Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Configuración segura de un entorno Windows. Elaboración de un documento de buenas prácticas de seguridad en entornos Windows

Grado en Ingeniería Mecánica

ALUMNO: José Manuel Bausá Miranda

DIRECTORES: Belén Barragáns Martínez

Pablo Sendín Raña

CURSO ACADÉMICO: 2014-2015

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Configuración segura de un entorno Windows. Elaboración de un documento de buenas prácticas de seguridad en entornos Windows

Grado en Ingeniería Mecánica

Intensificación en Tecnología Naval

Infantería de Marina

Universidad de Vigo

RESUMEN

En la actualidad, en todos los ámbitos de trabajo, se implementa el uso de los medios informáticos para almacenar, enviar, recibir y gestionar información de diversos tipos. Debido a esto, la correcta gestión de estos equipos para convertirlos en sistemas seguros, y con ello proteger la información y datos que almacenan, ha adquirido una importancia crucial en los últimos años.

En el presente TFG, se ha llevado a cabo una recopilación exhaustiva de información relacionada con la seguridad de los equipos. Tras su estudio, se ha elaborado un documento que sirve de guía de buenas prácticas y recomendaciones a llevar a cabo, por cualquier usuario de nivel medio de experiencia. Las medidas se centran en un equipo operado con Windows 7, con el objetivo de convertirlo en un entorno seguro.

Estas medidas se han abordado siguiendo una aproximación por capas, desde la seguridad física al más bajo nivel hasta llegar a la seguridad de los datos. Además se han tratado aspectos relacionados con la seguridad en los dispositivos removibles y el borrado y recuperación de archivos. Con este método aseguramos no olvidar ningún nivel del sistema por gestionar y establecemos los medios necesarios para estar convenientemente protegidos frente a ataques e infecciones de *malware*.

Finalmente, se ha concluido, tras la realización del presente proyecto, que los objetivos que se buscaban han sido cumplidos. Se ha adquirido una mayor concienciación en lo referente a la seguridad de nuestra información y se han mostrado medidas que debemos aplicar a la hora de asegurar los equipos que utilizamos. Asimismo, presentamos unas posibles líneas futuras que permitan proseguir y ampliar la investigación y estudio en esta materia, como la aplicación de las medidas en otros S.O. o dispositivos móviles.

PALABRAS CLAVE

Windows 7, guía buenas prácticas, configuración segura, protección contra *malware*, seguridad información

AGRADECIMIENTOS

A mi padre, que pese a tener suficiente trabajo de por sí, supo con su incansable paciencia y enormes esfuerzos, proporcionarme información y consejos, muy valiosos y útiles, sin los que no hubiera sabido empezar y sin los que este proyecto carecería de cierto sentido. Gracias por, una vez más, nunca decir que no.

A Paloma, por ofrecerse en varias ocasiones, aun no estando familiarizada con la materia y sus términos, a leerse, revisar y corregir lo que pudiera del proyecto, arriesgándose a que le dijera que sí. Gracias por hacerme sentir ese apoyo constante.

A mis tutores, por no dejar ni una semana de lado la revisión de mis avances, incluso en sus tiempos libres, sabiendo aconsejarme y dirigirme de manera estricta, pero necesaria y a su vez provechosa. Gracias por no dejarme a la deriva y sin guías.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Contexto

Desde el hombre pre-histórico en defensa de su cueva, pasando por los reyes medievales y sus castillos, hasta el ciudadano de a pie del siglo XXI con sus bienes, todos han tenido que aplicar medidas de seguridad contra diferentes peligros para proteger sus intereses.

Hasta el momento siempre fueron contramedidas físicas, visibles e intuitivas. Pero ahora, con la invención de los ordenadores, el desarrollo de diferentes sistemas electrónicos y la evolución de las tecnologías de la información en la época actual, no estamos sólo expuestos a peligros "físicos". Aunque, por un lado, todas estas mejoras ofrecen un entorno con nuevas posibilidades y oportunidades de expansión, negociación e intercambio de información y comunicaciones, por otro lado, conllevan nuevos riesgos y amenazas y son claramente una vía para el robo de información sensible.

Nos enfrentamos a una era en la que las amenazas pueden encontrarse en un ámbito del que poco sabemos. Este ámbito es el conocido como "virtual" y está constituido por las redes, los dispositivos a ellas conectados y la información que contienen.

La facilidad con la que estos ataques pueden perpetrarse, el bajo coste de las herramientas necesarias, el anonimato bajo el que se puede actuar desde cualquier parte del mundo, son algunas de las motivaciones de los atacantes. Esto se debe a que uno de los bienes más preciados de hoy en día se guarda de forma electrónica, ya sean documentos clasificados, proyectos, prototipos, planos, diseños, trabajo, recuerdos e imágenes, etc. Toda esta información se considera un activo valioso y requiere en consecuencia una protección adecuada. Por ello es de sumo interés profundizar para conocer la naturaleza y funcionamiento de los peligros y ataques, para poder hacerles frente y mantener a buen recaudo nuestros datos.

1.2 ¿Por qué es necesaria la seguridad de la información?

Las diferentes empresas y órganos de distintos ámbitos y sus sistemas de información se enfrentan cada vez con más frecuencia a riesgos procedentes de diversas fuentes, incluyendo fraudes informáticos, espionaje industrial, sabotaje o simple vandalismo. Ciertas amenazas como virus, ataques de intrusión, denegación de servicio, etc., se están volviendo cada vez más comunes, ambiciosas y sofisticadas.

El buen desarrollo de los trabajos de la época actual depende principalmente de los sistemas y servicios de información. Si estos sistemas no están correctamente protegidos, somos más vulnerables a las amenazas a su seguridad.

El uso de redes, el aumento de usuarios que utilizan los equipos y la necesidad de compartir información con entidades externas, son algunos de los ejemplos que nos muestran la dificultad de conseguir el control de la información. Muchos sistemas no están configurados para protegerse contra ciertas amenazas, por ello debemos apoyarnos en una gestión y unos procedimientos adecuados.

La seguridad de los equipos es un tema abordado en todo tipo de ámbitos y niveles. Ya sea por propia privacidad de datos personales de un individuo, por temas de espionaje industrial a nivel empresarial o, al más alto nivel, por estrategias de seguridad nacional (esto nos da una idea de la magnitud de importancia de la cuestión), la seguridad informática está presente en los diversos ámbitos de la sociedad (empresas, entornos familiares, etc.) y a distintos niveles (nacional, europeo, internacional, etc.).

La seguridad de la información está definida en algunos ámbitos (como en la norma ISO-UNE/IEC 17799 [1]) como la adquirida al alcanzar y preservar la confidencialidad, integridad y disponibilidad de la información (Figura 1-1). Estas características se consideran esenciales para mantener la competitividad, tesorería, rentabilidad e imagen comercial de una empresa.

Figura 1-1 Tres aspectos que definen la seguridad de la información

Entendemos la confidencialidad como la propiedad que impide la divulgación de información a personas o sistemas no autorizados; la integridad como la cualidad que persigue que los datos permanezcan libres de modificaciones no autorizadas; y la disponibilidad como la característica de la información de encontrarse a disposición de quién debe acceder a ella.

Además, en el dominio empresarial, el espionaje industrial es un riesgo con el que empresas pertenecientes a ciertos ámbitos de especial competencia han de lidiar constantemente. Muchas organizaciones no logran comprender cómo la competencia pudo dar con cierta información sensible o clasificada que se encontraba en un entorno que consideraban “seguro”.

Pocas empresas o países reconocerían que les han robado información por razones de prestigio o miedo a los escándalos que suscitan este tipo de hechos en los medios de comunicación social. Además de estas grandes pérdidas económicas, este tipo de actividades también llevan aparejadas pérdidas de contratos, puestos de trabajo y la posible degradación de la imagen del país o empresa.

Mientras un caso de sustracción de información en un usuario aislado puede ocasionar pérdidas sentimentales o laborales, en mayor o menor medida recuperables, en el caso empresarial podría

conllevar pérdidas económicas muy elevadas e incluso, en el ámbito estratégico, a una situación de amenaza nacional.

Por todo ello, es aconsejable fomentar el interés por profundizar y descubrir las amenazas y contramedidas necesarias para crear un entorno de trabajo y vida social seguro. Tanto a título e interés personal como colectivo, se debería comenzar por los dispositivos utilizados más habitualmente.

1.3 Objetivos

Este trabajo fin de grado pretende, tras una exhaustiva búsqueda, filtrado y análisis de información relevante relacionada con la seguridad de la información, sentar unas bases y esquemas de configuración necesarios para que un usuario, tanto en un ámbito personal, empresarial, civil o militar, de un equipo con un sistema operativo (S.O.) específico conozca y sepa aplicar una configuración segura que proteja al equipo, y la información que guarde, tanto de amenazas externas como internas. Es importante dejar claro que las medidas de seguridad no se centrarán por ello en la configuración ni administración de la red (intranet o Internet), lo cual escapa del ámbito del proyecto, sino en el equipo conectado (o no) a la misma.

Se elaborará un documento que servirá de "guía de buenas prácticas" que aglutine una serie de consejos y recomendaciones de configuración concernientes a la seguridad de un PC que permita que alguien no experto en la materia lo ponga en práctica. Este documento considerará Windows 7 como el sistema operativo elegido.

El hecho de haber elegido este sistema operativo se justifica por tratarse del sistema operativo más utilizado a nivel mundial como podemos apreciar en los datos oficiales de las Figuras 1-1 y 1-2 (Web Statcounter).

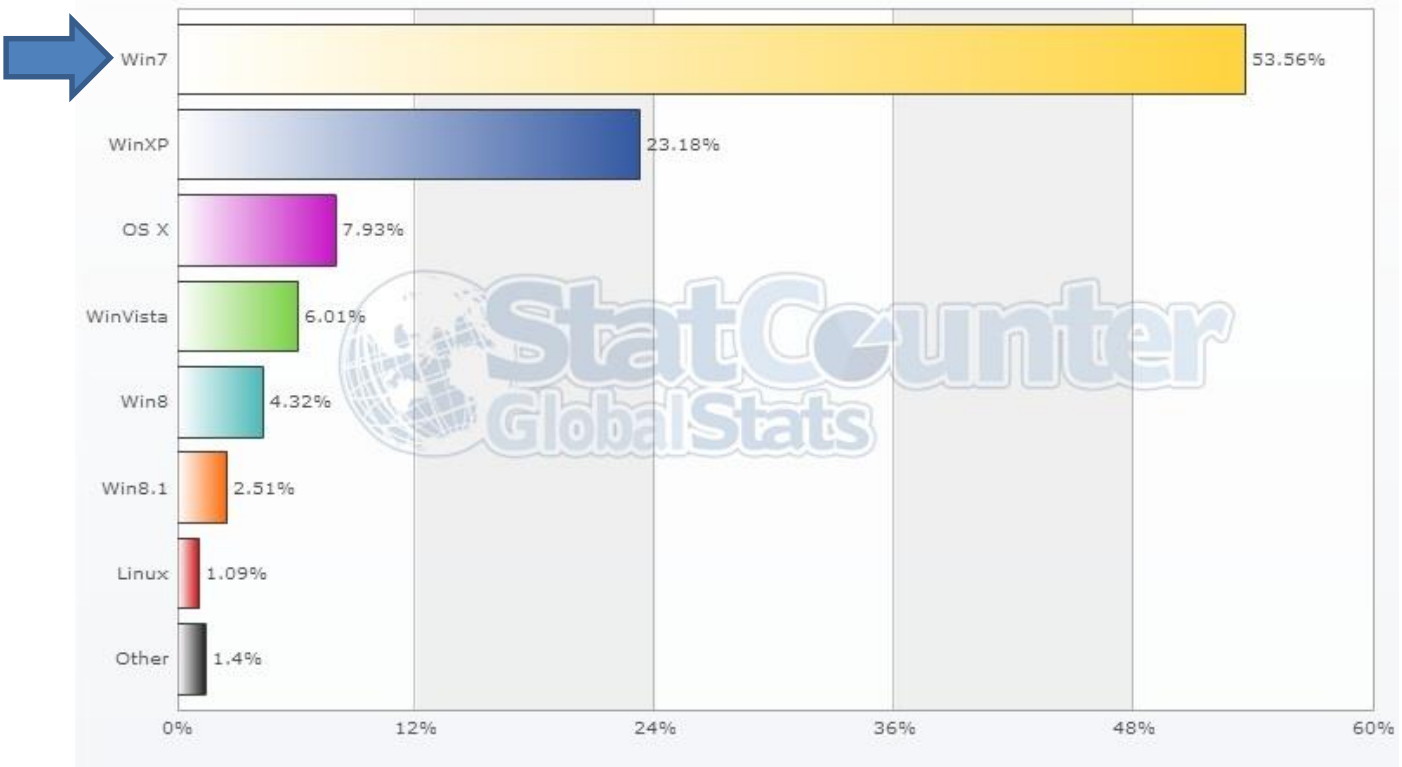

Figura 1-2 Siete S.O. más usados en el mundo en equipos de sobremesa en los últimos 3 años [2]

Figura 1-3 S.O. más usado en cada país en equipos de sobremesa (enero de 2015) [3]

Se puede apreciar en la Figura 1-3 el hecho indiscutible de que Windows 7 es, a día de hoy, el sistema operativo más utilizado en el mundo, ya que incluso comparándolo con otros tres sistemas operativos, apenas se aprecia rastro de que ninguno de ellos sea el más utilizado en otro país.

En este TFG se abordarán distintos aspectos:

- Se realizará un estudio y revisión de diferentes documentos relevantes, seleccionados entre muchos otros, que traten diversas recomendaciones de configuración segura del sistema, tomadas de varias fuentes (informes web, trabajos investigación, normativas, libros, etc.) que se citarán a lo largo del documento.
- Se filtrarán las diversas medidas de seguridad que traten los documentos recopilados, quedándonos con las medidas más repetidas, relevantes e importantes.
- Se elaborará una guía de buenas prácticas de seguridad que contenga los campos que se consideren más importantes y oportunos que se deben tratar para ofrecer seguridad a un equipo, lo cual constituirá el centro de gravedad del trabajo.
- Se citarán y explicarán las diferentes herramientas que servirán de ayuda en la prevención/recuperación ante diversos tipos de ataques.
- Se guiará al lector a través de la configuración segura recomendada/elegida en este TFG y se mostrarán las pruebas que se han ido realizando a lo largo del desarrollo del proyecto.
- Por último, se procederá a exponer las conclusiones extraídas tras la finalización del trabajo y se hará referencia a posibles líneas futuras que continúen el desarrollo de la temática tratada en este proyecto.

1.4 Metodología

El procedimiento a seguir para el desarrollo del proyecto consta de un estudio y análisis de lo que se pretende con el presente trabajo, una recopilación exhaustiva y filtrado de información relevante relacionada con el ámbito del TFG, y una síntesis de toda la documentación recogida. Posteriormente

se procede a aplicar lo aprendido sobre un equipo o máquina virtual y realizar las pruebas, análisis y anotaciones correspondientes. Se continúa explicando de manera detallada todo el desarrollo y aplicación de las medidas propuestas, apoyándose en capturas de pantalla e imágenes que ayuden al entendimiento por parte del lector. Por último, se elabora finalmente la guía de buenas prácticas de seguridad en Windows 7 y se presenta una tabla que resume y aglutina todas las medidas, categorizándolas según el impacto que tengan sobre la seguridad del equipo.

1.5 Organización de la memoria

En este capítulo, se ha presentado el marco donde se desarrolla el presente TFG y se ha expuesto por qué es crítico garantizar la seguridad de los equipos. Posteriormente, se han descrito los objetivos que se persiguen con el desarrollo del proyecto.

A continuación, en el capítulo 2, se procede a comentar, de manera general, las diferentes iniciativas similares a la temática en cuestión, así como hacer referencia a otros trabajos o documentación existentes relacionados con la seguridad en Windows. Se expone un diagrama mostrando las áreas en las que inciden ciertas guías de seguridad que hemos utilizado de referencia, para finalmente mostrar en las que nos centraremos al elaborar la guía de buenas prácticas de seguridad del presente TFG.

En el tercer capítulo, se explica el desarrollo completo del proyecto, entrando en detalle en las medidas aplicadas.

Posteriormente, en el capítulo cuatro, se expone, de manera esquemática y resumida, una tabla que aglutina todas las medidas explicadas en el capítulo tres. Se representa con un código de colores que facilitará la comprensión y ayudará al lector, con el objetivo de reflejar una valoración del grado de importancia que tiene el aplicar algunas medidas para la seguridad del equipo.

Se cierra el TFG presentando las conclusiones derivadas de todo el desarrollo del trabajo, que resume las principales contribuciones de este trabajo. A posteriori, planteamos unas posibles líneas futuras que permitirían continuar el trabajo desarrollado en el presente TFG.

2 ESTADO DEL ARTE

El establecimiento de configuraciones seguras en equipos informáticos es un tema que se ha venido abordando en los distintos ámbitos que se han citado en el capítulo anterior.

Podemos encontrar ejemplos de ello en normativas, guías, artículos, investigaciones y trabajos entre los que se ha realizado una selección, manteniendo los que muestran una clara relevancia y relación con este TFG.

2.1 Normativas

Tras una búsqueda exhaustiva de normativas relacionadas con la seguridad informática, las primeras normas que conviene destacar son las ISO 71501 [4], que tienen por objeto establecer unas metodologías para la preservación, adquisición, documentación análisis y presentación de evidencias electrónicas. No son de gran aplicación ya que tratan de "modelos teóricos y conceptos de gestión básicos" necesarios como introducción a la seguridad.

Más directamente relacionada con el ámbito del TFG se encuentra la norma ISO 17799 [5], cuyos orígenes datan de 1995. Es una norma de aplicación internacional con lo que observamos la preocupación de otros países en estas materias. Ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización. Se adentra un poco más en la temática ya que define conceptos clave como seguridad e información. Aun así, su objetivo se limita a desarrollar una base común para el resto de normas específicas de cada país y lo hace de manera general como vemos en la Figura 2-1.

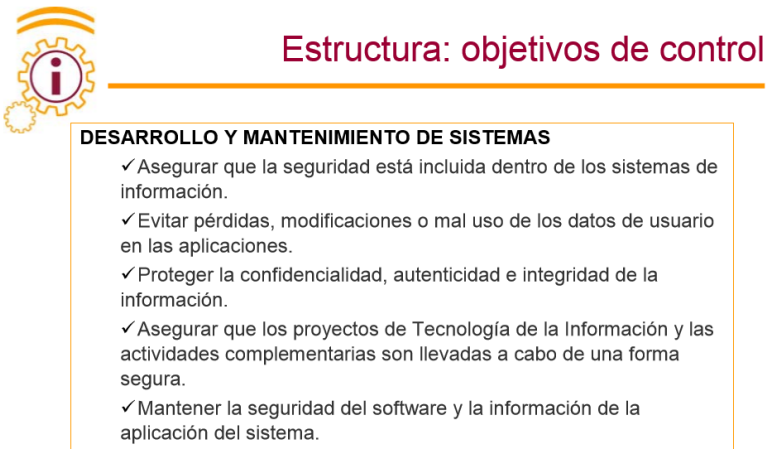

Figura 2-1 Normas generales ISO 17799

2.2 Informes de seguridad y trabajos de investigación

Se citan tres referencias de relevancia en el ámbito del TFG, de las cuáles se ha obtenido información a la hora de elaborar la guía de seguridad del proyecto.

El primero de los informes se denomina "*Seguridad Informática: recomendaciones básicas para los usuarios*" [6]. En él se tratan tanto el borrado seguro como la recuperación de archivos borrados, el cifrado de archivos, carpetas y directorios, y las contraseñas. Además hace alusión a diversas razones por las que un equipo Windows podría ser objeto de ataques y con ello cita los aspectos a tener en cuenta a la hora de gestionar un equipo Windows de manera segura y eficaz.

El segundo es un informe de Microsoft [7] que elabora las diferentes mejoras de seguridad que se han introducido con el nuevo S.O. Windows 7. Destaca la implementación de DEP (*Data Execution Prevention* o Prevención de Ejecución de Datos) y ASLR (*Address Space Layout Randomization* o lo que se conoce como aleatoriedad de memoria RAM), la existencia del UAC (*User Account Control)* para el control de cuentas de usuario, la protección sobre revisiones del software (kernel), la auditoría de eventos y la mejora en cuanto a cifrado.

Por otro lado, podemos nombrar trabajos de investigación relacionados con la temática en cuestión como el de *Jorge Mieres "Buenas prácticas en seguridad informática"* [8] de 2009. Este trabajo en concreto se centra en la seguridad referida a usuarios y sus credenciales de acceso, en las actualizaciones y parches de seguridad, y en la gestión correcta de los archivos (ocultos, extensiones…).

2.3 Empresas

Como se ha citado anteriormente, la seguridad de la información es un objetivo que persiguen todas las instituciones. No sólo afecta a la seguridad nacional o a los organismos relacionados con el Ministerio de Defensa, sino que las empresas han de aplicar estas medidas de seguridad con la misma rigurosidad ya que son objeto de numerosos ataques. De entre las diversas empresas y sus correspondientes guías, más o menos específicas según la importancia de la información con la que tratan y la frecuencia con la que sufren fallos de seguridad informática, vamos a citar algunas de las reglas que siguen a la hora de implementar la seguridad en sus equipos.

Por ejemplo, comentaremos el caso de NAVANTIA, una empresa de gran entidad que sufre espionaje industrial, como muchas otras de gran categoría, debido a la importancia de los datos con los que opera. NAVANTIA, dentro de las diversas políticas de seguridad informática que aplica, diferencia si las medidas se van a aplicar sobre equipos portátiles o sobremesa. Esto se debe a que, por razones de trabajo y/o desplazamientos, existen ocasiones en las que trabajan desde portátiles y transportan sus datos en ellos, siendo estos más susceptibles al robo de información o al hurto del equipo en sí. Por ello, tendríamos que asegurarlos con cifrado de disco duro (para evitar que la extracción de éste termine con su seguridad), antivirus activo con soportes extraíbles, evitar el modo "recordar contraseña" y permitir que el equipo se bloquee al no usarlo durante un determinado periodo de tiempo.

NAVANTIA además, establece para sus empleados algunas reglas como las siguientes: utilizar claves públicas y privadas (firma digital), mantener actualizaciones de seguridad al día, utilizar directorio activo con políticas adecuadas y proteger con contraseña documentos de diversa índole (*Word, Power Point, Excel, ZIP, RAR*…).

2.4 Seguridad Nacional

Pero la preocupación de la seguridad de los entornos informáticos no sólo existe a nivel personal o empresarial, puede apreciarse también en las distintas iniciativas que existen a nivel nacional, europeo e internacional que tratan aspectos similares a los que se van a tratar en este trabajo.

Desde el año 2000 se están elaborando estrategias de ciberseguridad a nivel mundial. En 2013 el Presidente del Gobierno firmó unos documentos estratégicos de ciberseguridad nacional [9]. El fin de estas directrices fue concienciar a los distintos órganos y administraciones de la creciente importancia y realidad de las ciberamenazas, y darles a conocer las medidas generales que debían adoptar. El documento establece unos fines específicos para órganos distintos pero no entra en detalle en los medios que han de aplicar para llegar a ellos.

2.5 Guías STIC del CCN

A nivel nacional ya existían un conjunto de guías de obligado cumplimiento para todos los sistemas que manejasen información clasificada nacional. Promulgadas por el Centro Criptológico Nacional (CCN) [10], con fecha de 2005, tratan de Seguridad en las Tecnologías de Información y Comunicaciones (STIC).

El documento introductorio del CCN cita lo siguiente: "*La serie de documentos CCN-STIC se han elaborado conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.*

Este conjunto normativo tiene por objetivo que los responsables de seguridad (Auditores, Supervisores de Seguridad, Administradores de Seguridad...) dispongan de las necesarias referencias que les faciliten el cumplimiento de los requisitos de seguridad exigibles a sus Sistemas."

Las guías, algunas enumeradas en la Figura 2-2, siendo mucho más específicas que los documentos nombrados anteriormente, se adentran en medidas relacionadas con hardware, software, protección contra el código malicioso, usuarios, contraseñas, cifrado, etc., llegando incluso a un nivel para el cual habría que documentarse antes y estar familiarizado con la terminología utilizada, ya que se trata de guías de muy alto nivel técnico.

CCN Centro Criptológico Nacional

Serie 500: Guías para Entornos Windows		
CCN-STIC-501A Seguridad en Windows XP SP2 (Miembro de Dominio)	2005	SIN CLAS.
CCN-STIC-501B Seguridad en Windows XP SP2 (Cliente Independiente)	2005	SIN CLAS.
CCN-STIC-502 A/B Seguridad para aplicaciones Cliente Windows. Navegador y correo electrónico	2006	SIN CLAS.
CCN-STIC-503A Seguridad en Windows 2003 Server (Controlador de Dominio y Servidor Miembro))	2005	SIN CLAS.
CCN-STIC-503B Seguridad en Windows 2003 Server (Servidor Independiente)	2005	SIN CLAS.
CCN-STIC-504 Seguridad en Internet Information Server	2005	SIN CLAS.
CCN-STIC-505 Seguridad para Microsoft SQL Server	2006	SIN CLAS.
CCN-STIC-506 Seguridad para Microsoft Exchange Server 2000	2006	SIN CLAS.
CCN-STIC-507 Seguridad ISA Server	2006	SIN CLAS.
CCN-STIC-508 Seguridad en Clientes W2000 (Cliente Independiente)	2005	SIN CLAS.
CCN-STIC-514 Seguridad para Microsoft Exchange Server 2003	2006	SINCLAS

Figura 2-2 Listado de guías STIC del CCN

2.6 Libros

La literatura base de referencia utilizada, elegida entre los numerosos libros escritos en referencia a seguridad informática o seguridad en equipos Windows, ha sido la obra "*Máxima Seguridad en Windows: Secretos Técnicos"* [11] de Sergio de los Santos. Ha sido seleccionado por la directa relación con el objetivo del presente TFG y por el hecho de que en él podemos analizar las distintas áreas en las que el autor (con profundidad) analiza qué medidas de seguridad aplicar para evitar ataques de distinta naturaleza.

