas que entren y salgan de nuestro equipo.

El cortafuego de Windows nos permite establecer tres perfiles de configuración diferentes con relación a qué tipo de red estemos conectados: Perfil privado, público o dominio. Estos perfiles ya están configurados con unas políticas predeterminadas que serán más o menos restrictivas dependiendo del perfil que tengamos asignados a nuestra red local.

6.2.2. BITLOCKER

6.2.2.1. ¿QUÉ ES BITLOCKER?

La información que poseemos en nuestros dispositivos cada vez es más valiosa, y hay que hacer lo posible para evitar su perdida realizando copias de seguridad. Pero en muchos casos, el daño radica en que otra persona pueda tener acceso a datos sensibles de manera física. Sustrayendo el equipo o teniendo acceso a él de manera física para modificarlo.

Desde Windows Vista, Microsoft proporciona un software en sus sistemas operativos que permite proteger los discos duros ante dos posibles frentes de ataque que son el robo del dispositivo o discos duros, y la modificación offline haciendo uso de un disco de arranque.

Este software recibe el nombre de Bitlocker y es una aplicación de cifrado que nos permite cifrar y proteger nuestros discos duros, permitiendo que solo sea descifrado si el disco de arranque está emparejado en el equipo correcto, es decir:

- Si se desmonta el disco para ponerlo como secundario en otro equipo, solo se tendrá acceso a los datos cifrados, si se conoce la clave de recuperación.
- Si se arranca el equipo de manera normal introduciendo las credenciales o medio de autenticación configurado, Bitlocker descifra los datos y el equipo se puede usar con total normalidad.

Bitlocker nos permite almacenar la clave que actúa como llave para acceder a los datos de cinco maneras posibles:

- En una cuenta Microsoft,
- En una copia impresa
- En una unidad de memoria USB
- En una cuenta de Azure Active Directory
- Está en posesión del administrador de sistema

6.2.2.2. ¿CÓMO FUNCIONA BITLOCKER?

En la documentación de Microsoft[9] se plantean dos escenarios, el equipo posea chip TPM o que no lo tenga. Ambas situaciones ofrecen diferentes niveles de seguridad.

Un chip TPM (Trusted Platform Module)[10], es un componente hardware agregado en las placas base de los equipos más modernos. Funciona junto a Bitlocker para ayudar a los usuarios a proteger sus datos y para asegurar que no ha existido modificación alguna en el equipo de manera física ni en el sector de arranque. Esto es posible porque al tratarse de un chip que guarda las credenciales para el descifrar los datos, puede realizar todas las comprobaciones antes de que el sistema operativo arranque.

En los equipos que no poseen un chip TPM aún se puede seguir usando Bitlocker para proteger la unidad de disco del sistema operativo de Windows, así como para cifrar unidades de datos como puedan ser discos auxiliares o externos. Requiere que se introduzca una llave USB o una contraseña para desbloquear el sistema.

6.2.3. POLÍTICAS DE USUARIO O GPO

Las políticas de grupo o GPOs son un conjunto de reglas usadas para controlar los entornos asociados a los sistemas operativos controlados por un directorio activo.

Se trata de una manera de establecer, controlar, limitar las características a las que puede acceder un usuario o grupo de estos. Además, permite establecer configuraciones para los equipos pertenecientes al dominio del directorio activo.

Cuando los equipos no pertenecen a un dominio, existen GPOs configurables a nivel local del sistema operativo llamadas Directiva Local de Grupo o LGP. Estas permiten al administrador, configurar localmente un sistema tanto a nivel de usuario como de equipo para ajustarlo a las necesidades de características y seguridad del usuario final.

6.2.4. VPN

6.2.4.1. ¿QUÉ ES UNA VPN?

Una VPN o Virtual Private Network (Red Privada Virtual) es una tecnología de red que nos permite crear una extensión de la red de área local sobre una pública, en otras palabras, es una red privada virtual a la que podemos acceder a través de Internet que por su naturaleza es pública y carece de privacidad

- Permite conectarse de forma segura y remota a redes privadas
- Puede enlazar redes diferentes e incluso servidores, de forma más segura.
- Permite navegar seguro en redes Wifi públicas
- Permite eludir la censura o las restricciones regionales de contenidos y sitios

Ventajas:

- Permite navegar de forma anónima pues la dirección IP de los dispositivos permanece prácticamente invisible para la red pues el tráfico está encapsulado y viaja con la dirección IP de la red virtual.
- Añade una capa extra de seguridad utilizando técnicas de tunelización y cifrado de datos.
- Permite eludir la censura y las restricciones regionales de contenidos y sitios.

Desventajas:

- Reduce la velocidad debido al encapsulado.
- Reduce velocidad debido al proceso de cifrado y descifrado.

Todos estos beneficios previenen ataques de Man-in-the-middle que se da cuando un atacante intercepta una comunicación legítima y asume el rol de un intermediario y simulando una conexión íntegra.

6.2.4.2. TIPOS DE VPN

6.2.4.2.1. VPN BASADO EN RED

Se trata de un enfoque que busca conectar diferentes redes entre sí a través de una red que no es segura, en el mayor de los casos, Internet. En el caso de las empresas con sedes en lugares diferentes geográficamente, supone un gran recurso para unir las redes de estas de manera virtual y segura como si fueran una sola red. De esta manera, los empleados o usuarios de dichas redes podrán acceder a los recursos de la otra como si estuvieran en la otra.

Para que este sistema funcione, se deben establecer y configurar los extremos del túnel, es decir, los dispositivos encargado de encapsular y desencapsular la información que vaya cifrada.

Existen varios tipos de redes virtuales basadas en red.

Uno de los más usados son los túneles IPSec[11]. Se basa en el establecimiento de un túnel virtual por el que pasa todo el tráfico de ambos lados de manera cifrada.

Esto nos lo puede proporcionar, por ejemplo, dos cortafuegos PFSense uno en cada extremo, ya que dentro de los módulos que se le pueden instalar se encuentra un módulo IPSec para creación de túneles virtuales.

6.2.4.2.2. VPN BASADO EN CLIENTE

Este tipo de modelo permite que un usuario se pueda conectar de manera remota a una red. En este caso se hace uso de alguna aplicación o software integrado en el sistema operativo que se encarga de establecer la conexión cifrada entre el cliente y la red, una vez este se haya autenticado con un usuario y contraseña. De manera adicional, servidores como OpenVPN pueden proporcionar un archivo de

configuración que utilizan clave privada y pública del usuario para autenticación y cifrado. Además, posee un cliente gratuito para Windows ya que se trata de software open source.

Un acceso remoto por VPN permite al usuario acceder a una red determinada desde cualquier lugar siempre que tenga acceso a Internet y este acreditado. Esto permite acceder a los recursos de esa red que tenga permitidos ese usuario de manera segura desde cualquier lugar, incluso desde conexiones Wifi-públicas potencialmente inseguras. VPN asegura el canal de comunicación ya que crea un túnel virtual privado y cifrado.

Se trata de uno de los modelos de VPN más usados en la actualidad debido a la realidad que se vive en el presente de este documento. Debido a la pandemia mundial Covid-19 se tuvo que realizar una gran reforma operativa en los trabajos, pues la población española ha tenido que estar confinada en sus hogares. Esto obligó a las empresas a crear alternativas para el trabajo remoto desde casa. Y uno de estos recursos fueron las conexiones remotas haciendo uso de VPNs basadas en el cliente

Los empleados que trabajan en remoto no tienen acceso directo a esa red y no pueden acceder a esos recursos ni trabajar bajo los estándares de red de la empresa. En este caso, es necesario habilitar un acceso remoto por VPN que permitan a los empleados acceder a recursos internos de la empresa, como puedan ser ficheros desde sus casas, pero de manera cifrada y sin comprometer los activos de la empresa.

6.2.4.3. ¿CÓMO FUNCIONA UNA VPN?

Una vez definido que es una VPN y las ventajas que nos proporciona, vamos a explicar cómo funciona colocándonos en el escenario que más afecta a un usuario estándar o, al menos, el que queremos proteger en estos escenarios y es el uso de VPN para proteger las conexiones a redes Wifi públicas.

Primero pensemos en cómo funciona una conexión a Internet de manera común.

Cuando un usuario obtiene acceso a Internet, de manera indiferente a qué tipo de red se haya conectado, y quiere, por ejemplo, acceder a una página web. Este le envía la petición a su proveedor de servicio o ISP y este a su vez, se encarga de hacer de intermediario y redirigir el tráfico de petición al servidor y las respuestas al cliente. Pero, este tráfico navega por una red pública sin cifrar, eso no quiere decir que los datos internos no lo estén, pero los paquetes y los datos que estos contienen no. Además, que existe la posibilidad que ciertas aplicaciones o páginas web hagan mal uso de los datos y se transmitan en texto claro, pero ese es otro problema (Ilustración 1).

Ilustración 1. Esquema de tráfico sin VPN[12]

Ahora bien, si añadimos un servidor VPN al esquema o al recorrido de la conexión sucede lo siguiente. Primero solicitamos a nuestro ISP que nos conecte con el servidor VPN a través del mecanismo de autenticación que se haya configurado (usuario/contraseña, certificado, etc.). En el momento que se establezca la conexión, todos nuestros datos entre nuestro dispositivo y el servidor VPN estarán "tunelizados", es decir, estarán cifrados y, además, los datos de nuestro dispositivo estarán ocultos, pues, de cara a Internet, nuestras peticiones se realizan desde el servidor VPN (Ilustración 2).

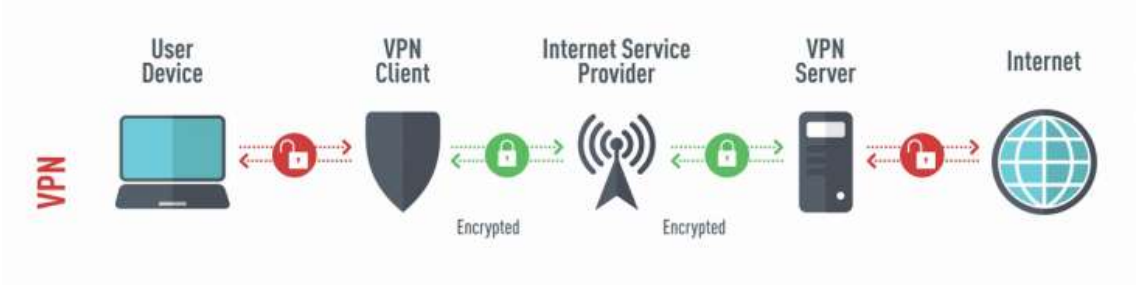


Ilustración 2. Esquema de tráfico con VPN[12]

6.2.5. WINDOWS DEFENDER

Windows ofrece el software Windows Defender Antivirus como primera línea de protección. Una herramienta diseñada para trabajar con su sistema operativo, lo cual la hace una herramienta eficiente, rápida, ligera y que se encarga de proteger en tiempo real al equipo.

Una de las principales ventajas que nos ofrece es que se trata de un antivirus que se instala en conjunto con el SO. Esto hace que el sistema esté protegido desde el primer arranque, reduciendo el riesgo de un ataque en un primer arranque. Y se fortalece en cuanto se realiza la primera actualización con Windows Update, que se encarga de mantenerlo actualizado ante amenazas en su totalidad.

Windows Defender está desarrollado para proteger en tiempo real al sistema mediante la detección de malware, virus y amenazas de seguridad. Analizando todo lo que se descarga y ejecuta en el equipo, así como las modificaciones que se intentan o realizan en el mismo.

6.3. APLICACIÓN PRÁCTICA Y USO DE LAS CONFIGURACIONES.

A continuación, se explicarán ciertos ataques que se pueden realizar de manera sencilla para demostrar lo vulnerable que puede resultar un sistema sin las protecciones adecuadas.

Además, se indicará que opciones nos proporciona Microsoft en su sistema Windows 10 para impedir o poner barreras a ese tipo de ataques, así como, otro tipo de configuraciones adecuadas para los diferentes escenarios explicadas de manera específica para los mismos.

6.3.1. USO DE BITLOCKER PARA EVITAR MODIFICACIONES OFFLINE

Como se explicó en el punto 4.2.2. la tecnología Bitlocker es un software proporcionado por Microsoft en sus sistemas operativos para cifrar los discos duros y evitar la modificación del sistema online o al acceso a los datos si se modifica el equipo desde el que se arranca el disco duro.

A continuación, se explica paso a paso como realizar un caso práctico de un ataque que consiste en obtener permisos de administrador haciendo uso de un disco o USB instalador para realizar cambios offline en el disco. Hay que modificar el comportamiento habitual de la activación de las teclas especiales (pulsación de la tecla shift 5 veces seguidas) para que abra un terminal en la pantalla de inicio de sesión con permisos de sistema, para que posteriormente permita realizar cambios en contraseñas u otros datos al arrancar el sistema.

Para realizar esta modificación en el sistema y obtener permisos de administrador, se precisa de una unidad de instalación (DVD o USB) y acceso físico al equipo.

Introducimos el medio de instalación que hayamos escogido y accedemos a la BIOS en el arranque para modificar el orden de dispositivos de arranque, en caso de ser necesario, para que tenga preferencia el medio de instalación escogido.

Una vez arranque el equipo desde el medio de instalación y llegue a la misma, hay que pulsar la combinación de teclas *Shift+F10* la cual abre un terminal de sistema o cmd con permisos de administrador. Desde aquí, al tener un cmd con permisos de administrador, se puede ejecutar el software de Microsoft *regedit.exe* como se muestra en la ilustración 3.

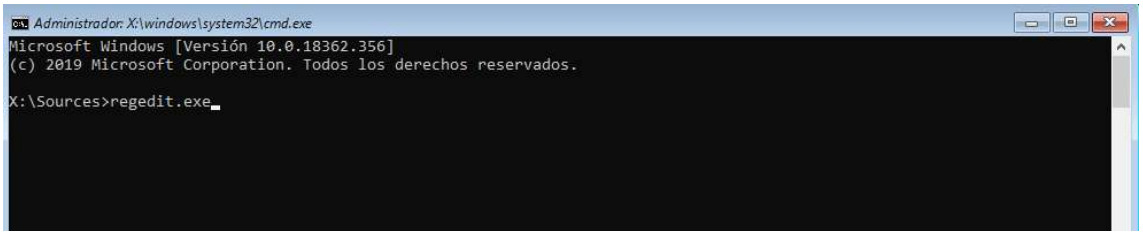


Ilustración 3. Cmd.exe usando Shift + F10 en un medio de instalación

Al ejecutar *regedit.exe* se abrirá la GUI (Graphical User Interface) o interfaz gráfica de usuario del editor de registros de Windows mostrado en la ilustración 4. En este árbol de registros se tiene acceso en primera instancia a los registros que pertenecen al medio de instalación. Para modificar los registros del equipo que se quiere atacar, se debe cargar los datos que son necesarios de los registros del disco a modificar.

Ilustración 4. Regedit.exe en su estado por defecto

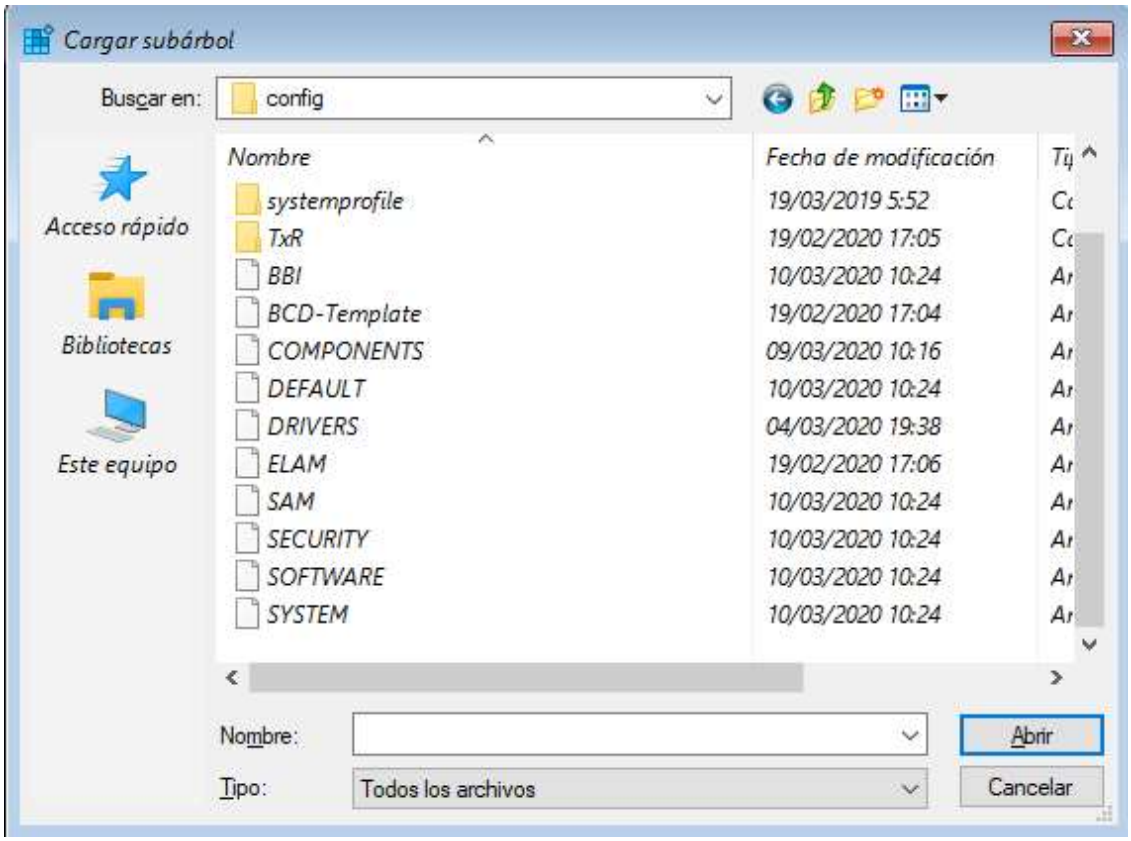


Ilustración 5. Cargar subárbol del sistema atacado

En la Ilustración 5 se observa cómo, primero, se debe seleccionar "HKEY_LOCAL_MACHINE". A continuación, en el menú superior archivo se selecciona la opción *Cargar subárbol*. Para seguir, se escoge el disco del sistema y se accede a la ruta *D:\Windows\System32\config\SOFTWARE*, una vez se tenga el subárbol SOFTWARE seleccionado se abre.

Tras tener el subárbol abierto, se le debe dar un nombre con el que se va a añadir a los registros del medio de instalación para cargar definitivamente el subárbol (Ilustración 6).

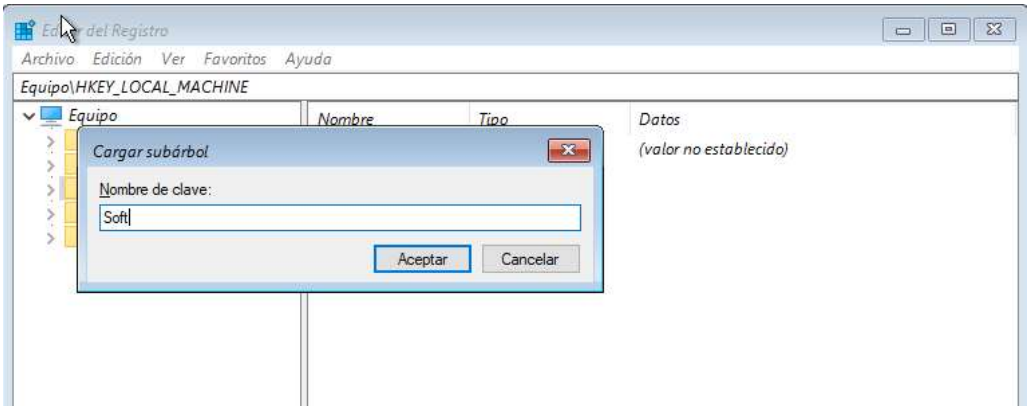


Ilustración 6. Nombre al subárbol cargado

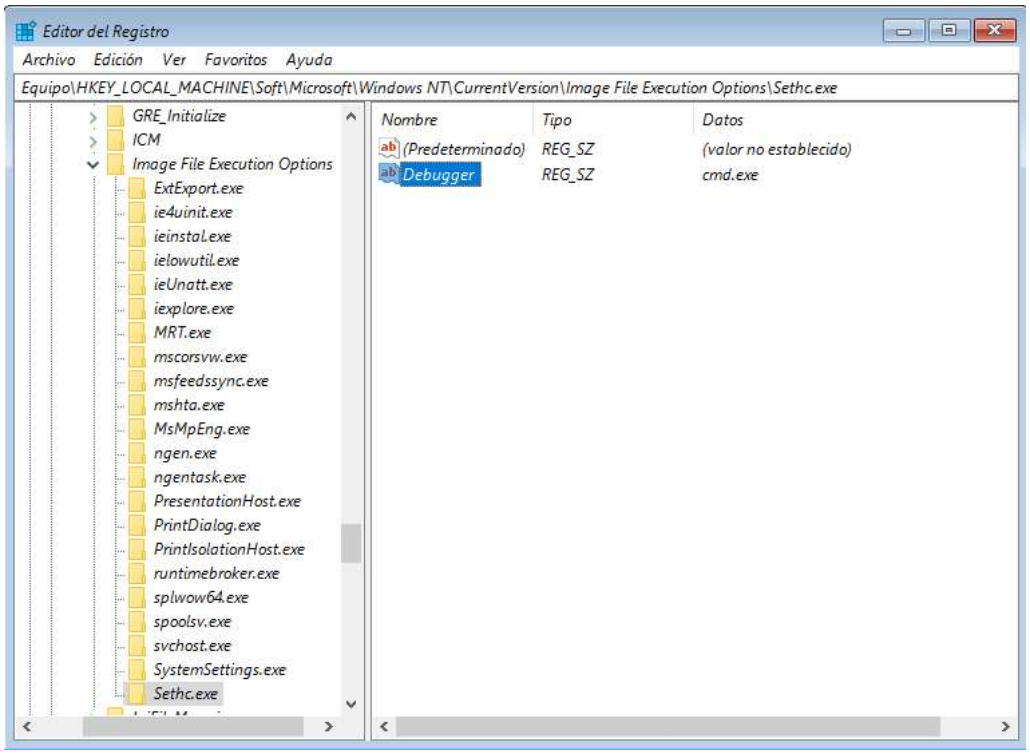


Ilustración 7. Ruta hasta Image File Execution Options y valor añadido

En este punto ya se tiene cargado un subárbol que corresponde a los registros de SOFTWARE del sistema atacado. Ahora, en el fichero importado, se accede a la ruta *Key_Local_Machine\Soft\Microsoft\Windows NT\Current Version\Image File Execution Option* y dentro de esta ruta se añade una clave de registro con el nombre "Sethc.exe" y se añade un valor de tipo cadena con el nombre "Debugger" y con valor "cmd.exe" (ilustración 7).

Una vez efectuados los cambios, es importante realizar correctamente el proceso de descarga de subárbol para que se guarden los datos en el disco. De otra manera, al reiniciar, se perderá todo, pues hay que recordar que estamos modificando registros en los archivos del medio de instalación. Para ello, se tiene que cerrar todo el árbol hasta *Soft*, tal y como se observa en la ilustración 8. Luego, se selecciona *Soft* y seguidamente, en el menú *Archivo*, se escoge la opción *Descargar subárbol.* Al realizar ese proceso se está descargando el subárbol modificado en los registros del disco atacado. Una vez realizado este proceso, se puede reiniciar el equipo para que arranque de una manera habitual.

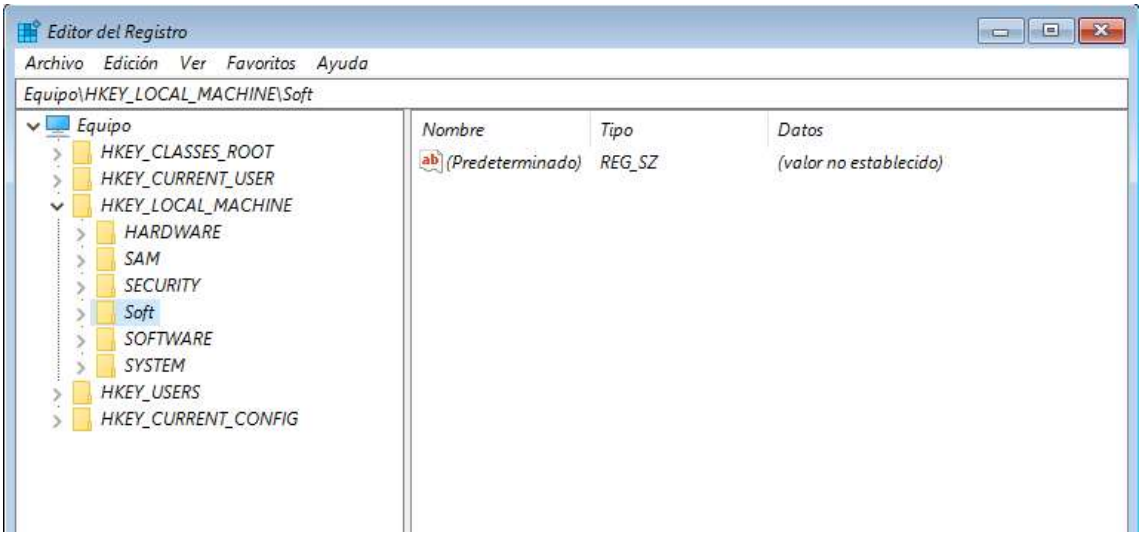


Ilustración 8. Estado final para descargar subárbol

Una vez el sistema arranque, en la pantalla de inicio de sesión de usuario, se procede a pulsar cinco veces seguidas el botón *Shift* y se abrirá una consola con permisos de administrador. Como se muestra en la ilustración 9 se observa el fondo la pantalla de inicio de sesión de Windows 10, con un terminal abierto con permisos de Administrador, aunque en este caso, de sistema.