En él, además de introducir el concepto de seguridad y desmentir ciertos dogmas conocidos comúnmente como "infalibles", se tratan aspectos de seguridad física (BIOS o *Basic Input/Output System*), seguridad del S.O. (parcheado, usuarios contraseñas, privilegios…), seguridad del software en sí (DEP, ASLR, *AppLocker*, etc.), seguridad del navegador (integridad, adjuntos, *ActiveX*, etc.) y seguridad de los datos (cifrado EFS o *Encrypting File System*, *BitLocker*, borrado seguro de datos, etc.).

El autor añade al final del libro un capítulo denominado "Miscelánea" que recoge diferentes conceptos y medidas útiles de seguridad como recuperación de errores, WPAD *(Web Proxy Auto-Discover Protocol)*, cortafuegos, antiexploits, etc.

2.7 Comparación de iniciativas y conclusiones

En la Tabla 2-1, se reflejan los aspectos que tratan cada una de las distintas propuestas anteriormente comentadas, indicando el nivel de profundidad con el que se abordan. Asimismo, en la columna más a la derecha, se señalan aquellos aspectos en los que nos centraremos en este TFG.

	Normativa ISO 17799 [5]	Informes seguridad [6][7]	Trabajo de investigación [8]	Empresa NAVANTIA	Guías CCN [10]	Libro [11]	Propuesta TFG
Seguridad física	NO	SI (bajo)	NO	SI (bajo)	NO	SI	SI
Seguridad del S.O	SI (bajo)	SI	SI	SI	SI	SI	SI
Seguridad del software	SI (bajo)	SI (bajo)	NO	NO	SI	SI	SI
Seguridad de los datos	SI (bajo)	SI	SI	SI	SI	SI	SI
Seguridad de los dispositivos removibles	SI (bajo)	SI	NO	SI	SI	NO	SI
Borrado y recuperación	NO	SI	NO	NO	NO	SI (bajo)	SI

Tabla 2-1 Comparación de las estrategias aportadas en diferentes fuentes y áreas donde aplican la seguridad

Entenderemos las distintas áreas nombradas en la tabla anterior como:

- Seguridad física: Todo lo relacionado con la BIOS, contraseñas de los discos duros, protocolos DEP, TPM (*Trusted Platform Module*), etc.
- Seguridad del S.O: Medidas que contemplen parcheado *offline*, protocolo WSUS (*Windows Server Update Services*), actualizaciones de seguridad, copias de seguridad, perfiles (conjunto de reglas definidas por el usuario que se aplican a una tarjeta de red) y usuarios, sus permisos correspondientes, contraseñas, cortafuegos, etc.
- Seguridad del software: Normas que regulen la integridad de los códigos, ASLR y DEP, EMET (*Enhanced Mitigation Experience Toolkit*), etc.
- Seguridad de los datos: Se trata del último escalón de seguridad y contiene todo lo relacionado con cifrados documentos *Word* o similares, proteger archivos comprimidos, cifrado EFS, agente de recuperación, etc.
- Seguridad de dispositivos removibles: Se explicará cómo evitar la reproducción automática de dispositivos portátiles para evitar infecciones y se hablará de cómo cifrar la información que estos contienen para evitar su lectura.
- Borrado y recuperación: En esta última sección abordaremos temas como el borrado por completo de un archivo para evitar que permanezca en la memoria y que sea sustraído por un atacante o la recuperación de archivos sensibles borrados accidentalmente.

Como se puede deducir de la Tabla 2-1, abordaremos en el siguiente capítulo todas y cada una de las áreas que se describen.

3 DESARROLLO DEL TFG

3.1 Sistemática

En esta sección del documento, se explicarán los experimentos realizados sobre el ordenador o máquina virtual que queremos configurar de manera segura.

Además de la información citada, se reflejarán diversas capturas de pantalla que nos ayudarán a la comprensión y aplicación de las medidas de seguridad.

El apartado comenzará plasmando las características del equipo/máquina virtual utilizados para el desarrollo de los experimentos. A continuación, se presentarán ciertas ideas base que hemos de tener presentes durante todo el desarrollo del TFG. Por último, nos centraremos en secciones o áreas donde se aplicarán las medidas de seguridad.

La aproximación a nuestro objetivo, que no es otro que definir una configuración segura del equipo, se va a realizar por capas, tanto para ofrecer una estructura ordenada al desarrollo del documento y asegurar la continuidad, como para poder cerciorarnos de que se incluyen todas las áreas que componen el sistema y por tanto la seguridad de éste. Realizaremos un análisis de los distintos niveles desde dentro hacia fuera, comenzando por la parte física o *hardware* (BIOS) y siguiendo por el sistema operativo y el software que utilizamos. Continuaremos por los datos y aplicaciones que manejamos y los dispositivos removibles con los que interactuamos diariamente para terminar con unas recomendaciones sobre borrado seguro y recuperación. Por lo tanto, abordaremos las siguientes capas:

- Seguridad física
- Seguridad del sistema operativo
- Seguridad del software
- Seguridad de los datos
- Seguridad en dispositivos removibles
- Borrado y recuperación

3.1.1 Características técnicas

Comenzaremos especificando las características de la máquina virtual y equipo utilizados para las pruebas realizadas.

Figura 3-1 Características del equipo del laboratorio con Windows 7

Las características del equipo, donde se han realizado los cambios y pruebas de seguridad, pueden observarse en la Figura 3-1. Se trata de un equipo con *Windows 7 Professional 64 bits 4 GB RAM y Service Pack 1* instalado como S.O. Por otro lado, la máquina virtual utilizada está emulada con el programa *Virtualbox* [12], con *Windows 7 Professional 64 Bits 8 GB RAM y Service Pack 1*.

3.1.2 Conceptos fundamentales

Exponemos una serie de ideas clave que debemos tener presentes durante la lectura de todo el documento:

- Tras lo comentado en los capítulos 1 y 2, debemos tener claro que los datos que todos manejamos (en el trabajo o entorno personal) son elementos importantes y susceptibles de ser atacados.
- Hay que tener en cuenta que la comodidad va en contra de la seguridad, por lo que debemos encontrar un equilibrio entre ambas.
- No existe la configuración de seguridad fija y efectiva al 100%, hay que entender el problema, conocer las amenazas y actuar de forma racional.
- Una medida de seguridad que nunca fallará es tener respaldo de nuestros datos, con copias de seguridad en otros dispositivos (como discos duros portátiles, la nube, memorias flash, etc.) por si nuestro equipo fuera infectado o inutilizado (o incluso por si nosotros, aplicando cambios para aumentar la seguridad, inhabilitamos el uso del equipo).
- También debemos tener en cuenta que existen distintos tipos de equipos, usos y usuarios, los cuales serán objeto de distintas amenazas y debemos considerarlo a la hora de configurar un equipo de forma segura.
- La seguridad es un proceso que consiste en:
  1. Aplicar seguridad por capas y defensa en profundidad (seguridad física, seguridad en la aplicación y seguridad en los datos).
  2. Ofrecer el mínimo punto de exposición.
  3. Proporcionar el mínimo privilegio posible a usuarios y procesos.

3.2 Medidas de seguridad

Tras las premisas generales citadas, comenzamos con la aplicación de las medidas específicas.

Como apunte, reiterar que este TFG ofrece recomendaciones de seguridad y que, por tanto, no son la solución perfecta a las amenazas. Algunas medidas se ajustarán mejor que otras a nuestro equipo específico según nuestro ámbito. Por último, todas las realizamos bajo nuestra propia responsabilidad, por lo que se recomienda tener los conceptos claros, hacer seguimientos de los cambios y experimentos que llevemos a cabo y tener copias de seguridad para evitar pérdidas de información.

3.2.1 Seguridad física

En este apartado, se estudia la seguridad básica del PC: el componente físico o hardware del equipo. Hablaremos de cómo establecer contraseñas de BIOS y HD (*Hard Drive* o Disco Duro), cómo evitar que se ejecute código con DEP, el uso del TPM, cómo establecer un orden de arranque del sistema, etc.

Con estas medidas evitamos, por ejemplo, un primer acceso al ordenador por parte de un atacante que tenga acceso físico a él, que alguien acceda a nuestro equipo introduciendo un USB para arrancar el sistema saltándose nuestras contraseñas o que si sustraen el disco duro puedan acceder a sus datos, entre otras problemáticas.

Se explicarán las acciones, paso a paso, para la correcta aplicación de las medidas de seguridad.

3.2.1.1 Contraseña BIOS

Esta medida hará que se nos solicite una contraseña al iniciar el equipo para poder arrancar el sistema.

Para ello, realizaremos los siguientes pasos: Reiniciar ordenador > Acceder a la BIOS con la tecla predeterminada > pestaña *Seguridad* (se muestra una captura en la Figura 3-2) > *Contraseña de Config.* > *Establecer contraseña de usuario* (para controlar el acceso al sistema de arranque) o *Establecer contraseña de supervisor* (también denominada *contraseña de Administrador* sirve para controlar el acceso a la configuración de la BIOS).

Si se ofreciera la opción, como hacen ciertas BIOS, no se recomienda utilizar contraseñas *backdoor* para reestablecer la contraseña de la BIOS (ya que las más utilizadas son conocidas por los atacantes) por lo que hay que recordar bien la contraseña BIOS.

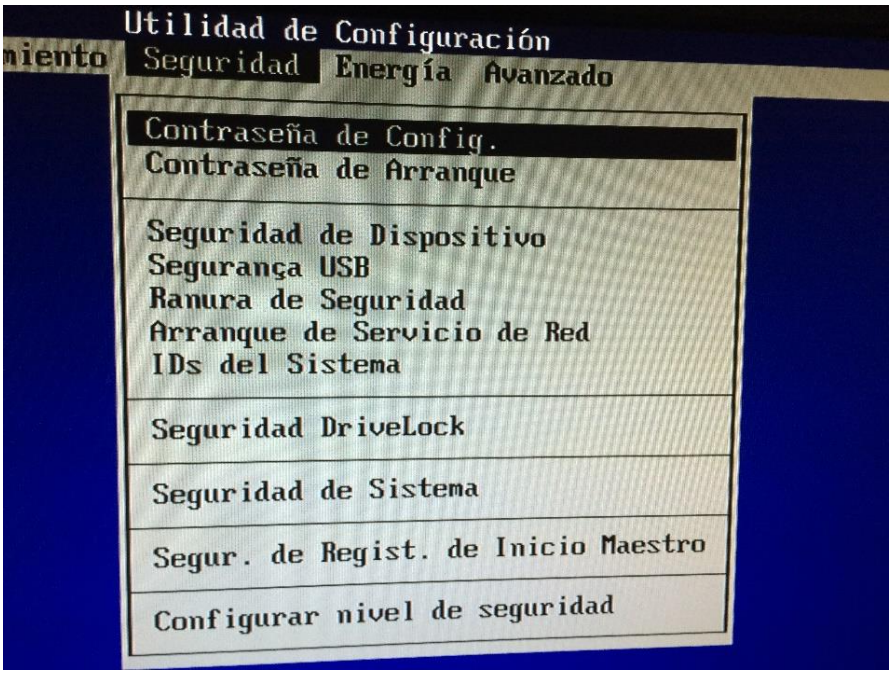

Figura 3-2 Pestaña *Seguridad* en la BIOS

3.2.1.2 Establecer un orden de arranque del sistema

Aplicando un orden de arranque específico, controlamos cómo queremos iniciar el sistema, evitando permisos a dispositivos que no nos convienen por seguridad.

Para ello, repitiendo los pasos anteriores para acceder a la BIOS, accedemos a la pestaña *Almacenamiento*, y en *Configuración de Dispositivo* seleccionaremos *Orden de Arranque*. Ahí podremos desactivar, con sólo pulsar F5, la posibilidad de arrancar desde cualquier dispositivo que no sea el propio SO. Las Figuras 3-3 y 3-4 muestran estas opciones dentro de la BIOS.

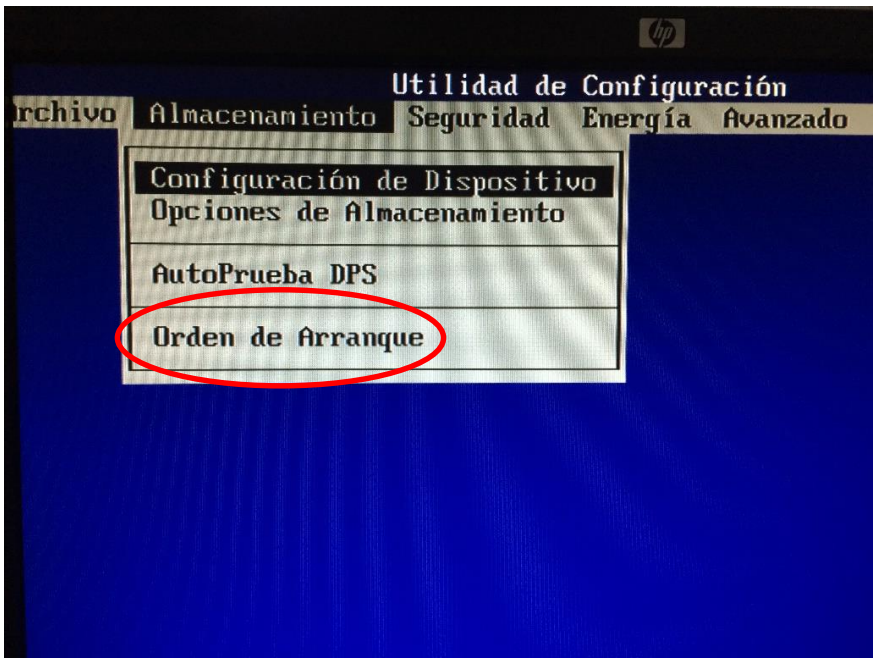

Figura 3-3 Pestaña Almacenamiento para acceder a la configuración del *Orden de arranque*

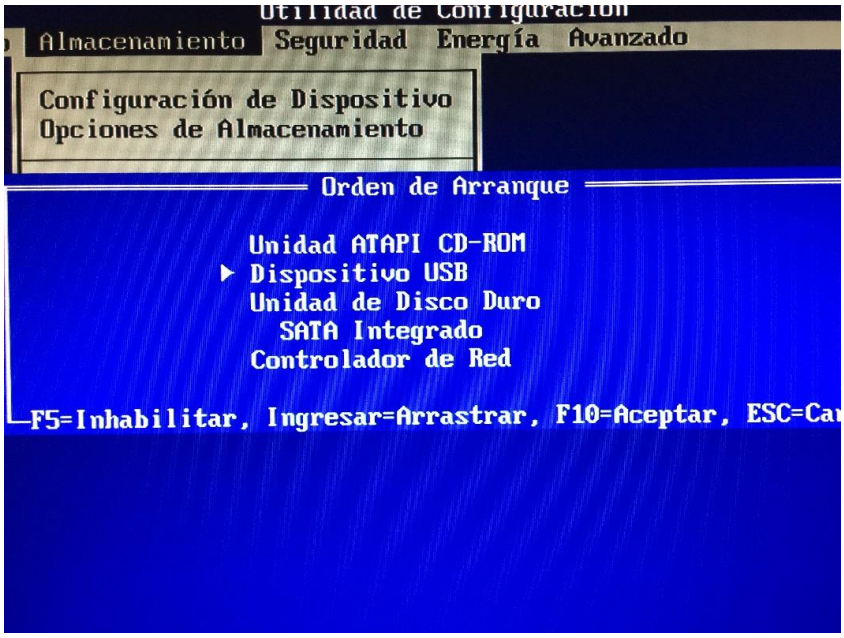

Figura 3-4 Opciones dentro de la configuración del *Orden de arranque* de la BIOS

3.2.1.3 Opciones inseguras a desactivar en BIOS

Algunas BIOS ofrecen una serie de opciones, que no suelen ser necesarias ni utilizadas en nuestro día a día, que comprometen la seguridad. Entre otras, debemos desactivar *Wake on Lan* (ya que permite, con conocer la dirección MAC de la tarjeta de red, encender el sistema de manera remota), *Password Bypass* si lo ofreciera (por el hecho de que no vuelve a solicitar la contraseña BIOS cuando el ordenador se reinicia o vuelve del estado "en suspensión"). Asimismo, es recomendable desactivar los periféricos micrófono, cámara, módem, etc. si no se utilizan.

3.2.1.4 Activar TPM en BIOS

La tecnología TPM actúa en combinación con el hardware del ordenador. Es una opción implementada en ciertas placas que permite generar una especie de inventario de cómo está configurado el equipo. El software se comunica con el hardware y genera unas claves que protegen al más bajo nivel para evitar que ocurra una modificación no autorizada de los componentes. TPM sella estas claves impidiendo que se reemplacen hasta que el equipo no se reinicie y compruebe que coinciden y que nada ha sido modificado.

Para activarlo, debemos escribir desde la búsqueda de inicio de Windows *tpm.msc* > Una vez iniciado el *Administrador del Módulo de plataforma segura (TPM)* debemos seleccionar *Inicializar TPM* (ya que no se encuentra en los estados poseído ni activado, como ocurre en la Figura 3-5) > Reiniciar ordenador para crear nuevas claves raíz > Seguir instrucciones Asistente BIOS > Elegir *Crear contraseña automática* (recomendado) o *Crear contraseña manual* > Guardar contraseña (en otro ordenador, dispositivo removible o cualquier otro lugar seguro. Podemos ver estas opciones en las Figuras 3-6 y 3-7). Tras Inicializar debemos repetir acceso a *Administrador TPM* y proceder a *Activar TPM*.

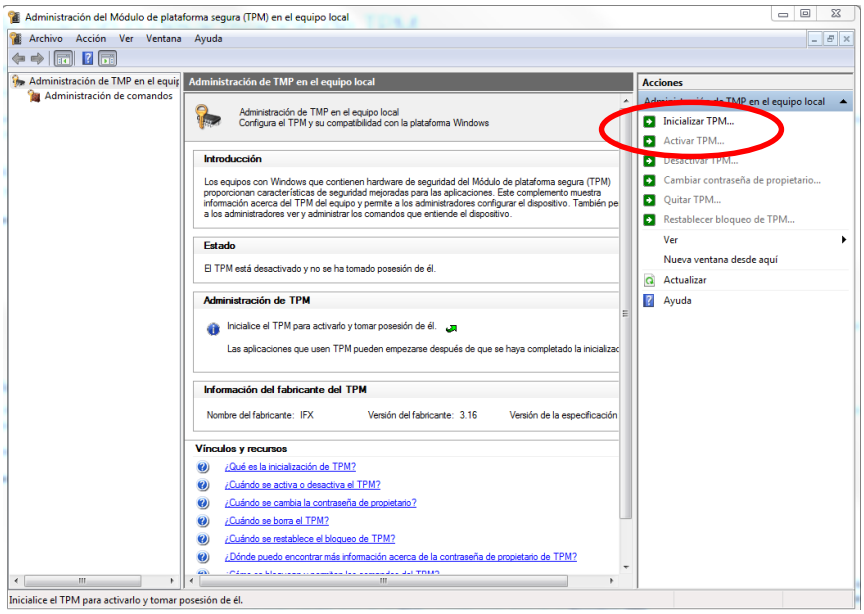

Figura 3-5 Administración de TPM

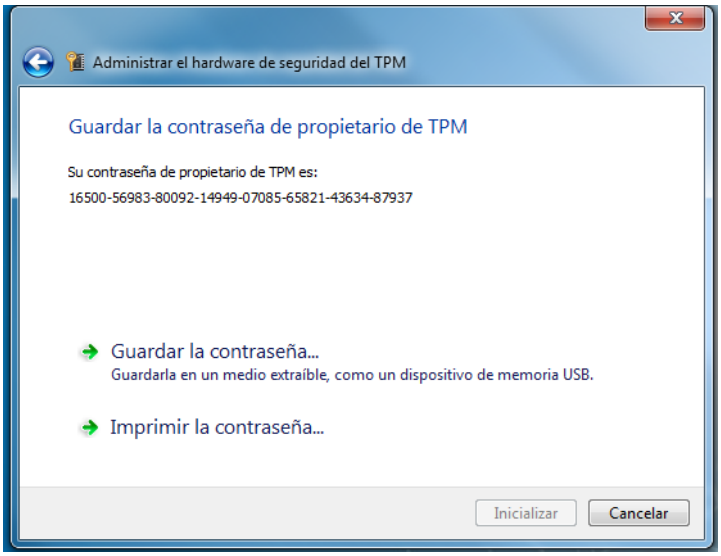

Figura 3-6 Contraseña TPM

Esta página es una copia de seguridad de la información de la contraseña de propietario del hardware de seguridad del Módulo de plataforma segura (TPM). Cuando se le solicite, use la contraseña para probar que es el propietario del TPM del equipo. Incluya los guiones cuando escriba la contraseña.

Nombre del equipo:
LABCUD

Contraseña de propietario del TPM:
16500-56983-80092-14949-07085-65821-43634-87937

Esta página fue impresa el 23/02/2015 12:21 Hora estándar romance por labCUD\bausa.

IMPORTANTE:
Guarde esta página en un lugar seguro apartado del equipo.

Figura 3-7 Ejemplo de contraseña de TPM generada

La inicialización del TPM requiere el acceso físico al equipo (aceptar la nueva configuración tras arrancar el equipo) para activar este mecanismo de seguridad, lo que nos ayuda a proteger el ordenador contra amenazas de software malintencionado que puedan llegar a atacar a través del TPM. Podemos ver el mensaje de la BIOS en la Figura 3-8.

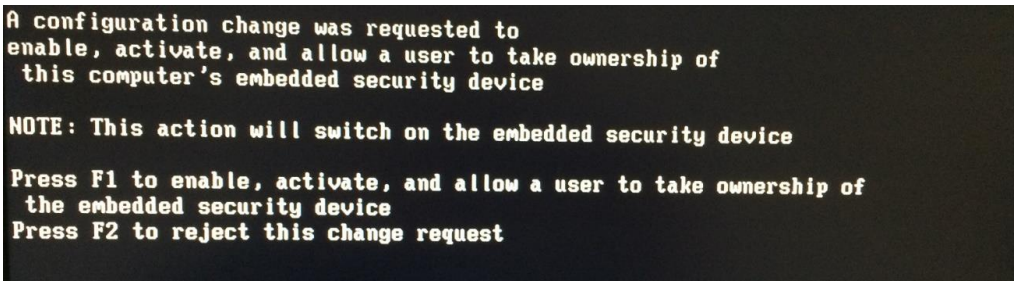

Figura 3-8 Confirmación de nueva configuración tras inicializar el TPM y reiniciar el equipo

El administrador puede, a priori, inicializar el TPM evitando así necesitar la posible futura intervención de un usuario que pueda configurarlo de manera errónea.

Es necesario inicializar el TPM para usar software como el cifrado de unidad *BitLocker*. De otro modo, el asistente para la inicialización de *BitLocker* inicia el proceso de inicialización de TPM automáticamente.

3.2.1.5 Contraseña HD

Este mecanismo de seguridad posee una ventaja y es que la contraseña para proteger nuestro disco duro no se guarda en la BIOS, sino en el propio firmware del disco. Por esta razón se dice que viaja con el disco duro. Si se diera el caso en el que físicamente roban nuestro disco duro, no tendrían acceso a los datos debido a la contraseña. Además, conseguimos que con un reseteado del CMOS (operación que podrían utilizar los atacantes y que se utiliza para restaurar a parámetros de fábrica la BIOS y evitar que la contraseña BIOS sea efectiva) no se elimine la contraseña.

Para evitar que la medida deje de funcionar, el usuario no debe suspender ni hibernar el ordenador en ausencia ya que, por defecto, la contraseña HD no se activaría y seríamos potenciales víctimas de acceso por terceros no autorizados.

La manera de establecer la contraseña es acceder a la BIOS y en la pestaña *Seguridad*, en *Contraseñas*, elegir opción *Contraseña disco duro* (será distinta a la contraseña de la BIOS).

No todas las BIOS poseen esta opción.

3.2.1.6 BitLocker

Si nuestro Windows 7 fuera versión *Enterprise* o *Ultimate* tendríamos acceso al programa *BitLocker* [13], el cual ofrece diversas acciones de seguridad, como el cifrado con contraseñas.

Se activaría accediendo al programa *BitLocker* > Discos duros internos > Encender protección > Establecer contraseña.

3.2.1.7 DEP

A través de DEP, evitamos que un atacante ejecute código que sería de solo lectura, lo cual es una modalidad de ataque muy conocida. Windows establecerá diferencias entre la memoria que puede contener partes ejecutables y la que no.

Para activarlo, debemos entrar en *Seguridad* dentro de la BIOS y habilitar la opción *Prevención de Ejecución de Datos* (Figura 3-9).