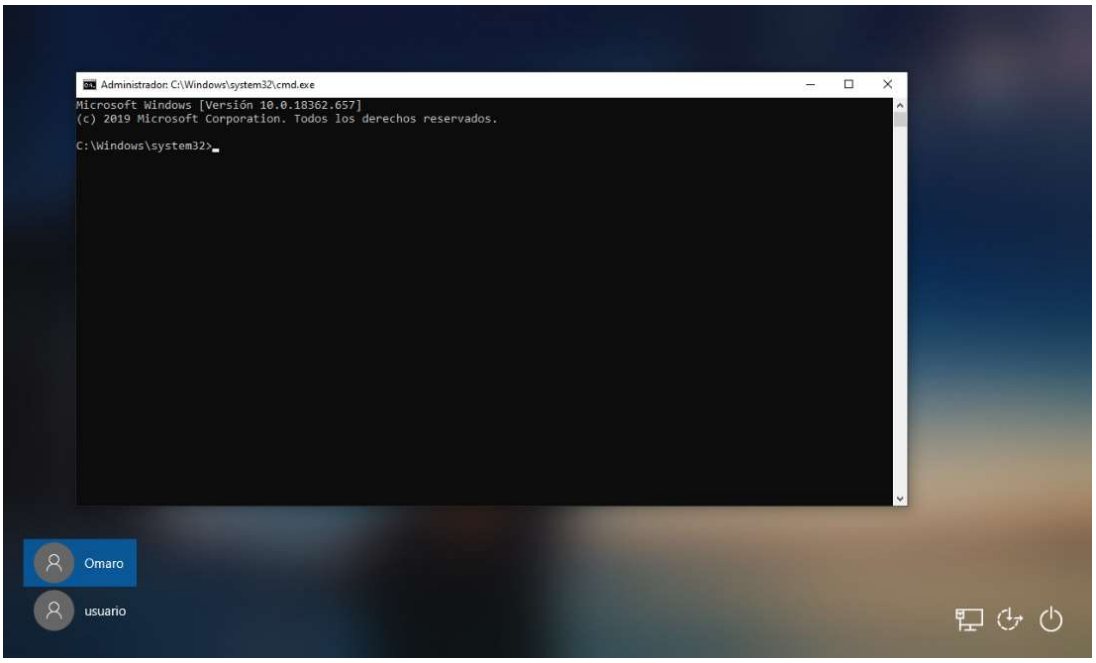


Ilustración 9. Cmd.exe con permisos de sistema en la pantalla de inicio de sesión

En este punto, se puede ejecutar cualquier cosa que permita cmd.exe, con permisos de sistema. En esta muestra, se ejecuta *mmc.exe*[13] o Microsoft Management Control que es la consola de administración de Microsoft(Ilustración 10).

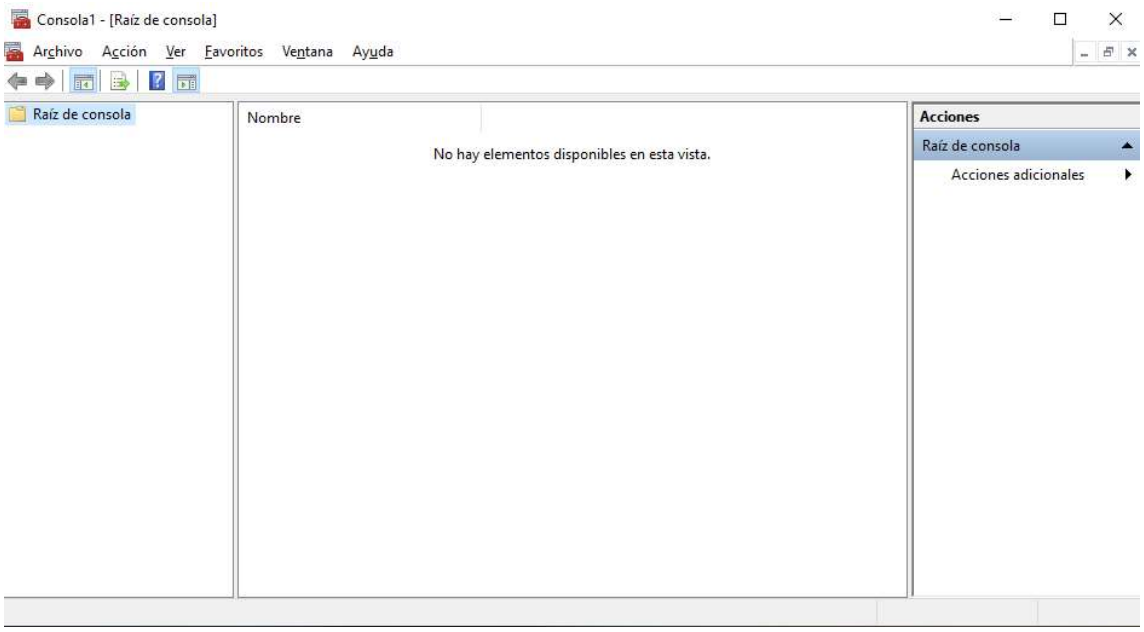


Ilustración 10. Mmc.exe ejecutándose en pantalla de inicio de sesión

Aquí se tiene acceso a multitud de herramientas desde un lugar centralizado. En este caso, se abre el menú *Archivo – Agregar o quitar complementos* y se añade el

complemento *Usuarios y grupos locales* que nos permitirá tener control total sobre los usuarios del sistema (Ilustración 11).

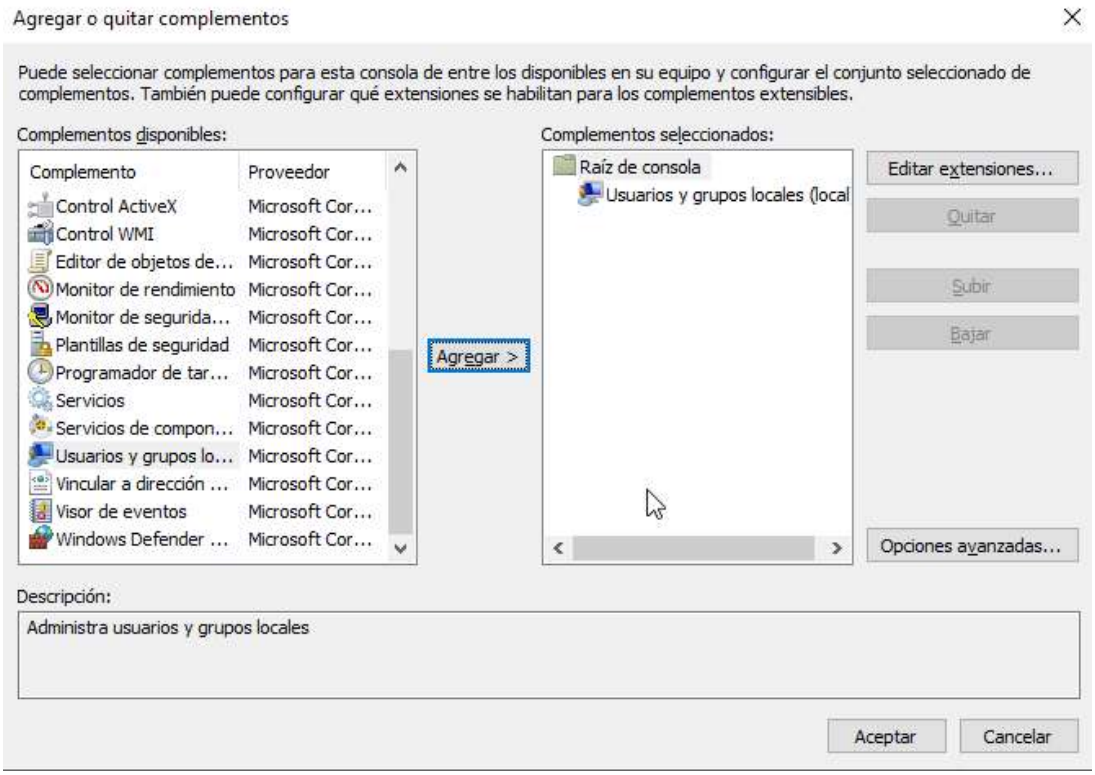


Ilustración 11. Agregar o quitar complementos en mmc.exe

Llegados aquí, en la ilustración 12, se observa un listado de todos los usuarios y grupos presentes en el sistema y entre otras opciones, permite cambiar la contraseña de cualquiera de los usuarios (porque se tiene permisos de sistema), sin necesidad de conocer la contraseña que tenía previamente. Con esto, se puede cambiar la contraseña del usuario administrador y tener acceso inmediatamente al equipo atacado.

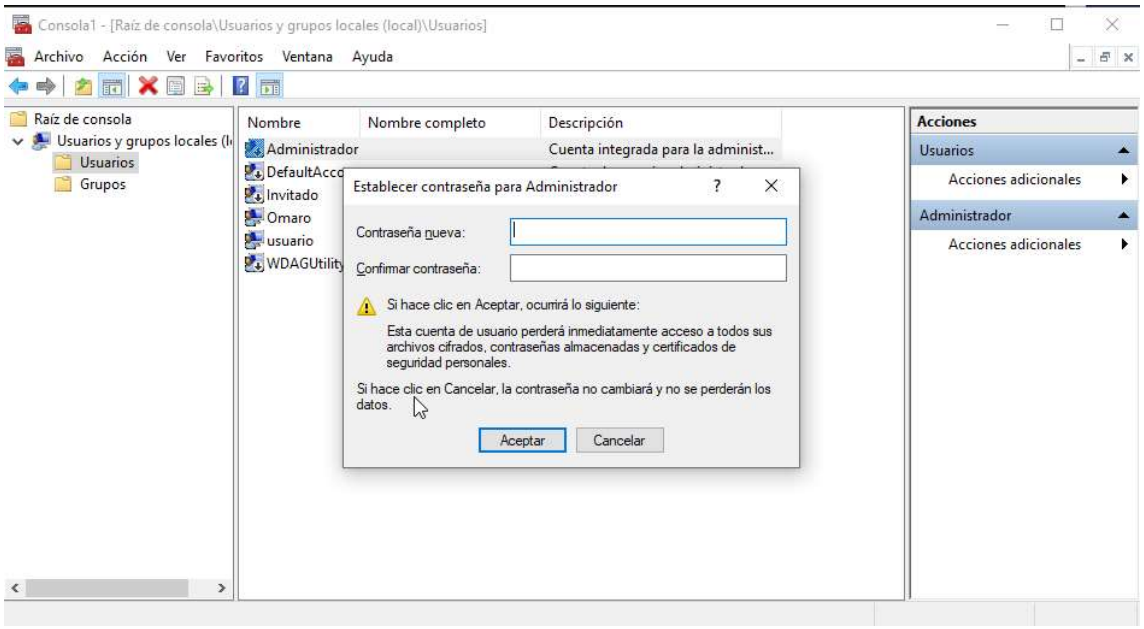


Ilustración 12. Cambiar contraseña de un usuario en mmc.exe

La defensa contra este tipo de ataque es bastante sencilla de aplicar, a la par que efectiva. Haciendo uso del software Bitlocker, ya nombrado con anterioridad, para cifrar el disco del sistema.

En el momento de seleccionar el disco del sistema como se mostró en la ilustración 5. El editor de registros se encuentra con un disco cifrado (pues Bitlocker solo descifra el disco si se realiza un arranque de manera normal y se introduce la clave necesaria) y desde el que no puede ni cargar ni descargar subárboles, por lo tanto, no se pueden realizar modificaciones de registro offline.

Para activar Bitlocker se accede a la ruta *Panel de control – Sistemas y Seguridad – Cifrado de unidad Bitlocker* y se activa para comenzar el proceso de cifrado del disco. Cabe destacar que se necesita permisos de Administrador para realizar este proceso (ilustración 13).

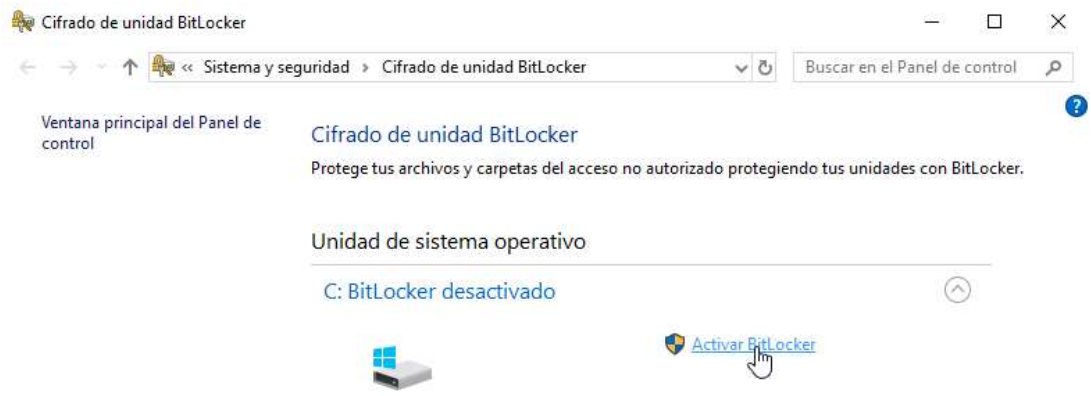


Ilustración 13. Activar Bitlocker

Como se ve en la ilustración 14, se selecciona que el equipo se descifre con una contraseña o insertando un USB. Como dato curioso, si en este paso se selecciona una contraseña, y luego donde se guarda la clave de recuperación en una unidad USB, se tienen dos maneras para descifrar el equipo, una contraseña y una llave USB. La clave de recuperación no se puede guardar en el mismo disco a cifrar.

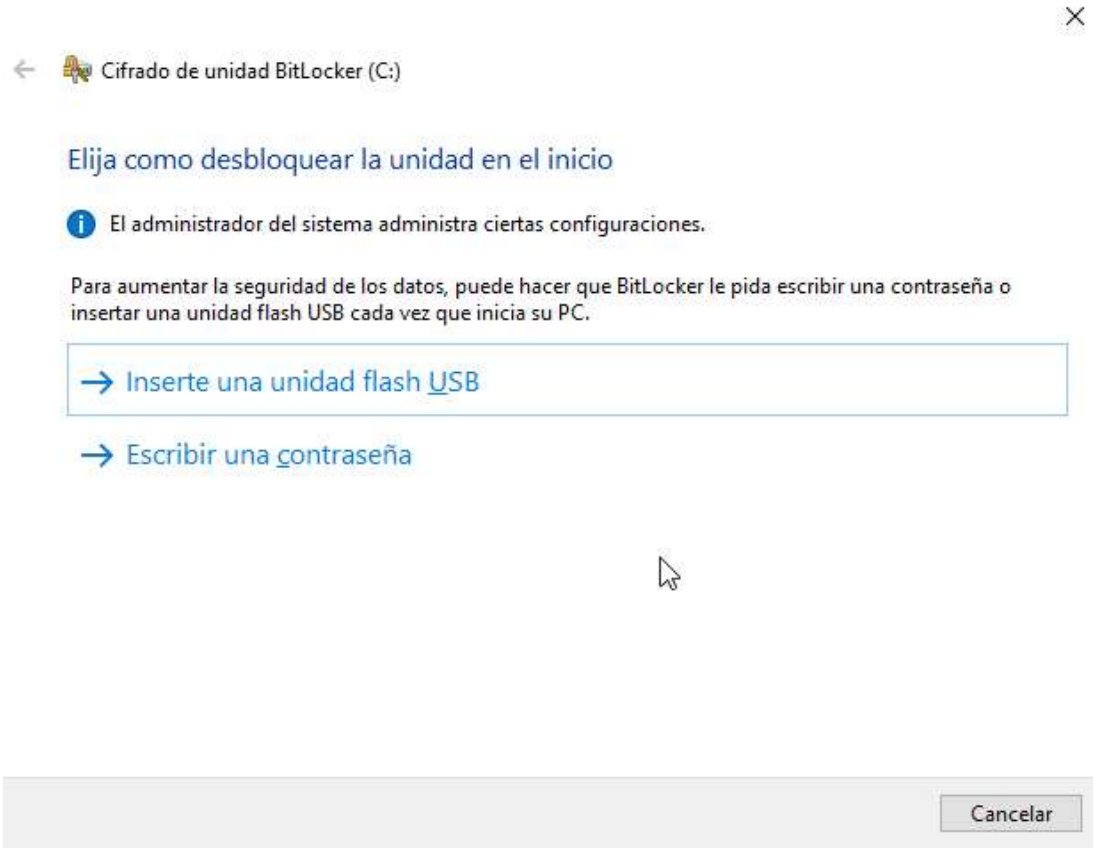


Ilustración 14. Opción de desbloqueo en la configuración de Bitlocker

Como paso final, comprobar que se ha realizado correctamente y que el equipo está defendido ante el tipo de ataques mostrado. Como muestra la ilustración 15, al abrir el editor de registro desde un medio de instalación e intentar cargar un subárbol del disco principal, no muestra el contenido de este ya que está cifrado. El contenido que vemos en la imagen son los archivos correspondientes al medio de instalación.

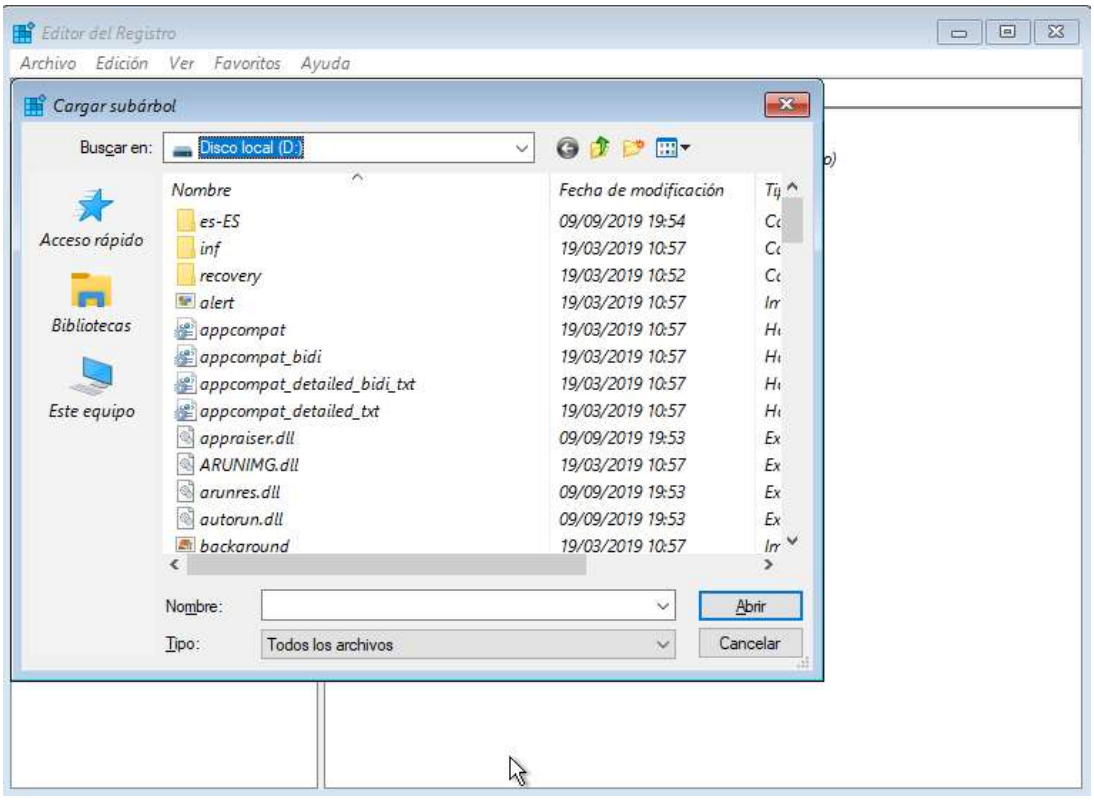


Ilustración 15. Comprobación al cargar subárbol de un disco cifrado

En caso de que el equipo se rompa o no se pueda acceder al disco por que sea imposible arrancar el sistema, se podrá acceder a los datos para recuperarlos. Para ello, se debe conectar el disco duro como un disco auxiliar en otro equipo que en primera instancia lo mostrará como un disco de datos cifrado (Ilustración 16).

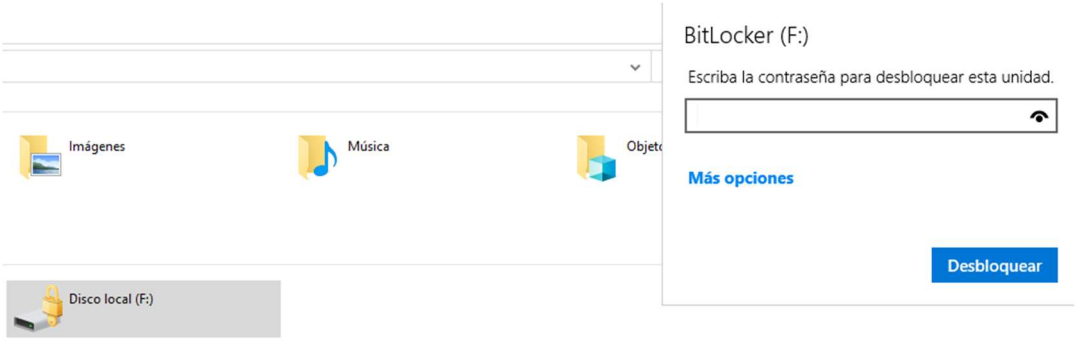


Ilustración 16. Disco cifrado conectado a otro equipo

Si se introduce la contraseña o la clave de recuperación, que se genera cuando se cifra, para descifrar el disco, Windows descifrará el mismo y nos permitirá acceder a nuestros datos para recuperarlos ante una rotura de equipo (Ilustración 17).

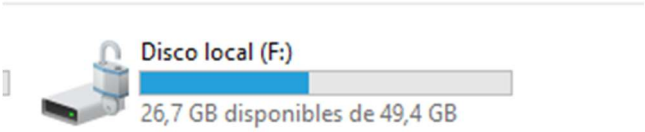


Ilustración 17. Disco descifrado conectado a otro equipo

6.3.2. USO DE LGP PARA EVITAR MODIFICACIONES DE SISTEMA

En los siguientes apartados se explican algunos ataques que se pueden realizar en el sistema operativo Windows 10, y como hacer uso de las políticas de grupo o GPO, que cuando se aplica a equipos locales reciben el nombre de LGP.

6.3.2.1. EJECUTAR UNA MODIFICACIÓN DE REGISTRO HACIENDO USO DE UNA HERRAMIENTA DE WINDOWS

La técnica llamada Wrapper, empleada habitualmente por los cibercriminales para engañar a los controladores, juegos, las aplicaciones piratas, los generadores de claves de licencias, que los usuarios descargan con frecuencia en Internet. Pues son programas o métodos para cambiar el aspecto real de un archivo que contiene código malicioso en uno que parezca legítimo.

En esta muestra, se prepara en un equipo ajeno al que se quiere infectar un archivo ejecutable malicioso, y que, haciendo uso de ingeniería social debemos intentar que sea ejecutado en el ordenador objetivo. Posteriormente, se explica cómo configurar un posible equipo objetivo para que esté protegido ante este tipo de ataques.

Para realizar este tipo de ataque, se va a usar un programa integrado en Windows desde la versión 2000, llamado "iexpress.exe"[14] para generar un ejecutable que lance dos rutinas. Una será un .exe de instalación de confianza (en este caso usaremos el instalador de 7zip) y otra un script.

Para empezar, se crea un archivo de texto llamado "modif.reg" (no es el nombre obligatorio, se puede usar el que se quiera), se añade el texto (ilustración 18) y se guarda. Lo que hace este script es crear un valor de registro en la ruta indicada en la segunda línea con el valor indicado en la tercera. A efectos finales, modifica el comportamiento del equipo cuando se activan las teclas especiales (pulsar Shift cinco veces seguidas) para que abra una consola cmd.exe en lugar de activar las teclas especiales.

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe]

"debugger"="cmd.exe"

Ilustración 18. Script modif.reg

Se crea un acceso directo en el escritorio a iexpress.exe (ilustración 17), lo cual genera un acceso directo al asistente de generación de paquetes de Windows.

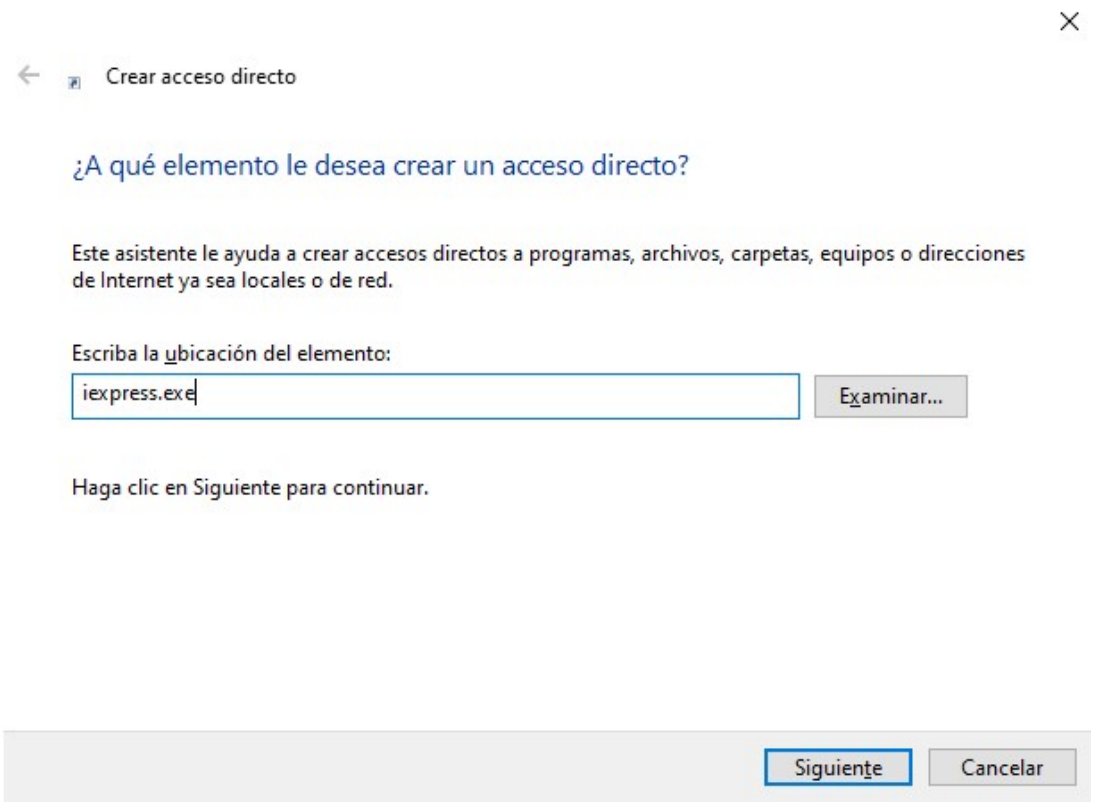


Ilustración 19. Crear acceso directo a iexpress.exe

En las propiedades de este acceso directo que se ha creado, se cambia la ruta de ejecución, a una ruta que represente una carpeta en la que se tenga permisos de escritura como se muestra en la ilustración 20, en este caso *C:\Temp*.

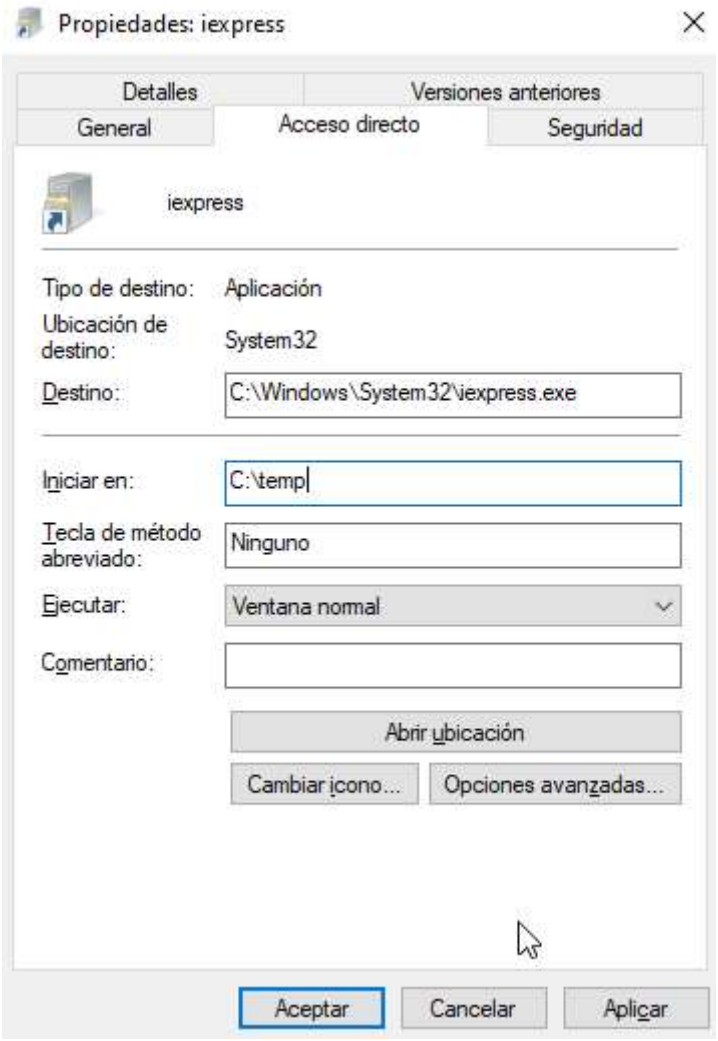


Ilustración 20. Configuración del acceso directo iexpress.exe

A continuación, se procede a ejecutar el elemento iexpress.exe, que hará que comience el proceso para la creación de un ejecutable como se puede observar en la ilustración 21.

Ilustración 21. Primer paso del asistente iexpress

Siguiendo los pasos se escogen los valores por defecto hasta llegar a la ventana que se ve en la ilustración 22, aquí se indica el nombre que tendrá el paquete.

Ilustración 22. Segundo paso del asistente iexpress

Nuevamente, se continúa dejando todas las opciones por defecto hasta llegar al paso que se muestra en la ilustración 23, donde se pide añadir los archivos que formarán parte del paquete. En este paso, se añade el ejecutable que servirá de cebo, en este caso 7zip, y el archivo modificador de registro que se creó en el primer paso.

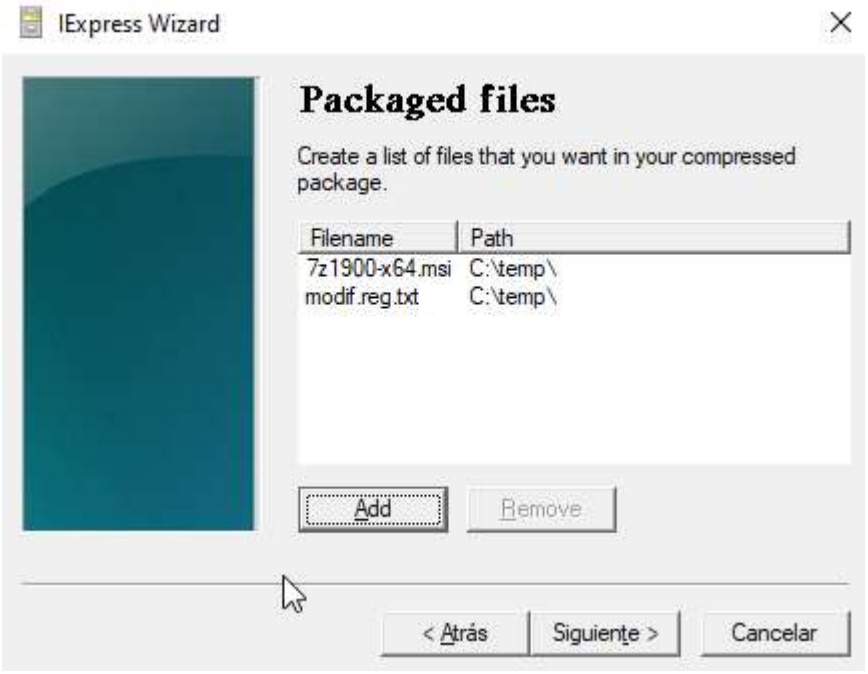


Ilustración 23. Tercer paso del asistente iexpress

Seguidamente, se indica a iexpress qué, cómo y en qué orden ejecutar los archivos que forman parte del paquete a generar. En este caso, se ejecuta primero nuestro modificador que es el archivo .reg, y luego el instalador normal del programa cebo que en este caso es un .msi de 7zip.

Como se va a ejecutar un archivo .reg, se usa regedit.exe que es el ejecutable de Windows encargado de ejecutar este tipo de fichero. Se añade al comando "/s" para que se ejecute en modo silencioso[15], que quiere decir, que no se pedirá mensaje de confirmación. Y luego, para el instalador de 7zip, como se usa un archivo msi, tenemos que hacer uso de msiexec con la opción "/i" para indicarle que se trata de una instalación[16] (Ilustración 24).

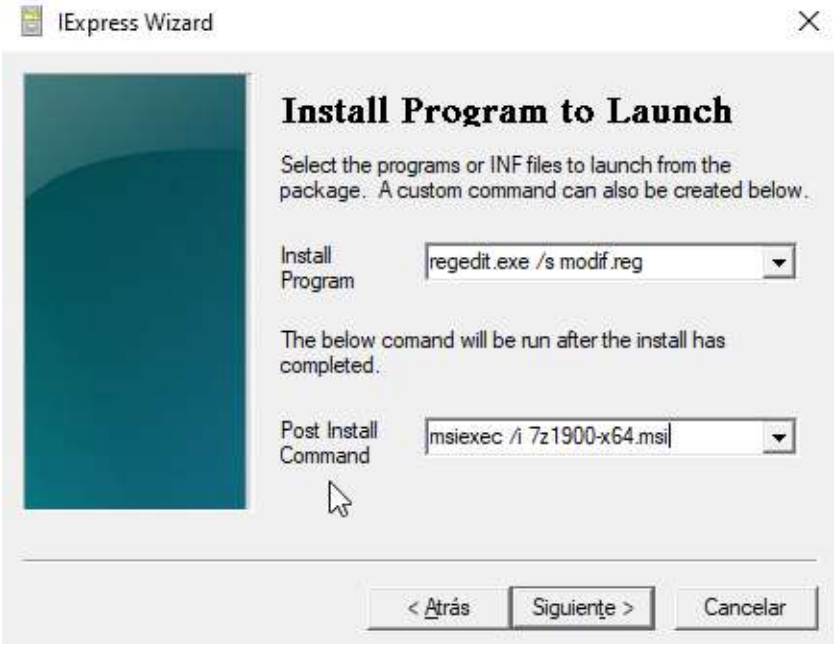


Ilustración 24. Cuarto paso del asistente iexpress

Se sigue con los parámetros por defecto hasta llegar a la pantalla mostrada en la ilustración 25. Se marcan las dos opciones disponibles antes de compilar. La primera de ellas permite esconder la extracción de los archivos y la segunda permite que se obtenga el nombre completo de los archivos. Que es necesario para que Windows no tenga problemas a la hora de extraerlos por no encontrar la ruta completa de los archivos. Además, se indica la ruta y el nombre del ejecutable que se va a crear.

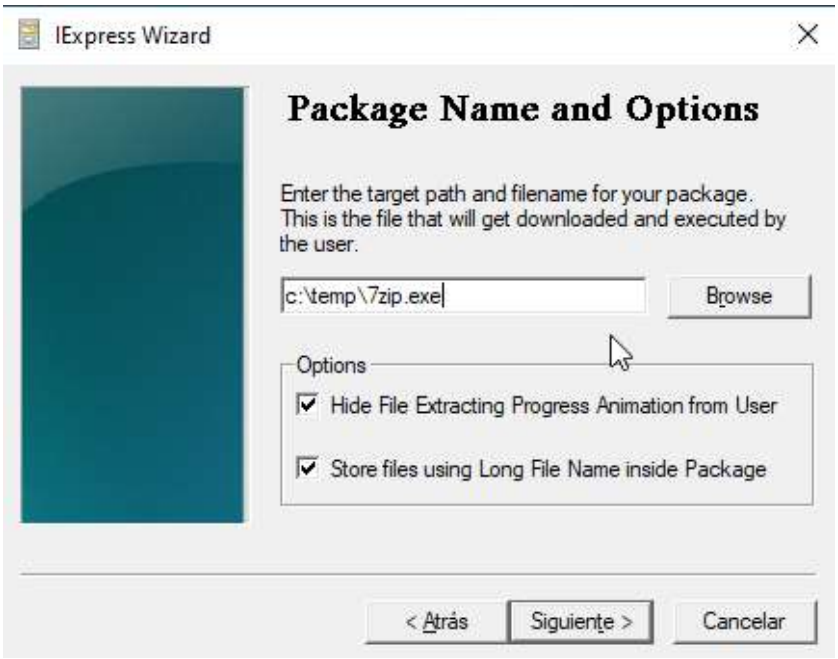


Ilustración 25. Quinto paso del asistente iexpress

Para terminar de preparar todo, una vez se tiene el ejecutable compilado creado se debe ir al mismo e indicarle que por defecto se ejecute como administrador. Para ello se accede *a Propiedades-Compatibilidad-Configuración y se marca la opción "Ejecutar este programa como administrador* (ilustración 26).

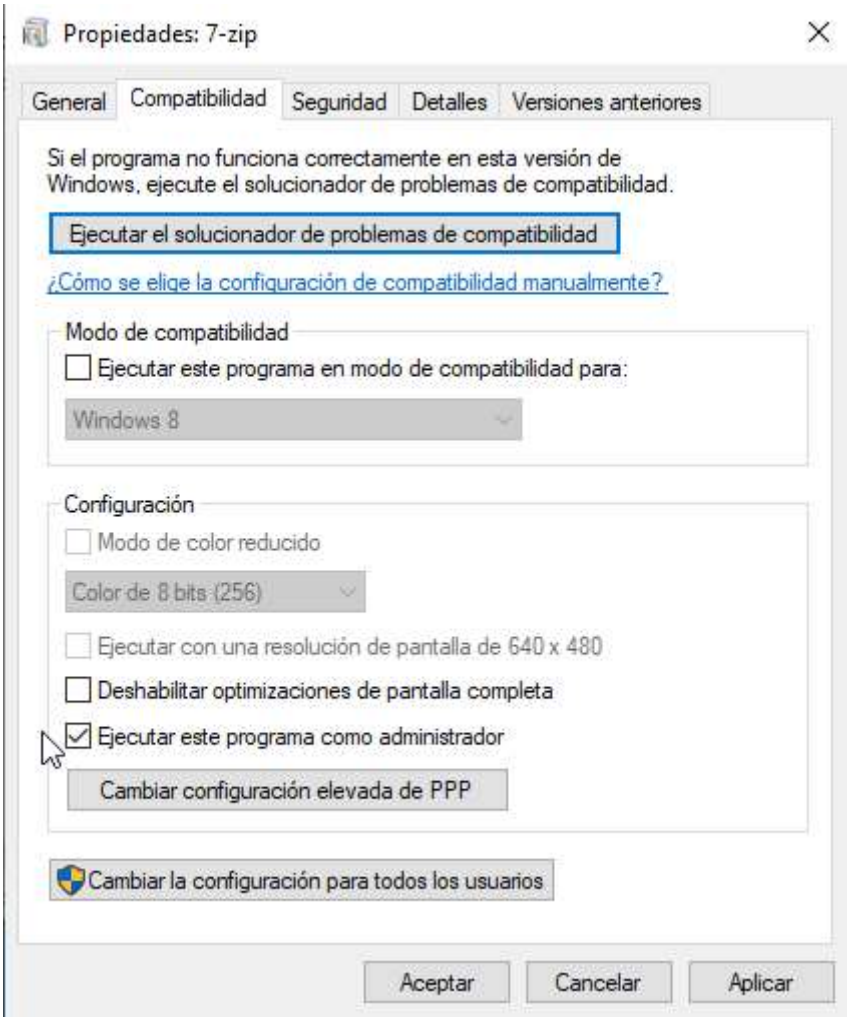


Ilustración 26. Configuración del ejecutable creado con iexpress

Tras esto, se ha creado un ejecutable listo para intentar que un administrador lo instale en el equipo que queremos infectar. Aquí entra la parte de ingeniería social, aunque muchas veces, una persona en su ordenador personal usa un usuario con permisos de administrador. Una vez instalado el ejecutable se habrá instalado el programa cebo y si se va a los registros se puede comprobar que el valor "debugger = cmd" ha sido añadido en la ruta adecuada, y si, se accede a la pantalla de bloqueo del equipo y se pulsa cinco veces el Shift, se tendrá acceso a cmd.exe con permisos de administrador (ilustración 27). Este tipo de ataque se puede realizar para ejecutar cualquier tipo de archivo y otro tipo de modificaciones, pero se ha usado este para mostrar la facilidad para realizar uno.

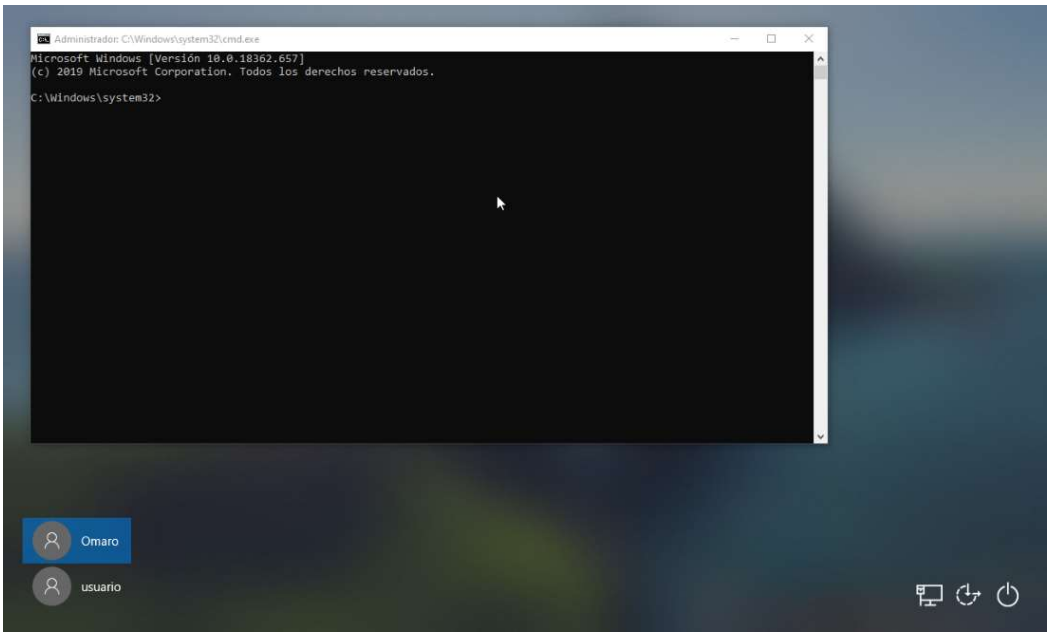


Ilustración 27. CMD en pantalla de inicio de sesión tras modificación con iexpress

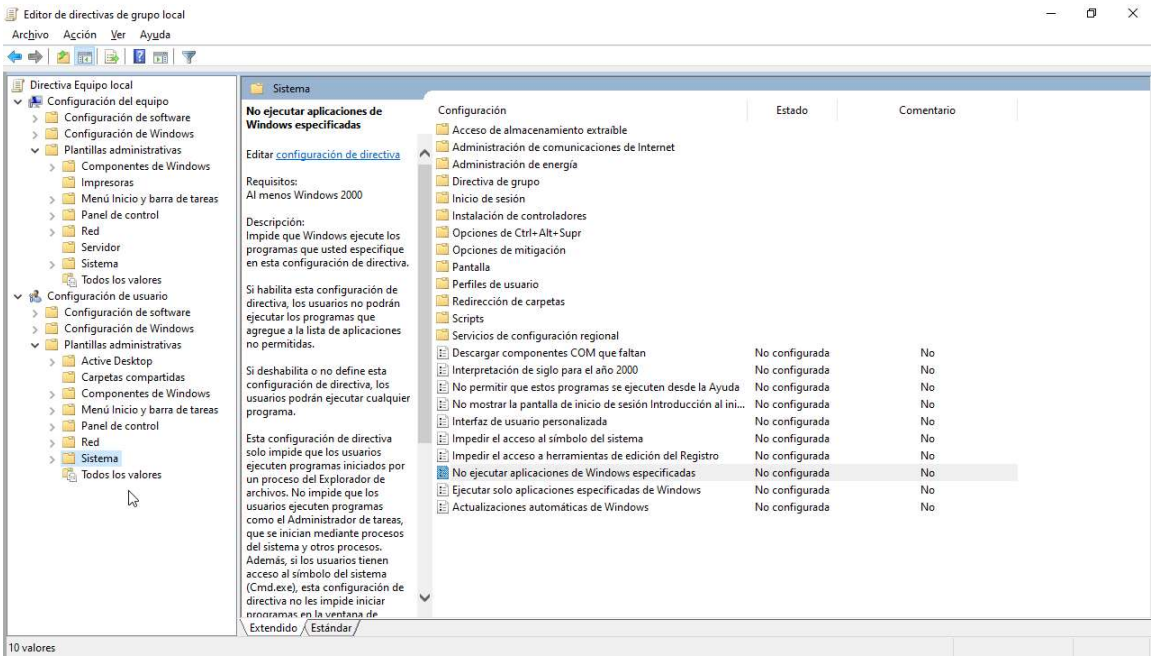


Ilustración 28. Gpedit

Para proteger los equipos ante este tipo de ataques, se puede hacer uso de las políticas de grupo o GPO[17]. Aunque es algo más usado en sistemas centralizados que pertenezcan a un dominio haciendo uso de Active Directory[18], también se puede configurar en equipos aislados donde adquieren el nombre de directivas de grupo local o LGP.

Se comienza pulsando la combinación de teclas *Windows+R* para abrir la opción Ejecutar y se ejecuta gpedit.msc, lo cual abrirá el editor de políticas de grupos. Se accede a la ruta *Configuración de usuario – Plantillas administrativas – Sistemas* (ilustración 28).

Una vez aquí, se procede a bloquear el uso del editor de registro que pertenece al ejecutable "regedit.exe" usado para ejecutar el script, y a su vez, cualquier ejecución automática del mismo. Como se observa en la ilustración 29, se selecciona la opción "Habilitada" lo cual solo habilita que se aplique la política, pero no significa que bloquee la ejecución. Para ello, se pone a **Si** la única opción que nos muestra.

Esto hará que el editor de registro no se ejecute, sin excepción alguna, salvo que el administrador desactive esta opción previamente.

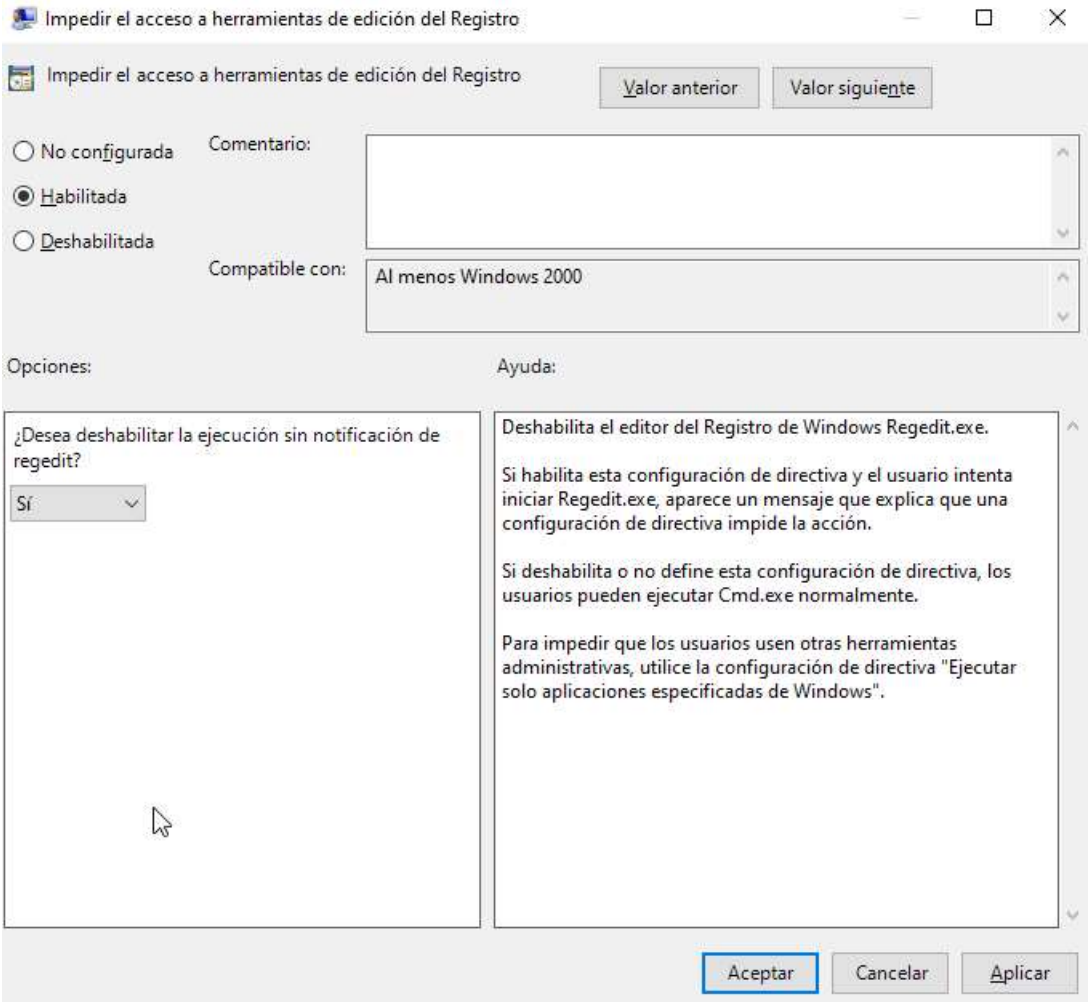


Ilustración 29. Política de grupo para regedit.exe

Como se indicó previamente, iexpress se puede usar para ejecutar otro tipo de archivos o programas de diferentes tipos. Uno bastante importante y que se recomienda bloquear, es el uso del CMD. Para ello, se accede a la opción "Impedir el acceso al símbolo del sistema", que permite tanto el acceso a cmd.exe, como la ejecución de scripts que hagan uso de este. Se habilita y en la opción que se muestra, se selecciona **Si** y se aplica (Ilustración 30).

Esto hará que el cmd no se ejecute en ninguna circunstancia, aunque se tenga permisos de administrador. Si el administrador quisiera hacer uso del cmd, tendría que desactivar esta opción y luego volver a activarla cuando haya terminado.