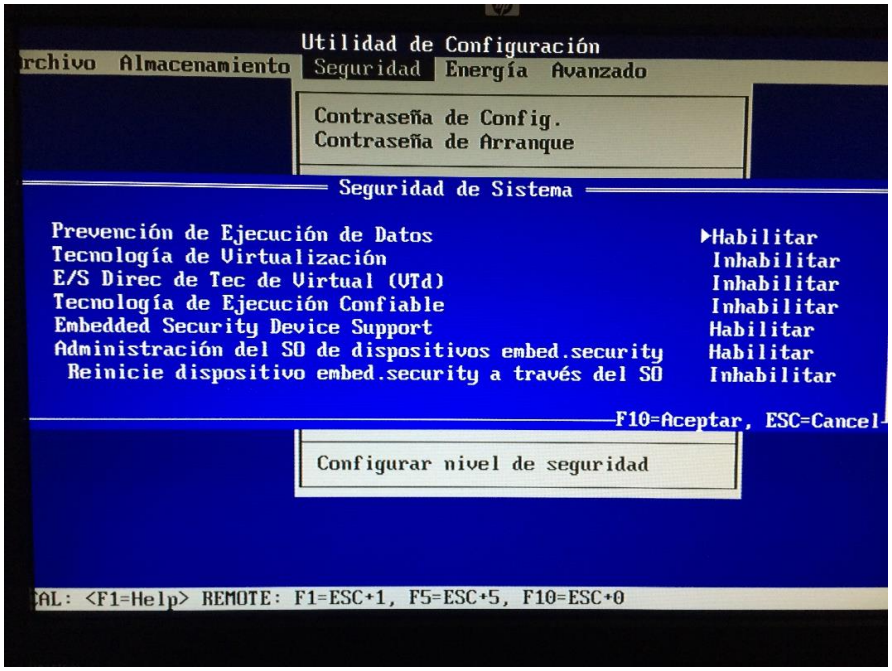

Figura 3-9 Activando DEP desde BIOS

Otra opción es entrar en Panel de control > Sistema > Configuración avanzada del sistema > Opciones avanzadas > Configuración en el área de Rendimiento (Figura 3-10) > Pestaña *Prevención de ejecución de datos* > Seleccionar la opción de *Activar DEP sólo para los programas y servicios de Windows esenciales* (Figura 3-11).

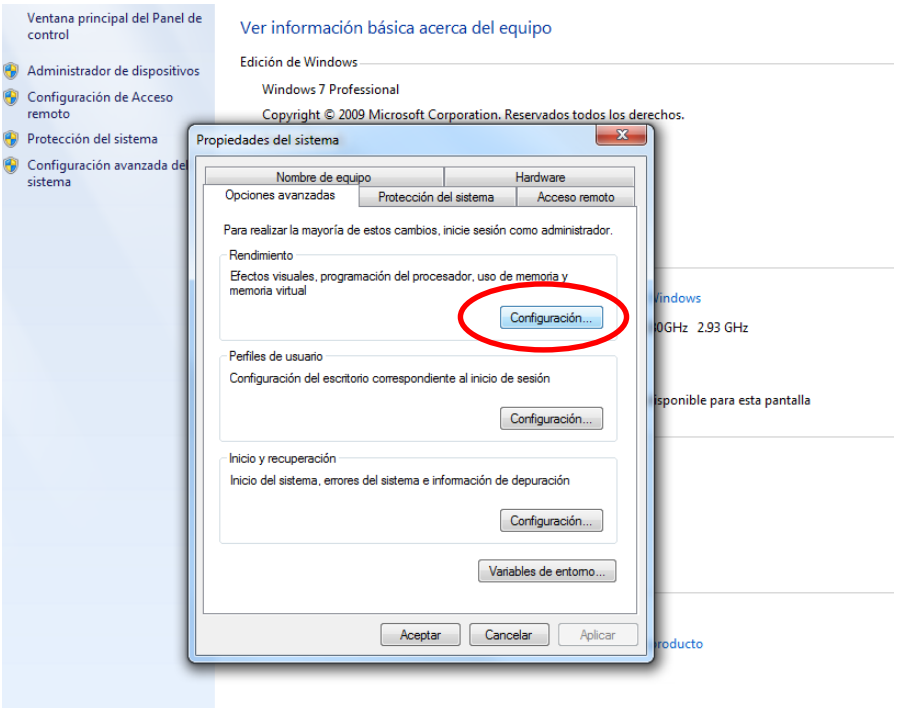

Figura 3-10 *Configuración del Rendimiento* dentro de *Propiedades del Sistema*

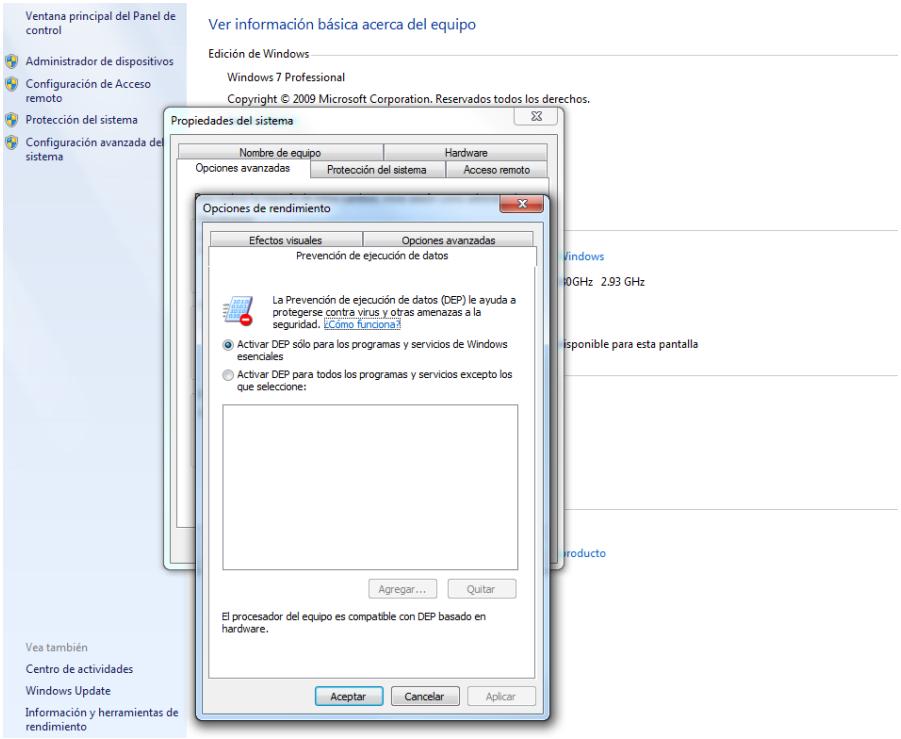

Figura 3-11 Activación DEP

3.2.2 Seguridad del sistema operativo

Tras estudiar el primer nivel de seguridad, subimos al segundo escalón de seguridad. En este apartado, se tratarán diversos temas que conciernen a la seguridad que ofrece el sistema operativo Windows 7 como tal. Empezando por la instalación de actualizaciones de seguridad y el parcheado *offline* (para evitar exponer el sistema a la red desprotegido), pasando por la gestión de usuarios y sus permisos, lo cual es una manera de controlar las acciones que pueden llevar a cabo en el manejo del ordenador. Proseguiremos tratando cómo evitar el *malware* de arranque, que no necesita ni que entremos en la cuenta de usuario para infectarnos. Por último, se citarán medidas relacionadas con las contraseñas (que suponen la puerta de acceso a nuestros datos), el cortafuegos y los servicios (permiten crear aplicaciones ejecutables de larga duración, en modo *background*).

3.2.2.1 Parchear offline

Procederemos a instalar todos los drivers que vengan con el ordenador (CDs de instalación) tras la instalación/formateo del S.O. antes de conectar y exponer el equipo a Internet sin que posea las mínimas barreras contra ataques de la red.

Durante la instalación, se recomienda que el S.O. permanezca en una partición del disco distinta a la que se utilizará para guardar los datos. Ésta es una práctica recomendada, de manera que cualquier infección del sistema operativo o cualquier necesidad de restaurarlo o formatearlo, no nos afectará a los datos almacenados en la otra partición del disco duro.

Para el parcheado *offline*, utilizaremos *WSUS offline* [14]**.** Es un programa gratuito que permite recopilar desde los servidores de Microsoft todos los parches, sabiendo que vienen de la fuente original, para después instalarlos sin necesidad de conectarse a Internet.

Comenzaremos por ejecutar *UpdateGenerator.exe* (Figura 3-12) > Elegir las actualizaciones de *Sistemas operativos, Office, idiomas y otros productos* que deseemos (Figura 3-13) > Elegir, a mayores, actualizaciones de *Service Packs, Windows Defender, Microsoft Security Essentials, etc.*

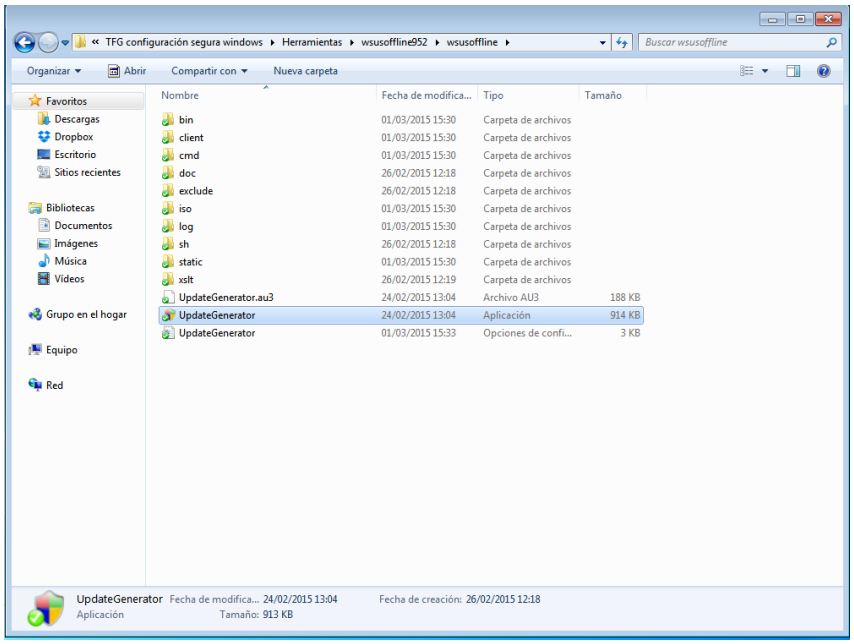

Figura 3-12 Ejecutable del programa *WSUS Offline*

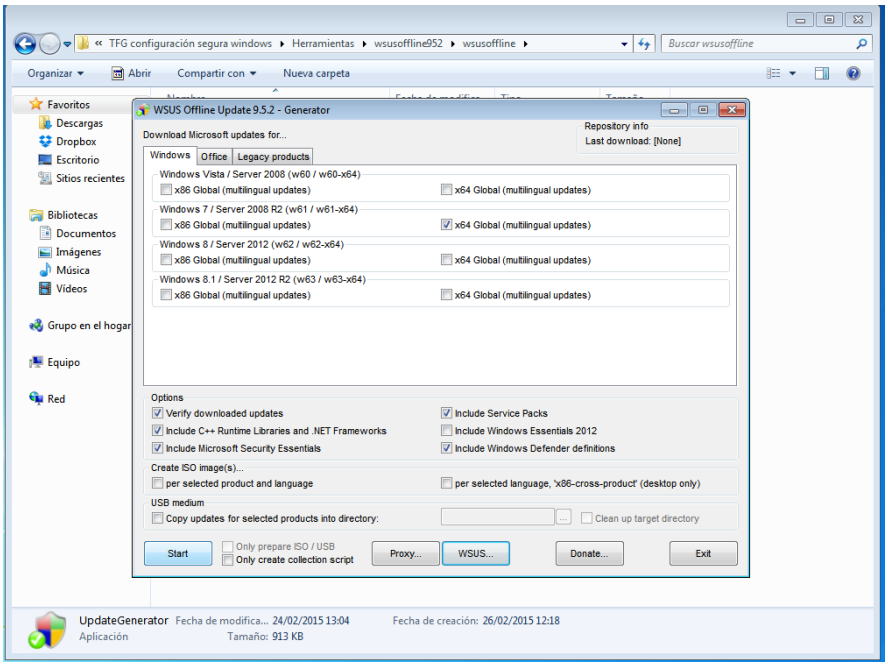

Figura 3-13 Display *WSUS Offline*

Tras estos primeros pasos, debemos seleccionar si queremos que las actualizaciones las descargue además en un USB o que cree una imagen .iso. Tras seleccionar la opción deseada, pulsaremos *Start* (Figura 3-14). Al finalizar la descarga, accederemos a la subcarpeta *client* que se encuentra en el

directorio de la carpeta *wsusoffline* y ejecutaremos *UpdateInstaller.exe* (Figura 3-15). Dentro de la interfaz, debemos seleccionar las actualizaciones que deseamos instalar y proceder a ello (Figura 3-16).

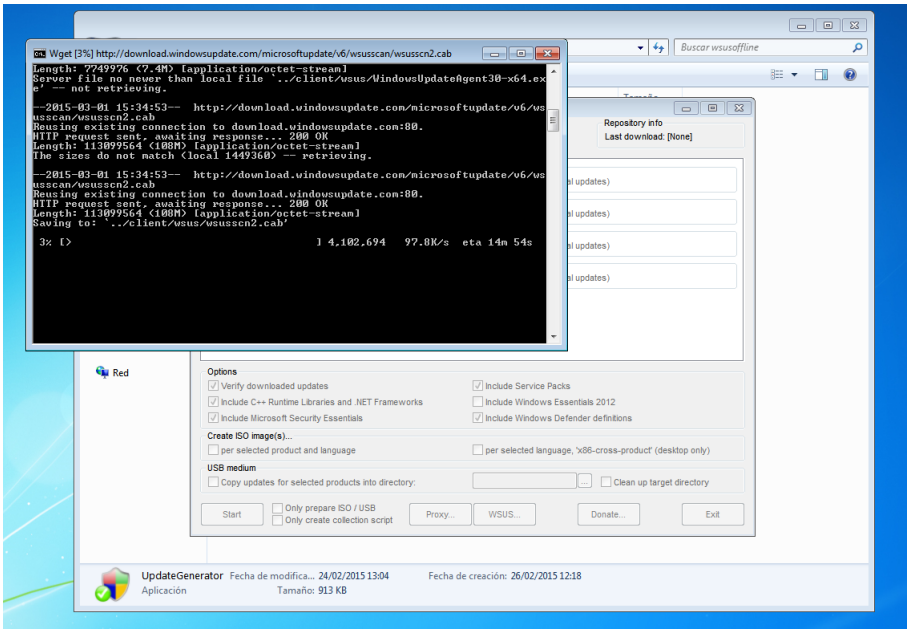

Figura 3-14 Actualizando la base de datos de parches y actualizaciones

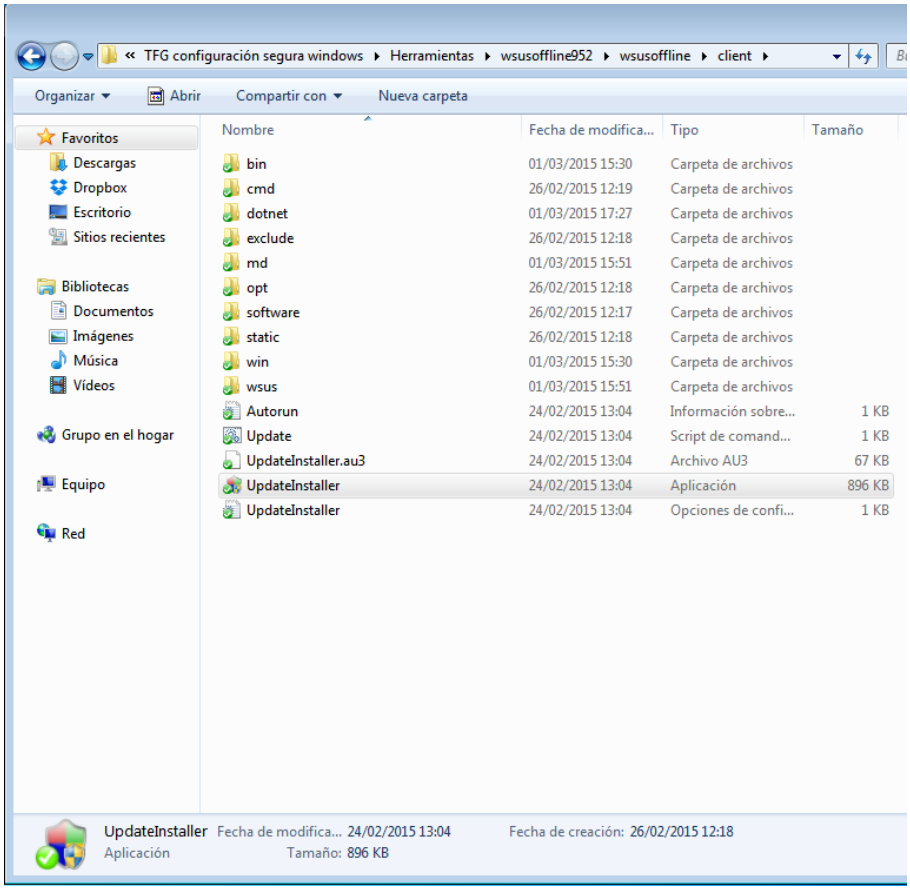

Figura 3-15 Acceso *UpdateInstaller*

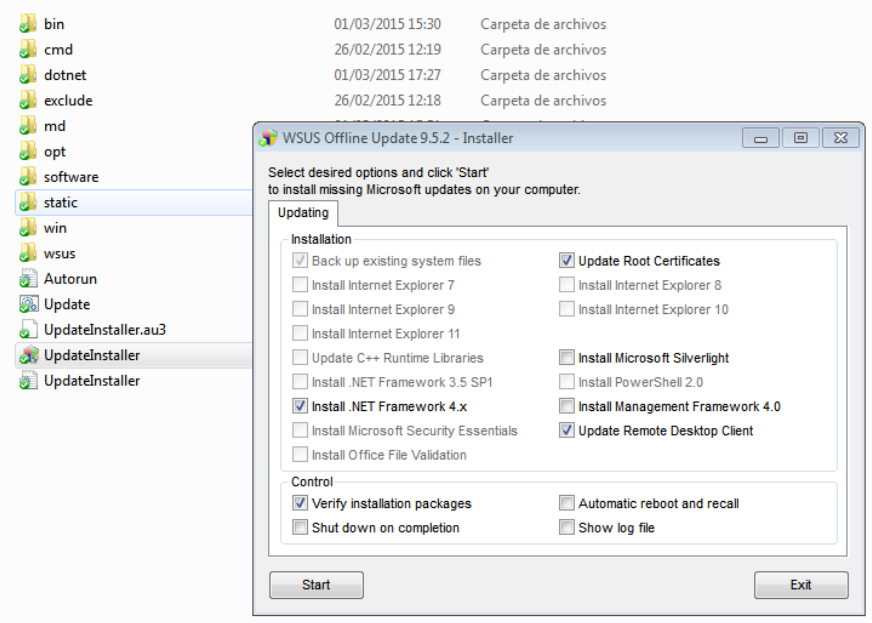

Figura 3-16 Selección de actualizaciones a instalar con *WSUS*

Tras la finalización, puede ser necesario un reinicio y volver a lanzar el proceso de actualización tras reiniciar el equipo. El proceso de actualización quedará confirmado con el mensaje *Ending WSUS Offline Update at* [Hora de finalización] (Figura 3-17).

Figura 3-17 Mensaje de confirmación de finalización de instalación de *WSUS*

Como otra medida, compatible con *WSUS Offline*, existe una herramienta gratuita denominada MBSA (*Microsoft Baseline Security Analyzer)* [15] que también nos brinda la opción de verificar la falta de actualizaciones del sistema.

3.2.2.2 Mantener el S.O. actualizado

Tras realizar la primera actualización *offline*, debemos mantener Windows 7 al día ejecutando *Windows Update* periódicamente. Así evitamos que el equipo se enfrente a la red sin las últimas actualizaciones de seguridad que Microsoft lanza cada semana para proteger nuestro equipo.

Actualizaremos entrando en Panel de control > Sistema y seguridad > *Windows Update* > Instalar actualizaciones (Figura 3-18).

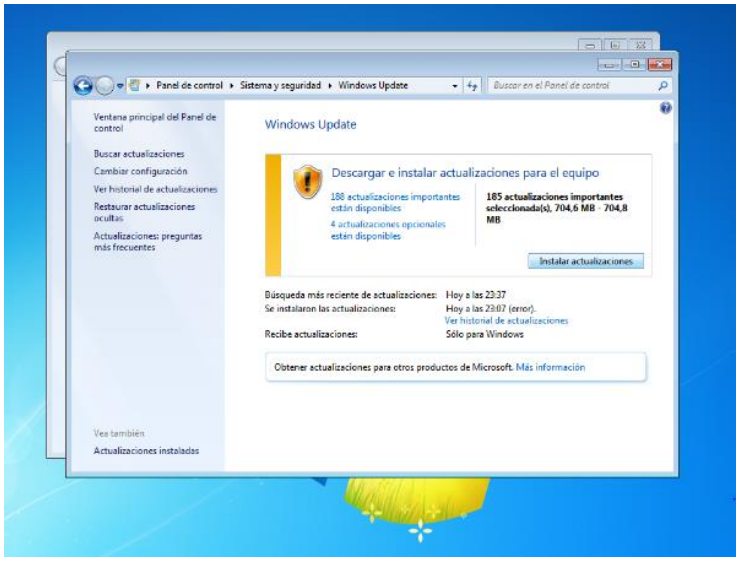

Figura 3-18 Actualizaciones con *Windows Update*

3.2.2.3 Inicio de sesión

En cuanto al inicio de sesión, debemos activar una opción que asegura que una persona física (usuario) está accediendo al equipo y, de este modo, evitar el *malware* de suplantación.

Para hacer uso de esta herramienta, escribimos en la barra de búsqueda *directiva seguridad local* (Figura 3-19) > Directivas locales > Opciones de seguridad (Figura 3-20) > Inicio de sesión interactivo: no requerir *Ctrl+Alt+Supr* > Deshabilitada (Figura 3-21).

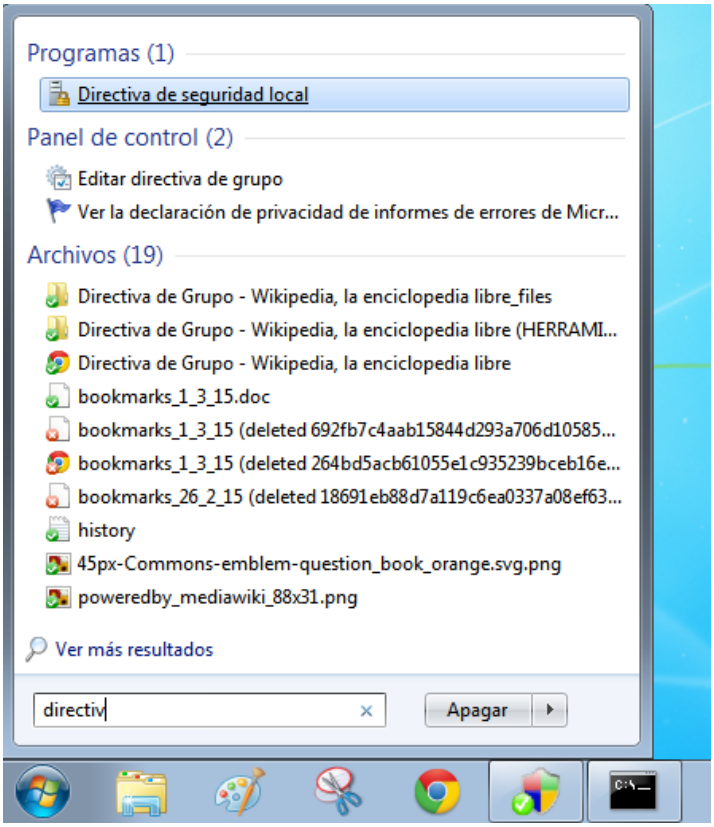

Figura 3-19 Ejecutando *Directiva de seguridad local* desde la barra búsqueda de Windows

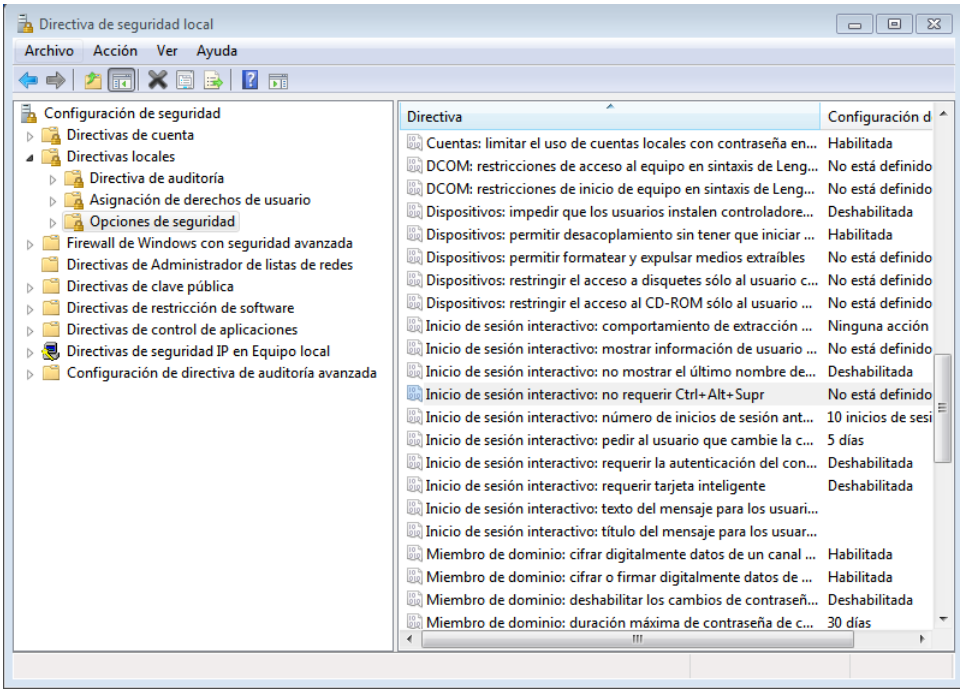

Figura 3-20 Opciones de seguridad

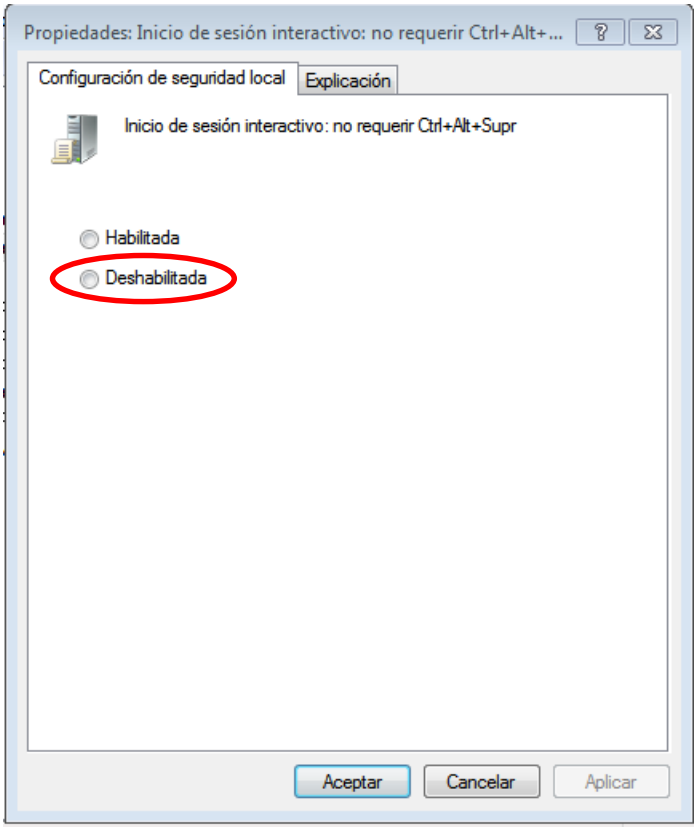

Figura 3-21 Activar requerimiento de *Ctrl+Alt+Supr*

Con esta medida además evitamos ataques de tipo GINA (*Graphical Identification and Authenticacion)* o pantalla de inicio de sesión falsa y troyanizada.

3.2.2.4 Malware de arranque

La trampa de inicio de sesión no es la única que podemos encontrarnos. Una gran parte de los virus aprovechan el arranque del equipo para hacerse con el control sin que nos demos cuenta. Lo hacen aprovechando los elementos que se arrancan automáticamente en cada reinicio del sistema sin que nosotros realicemos ninguna acción y accediendo al registro del S.O.

Comenzaremos advirtiendo que el registro es un elemento crítico del sistema operativo y la manipulación incorrecta del mismo puede provocar errores en el mismo. La práctica de las medidas que se explican queda bajo la exclusiva responsabilidad de los usuarios, ya que cualquier cambio en el registro puede dañar el sistema.

Para evitar que alguien modifique el registro se deben seguir los siguientes pasos:

Acceder a *regedit.msc* (Figura 3-22) > Ir a la rama del registro *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run* (Figura 3-23) > Permiso a Usuarios de solo lectura (Figura 3-24).

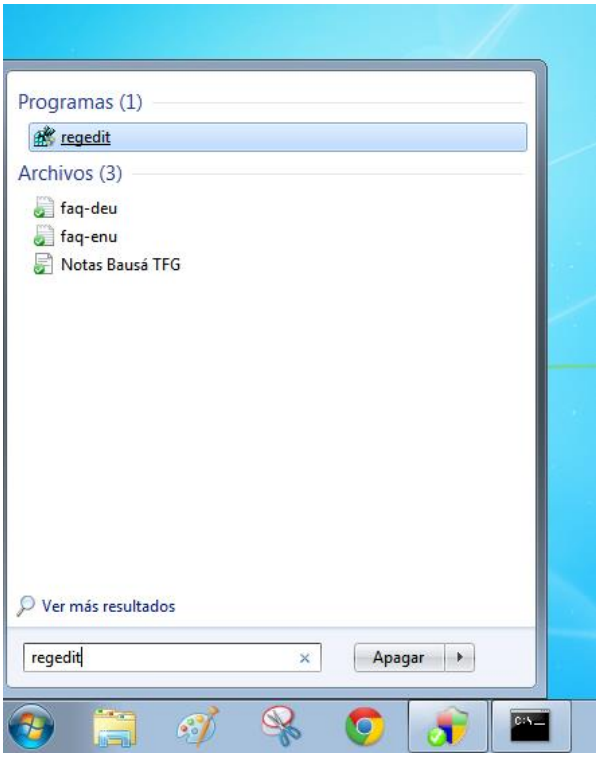

Figura 3-22 Ejecutar Editor del registro desde la barra de búsqueda de Windows

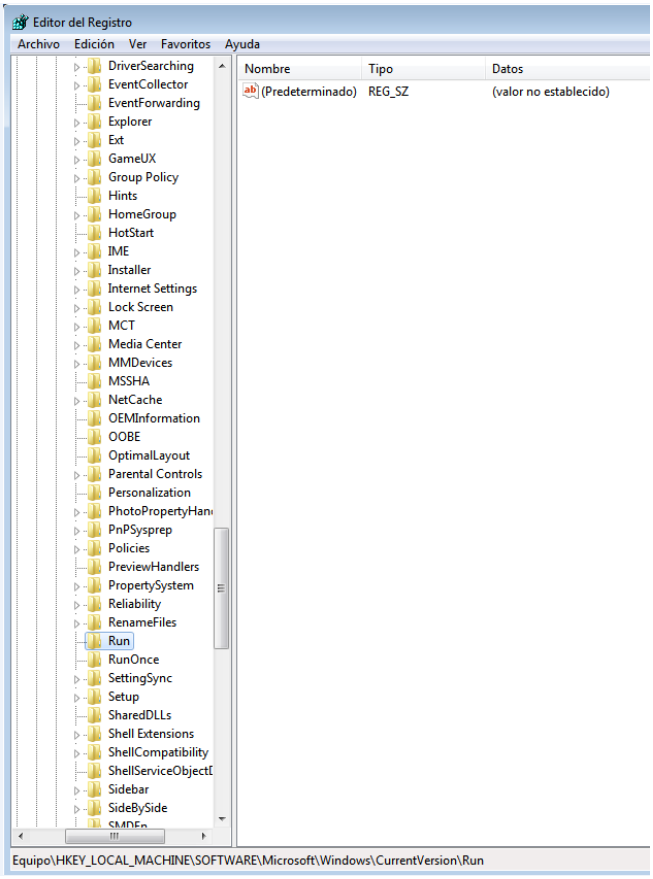

Figura 3-23 *HKLM > SW > Microsoft > Windows > Current Version > Run*

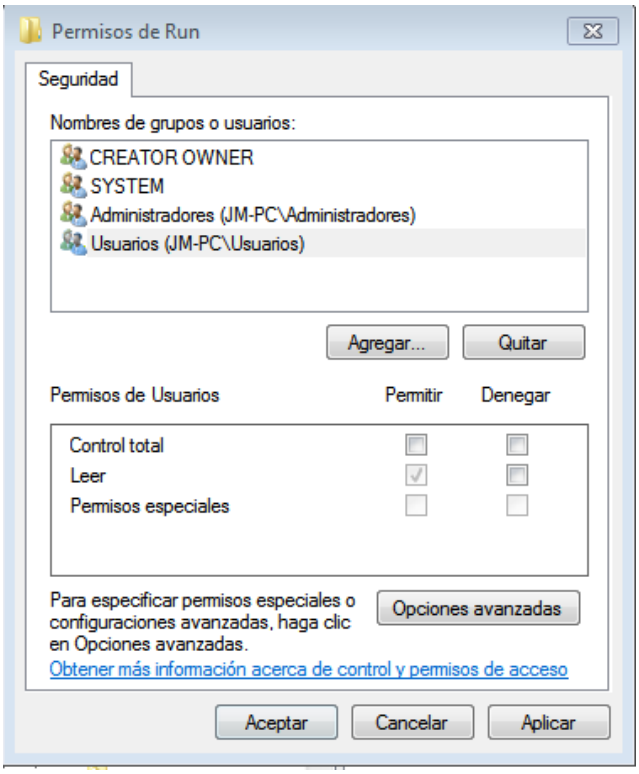

Figura 3-24 Cambio de permisos de usuarios sobre *Run*

Además, algunos troyanos se esconden tras ciertos valores del registro, dando lugar a su ejecución automática. Para evitarlo, debemos realizar la misma acción para la rama *HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon*. En este punto debemos comprobar que *userinit* no tiene añadido, por culpa de un atacante, ningún ejecutable con un valor del tipo *troyano.exe* (Figura 3-25).

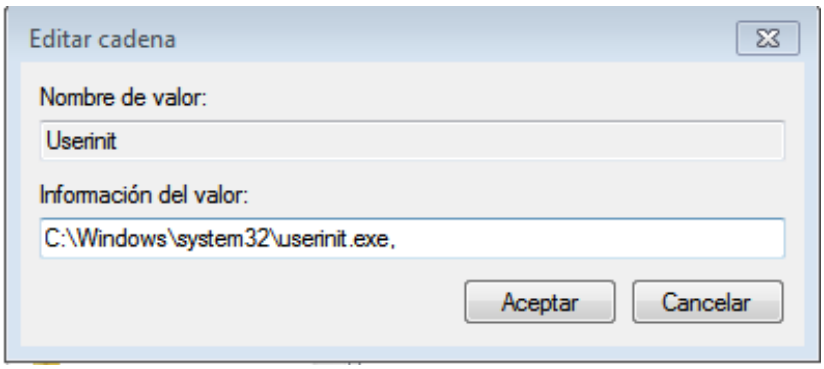

Figura 3-25 Comprobación de valores de *userinit*

Una herramienta para evitar, en cierta medida, algunos tipos de *malware* de arranque, conocidos por ejecutarse cuando Windows se inicia, con el fin de secuestrar el equipo, es *WinLockLess* [16]. Con este programa somos capaces de negar permisos de modificación o creación de subramas en ciertas ramas del registro (Figura 3-26) que son vulnerables a las infecciones del *malware* y que, si se infectan, no podríamos deshacernos del virus.

El usuario quedaría infectado igualmente pero, tras reiniciar el equipo, eliminaríamos el *malware*.

Si el usuario desea instalar algún programa que necesita permiso para modificar alguna de esas ramas, puede desactivar la protección y reactivarla al terminar.

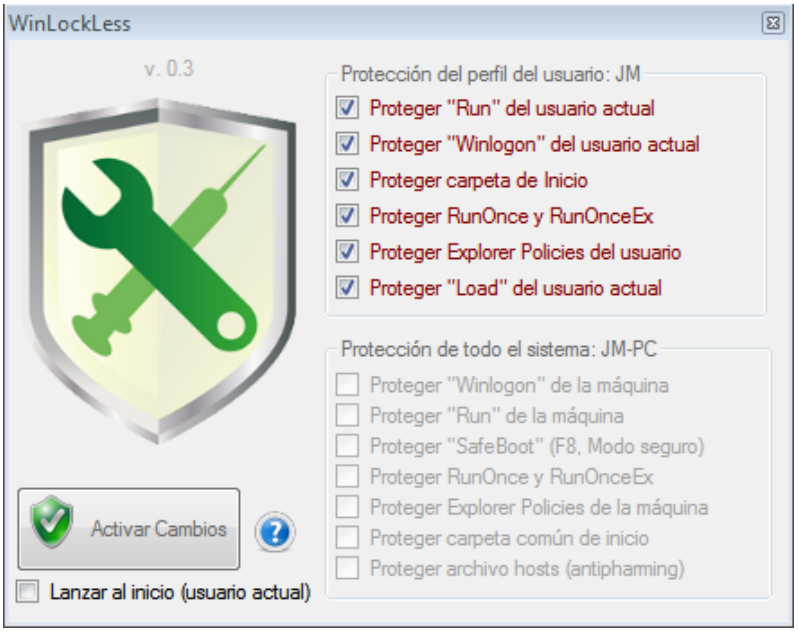

Figura 3-26 *WinLockLess*

3.2.2.5 Teclas especiales

Aun no siendo un proceso que se ejecuta automáticamente al inicio, podemos acceder al servicio de *Teclas especiales* antes de que un usuario acceda a su cuenta dando lugar a una posibilidad para que un atacante utilice este servicio.

Como una medida extra, debemos desactivar la posibilidad de que se activen las *Teclas especiales* (son una opción de accesibilidad) al pulsar cinco veces la tecla *shift* ⇧.

Para desactivarlas, pulsamos *shift* cinco veces (viene activado por defecto de Windows) y, accediendo al Centro de accesibilidad, desmarcamos la casilla *Activar las teclas especiales cuando la tecla Mayús se presione cinco veces*, como vemos en la Figura 3-27.

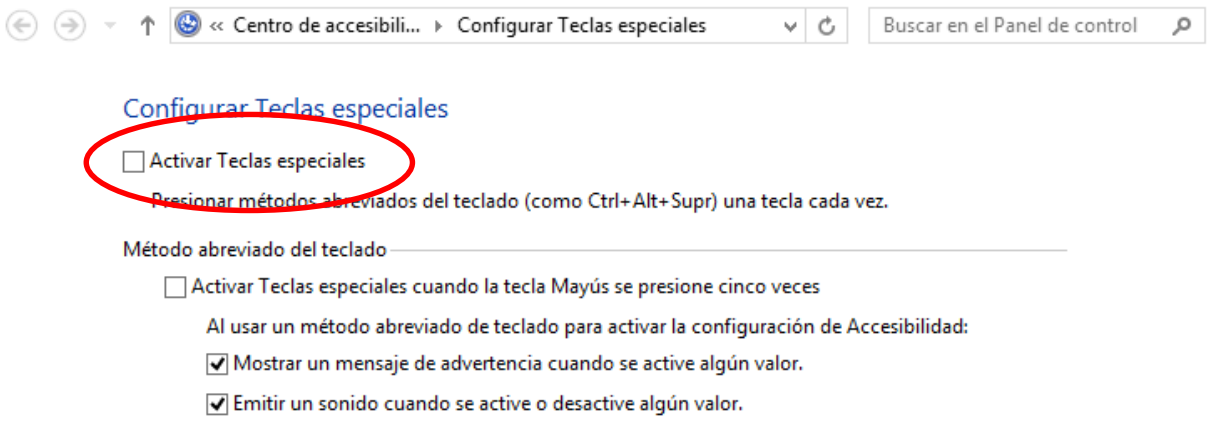

Figura 3-27 Desactivando las teclas de accesibilidad

3.2.2.6 MSConfig

Con este programa, podemos activar y desactivar acciones que se ejecutan para el usuario o la máquina. Además nos permite filtrar y observar si alguna aplicación de terceros ha instalado y ejecuta un servicio en el sistema o qué aplicaciones se inician automáticamente en *Inicio de Windows*. De esta manera, comprobamos si algún software de terceros está ejecutando algo sospechoso y si lo hace de forma automática al inicio del arranque del sistema.

Iniciamos *msconfig* en barra búsqueda > Servicios > Ocultar servicios de Microsoft (Figura 3-28), y las pestañas de Servicios e Inicio de Windows nos muestran la información que buscamos.

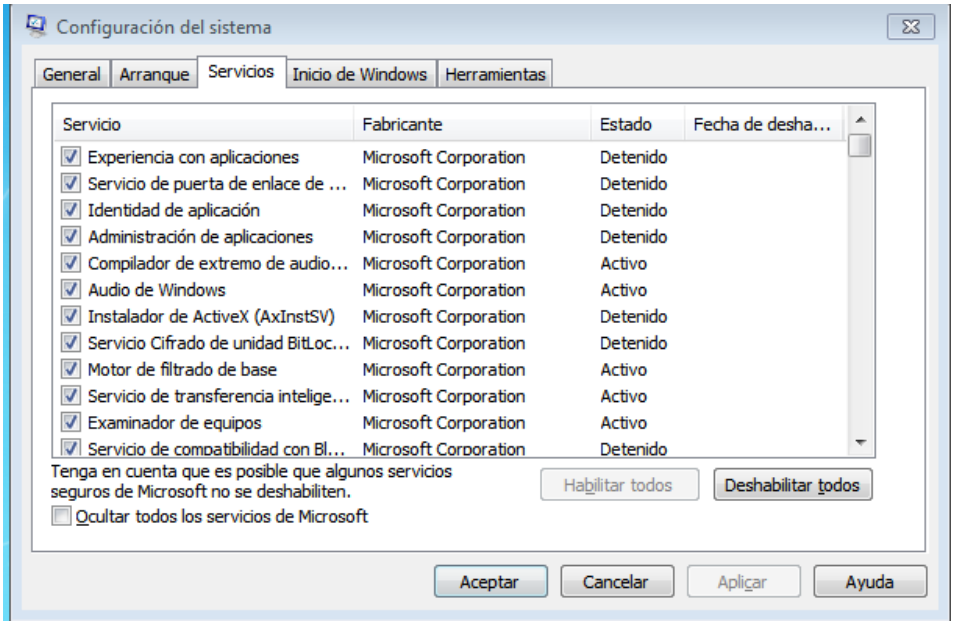

Figura 3-28 Comprobación de los servicios que se ejecutan en el sistema

3.2.2.7 Usuarios

Si el equipo sirve a diversos usuarios, debemos conocer la manera de gestionarlos, tanto sus cuentas como permisos y privilegios. Con estas medidas evitamos que un atacante controle un usuario con posibilidades de cambiar configuraciones sensibles del equipo o que se produzca un ataque (intencionado o accidental) desde dentro del propio equipo.

En el caso de pretender introducir la máquina en un dominio, no se deben crear usuarios locales, sino de dominio. Esto se debe a que sus permisos y privilegios se gestionarán desde un controlador central o administrador del servidor de manera más segura, al poder asignarlos o sustraerlos conforme se crea conveniente para la seguridad.

Por otro lado, de manera general, cuando utilicemos en el día a día el ordenador, debemos crear una cuenta usuario, perteneciente al grupo *usuarios* para realizar todas las actividades y así cerciorarnos que lo hace con permisos de usuario sin privilegios de administración. Por otro lado, cuando queramos llevar a cabo tareas de administración, utilizaremos una cuenta de usuario, creada previamente, que pertenezca al grupo *administradores* y que posea todos los privilegios y permisos para configurar el sistema.

Con esta medida reducimos el riesgo de que un atacante infecte el equipo mientras lo utilizamos como administrador, y tome el control con los privilegios que este tipo de usuario tiene.

Si preferimos no utilizar dos cuentas de usuario y administrador, se puede aprovechar el UAC (*User Account Control)*. Como ya hemos citado anteriormente, se debe hacer un uso de mínimos privilegios posibles y permisos de usuario normal, accediendo a la condición de *administrador* en ocasiones contadas y sólo cuando sea necesario. Esto se realiza tanto para minimizar el riesgo de acometer una acción peligrosa para el equipo como para evitar que un atacante tome control de un usuario con control total del equipo. Para esto, utilizamos el UAC.

Mediante el UAC es el S.O. el que elige, decide y hace un uso responsable de los permisos que tenemos como usuario y da mínimos privilegios posibles en todas las situaciones. Evita que modifiquemos lo que no debemos, protegiendo, por tanto, la seguridad del equipo.

Para comprobar que el UAC está activado, debemos acceder a *secpol.msc* o *Directivas seguridad local* en búsqueda > Directivas locales > Opciones de seguridad > Control cuentas usuario > Ejecutar todos los administradores en Modo aprobación de administrador > Habilitada (Figura 3-29).

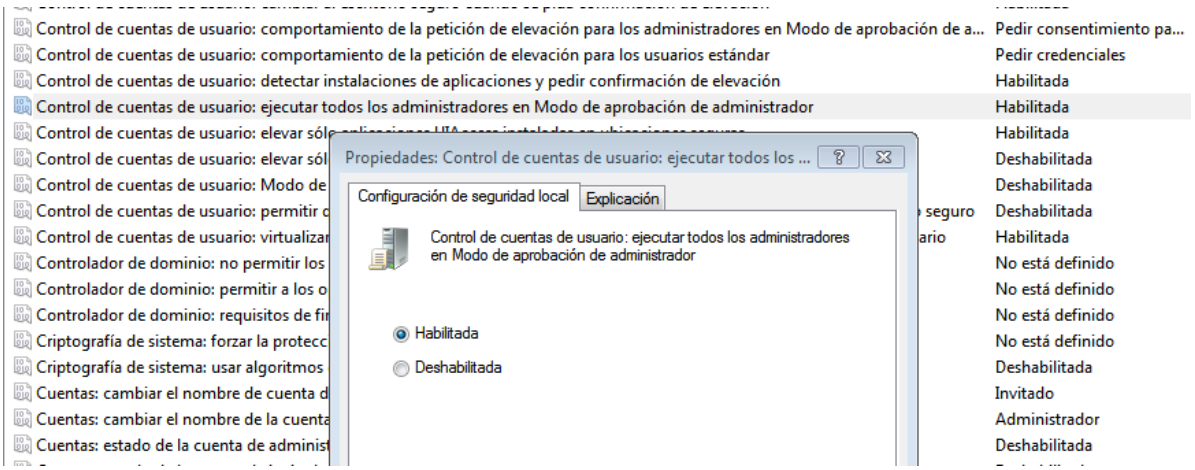

Figura 3-29 Comprobación del UAC activado

Asimismo, debemos también acceder a *Control Cuentas Usuario* en barra búsqueda > Elegir *Notificarme siempre* (Figura 3-30).

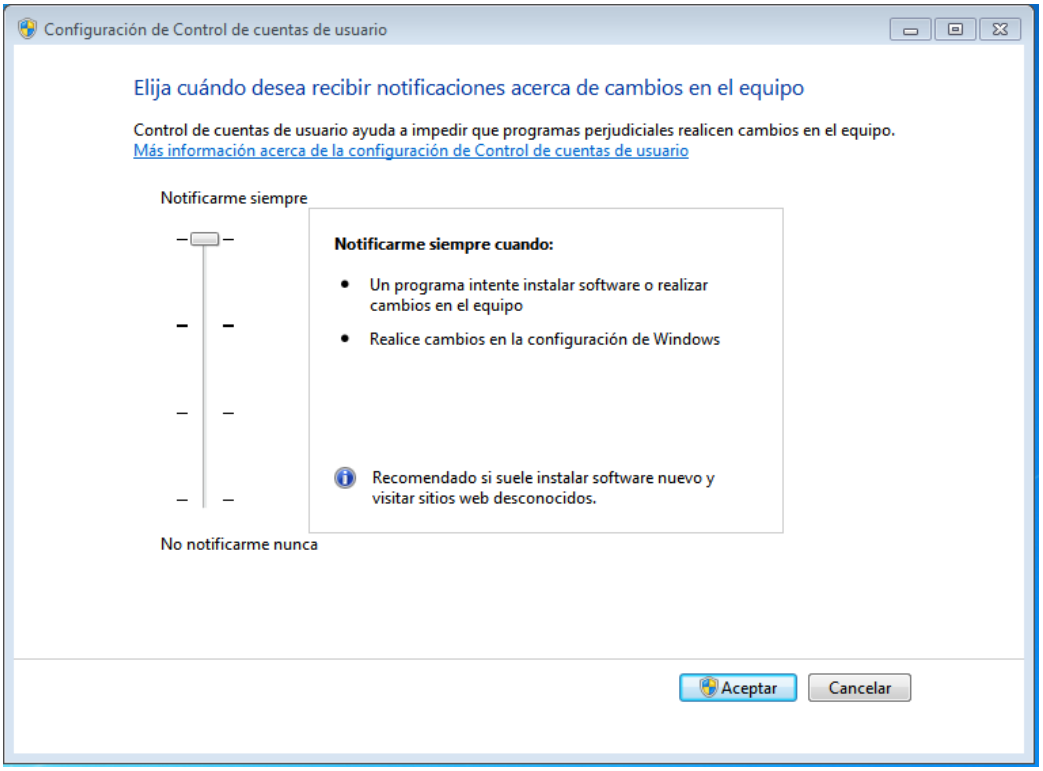

Figura 3-30 Configuración de notificaciones de UAC

Con esta medida, evitamos la autoelevación de permisos de un proceso de bajo nivel a uno de nivel superior sin nuestro conocimiento, y nos aseguramos de que todo usuario es consciente cuando va a realizar un cambio que puede conllevar peligros, ya que debemos dar nuestro consentimiento.

Además, se muestra un código de colores dependiendo del grado de *peligrosidad* que conlleve la aplicación que vamos a ejecutar, como se observa en la Tabla 3-1.

Color	Significado
Rojo	Firmante bloqueado o sin firmar (de Internet)
Verde	Firmado por Microsoft
Gris	Firma de terceros
Amarillo	No firmada o firmada por alguien que no es de confianza

Tabla 3-1 Códigos de colores del UAC

Con esta medida podemos apreciar de manera visual qué consecuencias podría acarrear ejecutar la aplicación que está intentando elevar privilegios.