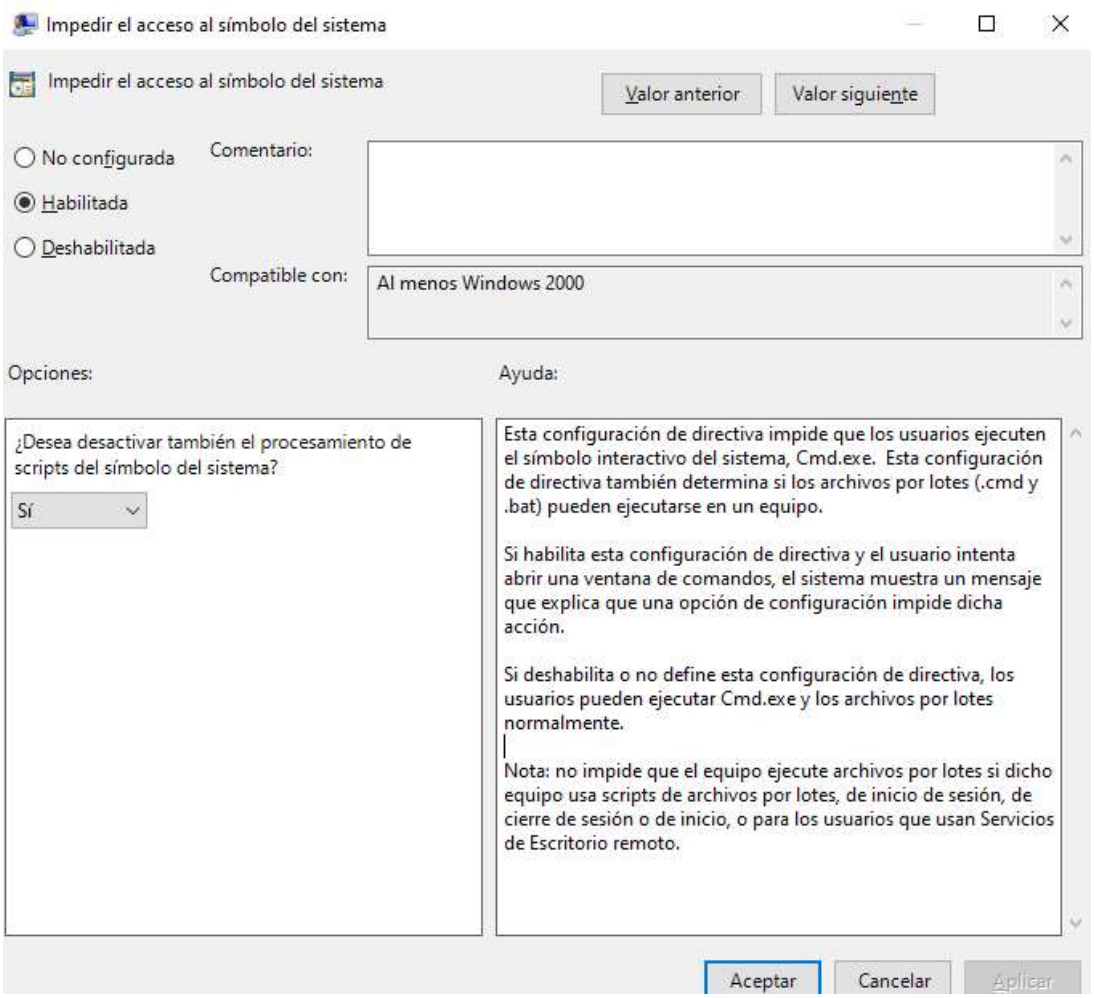


Ilustración 30. Política de grupo para cmd.exe

Para evitar otro tipo de ataques es prudente bloquear Powershell e incluso iexpress, que es la herramienta que se usa en el ataque. Para ello, se accede a la política de grupo "No ejecutar aplicaciones de Windows especificadas". Se habilita y en la lista de aplicaciones añadimos iexpress.exe y powershell.exe (ilustración 31).

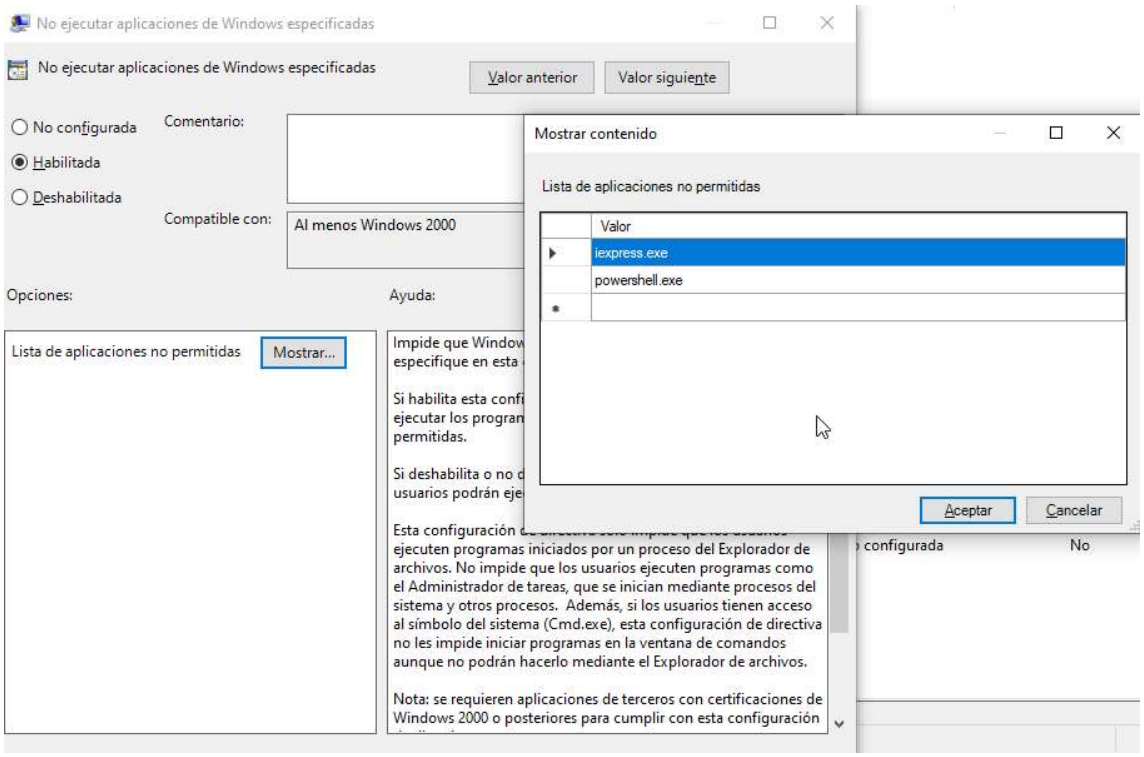


Ilustración 31. Política de grupo para iexpress.exe y powershell.exe

En este punto, si se intenta ejecutar el paquete trampa creado anteriormente, no se ejecutará el modificador de registros y el sistema advertirá con un mensaje (ilustración 32).

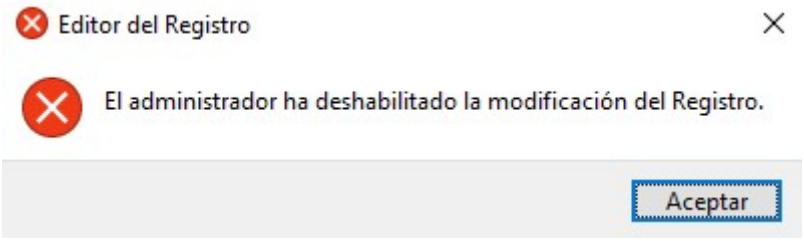


Ilustración 32. Intento fallido de ataque con iexpress

6.3.2.2. EJECUTAR UNA APLICACIÓN HACIENDO USO DE UN PDF

Se va a explicar cómo aprovechar la capacidad que tiene el explorador de archivos de Windows para abrir archivos ZIP para hacer que un usuario abra un archivo que modificará un registro mostrándole un inofensivo pdf.

En este ejemplo se modifica un registro para que se abra un programa automáticamente al iniciar el sistema y se mostrará un archivo pdf como tapadera, el archivo malicioso se prepara en otro equipo, para posteriormente ser distribuido a las

víctimas. En este ejemplo se va a usar Internet Explorer como programa a arrancar, pero puede ser cualquier tipo de programa se quiera arranca al inicio, de manera oculta.

Lo que hará será ejecutar un comando usando cmd y acto seguido con "|" le indicamos qué segundo comando queremos que ejecute (Ilustración 33). Se crea un acceso directo configurado con los parámetros que se muestran a continuación:

cmd.exe /c start reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v myAPP /t REG_SZ /d "c:\Ruta\miAplicacion.exe" /f| explorer http://servidorweb/directorio/mifichero.pdf

MyAPP = nombre que queramos ponerle al valor del registro

Ruta\miAplicacion.exe = ruta de la aplicación que queramos ejecutar

Ruta web = enlace a algún pdf que esté online, lo podemos buscar en Google añadiendo filetype:pdf a la búsqueda.

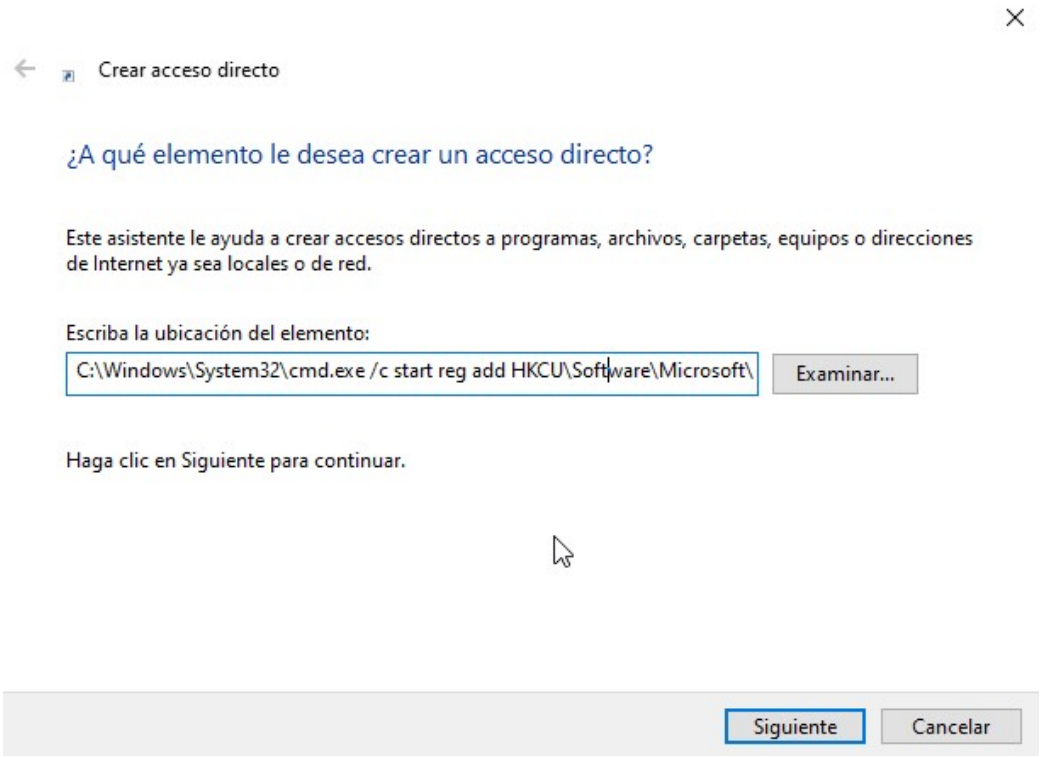


Ilustración 33. Ejecución de doble comando en acceso directo

Importante nombrar al acceso directo de la misma manera que se llama el archivo pdf para que la trampa pase desapercibida (Ilustración 34).

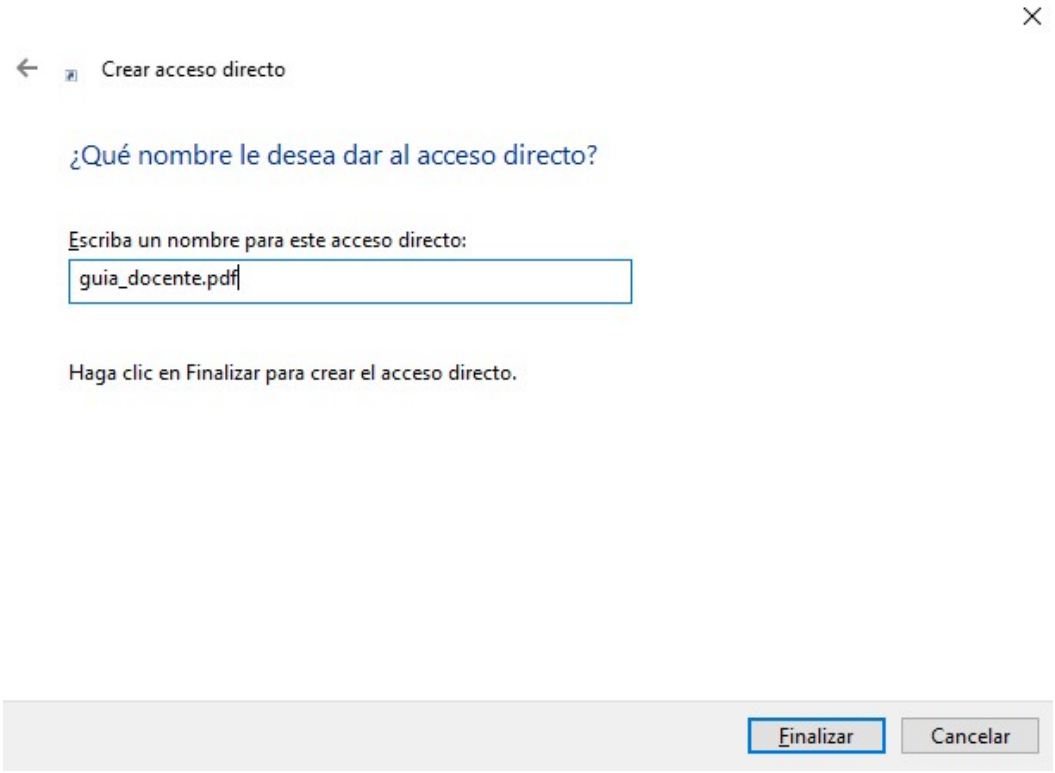


Ilustración 34. Acceso directo con nombre de pdf

Una vez el acceso directo esta creado, dentro de sus propiedades, se modifica el icono del acceso directo para que sea el icono más usado para los pdf (Ilustración 35). Esto servirá como medida extra por si la víctima se toma la molestia de extraer el archivo del archivo comprimido.

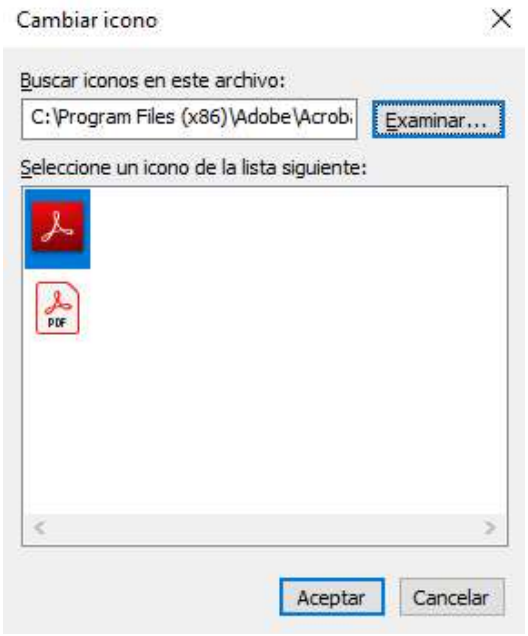


Ilustración 35. Cambio de icono de acceso directo

Con el archivo trampa listo, ahora, se hace clic derecho en nuestro archivo y se selecciona *Enviar – Carpeta comprimida (zip)* y se renombra a "nuestroNombre.zip" (nombre del fichero pdf para que sea más creíble). Al abrir el zip, la víctima se encontrará con el nombre del fichero y el tipo. Pero un usuario confiado o poco experimentado solo se fijará en el nombre de este y no se dará cuenta que se trata de un acceso directo y no un pdf (ilustración 36).

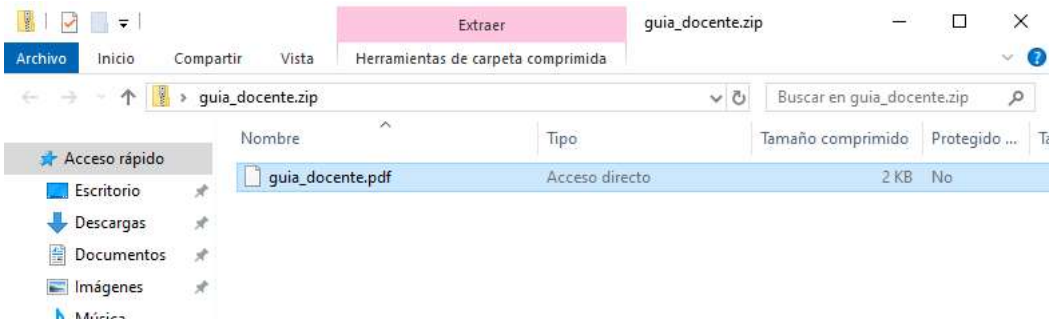


Ilustración 36. Zip abierto con navegador de Windows

Cuando la víctima haga clic en el fichero, se abrirá muy brevemente el cmd y se cerrará, pudiendo ser algo imperceptible (todo depende de la velocidad del equipo) y acto seguido se abrirá el pdf como si no hubiera pasado nada. Pero si se accede al registro se comprobará que se ha modificado el valor del registro Run (ilustración 37), el cual indica programas que van a ser arrancados en el momento del inicio de la sesión.

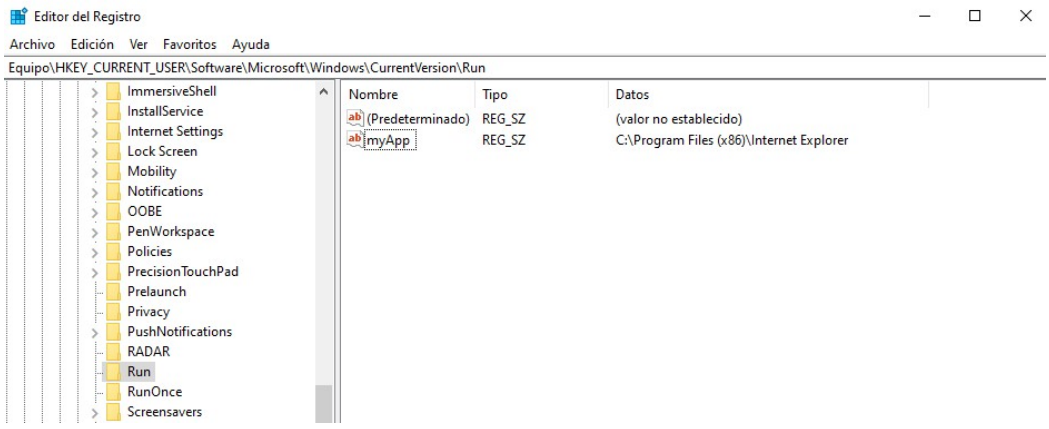


Ilustración 37. Registro Run modificado

Con esto se ha mostrado como modificar un registro de manera externa y sin tener acceso físico al ordenador. Y aunque, para el ejemplo se usa un programa inofensivo como es Internet Explorer, cualquier tipo de software puede ser ejecutado.

Para proteger el equipo de este ataque, debemos bloquear como ya se ha explicado en casos anteriores con políticas de grupo, la ejecución del CMD, y aunque con eso sería suficiente, no estaría de más, bloquear también regedit.

6.3.3. CONFIGURAR VPN

Uno de los mayores miedos dentro del usuario medio y que más se repite es el robo de información, ya sea contraseñas, datos bancarios, conversaciones, imágenes y demás información que exista en dispositivos que se conecten a una red Wifi pública.

Las redes Wifi públicas pueden ser maliciosas, poco fiables o simplemente, por la naturaleza de la red comparte los datos con el resto de las personas que están conectadas a la misma si la configuración de del usuario no es la adecuada.

La mayor amenaza existente dentro de una red Wifi es la posibilidad del atacante de posicionarse entre el usuario y punto de conexión. Esto se conoce como Man-in-the-middle y se trata de una técnica donde el atacante hace de intermediario. El usuario, en lugar de enviar sus datos al router Wifi, se lo envía al atacante y este a su vez se los envía al punto de conexión para crear una conexión "normal" para el usuario. En este punto, el atacante tiene acceso a toda la información que se transmite: Correos electrónicos, información bancaria, credenciales, etc.

Para proteger la conexión a este tipo de ataques, es indispensable que los datos vayan cifrados. Una solución es hacer uso de una conexión de red privada virtual o VPN. Como ya se explicó en el punto 4.2.4.3., aunque el atacante consiga posicionarse entre nosotros y el punto de conexión, solo tendrá acceso a datos cifrados y no podrá hacer nada con ellos.

Microsoft ofrece en su sistema Windows 10, una aplicación integrada en su sistema para configurar conexiones VPN sin necesidad de usar software de terceros para realizar este tipo de conexiones. A continuación, se explicará cómo configurar dicha conexión y hacerla funcionar.

Se accede a la ruta *Configuración – Red e Internet – VPN* para llegar al panel de configuración y control de las distintas conexiones VPNs (Ilustración 38).

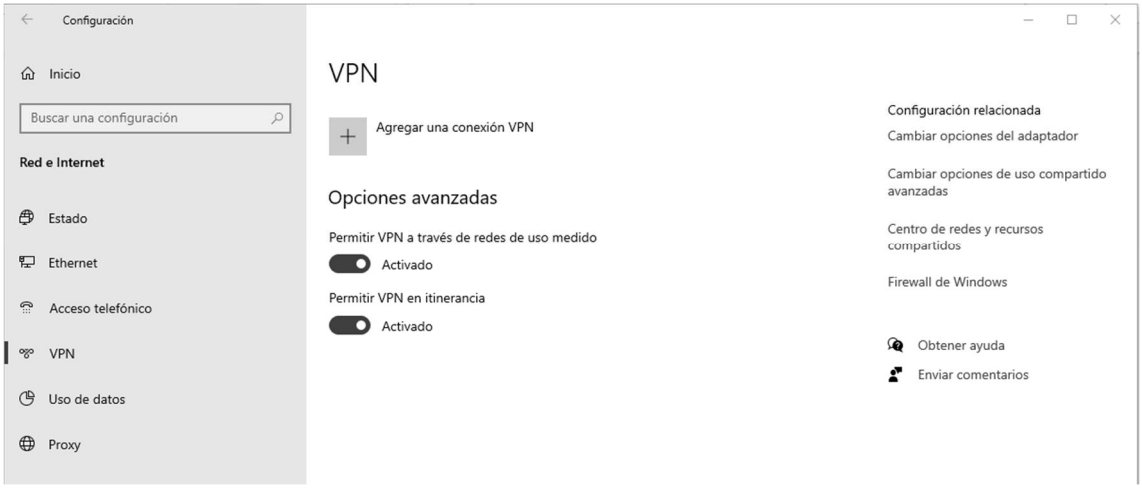


Ilustración 38. Configuración VPN

A continuación, se selecciona "Agregar una conexión VPN", que nos llevará al panel para la configuración de una nueva conexión VPN. En este caso ejemplo, se ha usado datos de un servidor VPN gratuito alojado en Rusia para mostrar que realmente de cara a Internet, estamos en Rusia (Ilustración 39).

Se aclara encarecidamente, que no se recomienda el uso de VPNs gratuitas o al menos de procedencia sospechosa, y menos aún usarlas para manejar datos personales de riesgo como correos, datos bancarios y demás. Siempre se recomienda usar un servidor VPN propio o uno de confianza, normalmente de pago en estos casos.