Aun así, hay que dejar claro que hoy en día el software legítimo sin firmar y el *malware* firmado va *in crescendo,* por lo que esta medida no sería infalible.

Para aumentar esta seguridad, debemos realizar cambios en las plantillas de seguridad tales como:

- Activar el *Modo aprobación del administrador*.
- Activar *Detectar instalaciones de aplicaciones y pedir confirmación de elevación*.
- Comprobar que, dentro de opciones como *Comportamiento de la petición de la elevación para [acción]*, no tenemos activado el modo *Pedir consentimiento* sino que cambiamos a la opción de *Obligar al usuario a introducir sus credenciales en el escritorio seguro* (Figura 3-31).

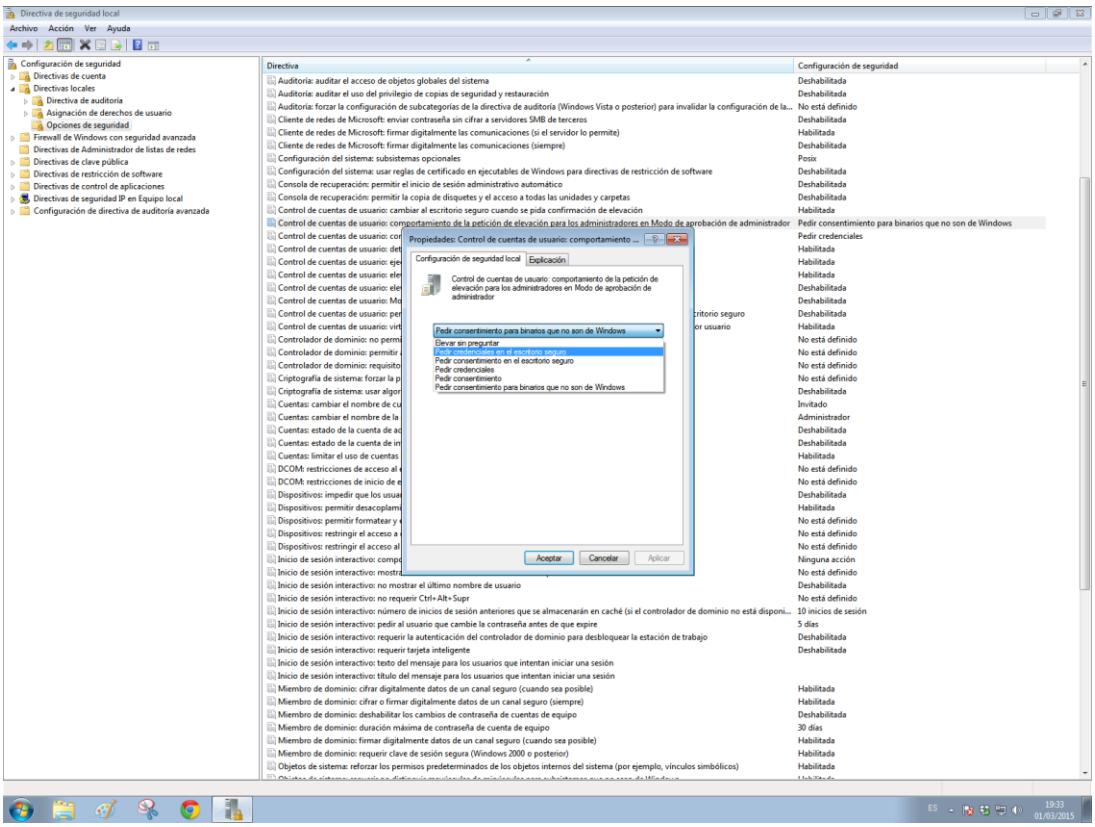

Figura 3-31 Configuración de solicitud de credenciales al elevar privilegios

- Activar *Cambiar al escritorio seguro cuando se pida confirmación de elevación*. Con este escritorio seguro, que reconocemos que se está ejecutando por el oscurecimiento de la pantalla, conseguimos que la solicitud de credenciales vaya aparte del escritorio normal y evita que un *malware* alojado en el sistema apruebe por sí mismo la elevación de privilegios.
- Desactivar *Permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro*.

Para realizar estas acciones, procederemos escribiendo *secpol.msc* o *Directivas seguridad local* en búsqueda > Directivas locales > Opciones de seguridad > Control cuentas usuario (Figura 3-32).

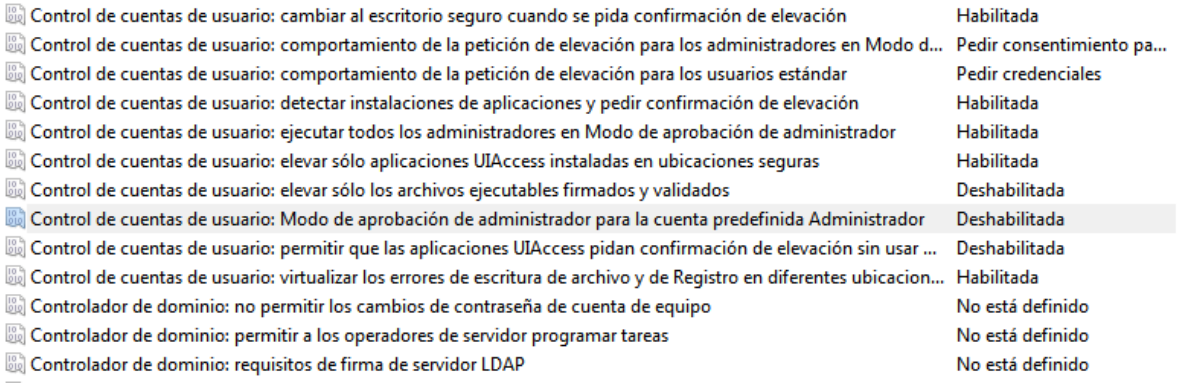

Figura 3-32 Diversas acciones de configuración desde las Directivas de Seguridad Local

Por otro lado, ejecutando *gpedit.msc* > Configuración equipo > Plantillas administrativas > Componentes de Windows > Interfaz de usuario de credenciales > Deshabilitar *Enumerar las cuentas de administrador al realizar una elevación* (Figura 3-33) y habilitando *Requerir ruta de acceso de confianza para la entrada de credenciales* (Figura 3-34), añadimos una capa más de seguridad al control de cuentas de usuario.

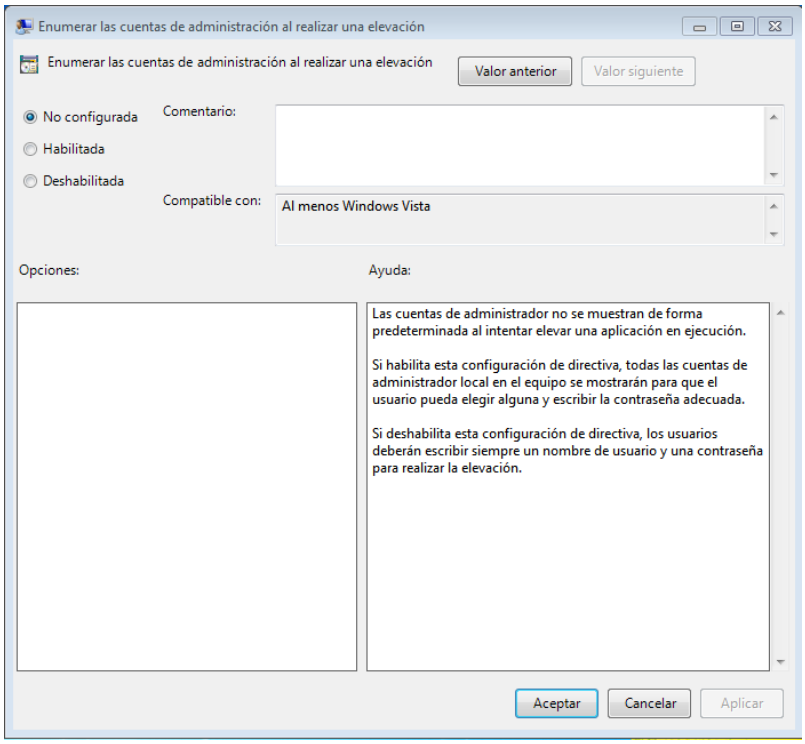

Figura 3-33 Evitar la enumeración de las cuentas de administradores

Con esta medida, ocultamos las identidades de los administradores, lo que se considera información sensible y útil para un atacante.

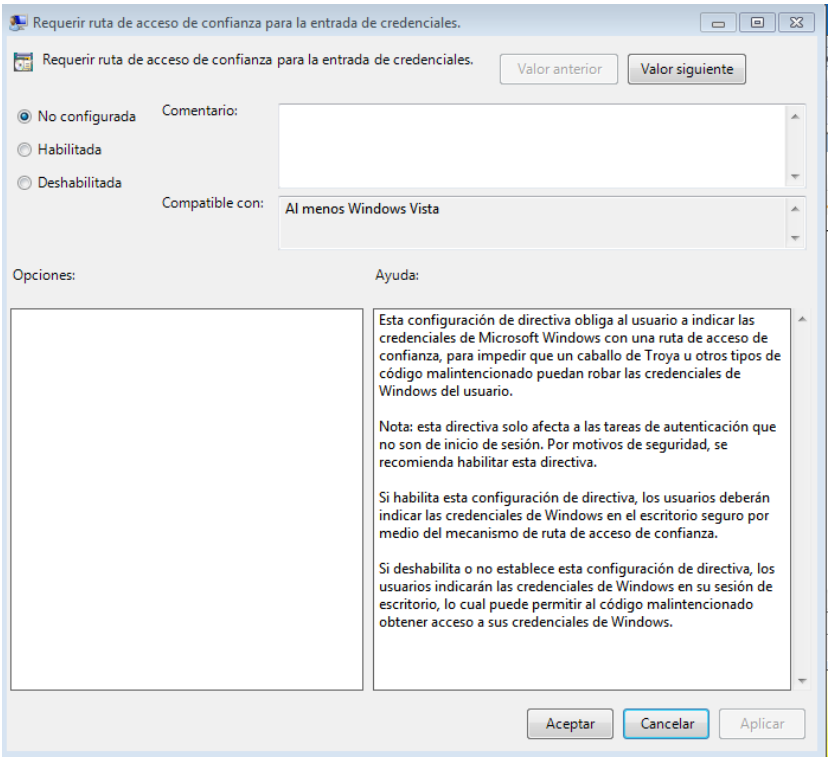

Figura 3-34 Añadir seguridad a la solicitud de credenciales y escritorio seguro

Accediendo a *gpedit.msc* > Configuración del usuario > Plantillas administrativas > Prohibir Acceso a Panel de Control, evitamos que un usuario, que no deba, pueda configurar elementos sensibles que se encuentren accesibles desde el Panel de Control.

En caso de no querer prohibir el acceso total al Panel de Control, dentro de las *Plantillas administrativas*, en la opción *Panel de Control*, podemos activar o desactivar diversas opciones (Figura 3-35) con el fin de restringir, en mayor o menor medida, las posibilidades que tiene el usuario para modificar configuraciones (agregar o quitar programas, entrar en pestaña de *configuración*, etc.).

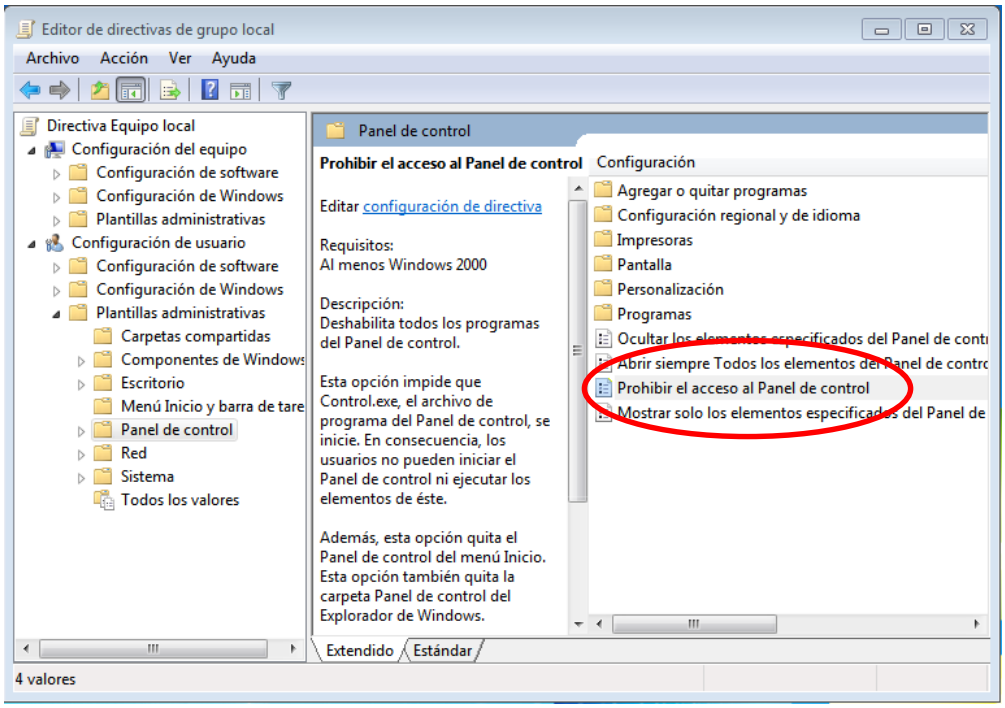

Figura 3-35 Diversas opciones de configuración de las *plantillas administrativas*

Como herramienta que complemente esta seguridad, está evitar compartir archivos entre usuarios, accediendo a *Panel de Control* > Redes e internet > Centro de redes y recursos compartidos > Cambiar configuración de uso compartido avanzado, como vemos en la Figura 3-36.

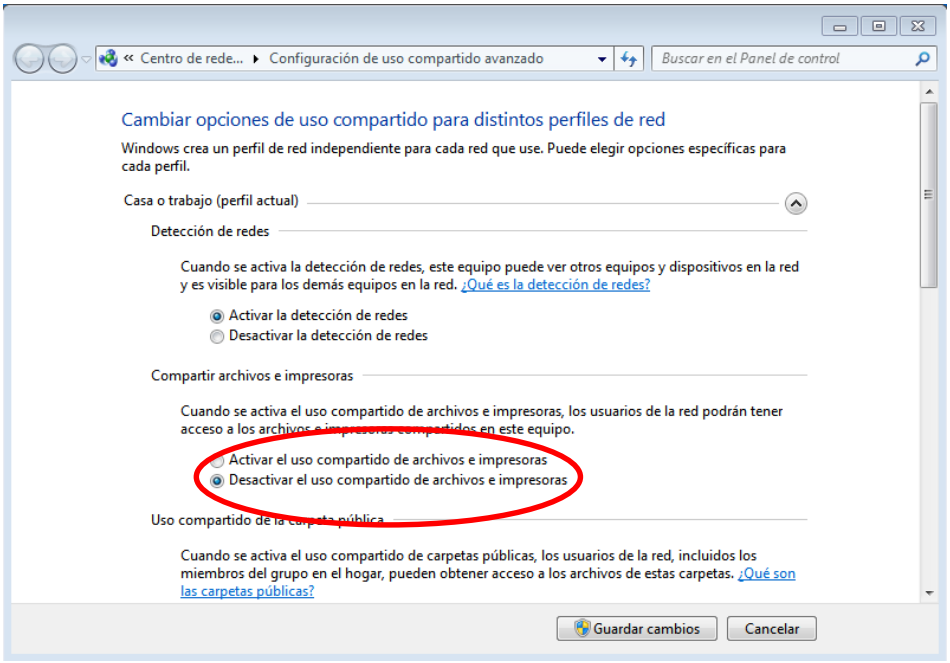

Figura 3-36 Desactivar el uso compartido de archivos

Queda decir que la configuración más efectiva y segura sería utilizar dos usuarios, cada uno para sus propósitos, controlar los permisos que ofrecemos a cada usuario y, a su vez, activar el UAC para ser conscientes de cuándo estamos elevando privilegios.

3.2.2.8 Escritorio remoto

No es recomendable permitir el acceso y control de un equipo en una red a través de un escritorio remoto. Evitaremos así que puedan desconfigurarnos el equipo o incluso sustraernos información. Por ello accederemos a *gpedit.msc* > Configuración Equipo > Plantillas Administrativas > Componentes Windows > *NetMeeting* > Desactivar el uso compartido de escritorio remoto (Figura 3-37).

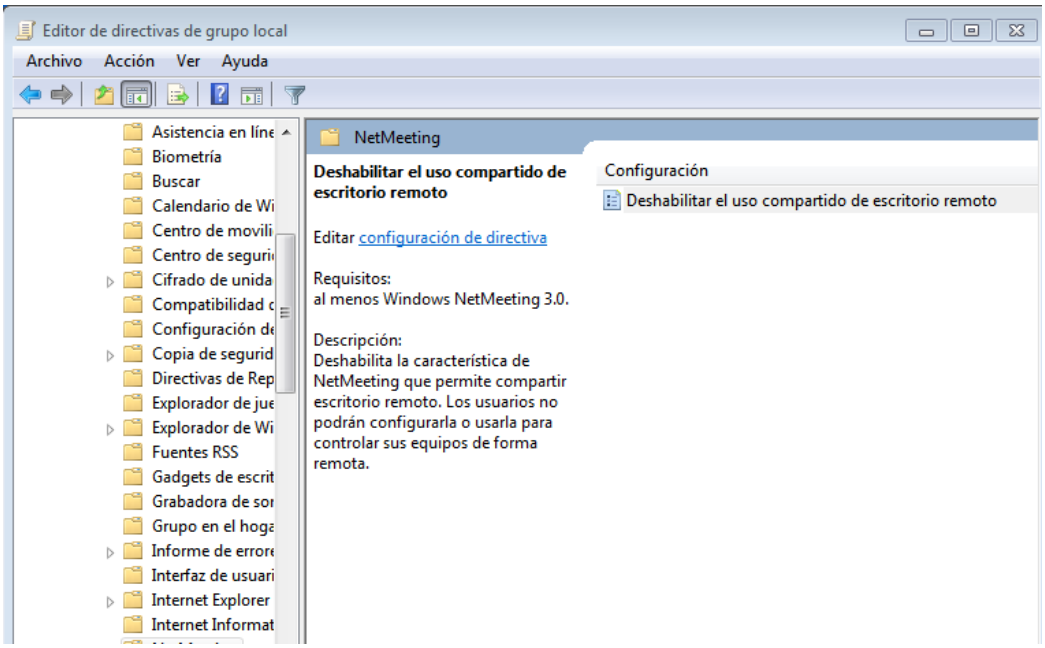

Figura 3-37 Evitar el acceso desde escritorio remoto

3.2.2.9 Archivos ocultos y extensiones

Pese a ser una medida rudimentaria, existe mucho *malware* que se aloja en nuestros directorios simplemente como archivos ocultos. Por consiguiente, para poder eliminarlos, debemos habilitar la opción de carpeta de *Mostrar archivos, carpetas y unidades ocultos*.

A esta opción se accede, dentro de cualquier carpeta, en *Organizar* > Opciones de carpeta y búsqueda > Pestaña *Ver* > *Mostrar archivos, carpetas y unidades ocultos*, como se aprecia en la Figura 3-38.

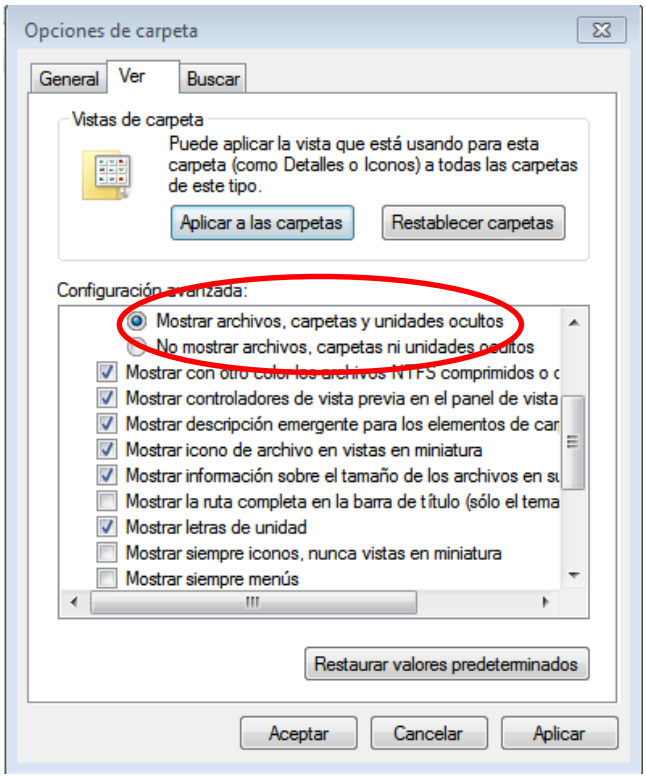

Figura 3-38 Cuadro de diálogo para evitar archivos ocultos

Como complemento, deshabilitar la opción de *Ocultar las extensiones de archivo para tipos de archivo conocidos* y así poder comprobar la concordancia entre la extensión y la naturaleza supuesta de un archivo ya que cierto *malware* intenta, de esta manera, disfrazarse para pasar inadvertido. Podemos ver la opción en la Figura 3-39.

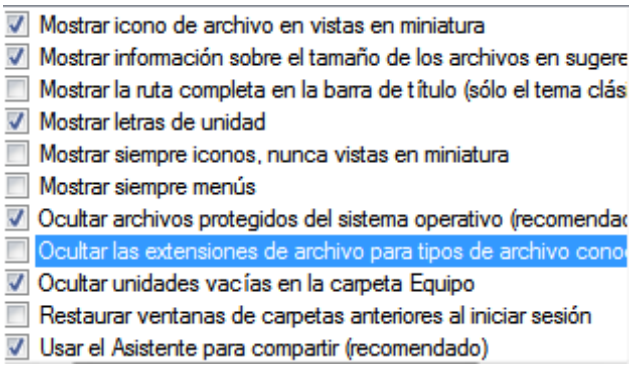

Figura 3-39 Opciones en el cuadro de diálogo para evitar ocultar las extensiones de archivos

3.2.2.10 Contraseñas

Antes de tratar directivas de contraseñas en sí, se debe privar a los usuarios de la opción (innecesaria para el trabajo diario) de *Depurar programas*, para evitar que ciertos programas de atacantes utilicen volcados de *hashes* (o firmas) *offline* y *online*, y averigüen las contraseñas de las cuentas del equipo.

Se deshabilita en el *Editor de directivas de grupo local*, entrando en *Configuración del equipo* > Configuración de Windows > Configuración de seguridad > Directivas locales > Asignación de derechos de usuario > Depurar programas (Figura 3-40).

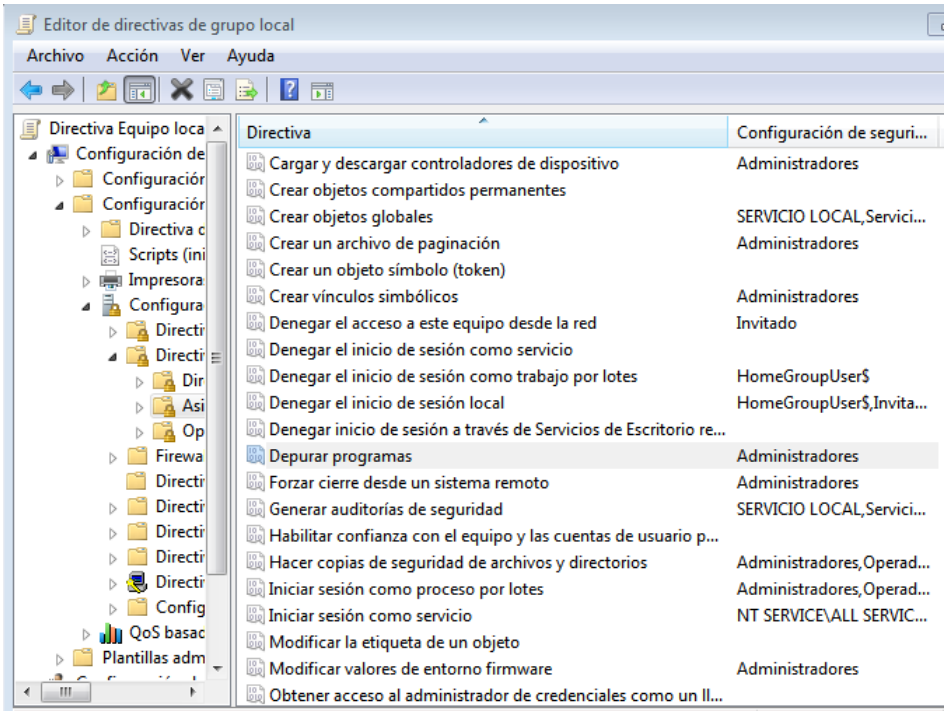

Figura 3-40 Opción *Depurar programas*

Una manera de aumentar la seguridad de las contraseñas se basa en utilizar más de catorce caracteres, ya que, con esta medida, anulamos un método de tratamiento de contraseñas obsoleto denominado LM (*Lan Manager*), y Windows utilizaría exclusivamente NTLM (*NTLan Manager*), que es más seguro ya que diferencia entre mayúsculas y minúsculas, e internamente es más simple y robusto.