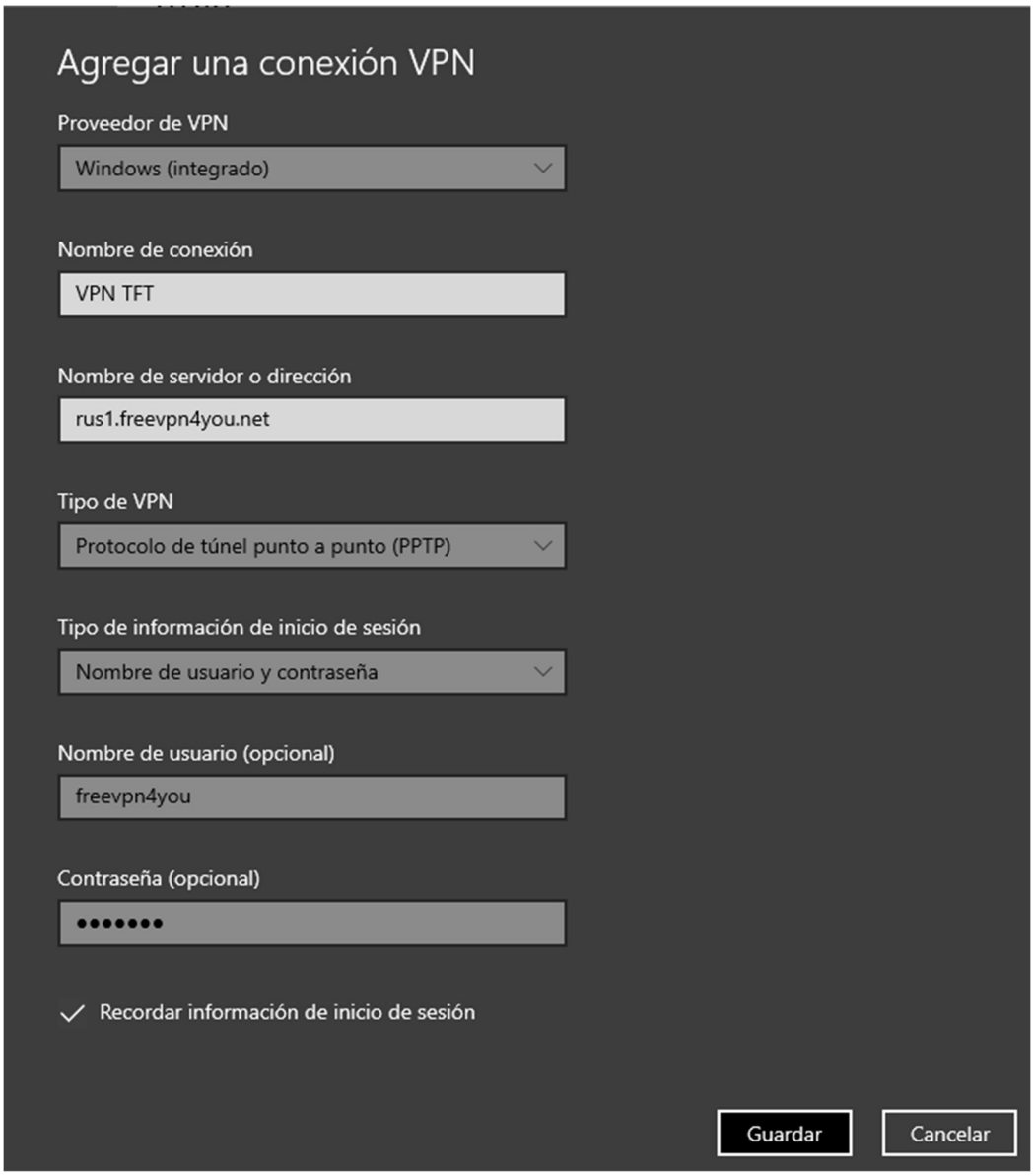


Ilustración 39. VPN configurada

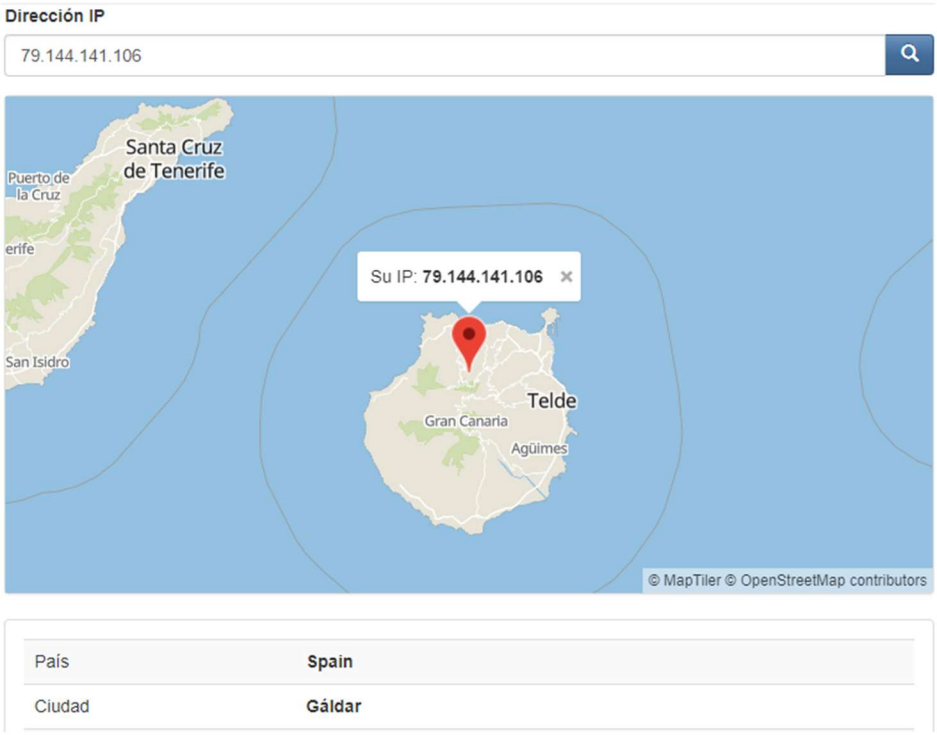


Ilustración 40. IP pública en Gran Canaria

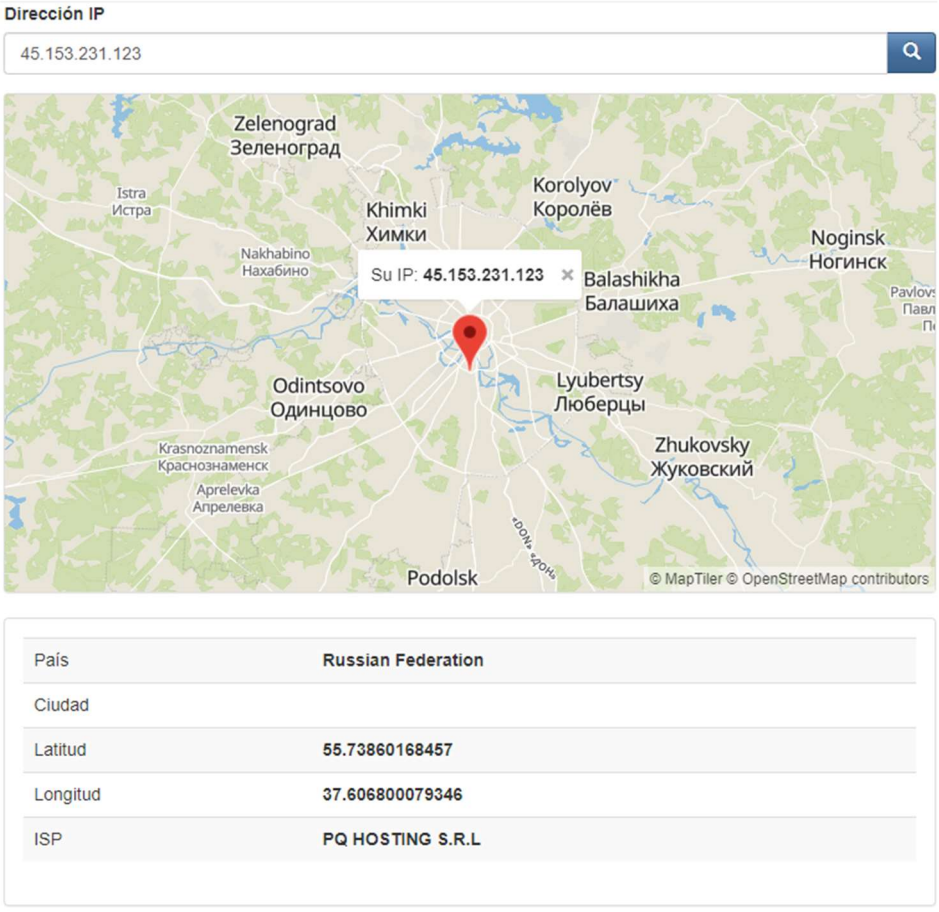


Ilustración 41. IP pública en Rusia

Con esto, ya se tendría configurada una conexión VPN. Para mostrar que funciona, en las ilustraciones 40 y 41, se muestra cómo las IPs públicas antes y después de la conexión al servidor VPN son diferentes. Además, se muestra cómo de cara a Internet, estas IPs, están localizadas en lugares totalmente diferentes. La original en Gran Canaria - España y la segunda en Rusia. Para comprobar la localización de la IP pública se ha hecho uso de la web cual-es-mi-IP.net[19]

6.3.4. BLOQUEAR EL USO COMPARTIDO

Normalmente, cuando se trabaja en un entorno de red local como puede ser el hogar o el trabajo, se activa el uso compartido y detección de redes para localizar impresoras en red, o acceder a recursos compartidos, por ejemplo.

Pero, existe otro vector de ataque asociado a conexiones Wifi-públicas que también se debe controlar. Si el equipo está configurado para compartir archivos en red local, el atacante puede tanto acceder a dichos archivos como insertar malware dentro de los ficheros del usuario.

Se trata de una configuración simple pero que evitará sustos a la hora de conectarnos a redes Wifi públicas poco seguras.

Para ello, vamos a *Configuración – Red e Internet – Opciones de uso compartido* y desactivamos la detección de redes y compartir archivos e impresoras (Ilustración 42).

Windows permite, además, configurarlo para diferentes perfiles como puede ser una red privada o una pública además de configuraciones genéricas para todo tipo de redes.

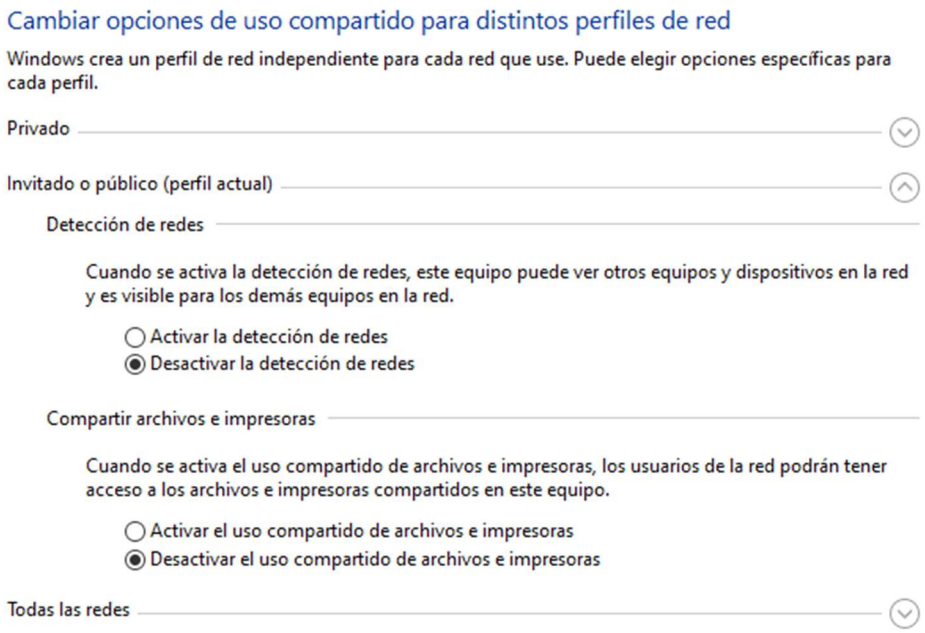


Ilustración 42. Configuración de uso compartido

6.3.5. CONFIGURACIÓN DEL CORTAFUEGO

Como ya se nombró anteriormente, Microsoft incluye dentro de su software de seguridad "Windows Defender" un cortafuego del que se podrá valer el equipo para protegerse si configura de una manera adecuada.

Primero, hay que tener en cuenta un detalle y es que el cortafuego de Windows tiene por defecto la siguiente configuración:

- Conexiones entrantes: BLOQUEADAS, es decir, sólo se permitirán aquellas que estén especificadas como regla.
- Conexiones salientes: PERMITIDAS, es decir, solo se bloquearán aquellas que estén especificadas como regla.

Esta configuración, a primera instancia, es cómoda para la mayoría de los usuarios (Ilustración 43). Pero, por desgracia, permite que, si por algún motivo el equipo se ve infectado por un malware que envíe datos al exterior, el usuario no se daría cuenta. Al estar permitidas las conexiones salientes por defecto, Windows no le pedirá confirmación para añadir ninguna regla y por lo tanto el usuario no detectará nada sospechoso.

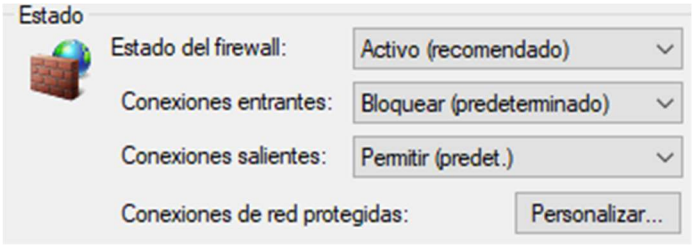


Ilustración 43. Configuración por defecto del cortafuego

Por lo tanto, hay que cambiar esa configuración y bloquear por defecto tanto las conexiones entrantes como salientes en el menú de configuración general del cortafuego. Para ello se debe ir a *Configuración – Red e Internet – Firewall de Windows – Configuración avanzada – Propiedades* y cambiar las conexiones salientes para que por defecto estén bloqueadas en todos los perfiles (Ilustración 44).

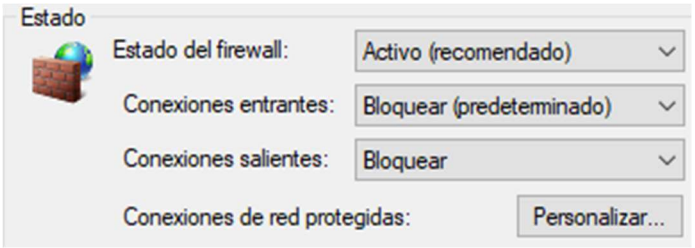
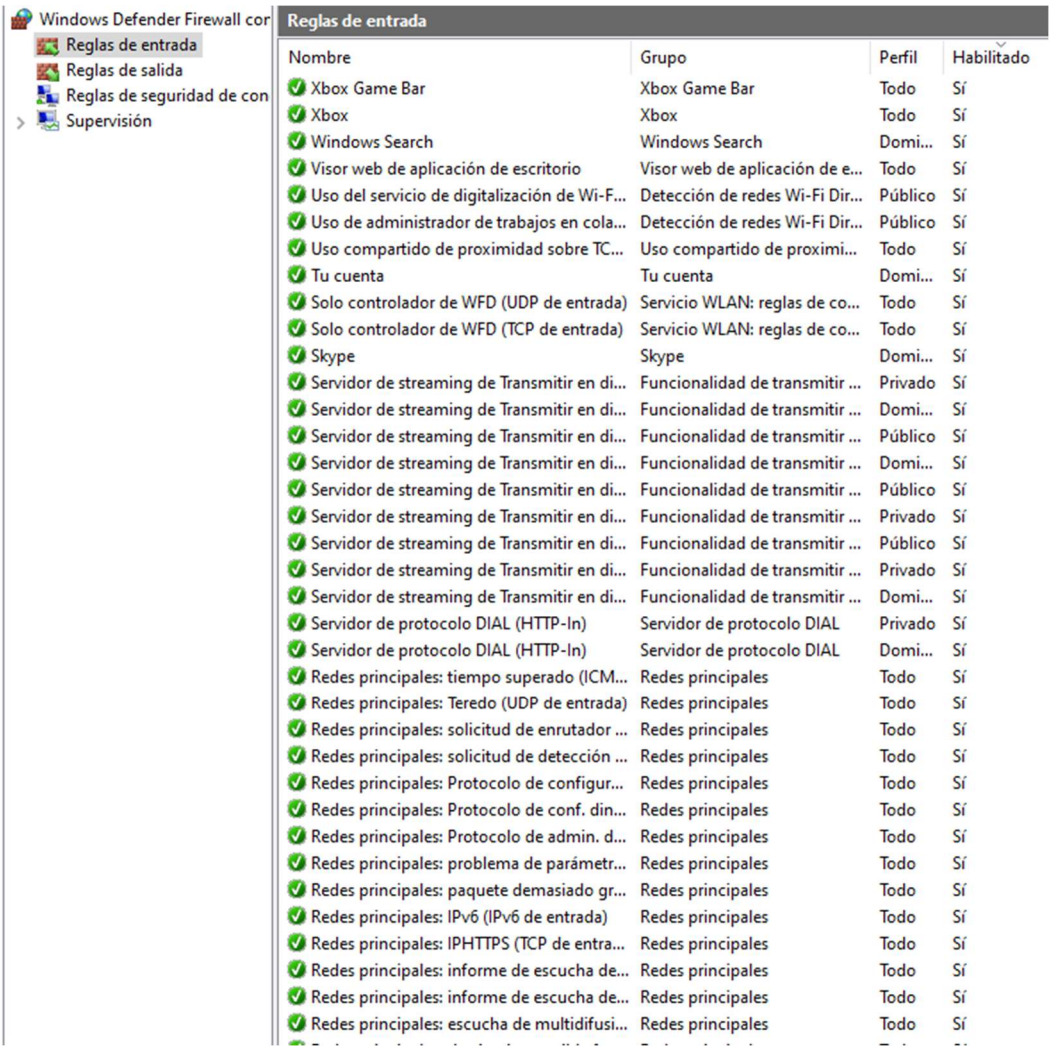


Ilustración 44. Configuración bloqueada del cortafuego

Como se ha nombrado anteriormente, se consideran cuatro configuraciones diferentes atendiendo a cuatro perfiles con diferentes necesidades. Inicialmente se deshabilitan todas las reglas preconfiguradas por Windows para hacer la experiencia del usuario más cómoda. Como se muestra en la ilustración 45, existen cantidad de reglas para muchos fines para los que estas máquinas no estarán destinadas (Xbox, Skype, Windows Search, Servidor de streaming, etc.).



Nombre	Grupo	Perfil	Habilitado
Xbox Game Bar	Xbox Game Bar	Todo	Sí
Xbox	Xbox	Todo	Sí
Windows Search	Windows Search	Domi...	Sí
Visor web de aplicación de escritorio	Visor web de aplicación de e...	Todo	Sí
Uso del servicio de digitalización de Wi-F...	Detección de redes Wi-Fi Dir...	Público	Sí
Uso de administrador de trabajos en cola...	Detección de redes Wi-Fi Dir...	Público	Sí
Uso compartido de proximidad sobre TC...	Uso compartido de proximi...	Todo	Sí
Tu cuenta	Tu cuenta	Domi...	Sí
Solo controlador de WFD (UDP de entrada)	Servicio WLAN: reglas de co...	Todo	Sí
Solo controlador de WFD (TCP de entrada)	Servicio WLAN: reglas de co...	Todo	Sí
Skype	Skype	Domi...	Sí
Servidor de streaming de Transmitir en di...	Funcionalidad de transmitir ...	Privado	Sí
Servidor de streaming de Transmitir en di...	Funcionalidad de transmitir ...	Domi...	Sí
Servidor de streaming de Transmitir en di...	Funcionalidad de transmitir ...	Público	Sí
Servidor de streaming de Transmitir en di...	Funcionalidad de transmitir ...	Domi...	Sí
Servidor de streaming de Transmitir en di...	Funcionalidad de transmitir ...	Público	Sí
Servidor de streaming de Transmitir en di...	Funcionalidad de transmitir ...	Privado	Sí
Servidor de streaming de Transmitir en di...	Funcionalidad de transmitir ...	Público	Sí
Servidor de streaming de Transmitir en di...	Funcionalidad de transmitir ...	Privado	Sí
Servidor de streaming de Transmitir en di...	Funcionalidad de transmitir ...	Domi...	Sí
Servidor de protocolo DIAL (HTTP-In)	Servidor de protocolo DIAL	Privado	Sí
Servidor de protocolo DIAL (HTTP-In)	Servidor de protocolo DIAL	Domi...	Sí
Redes principales: tiempo superado (ICM...	Redes principales	Todo	Sí
Redes principales: Teredo (UDP de entrada)	Redes principales	Todo	Sí
Redes principales: solicitud de enrutador ...	Redes principales	Todo	Sí
Redes principales: solicitud de detección ...	Redes principales	Todo	Sí
Redes principales: Protocolo de configur...	Redes principales	Todo	Sí
Redes principales: Protocolo de conf. din...	Redes principales	Todo	Sí
Redes principales: Protocolo de admin. d...	Redes principales	Todo	Sí
Redes principales: problema de parámetr...	Redes principales	Todo	Sí
Redes principales: paquete demasiado gr...	Redes principales	Todo	Sí
Redes principales: IPv6 (IPv6 de entrada)	Redes principales	Todo	Sí
Redes principales: IPHTTPS (TCP de entra...	Redes principales	Todo	Sí
Redes principales: informe de escucha de...	Redes principales	Todo	Sí
Redes principales: informe de escucha de...	Redes principales	Todo	Sí
Redes principales: escucha de multidifusi...	Redes principales	Todo	Sí

Ilustración 45. Reglas por defecto del cortafuego

6.3.5.1. CORTAFUEGO MÁQUINA BLINDADA

Para configurar el cortafuego de Windows 10 para ser lo más impermeable posible simplemente se debe deshabilitar todas las reglas que estén habilitadas en el cortafuego por defecto. Esto deja al equipo en un estado de bloqueo absoluto, tanto de conexiones salientes como entrantes (Ilustración 46).

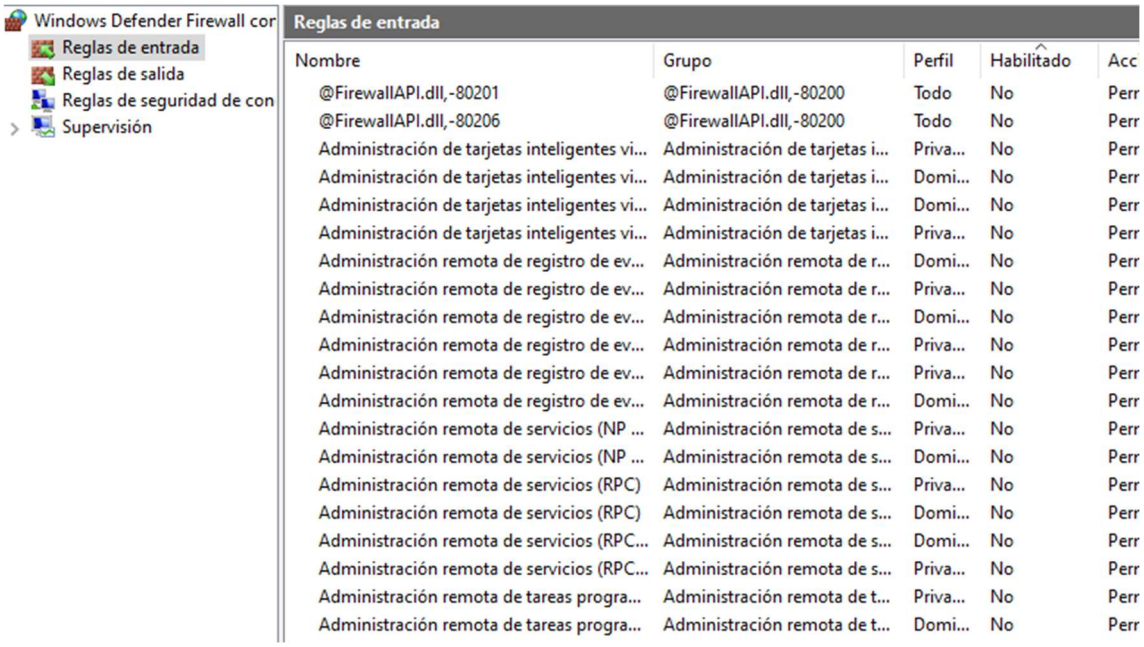


Ilustración 46. Cortafuego máquina blindada

Al bloquear todo tipo de conexiones entrantes y salientes, nos encontraremos con un sistema operativo que no podrá siquiera encontrar una red a la que conectarse, aunque sea a través de cable Ethernet. Esto implica que incluso para conexiones locales será inaccesible.

6.3.5.2. PROCEDIMIENTO PARA CREACIÓN DE NUEVA REGLA EN EL CORTAFUEGO

Si partimos de un estado limpio donde todas las reglas preconfiguradas se encuentran inhabilitadas, primero se debe habilitar las reglas que permitan a nuestro equipo encontrar la red a la que está conectado. Estas reglas vienen preconfiguradas y son las reglas pertenecientes al grupo "Redes principales" que permite que el equipo use IPv4 e IPv6 para conectarse a recursos de red (Ilustración 47).

Siempre, hay que mantener la mayor seguridad posible y no dejar abiertas puertas que no se usan. En el caso que solo se esté usando IPv4, se deberán habilitar solo las reglas que permitan el tráfico IPv4 y bloquear el tráfico IPv6 pues no sería necesario. Solo en caso de que este sea necesario se deberán habilitar.

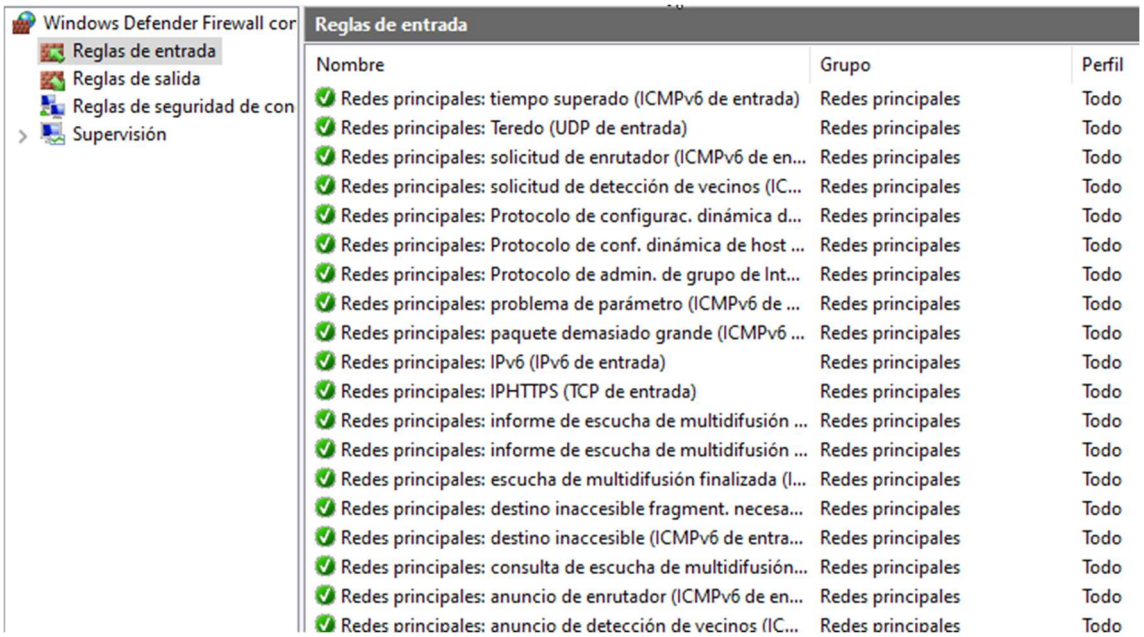


Ilustración 47. Redes principales habilitadas

Esto es necesario como ya se ha nombrado, para que el equipo pueda conectarse a los recursos de red y por lo tanto tener acceso a la transmisión de datos dentro de su propia red hasta el Gateway que le corresponde.

A continuación, a modo de ejemplo se mostrará el proceso para la creación de nuevas reglas en el cortafuego, necesario en todos los estadios representados posteriormente. Para ello, se crearán dos reglas que permitan las conexiones tanto entrantes como salientes en los puertos: 80,443 para HTTP/HTTPS.

Para crear una regla se debe ir a la sección en la que la queramos añadir, entrada o salida y seleccionar la opción **Nueva regla…** que llevará al asistente para la creación de esta. En el primer paso se selecciona el tipo de regla que queremos añadir (Ilustración 48):

- **Programa:** Permite configurar una regla para las conexiones de un programa en específico.
- **Puerto:** Permite configurar una regla orientada a permitir o bloquear los puertos TCP o UDP.
- **Predefinida:** Permite hacer uso de diferentes reglas predefinidas por el sistema Windows 10 como pueden ser las nombradas Redes principales.
- **Personalizada:** Permite crear reglas con mayor número de parámetros de configuración, como puede ser, IPs origen y destino.

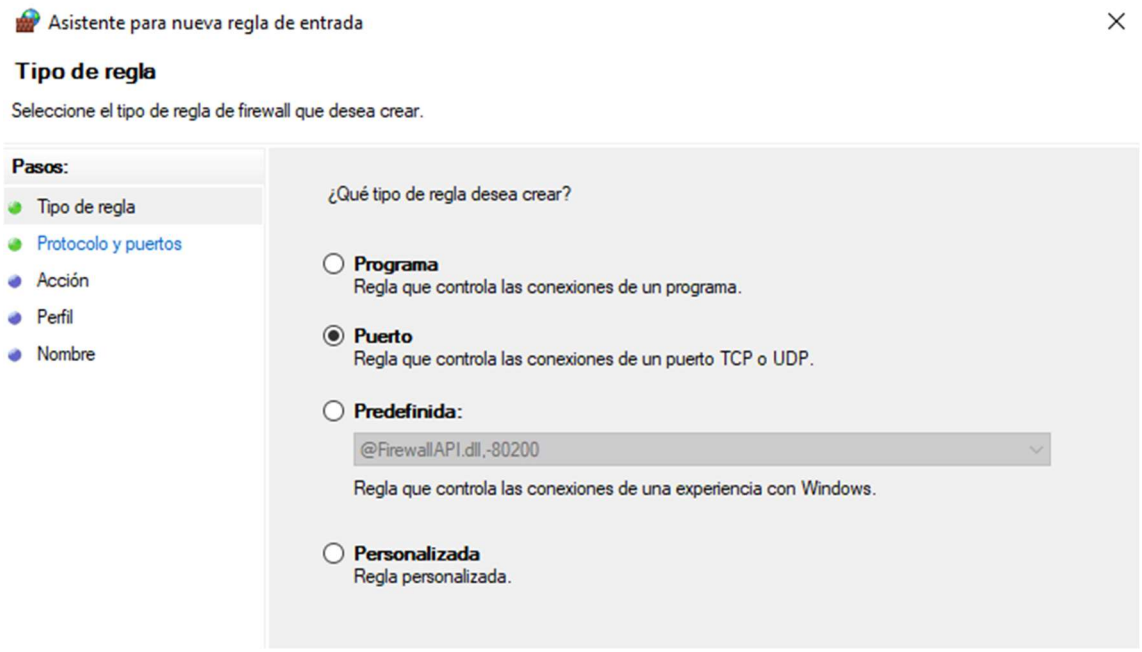


Ilustración 48. Nueva regla de cortafuego 1

Haciendo uso del tipo de regla para puertos, se continua para indicar que protocolo (TCP[20] o UDP[21]) y que puerto, puertos o rango de puertos se quiere usar (Ilustración 49), en este caso, se necesita TCP y los puertos 80 y 443.

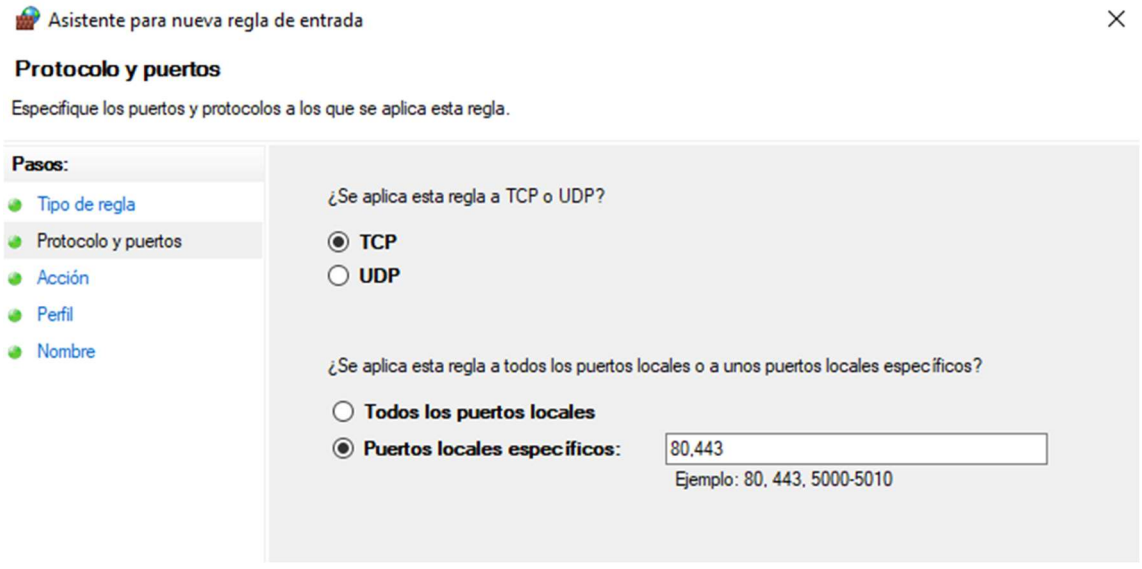


Ilustración 49. Nueva regla de cortafuego 2

Seguidamente, se selecciona que comportamiento debe tener la regla, permitir, permitir solo si es seguro o bloquear en caso de que la conexión coincida con los parámetros indicados en la misma (Ilustración 50).

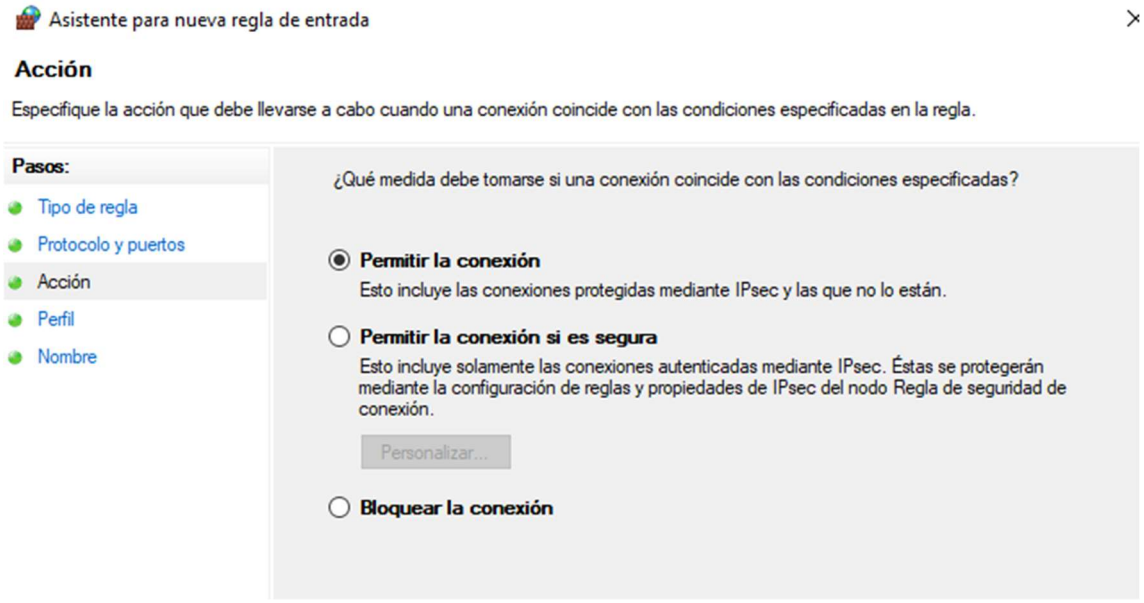


Ilustración 50. Nueva regla de cortafuego 3

Como último paso de este proceso, se debe seleccionar a que perfil de conexión aplicar esta regla. Entre ellos está perfil privado (aplicado en redes como el hogar y redes de confianza), público (aplicado en redes públicas) y dominio (aplicada a equipos pertenecientes a un dominio). Es este caso, aplica seleccionar privado y público pues no se trata de una máquina perteneciente a un dominio (Ilustración 51).

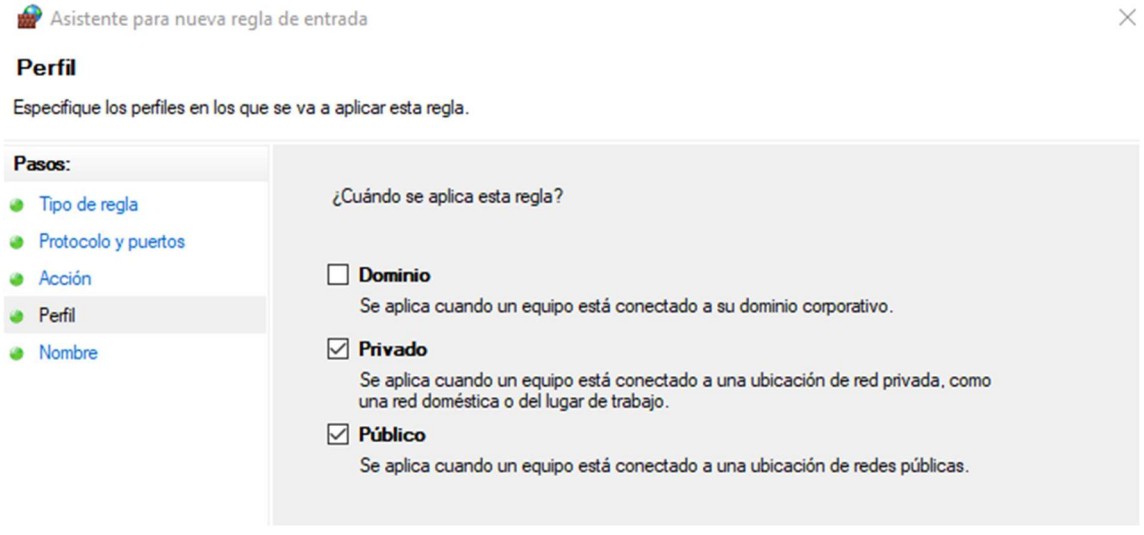


Ilustración 51. Nueva regla de cortafuego 4

6.3.5.3. CORTAFUEGO MÁQUINA PARA USO BÁSICO

Como ya se explicó en el punto 1.3, se considera esta máquina, como una máquina para uso básico ofimático, además, debe tener acceso a Internet, uso de correo electrónico y posiblemente acceso a recursos compartidos.

Para tener acceso a ese tipo de recursos es necesario configurar ciertos puertos en el cortafuego añadiendo reglas tanto de entrada como de salida.

Primero, para poder tener acceso a los recursos de red y por lo tanto poder tener conexión a la misma, se debe habilitar las reglas preconfiguradas asignadas en el grupo "Redes principales" como se explicó en el punto 4.3.5.2.

Para acceso a páginas webs se necesita abrir los puertos correspondientes a HTTP y HTTPS para tener acceso a páginas webs seguras. Los puertos correspondientes a estos protocolos por defecto son el 80 y el 443 respectivamente.

Para acceso al correo electrónico desde un cliente de escritorio como pueda ser Outlook o Thunderbird existen dos opciones para la lectura de los buzones, IMAP[22] o POP, en este caso se ha abierto el puerto para el protocolo IMAP al que le corresponde los puertos 143 y 993. Así mismo para el envío de correo hay que habilitar el puerto 25 o el 465 según lo que especifique el servidor de correo. Si el uso del correo electrónico es vía web como el caso de cuentas pertenecientes a un Exchange como puedan ser las cuentas pertenecientes a un dominio privado como las de la universidad, no es necesario pues hacen uso de HTTPS para la conexión[23].

6.3.5.4. CORTAFUEGO MÁQUINA CON ACCESO REMOTO

Esta máquina se considera una extensión de la máquina explicada en el punto anterior. Se considera una máquina destinada a aun uso básico ofimático, así como acceso a Internet, correo electrónico y recursos compartidos en red.

Además, de lo nombrado con anteriormente, esta máquina se presenta como un estadio donde un posible administrador de sistemas, pueda tener acceso al equipo de manera remota con el objetivo, por ejemplo, de solucionar incidencias.

El puerto designado por defecto por Windows para las conexiones de escritorio remoto es el 3390, y aunque puede configurarse para designar otro[24]. En esta configuración se usará el que se ha designado por defecto.

Como se ha dicho, se debe crear una regla nueva, tanto entrante como saliente para el puerto 3390 con el protocolo TCP.

Abriendo este puerto y habilitando las conexiones de escritorio remoto en el equipo receptor, tendremos acceso desde la red local al mismo. Si se quisiera acceder estando fuera de la red, se recomienda el uso de una VPN para emular que nos encontramos en la misma red que el receptor.

6.3.5.5. CORTAFUEGO MÁQUINA PARA DESARROLLO

Esta máquina se considera un posible entorno de trabajo para una persona que se dedique a cualquier ámbito de la informática relacionado programación con control de versiones (Git o Git+Github/Bitlocker), servidores locales de testeo como pueda ser apache o NPM server. Además de las herramientas comunes en entornos de trabajo como pueda ser acceso a Internet, correo electrónico y recursos compartidos en red como impresoras o archivos.

Primero, para poder tener acceso a los recursos de red y por lo tanto poder tener conexión a la misma, se debe habilitar las reglas preconfiguradas asignadas en el grupo "Redes principales" como se explicó en el punto 4.3.5.2.

Para tener acceso a páginas web que usen tanto el protocolo HTTP como el HTTPS se deben crear reglas en las conexiones de entrada y de salida, para permitir las conexiones a los puertos 80 y 443.

Luego, si utiliza correo electrónico con clientes de escritorio se usará IMAP. Para ello, debemos crear reglas para permitir las conexiones tanto de entrada como de salida en los puertos 143 y 993. Si el acceso al correo es vía web ya está habilitado pues realizan las conexiones usando el puerto del protocolo HTTPS 443.

A continuación, se van a configurar las conexiones para que sean compatibles con Git como software para control de versiones y además hacer uso de algún repositorio online como pueda ser Github o Bitbucket. El manual de usuario de Github[25] indica que dependiendo del protocolo que usemos debemos abrir unos puertos u otros:

- HTTPS: puerto 443
- HTTP: puerto 80
- SSH: puerto 22
- Git: puerto 9418

Si se quiere tener algún tipo de servidor como pueda ser apache o NPM se debe abrir los puertos correspondientes a los mismos. Depende mucho de que puerto uso el servidor que usemos. Algunos ejemplos:

- Apache: puerto 80 / 443
- NPM server: puerto 3000
- Laravel: puerto 8000
- Ionic: puerto 8100

6.3.5.6. TABLA RESUMEN DE PUERTOS ABIERTOS EN CADA MÁQUINA

Puertos	Blindada	Usuario básico	Acceso Admin	Desarrollo
HTTP/HTTPS 80/443		X	X	X
IMAP/IMAPS 143/993		X	X	X
Acceso rem 3390			X	
SSH 22				X
Git 9418				X
Ionic 8100				X

Tabla 3. Relación de puertos abiertos en el cortafuego

6.3.6. CONFIGURACIONES AÑADIDAS RECOMENDADAS

En esta sección se añaden algunas configuraciones que son complementarias a otras mencionadas con anterioridad pero que no encajan los mismos puntos.

6.3.6.1. CONFIGURACIÓN DE USUARIO PARA ACCESO REMOTO

En el punto 4.3.5.4. se ha hablado de la apertura de puertos para permitir que se tenga acceso remoto al equipo haciendo uso del software de Windows "Escritorio remoto". Pero, es recomendable asignar un usuario específico para dicho uso, es decir, tener en el equipo un usuario para usar las credenciales de este con el fin de conectarse al escritorio remoto y que no se pueda usar otro.

Tener un usuario con ese único fin en el sistema destino del escritorio remoto, nos evitará que alguien pueda acceder al equipo si consigue averiguar las credenciales de otro usuario habitual.

Para ello, se accede a la ruta *Configuración – Sistema – Escritorio remoto – Cuentas de usuario* y ahí seleccionamos la opción "Seleccione los usuarios que pueden tener acceso remoto a este equipo".

En esta pantalla (Ilustración 52) podemos tanto agregar usuarios que tendrán permiso para acceder por escritorio remoto como quitar los que no se les quiera dar ese poder. Se ha creado un usuario llamado "Remoto" para tal fin, como se ve, se ha agregado y se va a comprobar que si se quiere acceder con cualquier otro no se puede.

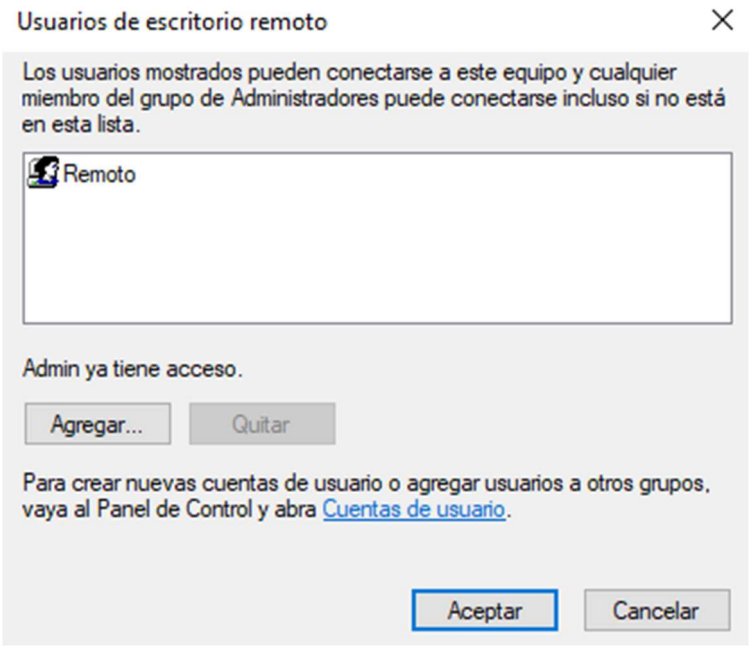


Ilustración 52. Añadir usuario remoto

Si se intenta realizar la conexión a escritorio remoto con el usuario "Omaro", un usuario estándar que no está añadido a los usuarios permitidos para acceder por escritorio remoto, nos denegará el acceso, aunque las credenciales sean correctas (Ilustración 53).

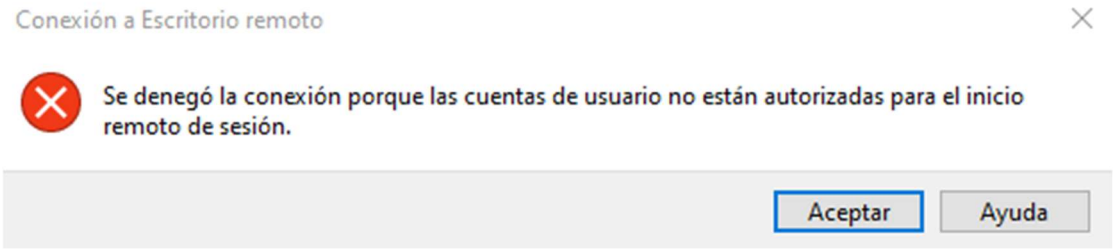


Ilustración 53. Acceso denegado al escritorio remoto

Si accedemos con el usuario "Remoto" e introducimos las credenciales correctamente, no habrá ningún problema para acceder al escritorio remoto.

6.3.6.2. CONFIGURAR UNA CONTRASEÑA, PIN O HUELLA DACTILAR.

Por defecto, en el momento de crear la primera cuenta de Windows, se crea con una contraseña, pero en caso de que no sea así, es recomendable proteger el equipo ante inicios de sesión indeseados. Para ello, es esencial que se le configure al equipo una contraseña, PIN, llave USB o algún sistema biométrico como una huella dactilar o desbloqueo facial.

Para ello, se accede a la configuración del sistema mediante el botón designado para ello en el menú inicio, o escribiendo "Configuración" en el mismo (Ilustración 54).

Ilustración 54. Menú configuración

Se entra en la opción "Cuentas" y de ahí en el apartado de "Opciones de inicio de sesión" para llegar al siguiente menú (Ilustración 55).

Ilustración 55. Opciones de inicio de sesión

En este menú podremos seleccionar el método con el que se quiera bloquear el sistema, contraseña, PIN, datos biométricos, llave USB y contraseña de imagen.

Tras seleccionar uno, se ha de completar el proceso que nos indica Windows. En el caso ejemplo de la ilustración 56, se ha escogido "PIN de Windows Hello" en el que se tiene que escoger un PIN y confirmarlo. Se reinicia el equipo y ya estará habilitada la opción.

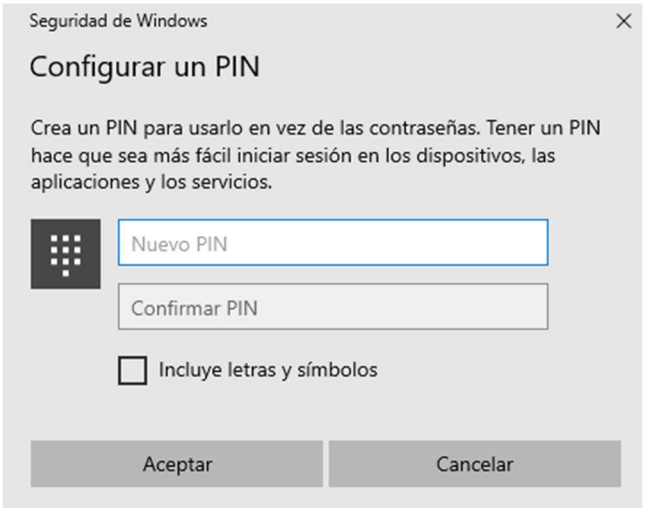


Ilustración 56. Configurar un PIN

6.3.6.3. FORZAR EL CAMBIO DE CONTRASEÑA DE FORMA PERIÓDICA.

Programar el cambio de contraseña para el inicio de sesión o para acceder a los servicios asociados al entorno laboral, es algo bastante común en los sectores empresariales. Pero, también es interesante plantearlo en un entorno de uso personal, sobre todo en equipo portátiles que tiendan a estar fuera de la seguridad física de una casa. En general, es buena práctica cambiar todas las contraseñas de forma periódica.

En Windows, se puede configurar el tiempo en el que es válida una contraseña y que sea necesario cambiar la misma cuando esta caduque.

Se abre una ventana ejecutar de Windows, con la combinación de teclas *Win+R* o escribiendo "Ejecutar" en el buscador del menú inicio.

Se escribe "netplwiz", que se trata de un gestor para los usuarios, y se le da al botón aceptar (Ilustración 57).

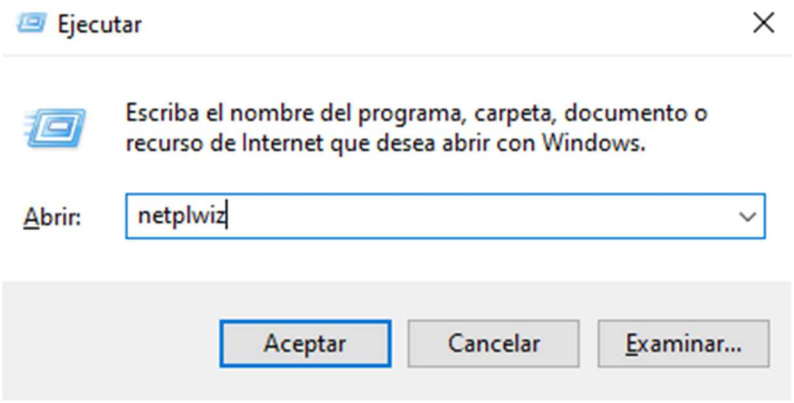


Ilustración 57. Ejecutar netplwiz

Dentro de la ventana que se ha abierto, se accede a la pestaña "Opciones avanzadas" y dentro de la sección "Administración avanzada de usuarios" se pulsa en el botón de Opciones avanzadas (Ilustración 58).

Ilustración 58. Administración avanzada de usuarios

En la zona de "Usuarios y grupos locales" se selecciona la opción "Usuarios" y en el panel central se elige el usuario que queramos configurar haciendo doble clic para acceder a sus propiedades. Una vez aquí se debe desmarcar la casilla "La contraseña nunca expira", esto hará que, por defecto, Windows pedirá que se cambie la contraseña de ese usuario cada 42 días (Ilustración 59).

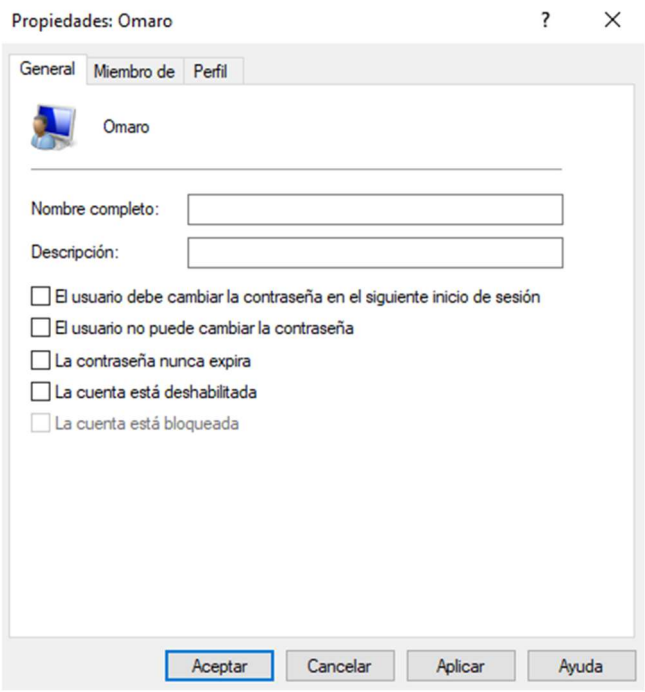


Ilustración 59.

Ya se ha comentado que el tiempo por defecto de renovación es de 42 días. Si se quiere cambiar el tiempo por defecto, se debe abrir una ventana ejecutar como en el primer paso, y ejecutar "gpedit.msc" que es el editor de políticas de grupo.

Se accede a la siguiente ruta *Directiva de equipo local – Configuración del equipo – Configuración de Windows – Configuración de seguridad – Directivas de cuenta – Directivas de contraseña* (Ilustración 60).