Para evitar dejar el ordenador desprotegido en caso de tener que ausentarnos del puesto de trabajo, debemos obligar a que se solicite la contraseña de acceso tras suspender o hibernar el equipo.

Dentro de las opciones de *gpedit.msc* podemos acceder a *Configuración Usuario* > Plantillas Administrativas > Sistema > Administración Energía > Solicitar Contraseña al reanudar tras hibernación o suspensión (Figura 3-41).

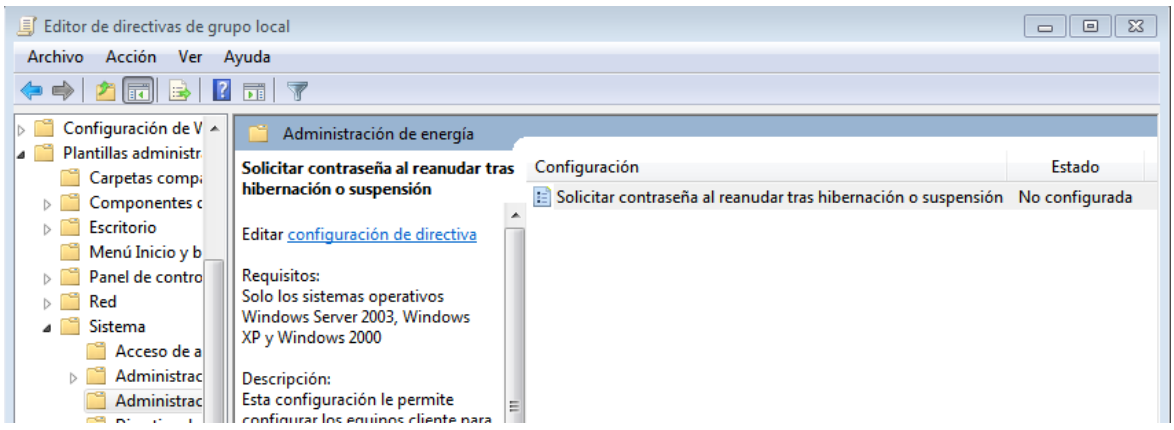

Figura 3-41 Opción para habilitar solicitar contraseña tras hibernar o suspender

Existen unas normas generales sobre las contraseñas que todos deben cumplir para aumentar la seguridad del equipo. El par nombre de usuario y contraseña es lo que permite a cualquier atacante tomar el control de nuestro equipo y de la información dentro de él. Debemos cumplir lo siguiente:

- Nunca dejar una contraseña vacía pues daría paso a cualquier intruso a la cuenta.
- Cambiar la contraseña que se nos asigne por defecto inmediatamente ya que estas contraseñas son conocidas por los atacantes.
- Evitar utilizar recordatorio de contraseña, o intentar que no de información sensible sobre la contraseña.
- No utilizar datos relacionados con nuestra vida personal (fechas de nacimiento, teléfonos, dirección, nombres, apellidos, etc.) pues son fáciles de adivinar.
- Intentar que nuestra contraseña no contenga únicamente caracteres y palabras de un lenguaje determinado, pues podrían sacarse a través de ataques basados en diccionarios.
- Como se ha comentado, no utilizar claves de menos de catorce caracteres.
- Mezclar letras, números y símbolos para dificultar un ataque por fuerza bruta sobre la contraseña.
- No repetir caracteres que aumenten la probabilidad de adivinar la contraseña.
- No mantener una parte de la contraseña modificando siempre el mismo patrón de caracteres.
- No establecer una contraseña por la situación de las teclas del teclado (qwerty, poiuyt, 12345, etc.).
- Actualizar la contraseña de manera regular.

En caso de querer forzar a los usuarios a cumplir estas medidas u otras, Windows, a través de *secpol.msc* > Directivas de cuenta > Directiva de contraseñas, contempla los siguientes cambios que podemos observar en la Figura 3-42.

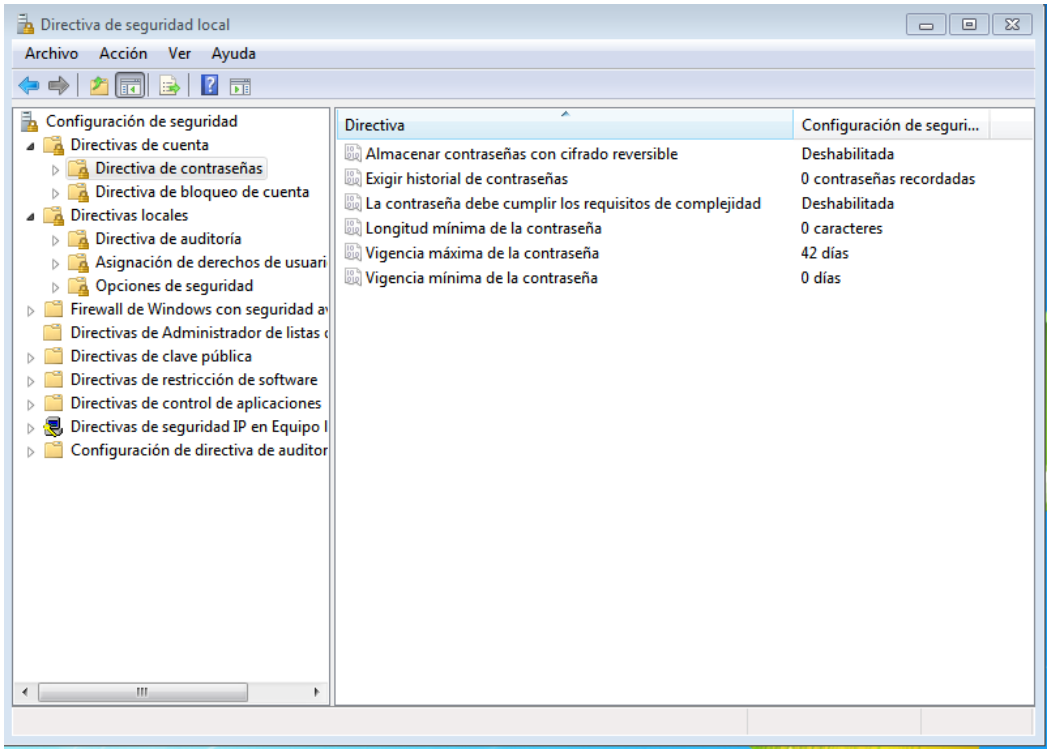

Figura 3-42 Directivas para forzar políticas estrictas de contraseñas

3.2.2.11 Syskey

Esta herramienta de Windows permite no sólo cifrar las contraseñas ya cifradas por LM y NTLM, añadiendo una capa de seguridad, sino que obliga a un atacante a descifrar una clave de acceso más: la

System Key (que hemos definido anteriormente y que se nos solicita incluso antes que las contraseñas de usuario).

La forma de utilizar la herramienta es escribir *syskey* en búsqueda > Cifrado habilitado > Actualizar > Inicio con contraseña (Figura 3-43).

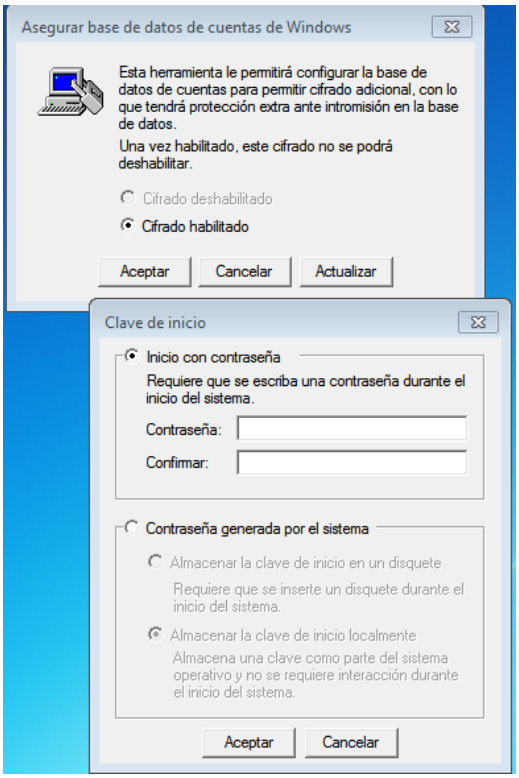

Figura 3-43 Añadir una capa más de seguridad a las contraseñas por medio de *Syskey*

3.2.2.12 Permisos y usuarios

La buena gestión de usuarios y permisos NTFS (*New Technology File System*) son una gran herramienta para dar seguridad al equipo por parte del administrador.

En cuanto a usuarios, como hemos comentado en puntos anteriores, la cuenta que utilicemos para administrar deberá, para empezar, estar protegida por una fuerte contraseña ya que se trata de la cuenta más importante (y por ello peligrosa) del equipo. Para cambiar la contraseña, desde *Panel de Control* accederemos a *Cuentas de usuario* (Figura 3-44) y debe ser cambiada de nombre para hacer más difícil su identificación por parte de un atacante.

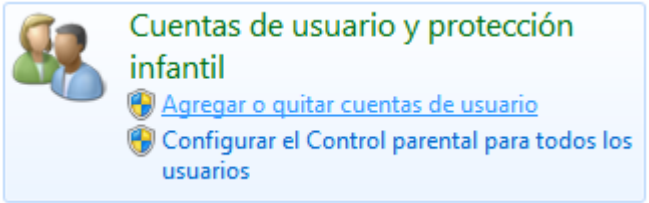

Figura 3-44 Administración de cuentas de usuario

Además, la cuenta de invitado si existe (y la cuenta *Administrador* que viene por defecto en el sistema), deberá deshabilitarse en:

Panel de Control > Cuentas de usuario > Agregar o quitar cuentas de usuario > Invitado > Desactivar la cuenta de invitado (Figura 3-45).

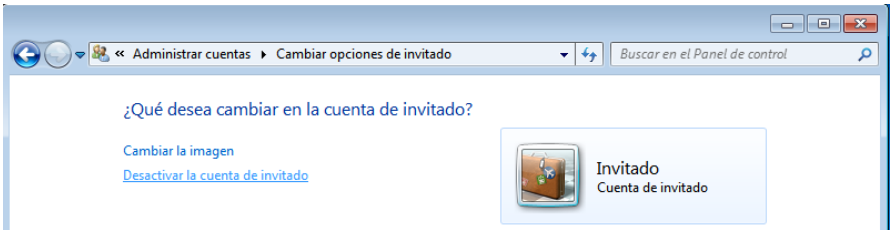

Figura 3-45 Desactivar la cuenta de Invitado

En cuanto a los grupos de usuarios [17], deberíamos tener exclusivamente un grupo de administradores y uno de usuarios normales para el uso diario. En el grupo Administradores, sólo debería existir el Administrador (deshabilitado) y el usuario que utilicemos para administrar. Conseguimos así aislar los distintos tipos de usuarios, evitando mezclar sus permisos y privilegios, y que un *malware* que acceda a una cuenta de un grupo normal, no pueda pasar a aprovecharse de una de administrador.

Para modificar la administración de los *Grupos y usuarios*, realizaremos las siguientes operaciones:

Teclearemos *mmc* en búsqueda para acceder a la interfaz de Microsoft Management Console > Archivo > Agregar o quitar complemento > Usuarios y grupos locales > Agregar > Equipo local > Aceptar (Figura 3-46).

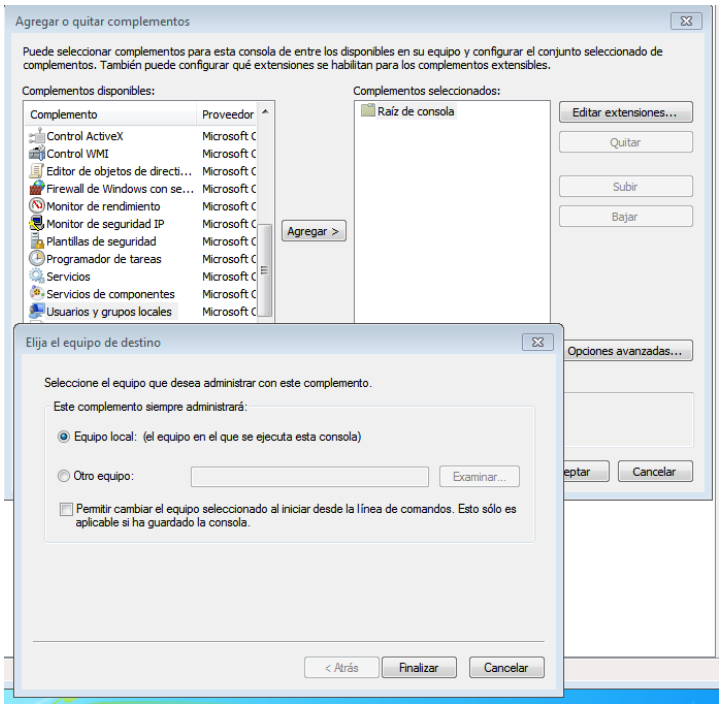

Figura 3-46 Acceder a control de usuarios y grupos

Ahora podremos gestionar los usuarios (habilitarlos y/o deshabilitarlos) y los grupos navegando por la interfaz del MMC (*Microsoft Management Console)* (Figura 3-47, Figura 3-48 y Figura 3-49).

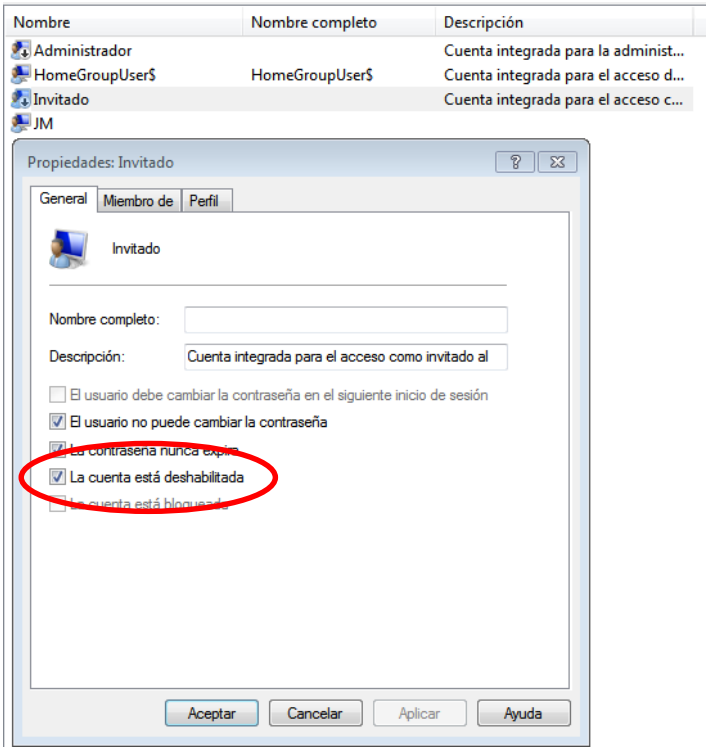

Figura 3-47 Comprobación de que la cuenta de Invitado está desactivada

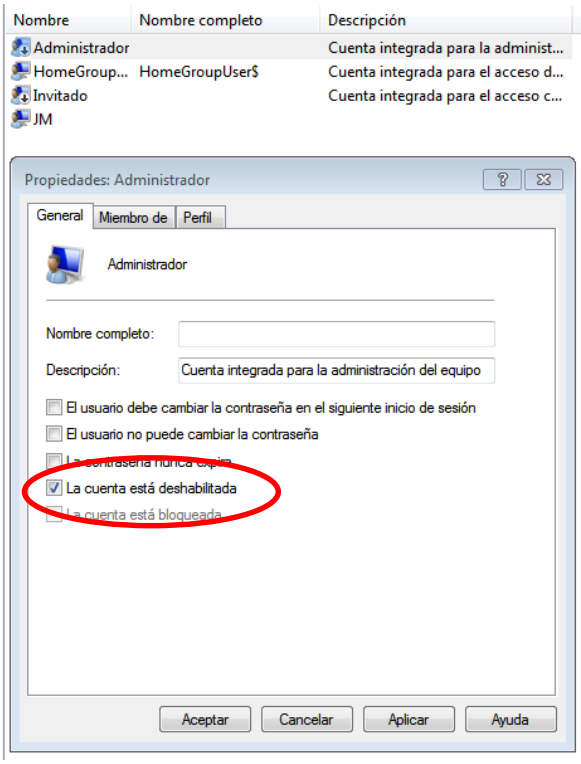

Figura 3-48 Desactivación de la cuenta Administrador

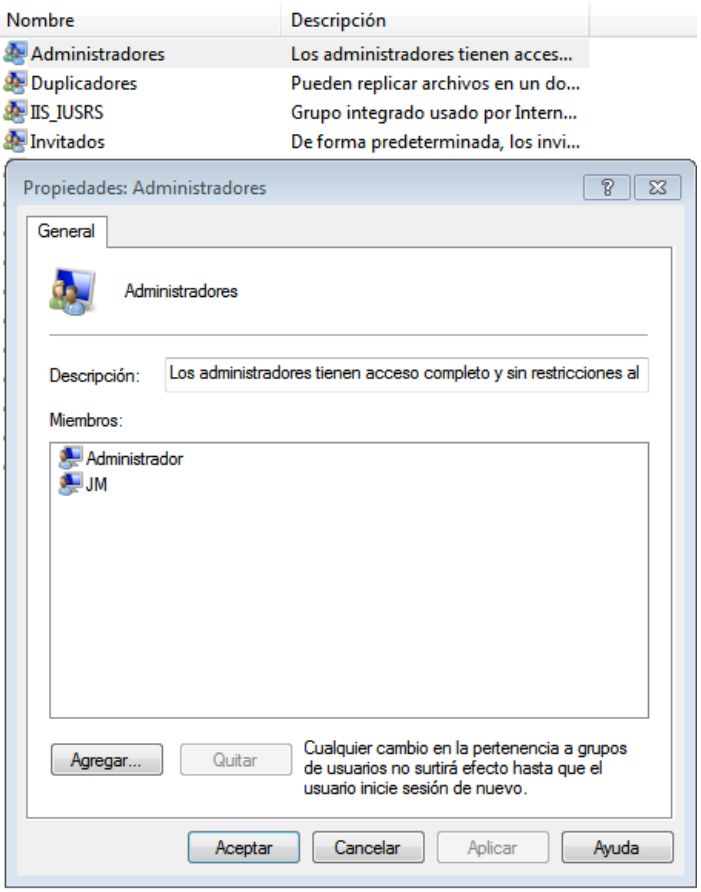

Figura 3-49 Gestión del grupo de administración

Por otro lado, los permisos NTFS permiten controlar lo que puede o no hacer un usuario en el sistema. La protección de NTFS se proporciona por medio de ACL (*Access Control List)* o Lista de Control de Acceso, que permite definir los permisos que tiene un usuario, grupo o programa sobre un archivo, por lo que están restringidos a lo que indiquen las ACL.

Un conflicto de seguridad existente ocurre por lo que se denomina *Omisión de comprobación de recorrido*. Si una carpeta posee una ACL restringida a ciertos usuarios, estos no podrán acceder a ella ni ver su contenido. Si existiera el caso en el que la carpeta contiene algún archivo sin una ACL restringida y el usuario/atacante conociese la ubicación exacta de ese fichero, teniendo activada la *Omisión de comprobación de recorrido*, podría acceder a él.

Debemos desactivar esa opción a los usuarios o grupos que consideremos oportunos desde *secpol.msc* > Directivas locales > Asignación de derechos de usuarios > Omitir comprobación de recorrido (Figura 3-50).

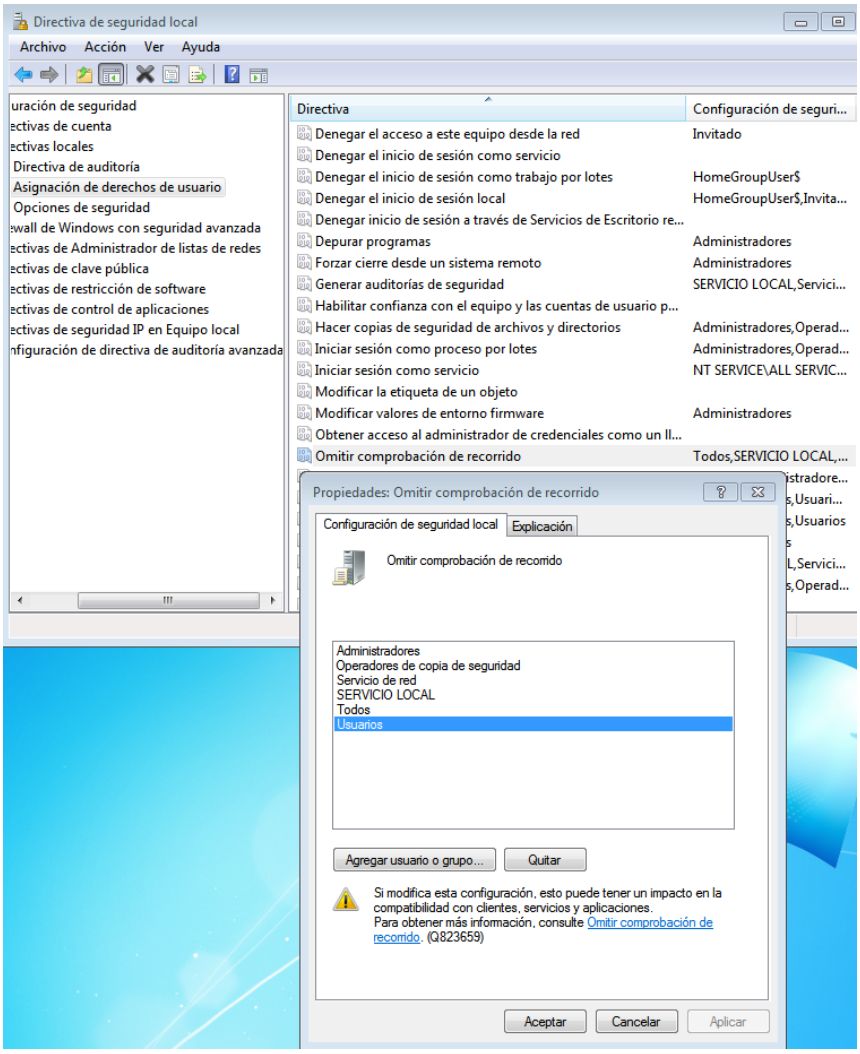

Figura 3-50 Gestión de grupos respecto a *Omisión de comprobación de recorrido*

Otra laguna de seguridad podría solventarse eliminando ciertos permisos (*Control Total*, *Cambiar permisos*, *Atravesar carpeta y ejecutar archivo*, *Tomar posesión*, etc.) de los usuarios, que les otorgan ciertas libertades que pueden comprometer la seguridad de los datos. Modificaremos los permisos, dependiendo de cuanto queramos restringirlo, en las carpetas *Mis documentos* y sus subcarpetas.

Carpeta *Mis documentos* > Clic derecho > Propiedades > Pestaña *Seguridad* > Opciones avanzadas > Cambiar permisos > Elegimos el usuario > Editar (Figura 3-51).

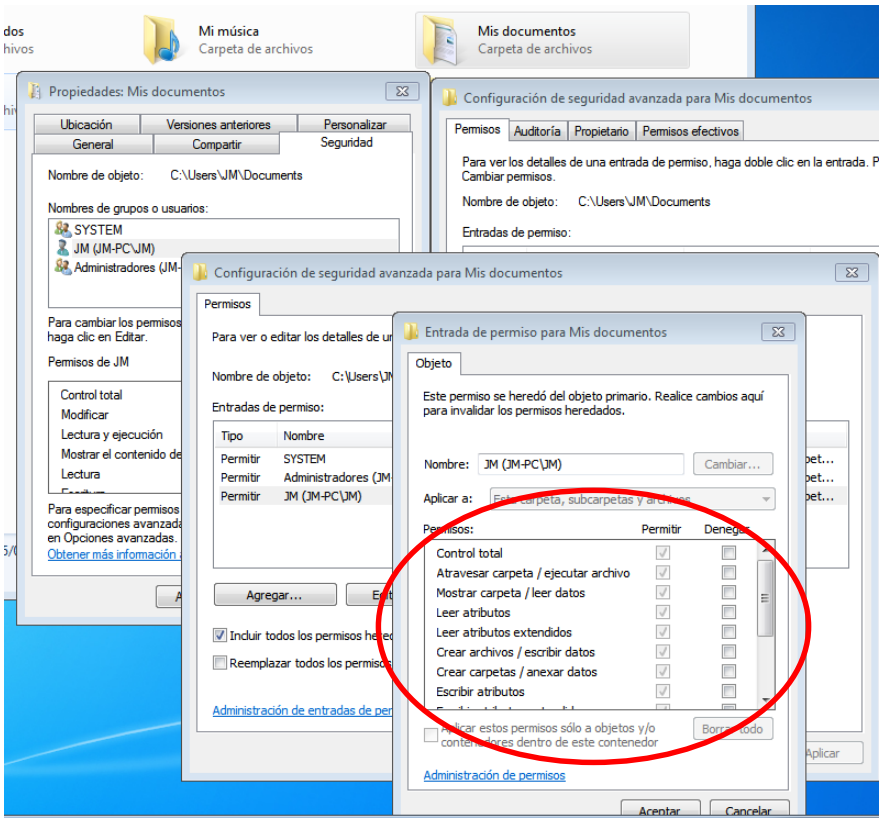

Figura 3-51 Gestión de permisos en la carpeta *Mis documentos* y subcarpetas

Con esto limitamos, en el directorio personal de cada usuario, la posibilidad de ejecución de ciertos archivos o software infectado que pueda realizar cambios importantes, debido a los bajos privilegios que el usuario posee tras haberle restringido libertad de acción. Además, nos cercioramos de que los usuarios normales no puedan excluir al *Administrador* de lo que hagan o guarden en sus carpetas personales.