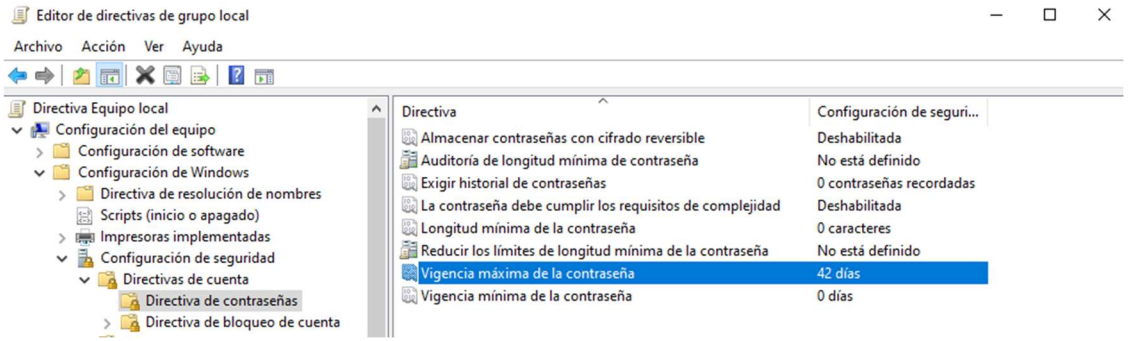


Ilustración 60. Cambiar vigencia de contraseña

Una vez aquí se edita la directiva "Vigencia máxima de la contraseña", que por defecto viene configurada a 42 días, en este caso se ha configurado a 30 días para que deba cambiarse mensualmente (Ilustración 61).

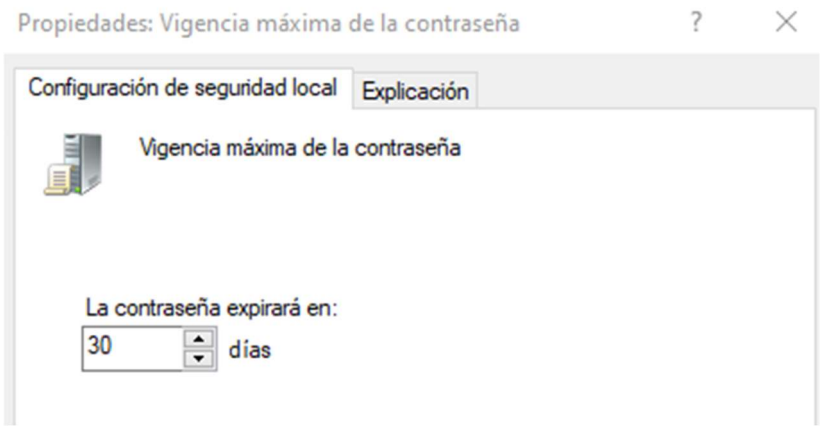


Ilustración 61. Vigencia máxima establecida en 30 días

6.3.6.4. CONTROL DE CUENTAS DE USUARIO

Una de las capas de seguridad que ofrece Windows 10 es el Control de cuentas o UAC. Se trata de una capa de seguridad en el sistema que trata de evitar cambios no autorizados en el sistema por parte de ciertas aplicaciones que puedan afectar a la seguridad o configuración del sistema. Esto lo hace mediante ventanas flotantes que avisan al usuario de que una aplicación va a realizar un cambio y si autoriza el mismo.

Es recomendable tener siempre activada esta función para evitar modificaciones indeseadas y que puedan comprometer la seguridad del sistema. Aunque a los usuarios pueda resultarles tedioso tener que avisos y tener que aceptar cambios.

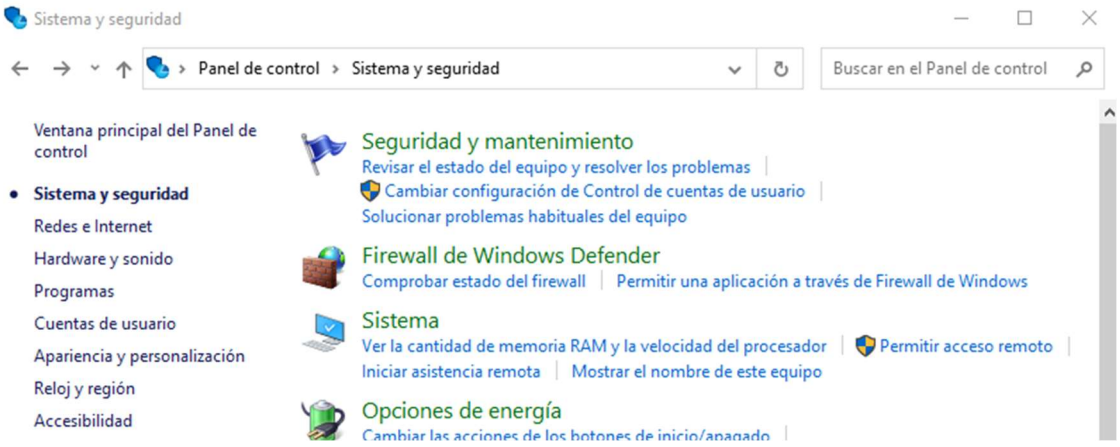


Ilustración 62. Sistema y seguridad en panel de control

Para activarla, se abre el panel de control y nos dirigimos a *Sistemas y seguridad – Seguridad y mantenimiento* (Ilustración 62).

Se hace clic en la pestaña Seguridad para desplegarla y se comprueba si el Control de cuentas de usuario está activado (Ilustración 63).

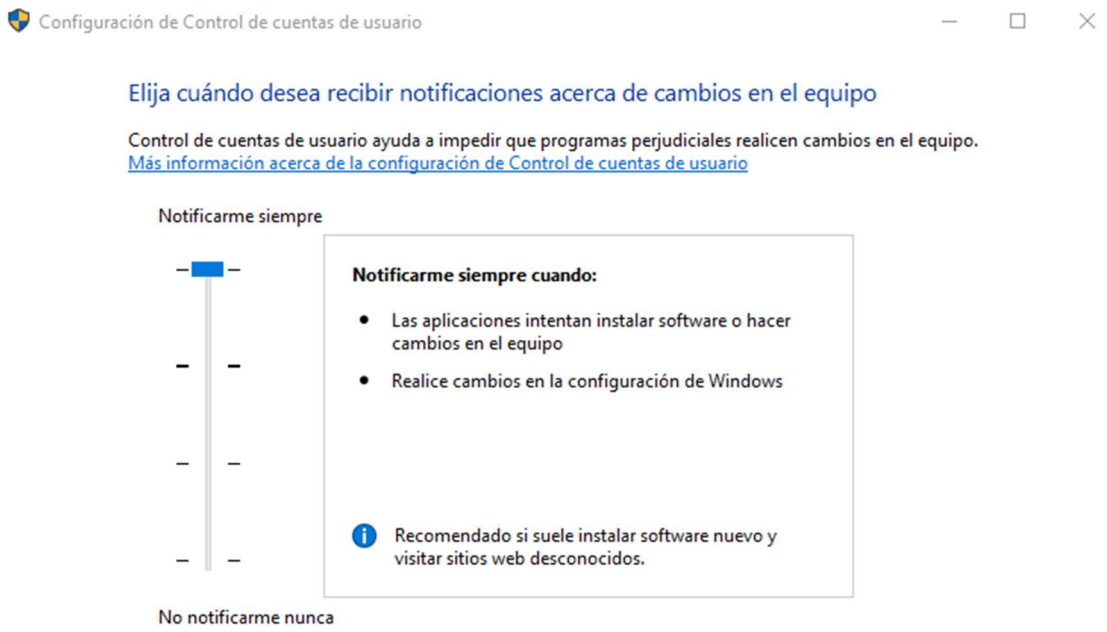


Ilustración 63. Control de cuentas de usuario

En caso negativo, se accede a cambiar configuración y se elige uno de los niveles que queramos para que se active, Windows recomienda el nivel tres que alerta cuando se intenta realizar un cambio en la configuración de Windows. Si se quisiera tener más seguridad, sería recomendable escoger el nivel cuatro, que además de lo anterior, alerta cuando se intenta instalar software o hacer cambios en el equipo. Para todos estos cambios se precisa permisos de administrador.

6.3.6.5. CUENTA DE USUARIO LOCAL

Microsoft en sus sistemas operativos Windows está tendiendo a promover el uso de cuentas de Microsoft basadas en la nube en lugar de cuentas locales pertenecientes al propio equipo en sí. El uso de ambas cuentas tiene sus ventajas e inconvenientes.

Por ejemplo, una configuración de cuentas basadas en la nube nos permite tener un ecosistema sincronizado con otros dispositivos Windows que tengamos asociados a la misma cuenta. Esto mismo hace que, si uno de los dispositivos es infectado y se logran cambiar ciertas configuraciones o aplicaciones, el resto de los dispositivos puedan estar comprometidos.

Por otro lado, una cuenta local no tiene las ventajas y la potencia para crear un ecosistema sincronizado entre varios dispositivos, pero permite tener una configuración más segura y privada.

En resumen, si se busca aumentar la seguridad, una opción más apropiada es utilizar una cuenta local en el equipo. Si se hace uso de una cuenta de Microsoft y se quiere hacer el cambio a una cuenta local en el equipo, el primer paso sería crear una cuenta local en el equipo si aún no existe una.

Se accede a la ventana de configuración y dentro de la misma a *Cuentas – Familia y otros usuarios – Agregar a otra persona a este PC* (Ilustración 64).

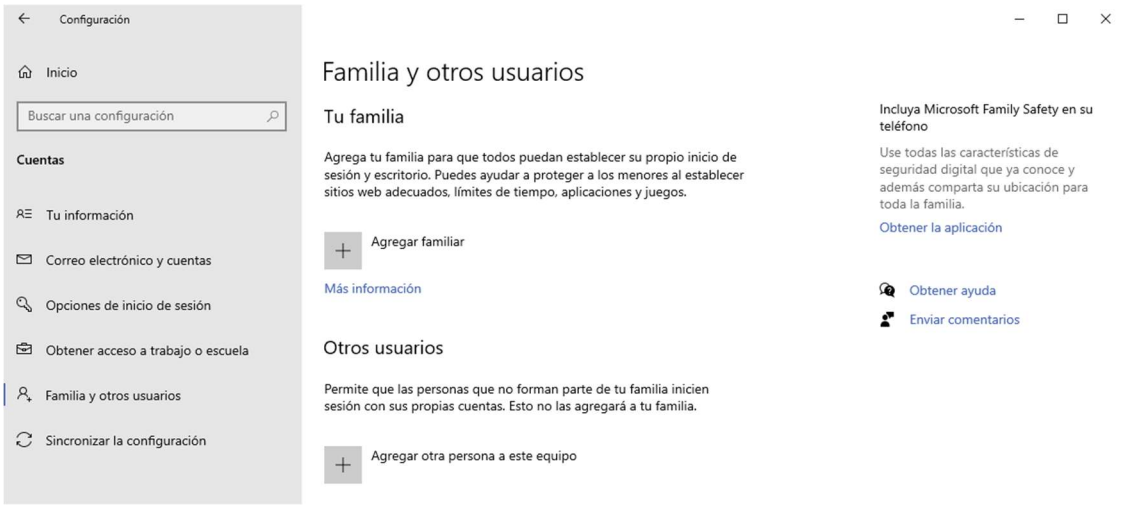


Ilustración 64. Familia y otros usuarios

En este momento, Windows pide que se introduzcan los datos de una cuenta Microsoft, debemos indicar que no tenemos los datos de inicio de sesión de esa persona y a continuación Agregar un usuario sin cuenta Microsoft. Completando el proceso se tendrá una cuenta local en el sistema (Ilustración 65).

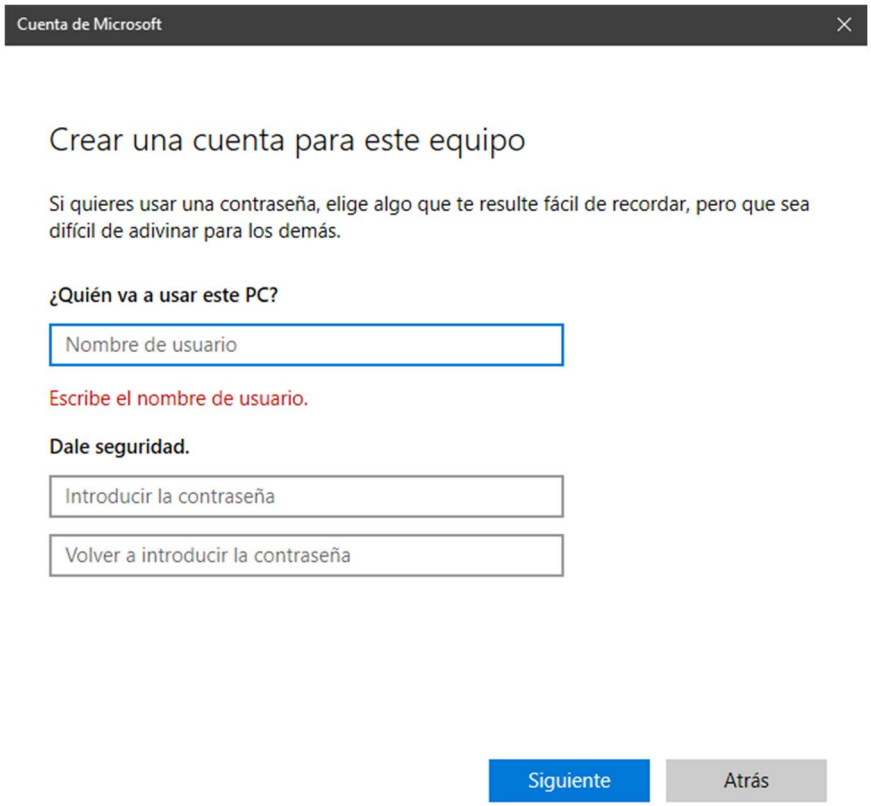


Ilustración 65. Crear cuenta de usuario local

Una vez creada la cuenta, si se accede a *Configuración – Cuentas* se podrá ver la opción "acceder con una cuenta local en su lugar". Si se selecciona, pedirá que se introduzcan tanto el usuario como la contraseña. Para terminar, se pulsa siguiente, se cierra sesión y Finalizar.

6.3.6.6. ACTUALIZACIÓN DE WINDOWS 10

Uno de los principales factores cuando se habla de seguridad en ordenadores se trata de tener todo el software actualizado. Esto permite contar con una mayor protección ante virus y amenazas, además de cubrir cualquier vulnerabilidad del sistema que haya sido arreglada con actualizaciones.

El sistema operativo cumple con esta misma regla aplicada a todo software, en Windows 10, Microsoft ha seguido una política bastante acertada en temas de seguridad. Pues pone al usuario en un escenario de máxima actualización y que las configuraciones se centran en atrasar o bloquear la misma.

Como el objetivo de este proyecto no es explicar todas las funcionalidades de Windows 10 al detalle, no se explicarán las opciones que se usan para configurar el retraso o desactivación de las actualizaciones de Windows 10.

Cabe destacar, que este apartado se incluye para hacer consciente al usuario de la importancia que tiene mantener el sistema lo más actualizado posible. Pues en las

actualizaciones, además de la incorporación de funcionalidades adicionales o mejoras en el rendimiento, se incorporan todos los parches para corregir las vulnerabilidades que se hayan descubierto en el sistema operativo y, por lo tanto, mantenerlo en el mayor estado de seguridad posible.

6.3.6.7. AUMENTAR LA PROTECCIÓN DE WINDOWS DEFENDER

El software de seguridad de Microsoft, Windows Defender, tiene una configuración por defecto funcional. Pero, existe una manera de aumentar la protección de Windows Defender que implica mejorar la seguridad de Windows 10. Realizar estos cambios en la configuración requiere hacer cambios en el registro del sistema, así que es recomendable crear un punto de restauración al que volver si algo sale mal.

Se abre una ventana ejecutar de Windows en la que se ejecutará regedit. Esto abre la interfaz gráfica del editor de registro. Una vez aquí, se navega por el árbol siguiendo la ruta *HKEY_LOCAL_MACHINE – SOFTWARE – Policies – Microsoft – Windows Defender*

En este nivel del árbol de registro, se crean dos claves con los nombres "MpEngine" y "Spynet" haciendo clic derecho sobre Windows Defender y en *Nuevo – Clave*. Se le dan los dos nombres nombrados con anterioridad a cada una de las claves.

Se entra en la clave de registro MpEngine y en una zona en blanco del panel derecho se hace clic derecho y se crea un nuevo valor DWORD de 32 bits. A este se le da el nombre "MpBafsExtendedTimeout" con valor "19" con la opción hexadecimal. Además, se hace lo mismo para añadir un nuevo valor DWORD de 32 bits con el nombre "MpCloudBlockLevel" y valor "2" en hexadecimal.

Ahora, se hace el mismo proceso en la clave Spynet. Aquí se crean tres nuevos valores DWORD de 32 bits con los siguientes nombre-valor, "DisableBlockAtFirstSeen" y "0", "LocalSettingOverrideSpynetReporting" y "1" y por último "SubmitSamplesConsent" y también valor "1".

Para que estos cambios sean efectivos se debe reiniciar. Estos cambios afectaran a Windows Defender otorgándole mayor protección en el momento de escanear y detectar amenazas que intenten infectar el sistema.

MpBafsExtendedTimeout[26] permite a Windows Defender bloquear archivos sospechosos durante un tiempo máximo de 60 segundos para examinarlos y comprobar si son seguros. En la documentación se indica que los tres valores asociados a Spynet deben estar activos porque esta característica depende de ellos.

MpCloudBlockLevel[27] indica la agresividad de la herramienta en cuanto a bloqueos y análisis de archivos sospechosos. El valor 2 indica el segundo nivel de protección, uno por encima del comportamiento estándar de Windows Defender.

DisableBlockAtFirstSeen: Garantiza que el equipo realiza las comprobaciones en tiempo real con Microsoft Activa Protection Service. El valor 0 indica que está activada.

6.3.6.8. CREAR UN PUNTO DE RESTAURACIÓN

Uno de los primeros pasos al instalar Windows es crear un punto de restauración del sistema para poder volver a ese estado del sistema en caso de que cualquier cambio que se realice salga mal y deje al sistema en un estado que no queremos. Esto permitirá dejar el sistema operativo en el mismo estado que estaba cuando se hizo el punto de restauración. Por defecto, esta opción no está activada, así que se debe activar de manera manual:

En el buscador de Windows se escribe restauración del sistema. Se selecciona la opción Crear un punto de restauración que pertenece al Panel de control. En el cuadro de dialogo Propiedades del sistema, se selecciona la pestaña Protección del sistema (Ilustración 66).

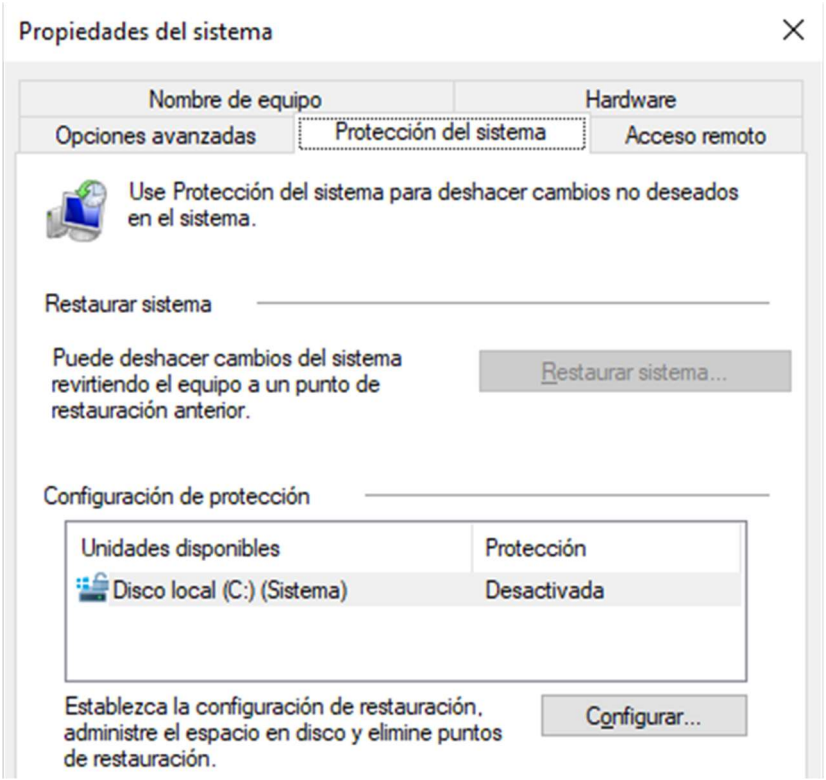


Ilustración 66. Protección del sistema, crear punto de restauración

En esta pestaña se podrán ver las unidades de disco conectadas y cuales tienen la protección activada. Se selecciona la unidad donde esté instalado el sistema operativo Windows. En la mayoría de los casos, el disco C, pero en caso de duda, el disco cuyo icono tenga añadido el logo de Windows. Se hace clic en configurar y en el cuadro de dialogo que aparece, se hace clic en la opción Activar protección del sistema, y para terminar en aceptar (Ilustración 67).

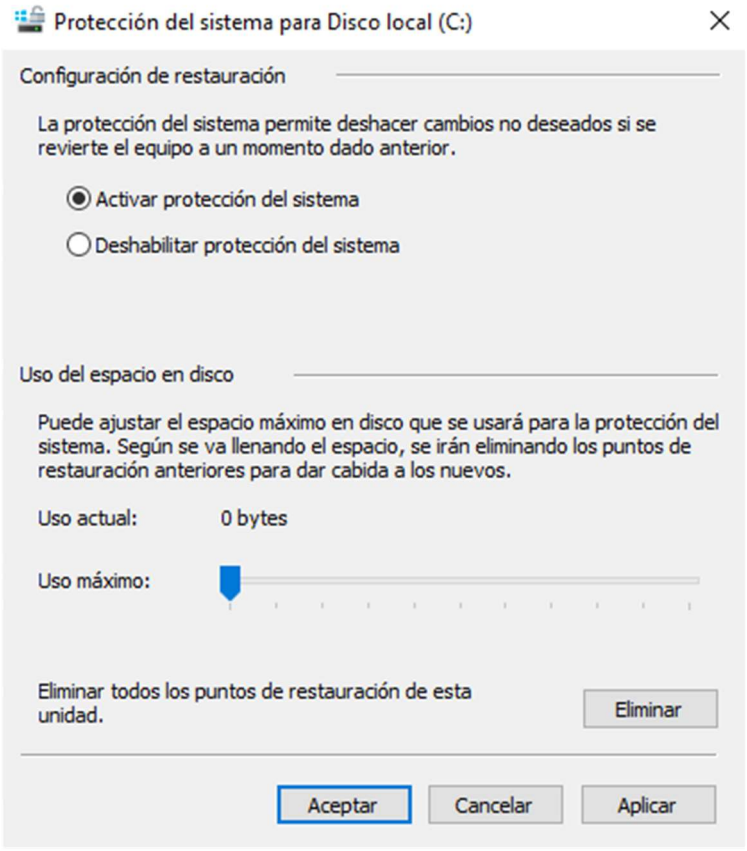


Ilustración 67. Activar protección del sistema

En este momento, se podrá volver a este cuadro y usar la opción Restaurar sistema para hacer que la máquina vuelva al punto de instalación deseado. También, si el sistema pasa a estar inoperativo, en el menú de arranque de Windows 10 podremos acceder a la restauración del sistema usando este mismo punto de restauración.

6.3.6.9. PROTECCIÓN CONTRA ALTERACIONES DE WINDOWS DEFENDER

A mediados del año 2019 Microsoft lanzó la actualización May 2019 Update de su sistema operativo Windows 10 que añadió una importante mejora Windows Defender, la "protección contra alteraciones".

Windows Defender es antivirus gratuito desarrollado por Microsoft, que viene instalado por defecto en su sistema operativo Windows 10. Actualmente, según Microsoft, más del 50% de los sistemas Windows se encuentran bajo la protección de Windows Defender[28], y, además, con los años de desarrollo y evolución, iguala en eficacia y protección a los antivirus comerciales

La protección contra alteraciones de Windows Defender se trata de una medida común en antivirus y herramientas comerciales con la que Windows Defender no contaba hasta el momento. El funcionamiento de esta se reduce en proteger de manera automatizada la configuración del mismo antivirus para así evitar que otras aplicaciones de terceros o algún tipo de malware puedan modificar esta configuración.

Dentro de esta mejora llamada protección contra alteraciones se incluye una protección en tiempo real, operaciones de análisis en la nube, Monitor de comportamiento, IOfficeAntivirus y opciones relacionadas con las actualizaciones inteligentes. Esto se traduce en que una vez activada la protección contra alteraciones de Windows Defender, ni los comando de cmd y Powershell, los cambios de registros de Windows, ni las aplicaciones empresariales de Microsoft, pueden cambiar ningún parámetro de la configuración del antivirus.

Para activar o comprobar si esta medida está activada, primeramente, se debe tener el sistema Windows 10 actualizado a la última versión. Se debe hacer uso del buscado de Windows y escribir "Seguridad de Windows" (Ilustración 68) y clicar en la opción "Protección antivirus y contra amenazas", para posteriormente acceder a Administrar la configuración en la sección "Configuración de antivirus y protección contra amenazas".

Ilustración 68. Menú de seguridad de Windows

Una vez se haya accedido a la ruta indicada se debe buscar la opción "protección contra alteraciones" y activarla (Ilustración 69).

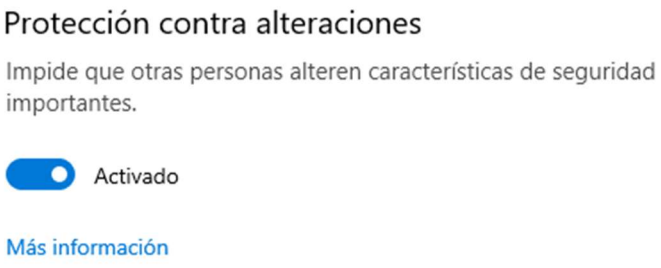


Ilustración 69. Activar protección contra alteraciones

6.3.7. PROTECCIÓN CONTRA WINDOWS

En puntos anteriores se ha centrado la seguridad del equipo desde un punto de vista externo, o al menos con agentes externos al sistema operativo o a la organización corporativa que hay detrás.

Pero existe un agente bastante importante a tener en cuenta, y ese es Microsoft. Se deben tener ciertas consideraciones a la hora de proteger los datos a los que accede del sistema operativo Windows 10 y, por consiguiente, que datos se le facilitan a la organización que hay detrás.