Como otras opciones de seguridad relacionadas con permisos que tienen o no los usuarios, se recomienda, dentro de las *directivas de seguridad local* (*secpol.msc*), en *opciones de seguridad*, modificar ciertas auditorías que nos ayudarán a disminuir riesgos. Entre ellas:

- Apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad (Figura 3-52).
- No permitir enumeraciones anónimas de cuentas y recursos compartidos SAM (*Security Account Manager* o administrador de cuentas de seguridad).
- No permitir enumeraciones anónimas de cuentas SAM.
- No permitir traducción *SID* (*Security Identifier* o identificador de seguridad de usuario) – *nombre* anónima.
- Restringir acceso anónimo a canalizaciones con nombre y recursos compartidos.

Con la primera medida evitamos que potenciales acciones de un atacante se queden sin registrar. Con el resto de cambios (Figura 3-53), evitamos que, en una red, un atacante se conecte como anónimo y consiga información sobre listados de usuarios o estado del sistema.

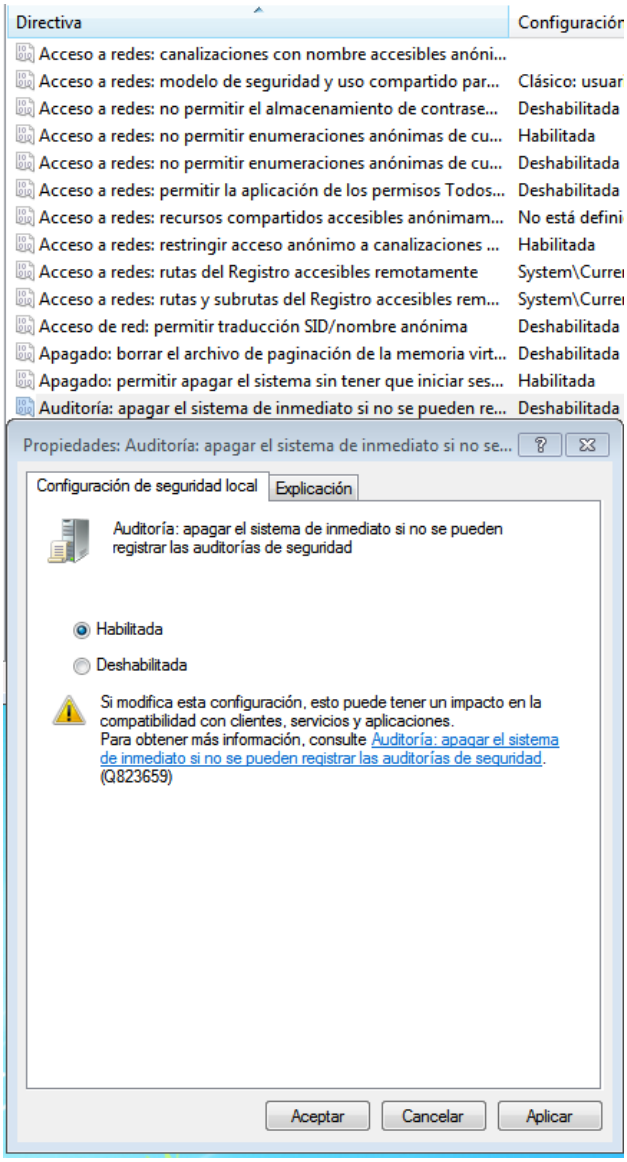

Figura 3-52 Auditoría *Apagar el sistema* para evitar acciones de atacantes sin registro

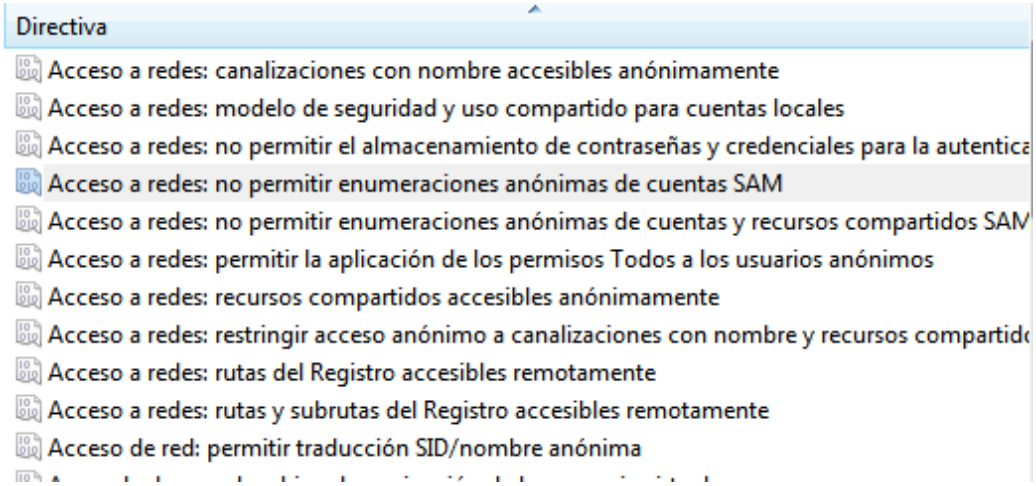

Figura 3-53 Diversas auditorías para evitar conexiones anónimas

En el presente TFG, recomendamos, a mayores de las anteriores, activar las siguientes auditorías:

- *No permitir almacenamiento de contraseñas y credenciales para la autenticación de la red*. Obligamos a que sea necesario introducir las contraseñas cada vez que alguien desee autenticarse y que no se almacenen en el sistema (donde cierto *malware* podría encontrarlas).
- *Forzar la protección con contraseñas seguras para claves de usuario almacenadas en el equipo*. Añadimos una capa de seguridad a los certificados y claves públicas, ya que no se permitirá su uso si no se conoce la clave que los desbloquea.
- La instalación de impresoras debe hacerse exclusivamente por el administrador para evitar fugas de información e instalación de drivers manipulados. Por ello, procederemos a activar *Impedir que los usuarios instalen controladores de impresora cuando se conecten a impresoras compartidas*.
- *Cargar y descargar controladores de dispositivo*. Cargar un controlador es como instalar un *rootkit* (puerta trasera) a través del cual pueden perpetrarse ataques sin que lo sepamos. Se puede otorgar este privilegio en los momentos puntuales en los que se necesite.
- Por último, desactivaremos *Mostrar información del usuario cuando se bloquee la sesión* y *Mostrar el último nombre de usuario*, para que nadie con acceso físico al equipo obtenga información sobre los usuarios del equipo y evitar que utilicen ataques de fuerza bruta sobre la contraseña.

3.2.2.13 Cortafuegos o firewall

Se trata de una de las herramientas de seguridad más antiguas y utilizadas cuyo objetivo es restringir puertos de acceso o salida del ordenador.

Para configurarlo correctamente, debemos escribir en búsqueda *wf.msc* (Figura 3-54).

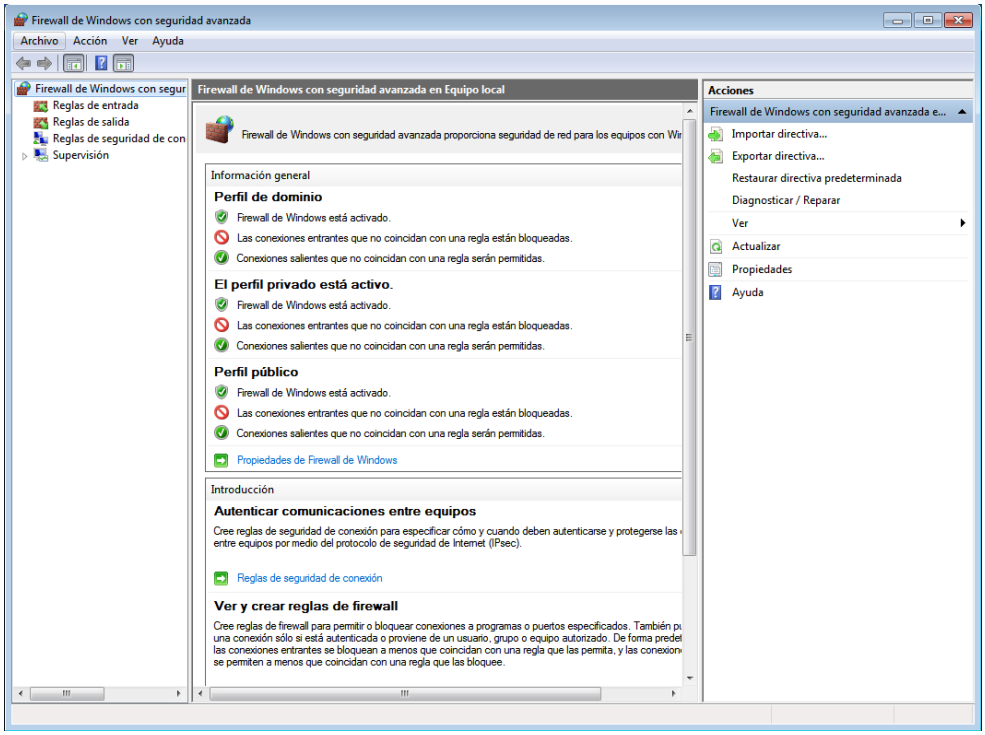

Figura 3-54 *Firewall*

El perfil debe asociarse con una situación. De manera general, el perfil *Dominio* es el adecuado para el trabajo y el *Privado* para casa, dejando el *Público* para utilizar en redes desconocidas. Este último debe ser lo más restrictivo posible.

Dentro de cada perfil podemos configurar las conexiones *entrantes* y *salientes*. En cuanto a las *entrantes*, tenemos infinidad de posibilidades de configuración (qué aplicación puede hacer uso, qué programas, qué usuarios, etc.) además de las ya activadas por defecto por parte de Microsoft.

Es la configuración del cortafuegos saliente lo que puede marcar la diferencia en cuanto a la seguridad. En Windows 7, a diferencia de versiones anteriores, no sólo se proporciona seguridad hacia dentro sino hacia fuera. Esto es algo que no tenemos en cuenta y que los creadores de *malware* explotan constantemente.

El *malware* de hoy en día ha aprendido a eludir el cortafuegos entrante, ya que en vez de intentar entrar por un puerto de la máquina, ahora el programa *malware* sale en búsqueda de su sistema de control y, por lo tanto, el cortafuegos entrante no actúa. Es, por esto, por lo que debemos realizar ciertas gestiones en las reglas de salida del cortafuegos.

Para empezar, saber que debemos filtrar por aplicaciones y no por puertos (ya que existen ingentes aplicaciones legítimas que utilizan los mismos puertos que otras ilegítimas y ocasionaríamos conflictos a la hora de ejecutarse). Necesitaremos acceder a *Reglas de salida* > Nueva regla > Programa (Figura 3-55). Con esta herramienta debemos ir eligiendo cuidadosamente las aplicaciones que queremos que salgan al exterior.

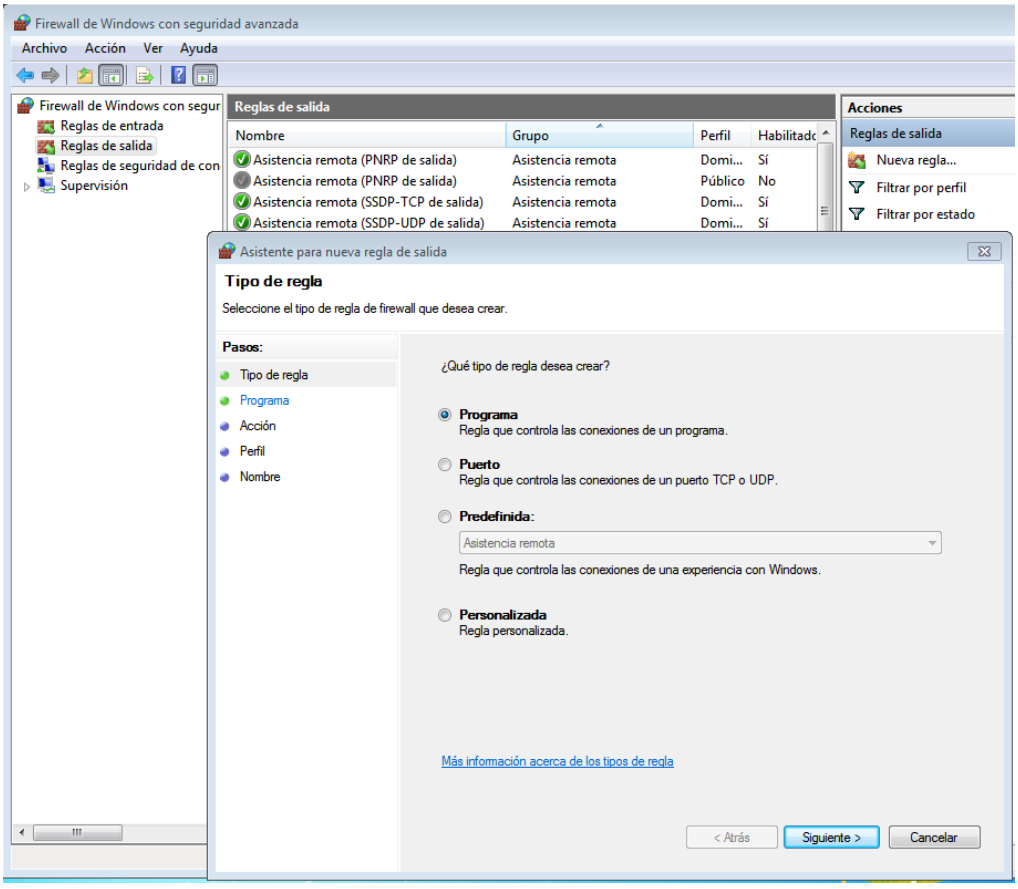

Figura 3-55 Creando regla de salida por programa

Existe una herramienta denominada *FWRulez* [18] que nos permite crear más fácil e intuitivamente estas reglas para bloquear hacia afuera los programas. Interactúa con el *Firewall* de Windows sin necesidad de comandos ni asistente y se puede acceder desde el menú contextual como vemos en la Figura 3-56.

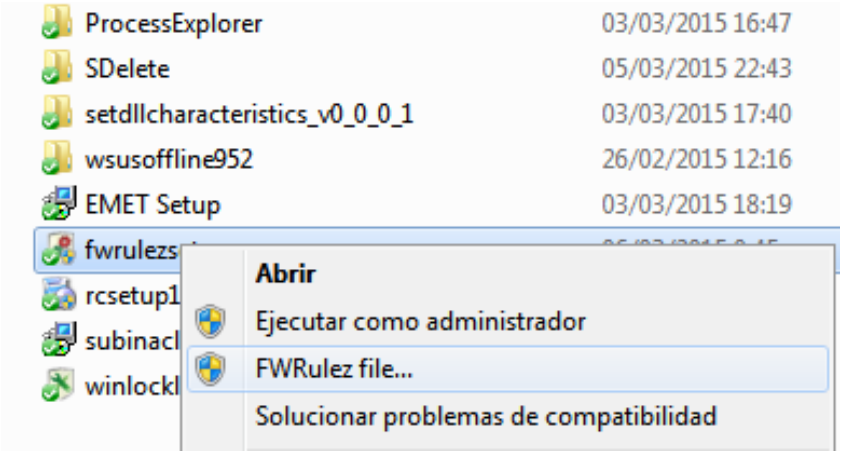

Figura 3-56 Menú contextual con opción *FWRulez*

3.2.2.14 Servicios

Los servicios son un importante punto de exposición ya que están permanentemente funcionando y no necesitan al usuario para ello, por lo que un atacante sabe que están siempre ahí para ser atacados.

A través de *services.msc* (Figura 3-57), podemos modificar los servicios que están habilitados o no, administrar los privilegios con los que se ejecutan y controlar quién los puede configurar, arrancar, parar, etc. Debemos deshabilitar los que no sean necesarios para aumentar la seguridad del equipo, reduciendo los posibles puntos de entrada.

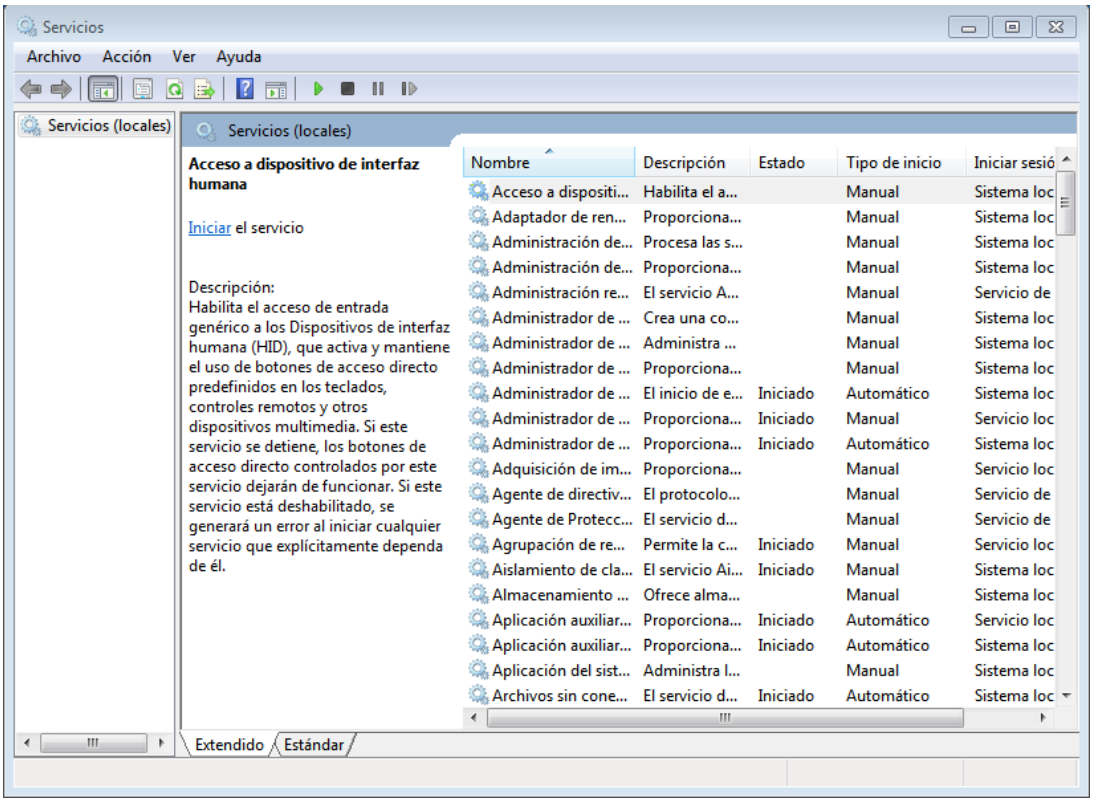

Figura 3-57 Servicios de Windows

Seleccionando cada servicio podemos configurarlo para que utilice una cuenta específica, controlando así los privilegios que posee, dependiendo del uso que queramos darle.

Las cuentas se ordenan como: Servicio Local, Servicio de red, Cuenta de usuario, de menos privilegios a más. La Cuenta de usuario consiste en crear una cuenta única local para que el servicio corra bajo los permisos que la cuenta posea. Deberá estar protegida por una fuerte contraseña y no estar sometida a cambios de contraseñas muy regulares.

Para finalizar, es importante que, conforme realicemos cambios en *Servicios*, avancemos con precaución y realizando copias de seguridad, ensayos y seguimientos para no interferir en el funcionamiento correcto del equipo.

3.2.3 Seguridad del software

Si el objetivo de un atacante es controlar el S.O., los programas y el software son las puertas que le darán acceso. Por ello, es importante conseguir una configuración robusta de las aplicaciones desde el primer momento. Aconsejaremos medidas tanto para la prevención como el bloqueo del código dañino, para evitar o reducir sus efectos una vez infectados. Se nombrarán herramientas como la criptografía PGP (*Pretty Good Privacy* o Privacidad Bastante Buena) y la combinación de DEP y ASLR por parte del programa EMET.

3.2.3.1 Prevenir el código dañino

Comprobar la integridad de los ficheros descargados es algo que debemos hacer siempre para evitar agujeros de seguridad y todos sabemos que no debemos pulsar en un ejecutable de un correo electrónico. Pero no todo es tan sencillo y por ello debemos poner los medios necesarios para comprender las herramientas de las que disponemos para construir un entorno seguro.

3.2.3.2 La firma criptográfica GPG

Este método permite no sólo comprobar la integridad de un archivo descargado sino que además garantiza que viene de la persona que dice haberlo creado.

Se publica, en la página web donde descargamos el fichero, un archivo con extensión SIG que resulta de firmar el archivo descargado con la clave privada del propietario del archivo. Con este archivo y con la clave pública (también tiene que estar disponible en la página web, con extensión ASC), podemos comprobar que el fichero concuerda y realmente es de quien dice haberlo creado, aumentando la fiabilidad del origen.

Para comprobar la concordancia de las firmas, utilizaremos la herramienta *GnuPG* [19]. Teniendo la clave pública del que firma, el archivo que queremos verificar y la firma del archivo (clave privada), podremos seguir las instrucciones de la herramienta, comprobar la integridad del archivo y verificar que proviene de la persona identificada con la clave pública (Figura 3-58).

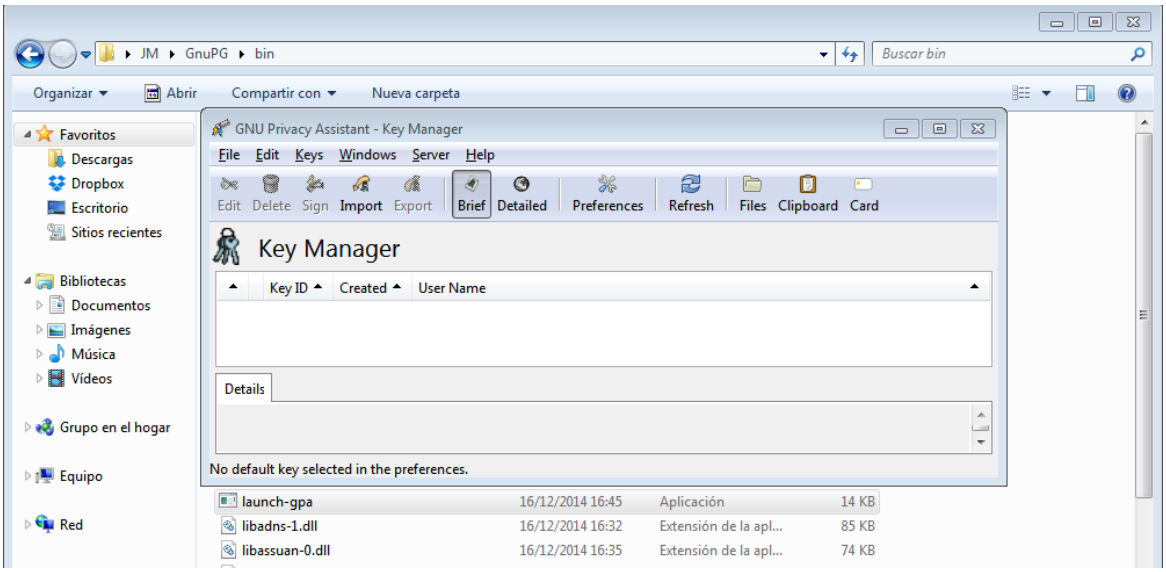

Figura 3-58 Interfaz *Key Manager* GnuPG

Tras haber instalado y ejecutado la herramienta, observamos que nos ofrece múltiples opciones de cifrado, descifrado, comprobación, etc. con el botón derecho sobre un fichero, como vemos en la Figura 3-59.

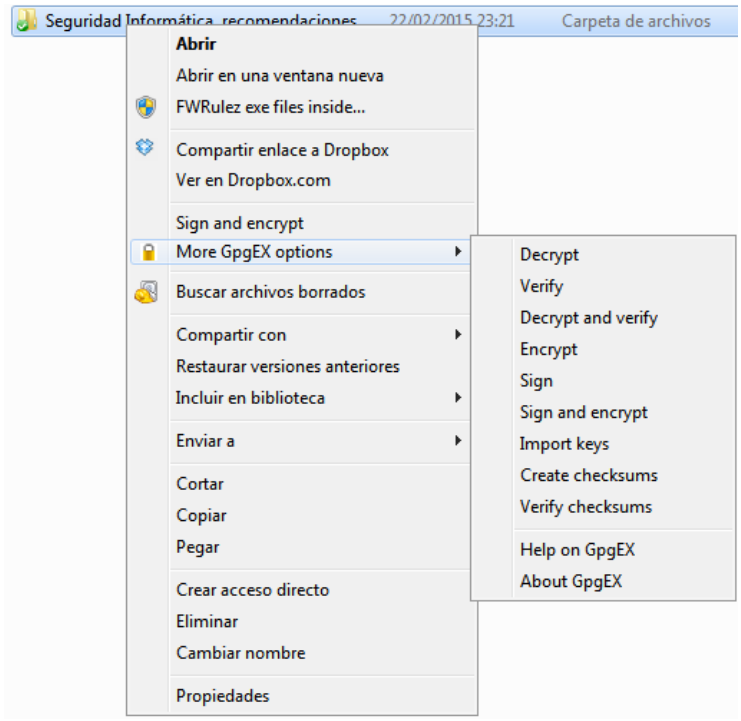

Figura 3-59 Opciones de GPG sobre un fichero

Ahora debemos comprobar que la firma asociada al archivo le pertenece a quien dice poseerla. Existen dos maneras: por medio de una autoridad certificadora o a través de un sistema de reputación, en el que usuarios que conocen a una persona y se han comunicado de manera fehaciente, dan validez a las firmas. Esto lo podemos conseguir a través de los servidores GPG universales como el del MIT (Figura 3-60) [20].