Los siguientes puntos tratan la seguridad de los sistemas Windows 10 desde un punto de vista de la privacidad del usuario con respecto a sus datos y como los gestiona Microsoft

6.3.7.1. DESACTIVAR CORTANA

Cada vez son más comunes y útiles los asistentes virtuales como lo son Siri, Alexa, Ok Google o en el caso que implica este trabajo, Cortana.

Para ser funcional, Cortana tiene acceso por defecto a un gran abanico de datos personales, así como datos referentes a lo profesional si se hace uso del ordenador para trabajar.

Es interesante, al menos, ser consciente de a qué información tiene acceso Cortana y si se quiere permitir que esto suceda o que simplemente Cortana esté activada en el equipo.

Primero, para saber a qué datos tiene Cortana permisos para acceder y usar se debe acceder a *Configuración – Cortana – Permisos*, una vez aquí se accede a administrar la información que Cortana puede tener acceso desde este dispositivo. Si se quiere aumentar la seguridad y la privacidad del sistema con respecto a Microsoft se deben desactivar todas las opciones (Ilustración 70).

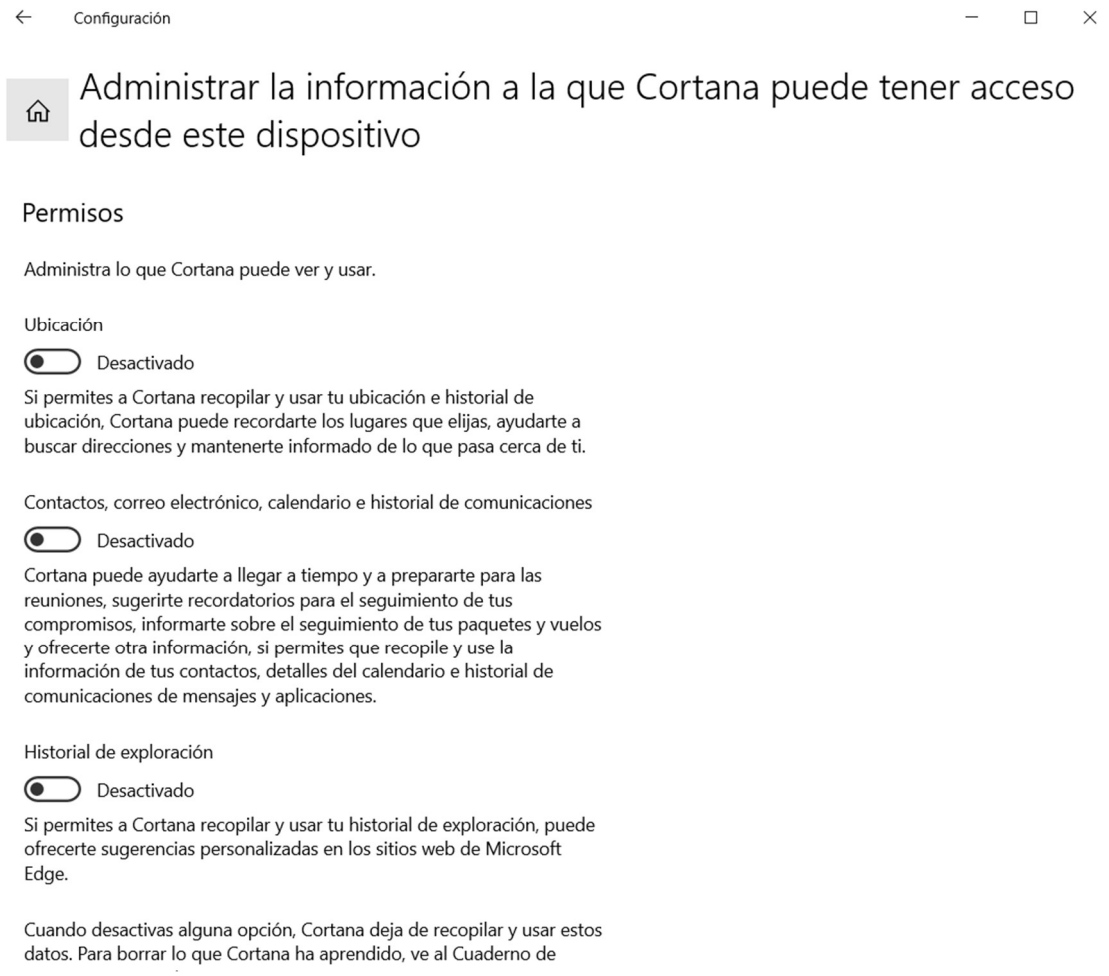


Ilustración 70. Administrar permisos de Cortana

Además, si se quiere evitar que Microsoft nos "escuche" usando Cortana, se deben desactivar tanto la opción "Hola Cortana" que se encuentra en la ruta *Configuración – Cortana – Hablar con Cortana*. Esto evitará que Cortana este activamente escuchando el micrófono a la espera de la palabra de activación (Ilustración 71).

Ilustración 71. Desactivar Hola Cortana

Como no solo Cortana usa el reconocimiento de voz, sino que hay también aplicaciones que usan el reconocimiento de voz en la nube, sería recomendable desactivar el reconocimiento de voz en línea. Para ello, se accede a la ruta *Configuración – Privacidad – Voz* y se desactiva el reconocimiento de voz en línea (Ilustración 72).

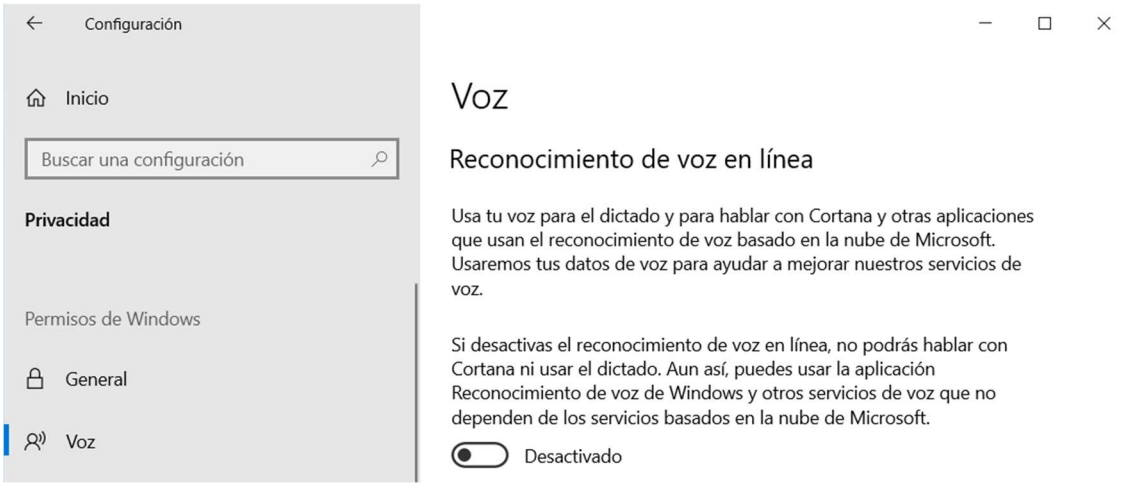


Ilustración 72. Desactivar reconocimiento de voz en línea

6.3.7.2. DESCARGAS DE OTROS EQUIPOS

Con la salida de Windows 10 al mercado, Microsoft incorporó una nueva característica a su sistema operativo para mejorar la velocidad de descargas. Se trata de una red de descarga tanto de actualizaciones como de aplicaciones, de otros sistemas Windows 10 que estén conectados a Internet en lugar de descargarlo de los servidores de Microsoft.

Esto se resume en que el equipo puede ser fuente de descarga de las aplicaciones o actualizaciones que tengamos instaladas desde otros equipos, ya sea de nuestra red o de Internet. Para evitar que suceda esto y añadir algo más de seguridad, es recomendable desactivar esta opción.

Se accede a la página de Configuración y dentro de esta a Actualizaciones y seguridad.

Dentro de la opción Windows Update se pulsa sobre Opciones avanzadas, dentro de esta se accede a Optimización de distribución.

Una vez aquí se desactiva la opción Permitir descargas de otros equipos para que no existan descargas donde este equipo sea la fuente (Ilustración 73).

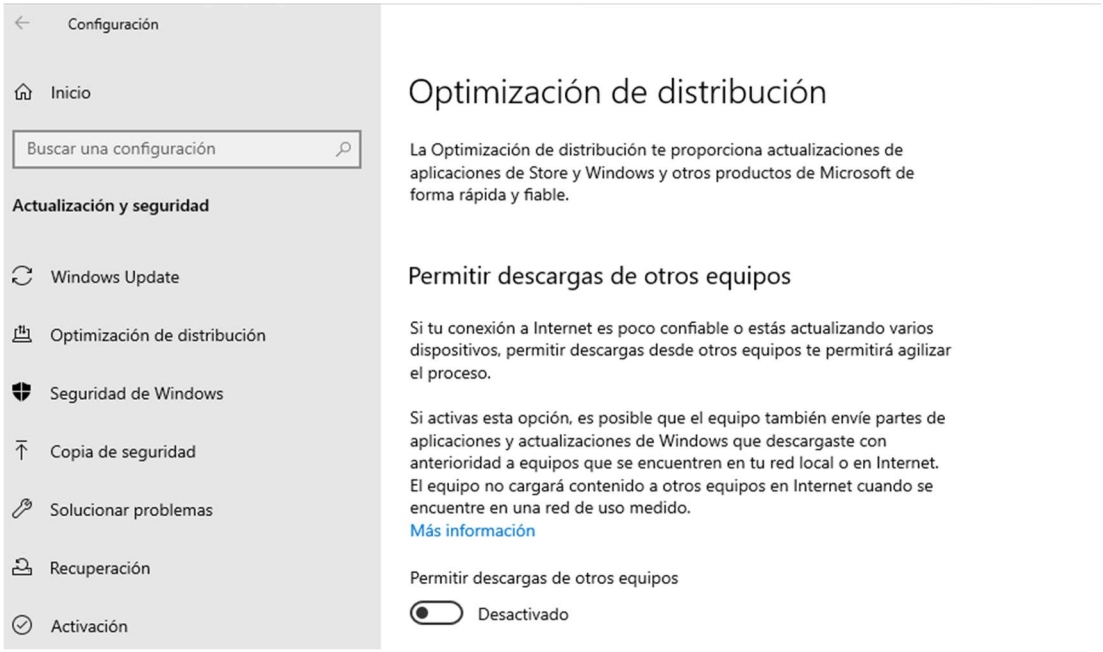


Ilustración 73. Desactivar permitir descargas de otros equipos

6.3.7.3. APAGAR LA UBICACIÓN

Como hace cualquier móvil, Windows 10 rastrea automáticamente la ubicación de manera continuada y guarda esa información durante 24 horas, para, entre otras cosas compartirla con aplicaciones de terceros que hayan sido descargadas en el equipo.

Esto puede parecer algo irrelevante si se es usuario de un ordenador sobremesa cuya ubicación será siempre la misma teóricamente. Pero, no lo es tanto si se plantea el problema en usuarios de equipos portátiles personales y además los equipos portátiles de empresa.

Se accede a la ruta *Configuración – Privacidad – Ubicación* y en la primera opción llamada "Permitir el acceso a la ubicación en este dispositivo" se puede desactivar la ubicación de este como se muestra en ilustración 74.

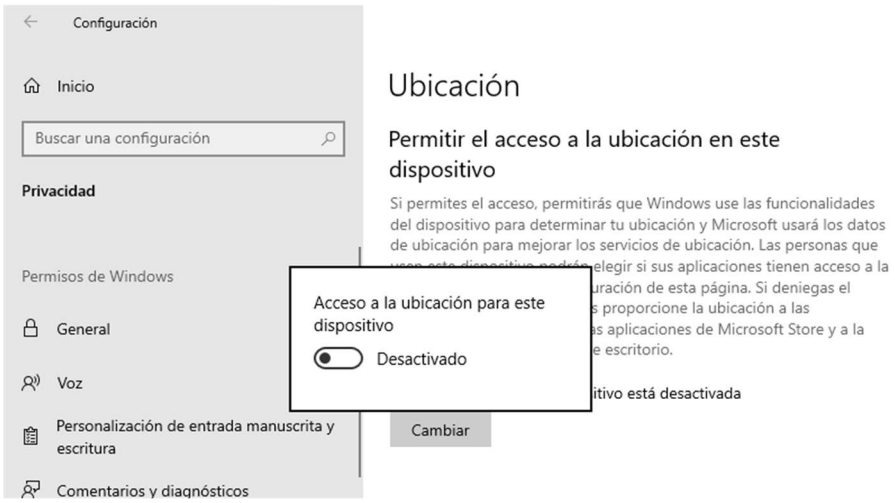


Ilustración 74. Desactivar la ubicación en Windows 10

6.3.7.4. BLOQUEAR EL SEGUIMIENTO DE ANUNCIOS

El seguimiento de anuncios puede ser una auténtica molestia en cuanto a la invasión de anuncios que se ofrecen en la red se refiere. Esto se traduce en que, si un día se está buscando información sobre el "Grado en Ingeniería Informática de la ULPGC" por poner un ejemplo, probablemente comience a aparecer publicidad sobre otros cursos privados y demás en posteriores navegaciones.

Windows tiene activado el seguimiento de anuncios de forma predetermina pues le interesa al ser un modelo de negocio bastante común en la actualidad, vendiendo esos datos a otras empresas.

Para desactivarlo se debe ir al apartado de privacidad del menú de Configuración, la ruta sería *Configuración – Privacidad – Cambiar opciones de privacidad*. Aquí se desactiva la opción "Permitir que las aplicaciones usen el id. de publicidad" (Ilustración 75).

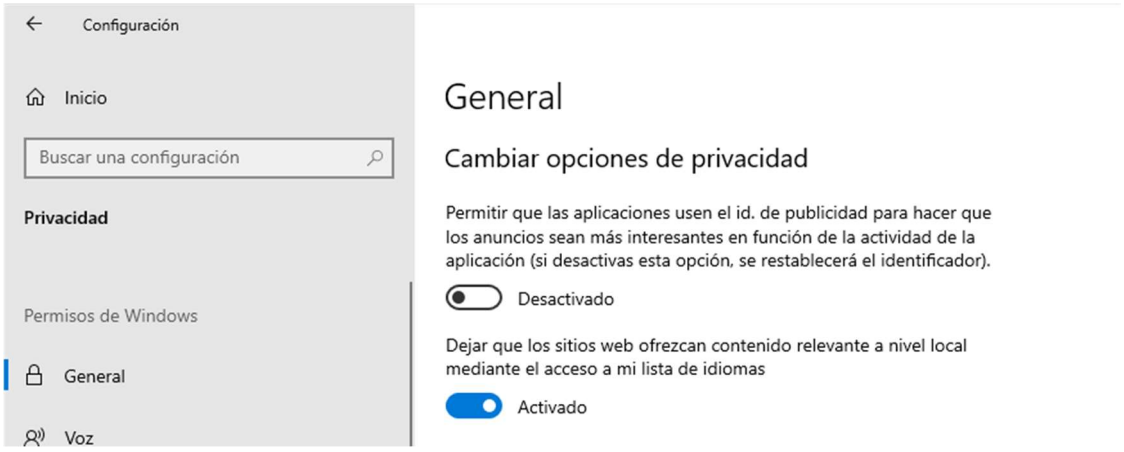


Ilustración 75. Desactivar seguimiento de publicidad

6.3.7.5. DESACTIVAR EL ACCESO A LA CÁMARA Y AL MICRÓFONO

Bien es sabido que es posible que los cibercriminales puedan lograr activar la cámara y micrófono de un equipo sin el consentimiento del usuario. No es algo tan raro como se muestra en la película "Snowden" de 2016[29], que, aunque se trata de ficción, representa muy bien lo que sucede en la realidad. Y, por lo tanto, es importante establecer medidas que impidan o dificulten estas acciones.

Para ello, lo primero sería desactivar la cámara y solo activarla en el momento que se vaya a usar como para realizar una videoconferencia o alguna llamada personal. Para desactivarla, se accede a *Configuración – Privacidad – Cámara* y desactivamos la opción "Permitir el acceso a la cámara en este dispositivo" (Ilustración 76). Sería recomendable además tapar la cámara con algún método físico.

Ilustración 76. Desactivar acceso a cámara

Del mismo modo, al igual que con la cámara, es recomendable desactivar el micrófono para evitar que exista manera de activarlo sin nuestro consentimiento. Para ello, se accede a *Configuración – Privacidad – Micrófono* y desactivamos la opción "Permitir el acceso al micrófono en este dispositivo" (Ilustración 77).

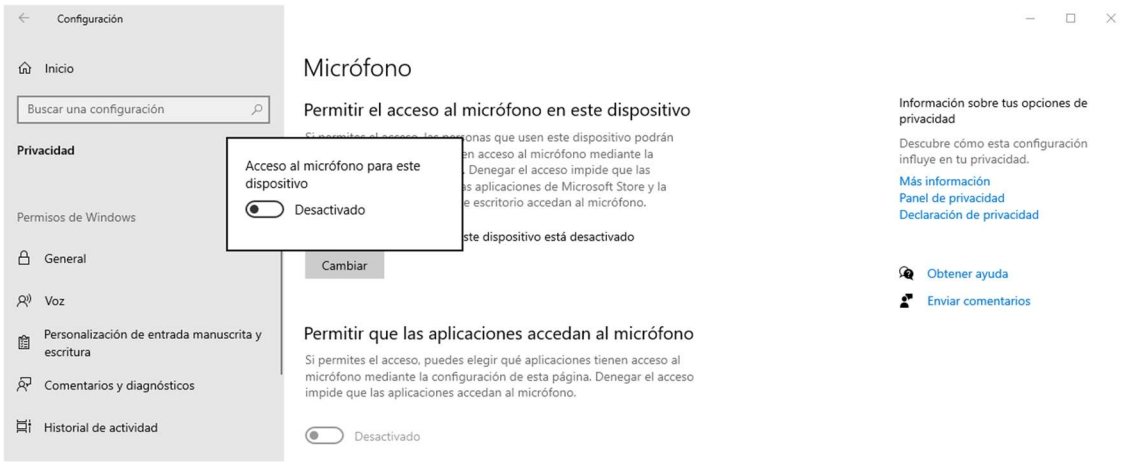


Ilustración 77. Desactivar acceso a micrófono

7. CONCLUSIONES Y TRABAJOS FUTUROS

Cada día vivimos en una sociedad más conectada y poco a poco el número de dispositivos y personas conectadas entre sí irá en aumento. Esto hace, de manera directamente proporcional, más importante que la sociedad sea consciente de preocuparse por la seguridad de sus dispositivos y los datos que estos poseen. Así mismo, Windows 10 es el sistema operativo que mayor cuota de mercado abarca lo que hace importante que el mayor número de usuarios sean conscientes y sepan usar las medidas de seguridad que el propio sistema operativo les ofrece, además del software de terceros que quieran usar para añadir seguridad complementaria.

En este documento se pueden encontrar algunas formas en la que los ataques pueden realizar ciertas acciones no deseadas en los sistemas Windows 10 y las contramedidas a aplicar para evitar que esto suceda, o al menos, para hacerles la tarea más complicada. Por otro lado, se recogen algunas prácticas recomendadas y que nos ofrece el sistema operativo para aplicarlas como pueda ser el caso de VPN. Y una serie de opciones que nos proporcionaran mayor seguridad y privacidad de cara a Microsoft.

Pero, todo el documento se centra exclusivamente en instalaciones locales sin un control centralizado. Así que, como posibles trabajos futuros y de expansión de este documento, podría darse un enfoque de carácter más empresarial pues, como ya se ha dicho antes, todas las medidas documentadas en este proyecto están enfocadas a instalaciones locales. Pero, Microsoft en su sistema operativo de servidores Windows Server, ofrece muchas más medidas y configuraciones aún más personalizables por usuario o grupo de usuarios e incluso por equipos particulares. Todo esto enfocado a un sistema centralizado basado en Active Directory donde cada equipo perteneciente al dominio, pueden ser configurados por el servidor.

Otro posible enfoque sería centrarse en configuraciones propias de Windows 10 como se ha mostrado en este documento, pero llevado a un nivel más técnico y profundo, hablando de modificación de registros y la investigación de todos los valores posibles que tiene cada registro y que no se ven en el sistema operativo, sino que se

encuentra en la documentación técnica de cada valor de registro. Además, existe la opción de centrarse en scripts de configuración lo cual podría ser otro enfoque de investigación. Centrando la investigación en la creación de un documento más técnico orientado a un perfil de usuario con un nivel medio – avanzado en sistemas operativos.

8. BIBLIOGRAFÍA

[1] "• How many people have access to a computer 2018 | Statista." https://www.statista.com/statistics/748551/worldwide-households-with-computer/ (accessed Apr. 28, 2020).

[2] Statista Research Department, "• Share of households with a computer in developed countries 2005-2019 | Statista," *Computer penetration rate among households in developed countries 2005-2019*, Mar. 02, 2020. https://www.statista.com/statistics/748557/developed-countries-households-with-computer/ (accessed Apr. 28, 2020).

[3] "Desktop Operating System Market Share Worldwide | StatCounter Global Stats." https://gs.statcounter.com/os-market-share/desktop/worldwide (accessed Apr. 28, 2020).

[4] "¿En qué consisten la tecnología de virtualización y las máquinas virtuales? | VMware | ES." https://www.vmware.com/es/solutions/virtualization.html (accessed May 04, 2020).

[5] "Wayback Machine." https://web.archive.org/web/20091007205439/http://www.madrimasd.org/informacionidi/biblioteca/publicacion/doc/VT/VT19_green_IT_tecnologias_eficiencia_energetica_sistemas_TI.pdf (accessed Jun. 02, 2020).

[6] "¿Qué es KVM?" https://www.redhat.com/es/topics/virtualization/what-is-KVM (accessed May 06, 2020).

[7] "pfSense® - World's Most Trusted Open Source Firewall." https://www.pfsense.org/ (accessed Jul. 26, 2020).

[8] "Windows Defender Firewall with Advanced Security (Windows 10) - Windows security | Microsoft Docs." https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security (accessed Jul. 26, 2020).

[9] "BitLocker (Windows10) - Microsoft 365 Security | Microsoft Docs." https://docs.microsoft.com/es-es/windows/security/information-protection/bitlocker/bitlocker-overview (accessed Jul. 13, 2020).

[10] "Recomendaciones para TPM (Windows 10) - Microsoft 365 Security | Microsoft Docs." https://docs.microsoft.com/es-es/windows/security/information-protection/tpm/tpm-recommendations (accessed Jul. 14, 2020).

[11] "IPsec - Wikipedia, la enciclopedia libre." https://es.wikipedia.org/wiki/IPsec (accessed Aug. 31, 2020).

[12] "VPN: A Key to Securing an Online Work Environment - Security Boulevard." https://securityboulevard.com/2020/03/vpn-a-key-to-securing-an-online-work-environment/ (accessed Jul. 16, 2020).

[13] "What is MMC?" https://support.microsoft.com/en-us/help/962457/what-is-mmc (accessed May 14, 2020).

[14] "IExpress - Wikipedia, la enciclopedia libre." https://es.wikipedia.org/wiki/IExpress (accessed May 19, 2020).

[15] "Batch files - Use REGEDIT to add, read or delete registry values." https://www.robvanderwoude.com/regedit.php (accessed May 19, 2020).

[16] "Command-Line Options - Win32 apps | Microsoft Docs." https://docs.microsoft.com/en-us/windows/win32/msi/command-line-options (accessed May 19, 2020).

[17] "Group Policy Overview | Microsoft Docs." https://docs.microsoft.com/es-es/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831791(v=ws.11) (accessed May 20, 2020).

[18] "Introducción a Active Directory Domain Services | Microsoft Docs." https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (accessed May 20, 2020).

[19] "Cuál es mi IP | Cómo saber mi IP pública." https://www.cual-es-mi-IP.net/ (accessed Jun. 04, 2020).

[20] "TCP protocol: así funciona el protocolo de transmisión - IONOS." https://www.ionos.es/digitalguide/servidores/know-how/que-es-tcp-transport-control-protocol/ (accessed Jun. 08, 2020).

[21] "UDP: ¿qué es UDP? - IONOS." https://www.ionos.es/digitalguide/servidores/know-how/udp-user-datagram-protocol/ (accessed Jun. 08, 2020).

[22] "Protocolo de acceso a mensajes de Internet - Wikipedia, la enciclopedia libre." https://es.wikipedia.org/wiki/Protocolo_de_acceso_a_mensajes_de_Internet (accessed Jun. 08, 2020).

[23] "Puertos de red para los clientes y el flujo de correo en Exchange | Microsoft Docs." https://docs.microsoft.com/es-es/exchange/plan-and-deploy/deployment-ref/network-ports?view=exchserver-2019 (accessed Jun. 09, 2020).

[24] "Cambio del puerto de escucha en Escritorio remoto | Microsoft Docs." https://docs.microsoft.com/es-es/windows-server/remote/remote-desktop-services/clients/change-listening-port (accessed Jun. 09, 2020).

[25] "Puertos de red - Ayuda de GitHub." https://help.github.com/es/enterprise/2.18/admin/installation/network-ports (accessed Jun. 09, 2020).

[26] "Configura la comprobación de la nube extendida." https://getadmx.com/?Category=Windows_10_2016&Policy=Microsoft.Policies.WindowsDefender::MpEngine_MpBafsExtendedTimeout&Language=es-es (accessed Jul. 31, 2020).

[27] "Selecciona el nivel de protección de la nube." https://getadmx.com/?Category=Windows_10_2016&Policy=Microsoft.Policies.WindowsDefender::MpEngine_MpCloudBlockLevel&Language=es-es (accessed Jul. 31, 2020).

[28] "Windows Defender: más de 500 millones de equipos con Windows utilizan este antivirus." https://www.genbeta.com/windows/mitad-todos-usuarios-windows-estan-utilizando-antivirus-microsoft (accessed Aug. 31, 2020).

[29] "Snowden (2016) - IMDb." https://www.imdb.com/title/tt3774114/ (accessed Aug. 10, 2020).