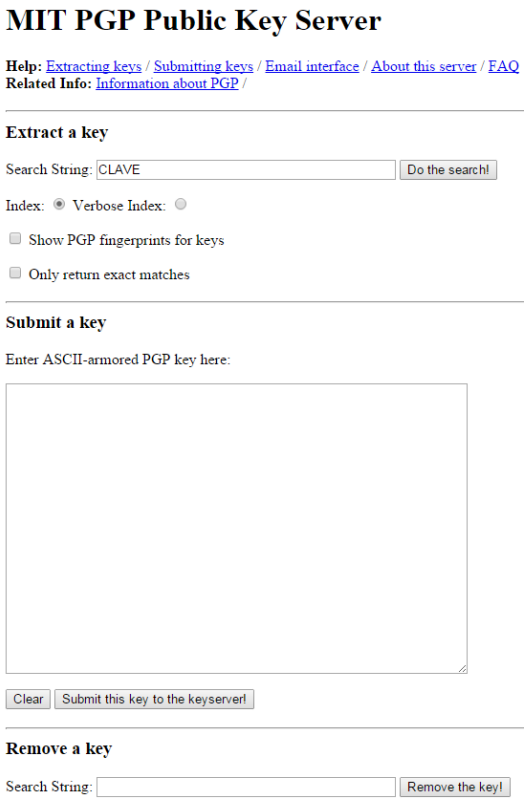

Figura 3-60 Servidor PGP del MIT

En caso de preferir que sea una compañía externa la que certifica la validez de la identidad del firmante, acudimos a firmas a través de certificados que proporciona una autoridad certificadora.

Sobre el archivo, podemos comprobarlo a través de Clic derecho > Propiedades > Firmas digitales > Clic sobre la firma > Clic sobre contrafirmas > Rutas de certificación (Figura 3-61).

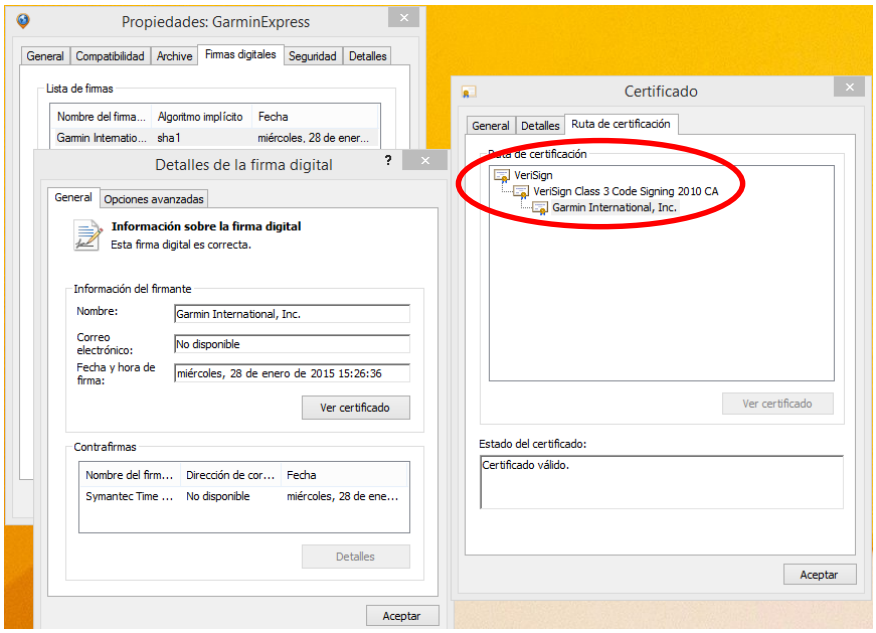

Figura 3-61 Comprobación de certificado

Existen diversas autoridades certificadoras como, por ejemplo, *Verisign.* Debemos comprobar y actualizar periódicamente la lista de *Certificadores Raíz* para tener acceso a las últimas modificaciones que se hayan podido producir por fallos de seguridad o implementación de nuevas autoridades.

Esto lo llevamos a cabo a través de las actualizaciones automáticas de Microsoft o en *mmc* > Agregar complemento > Certificados > Certificados de usuario actual > Certificados o Botón derecho en *Certificados* > Actualizar (Figura 3-62).

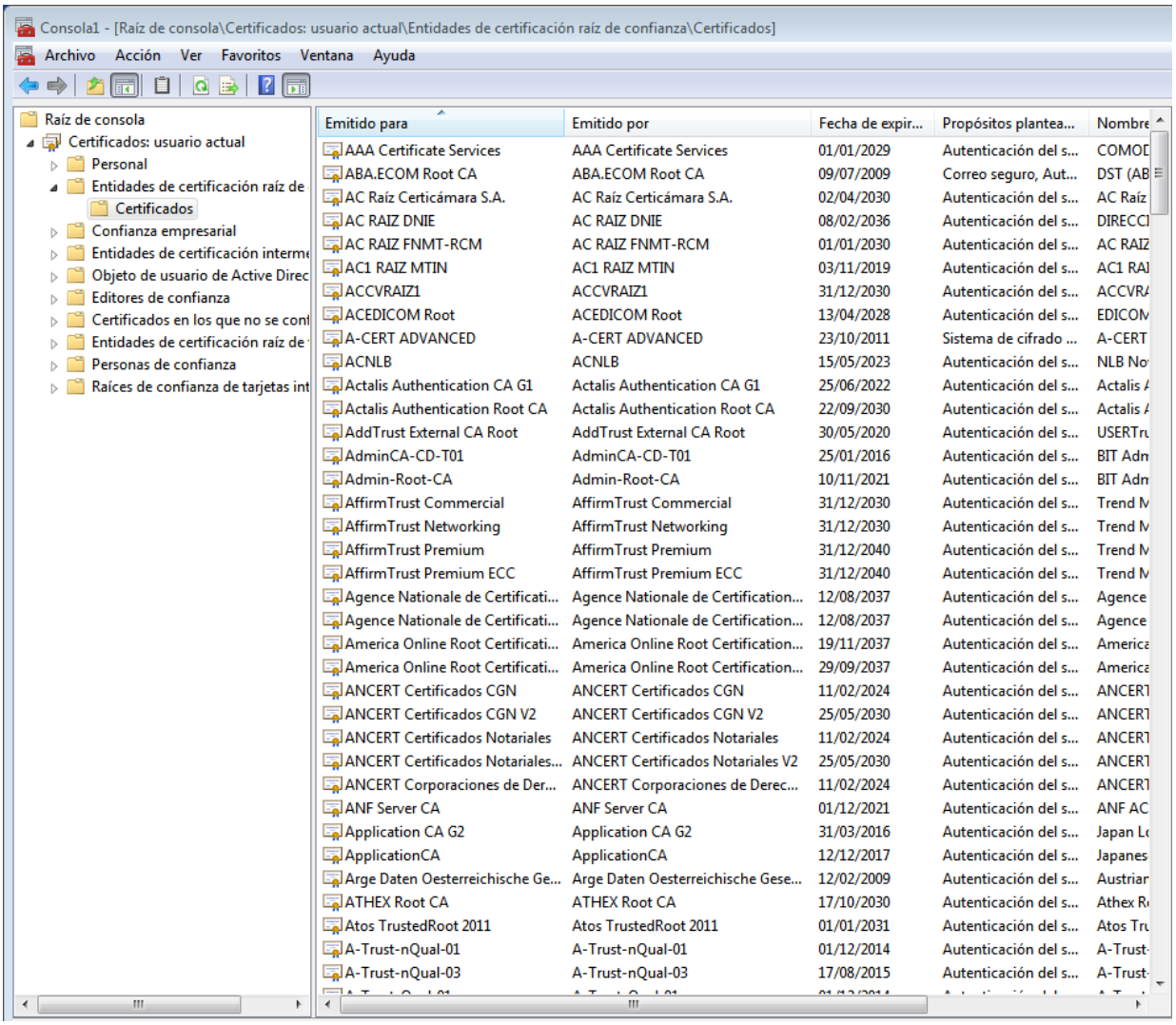

Figura 3-62 Lista de certificados de Microsoft

3.2.3.3 Búsqueda de infecciones

En caso de haber resultado infectados (situación que inevitablemente sucede en algún momento), debemos proceder a buscar el *malware* y deshacernos de él. Podemos hacer uso de un antivirus o de programas como *Microsoft Removal Tool* [21].

Es una herramienta de Microsoft que complementa el uso de antivirus y permite la búsqueda de *malware* conocido y predominante en el sistema y su eliminación. Se publican actualizaciones el segundo martes de cada mes (Figura 3-63).

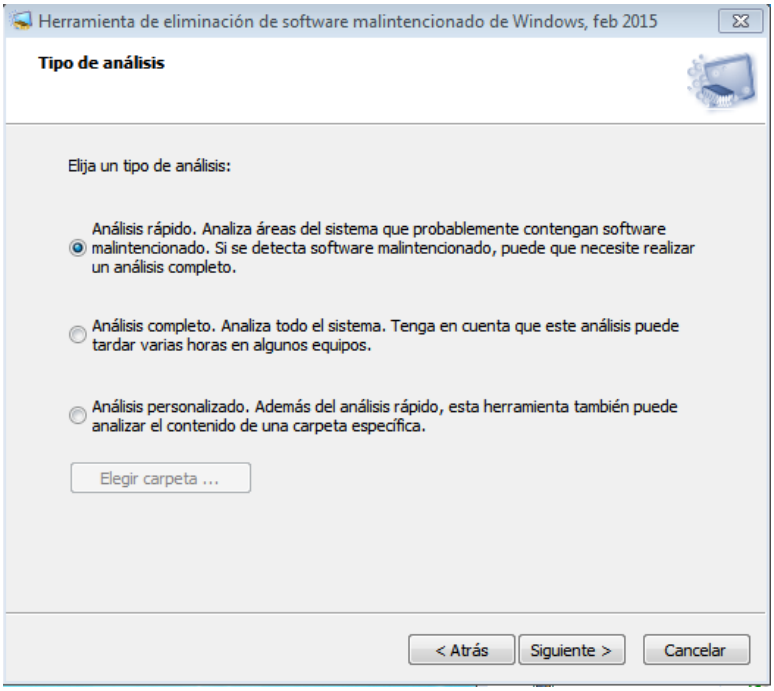

Figura 3-63 Tipos de análisis de *Microsoft Removal Tool*

Además de las medidas anteriores, podemos analizar en la web un archivo en búsqueda de *malware* (complementando, de nuevo, el uso de antivirus). Utilizando sistemas de análisis múltiple como *virustotal.com* (Figura 3-64) [22] podemos asegurarnos de si algunas casas de virus reconocen o no el archivo como peligroso.

Figura 3-64 Sitio web de *Virustotal*

3.2.3.4 DEP

Prevenir el código malicioso completamente es imposible, por lo que debemos saber cómo bloquearlo y defendernos ante las vulnerabilidades que se produzcan. Reiterando lo comentado previamente sobre DEP, impedir que cierto código se ejecute (o que se ejecute en ciertas áreas) es la base de esta seguridad. Por ello, recurrimos a DEP (sólo aplicable a programas de 32 bits; 64 bits ya vienen protegidos por defecto).

La configuración que se explicó en la Figura 3-11 fue la básica, en la que se aplicaba DEP a los servicios de Windows esenciales. Ahora profundizaremos y elegiremos la segunda opción, conocida como *Opt-Out*, en la que se aplica la protección DEP a todos los procesos excepto a los que incluyamos en la lista (útil por si un usuario no quiere que esta configuración afecte al funcionamiento de algún programa en especial) como se muestra en la Figura 3-65.

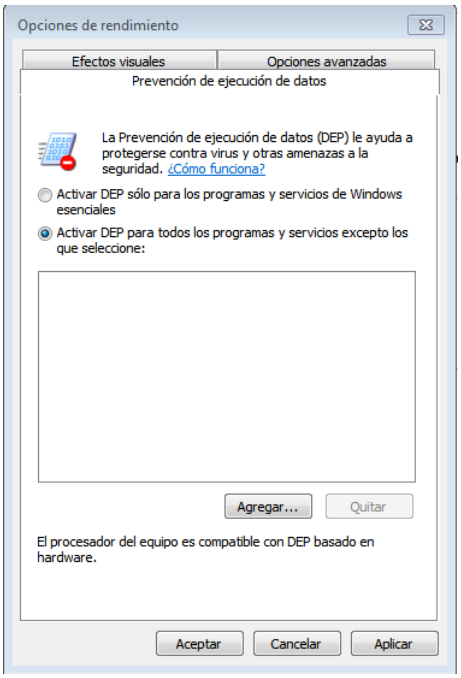

Figura 3-65 DEP *Opt-Out*

Otra manera de comprobar si tenemos activado DEP es ejecutando *bcdedit* en una consola de comandos y observar cómo está configurada la opción *nx* (que es la denominación de DEP), como se aprecia en la Figura 3-66.

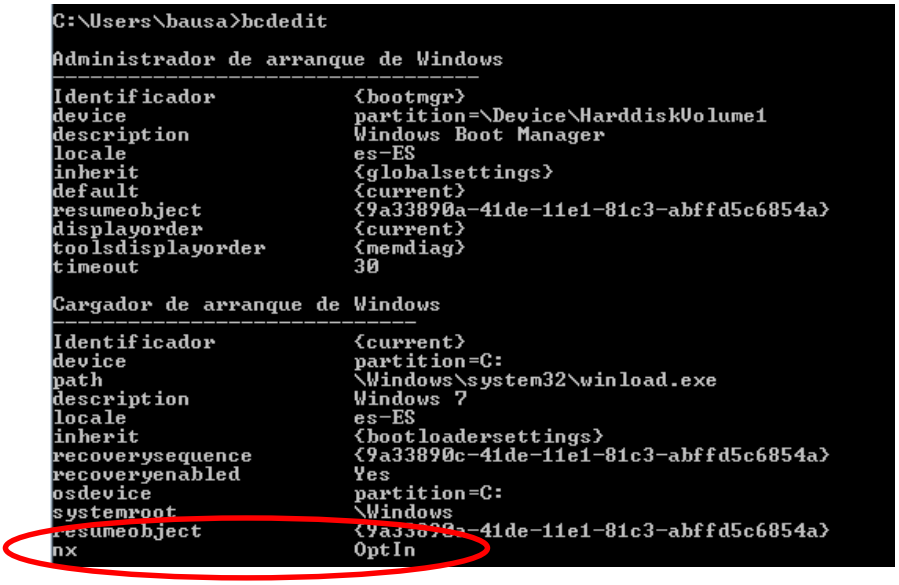

Figura 3-66 Comprobación *nx* (DEP) a través de consola de comandos

Se recomienda, en especial, comprobar *Office 2003*, ya que es un programa conocido que no posee el DEP activado por defecto.

3.2.3.5 ASLR

Se trata de otra medida adicional que ayuda a DEP a evitar la ejecución de código.

El objetivo de aplicar ASLR a todos los programas utilizados es evitar la facilidad que tienen los atacantes para predecir las direcciones comunes de memoria donde se alojan ciertos procesos, con el fin de que no puedan acudir a ellas e inyectar un código que se ejecute con posterioridad.

ASLR obliga a que esas direcciones donde se cargan las DLL (*Dynamic Link Library)* (y/o archivos EXE) cambien en cada reinicio, reduciendo en gran medida las posibilidades de un ataque. Cada vez que arranca el sistema, el método se encarga de cargar los procesos en espacios más o menos aleatorios, obligando a un atacante a tener que probar un ataque a la fuerza hasta 256 veces para tener la posibilidad de acertar con una dirección adecuada. Aun así, este valor no le serviría para otro sistema Windows, por lo que le impedimos que cree procesos automatizados de ataque.

Utilizaremos el programa *setdllcharacteristics* [23] (Figura 3-67) para ir activando y desactivando ASLR por ejecutable (.exe) y librería (.dll). El comando que debemos introducir será: *setdllcharacteristics +d program.exe*, siendo *+d* la opción para activar el ASLR (aunque podemos utilizarlo como otra manera para activar el DEP, aplicando *+n*).

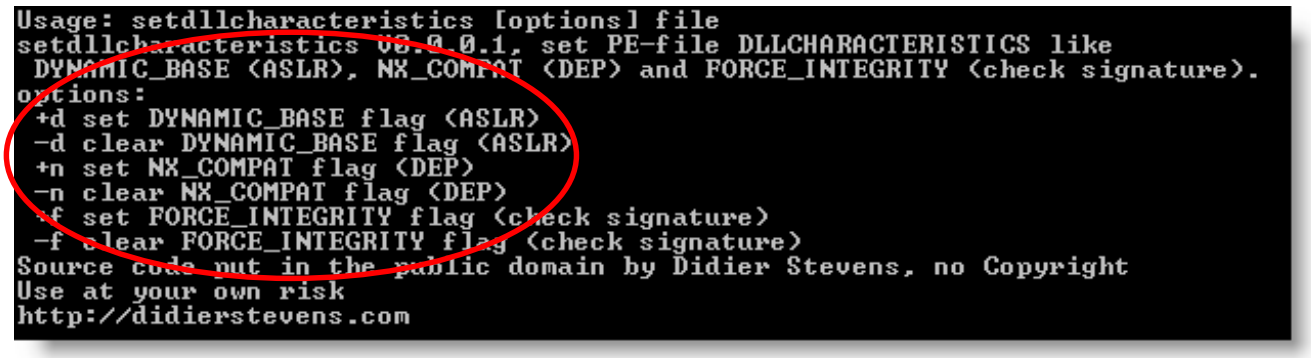

Figura 3-67 Uso de *setdllcharacteristics*

Con el programa *Process Explorer* [24], podemos comprobar, como vemos en la Figura 3-68, qué procesos se ejecutan protegidos por ASLR (así como por DEP). Con el botón derecho en la barra de columnas, podemos seleccionar qué datos queremos que nos muestre.

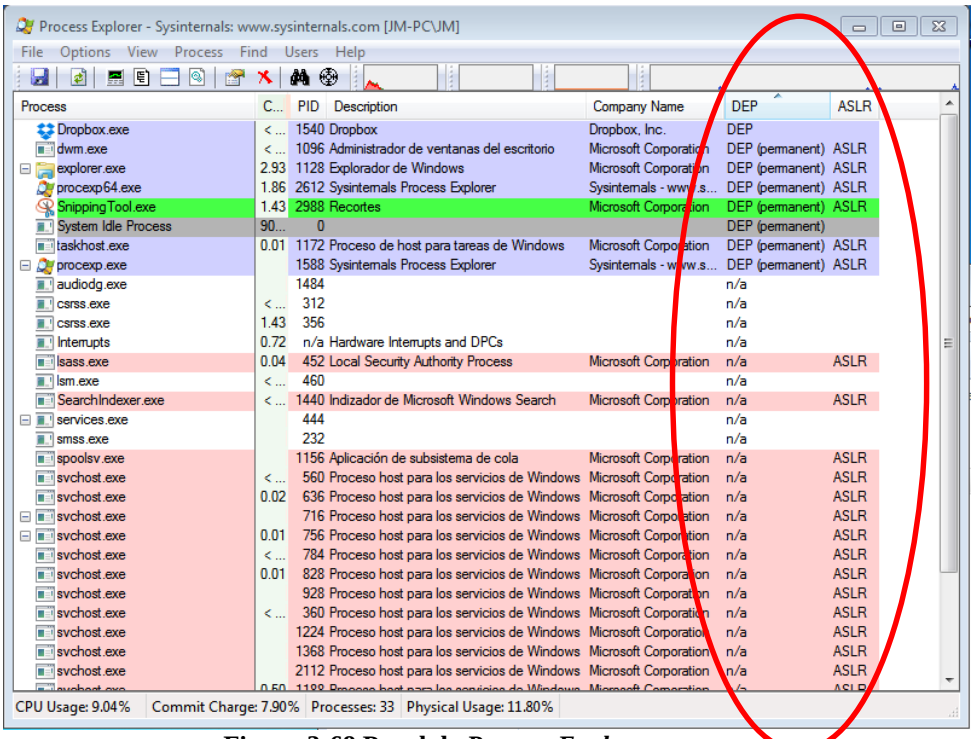

Figura 3-68 Panel de *Process Explorer*

3.2.3.6 EMET

La lucha contra los *exploits* (debilidad o descuido de una programación que un *malware* aprovecha para inyectar código infectado) es esencial y se debe invertir en ella como medida de seguridad para la lucha contra *malware* a día de hoy.

Un *exploit* necesita que la zona de memoria destinada a las variables de un programa sea ejecutable, para introducir en ella su código malicioso. Por ello, este programa EMET [25] es idóneo, pues combina la separación de zona de código ejecutable y no ejecutable (DEP) con la aleatoriedad de la memoria (ASLR).

Se trata de un complemento a mayores de las dos medidas anteriormente comentadas: ASLR y DEP. Sirve para forzar el uso de ambas medidas en todos los procesos y programas. Pero no termina ahí su función, ya que además implementa una serie de acciones encaminadas a prevenir las técnicas actualmente conocidas y comunes de evasión de DEP y ASLR por parte de los atacantes.

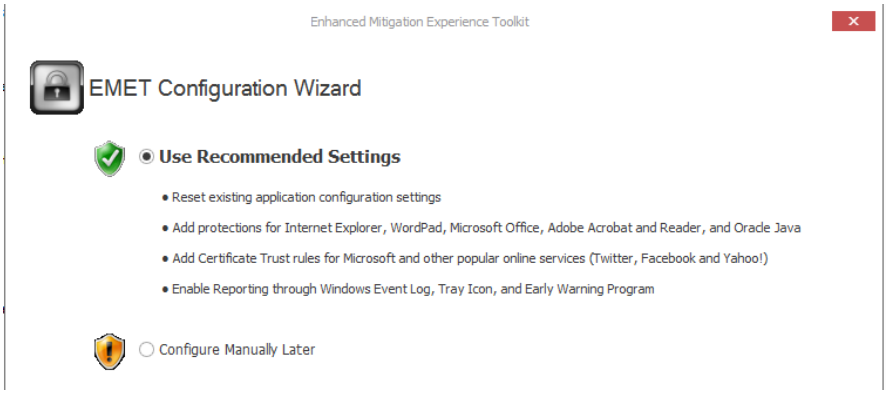

Figura 3-69 Configuración de instalación de EMET

Una vez en la interfaz (Figura 3-70) de la herramienta, debemos activar las medidas de seguridad que aparecen: DEP, ASLR, SEHOP (*Structure Exception Handler Overwrite Protection)*, etc. En la parte inferior, podemos comprobar los procesos y sus estados, así como añadir aplicaciones que pasarán a estar protegidas (lo contemplen o no) por estas medidas.

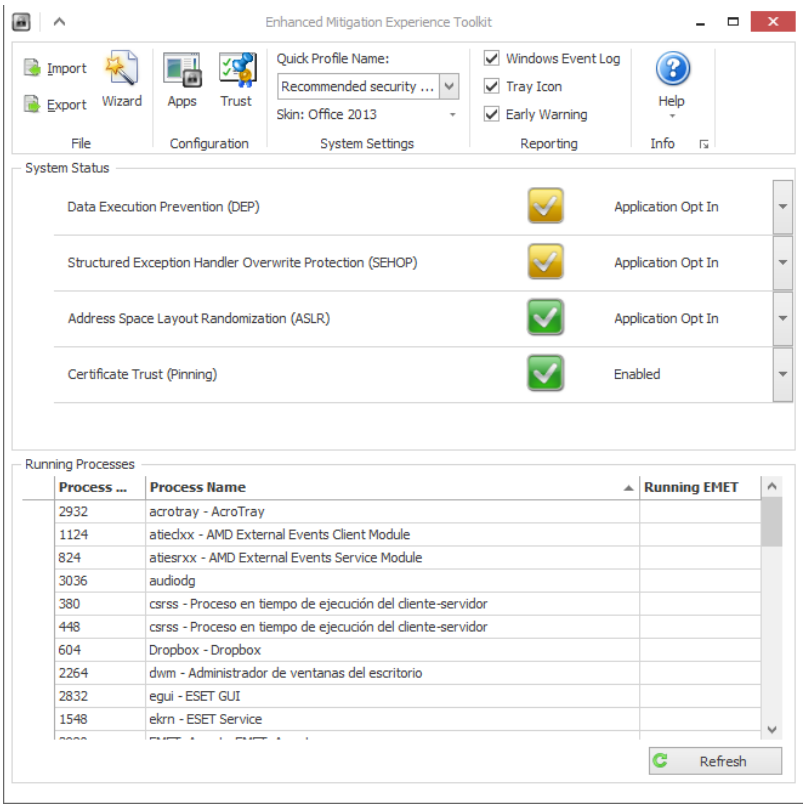

Figura 3-70 Interfaz de EMET

Si lo deseamos, o comprobamos que alguna aplicación tiene conflictos con aplicarle EMET, podemos desactivarle cualquiera de las protecciones (se recomienda comprobar una a una antes de eliminarla de la protección total del EMET).

En cuanto a qué software debemos proteger con EMET, debería ser todo aquel que esté orientado a Internet (navegadores y *plugins*), los que se sepa que suelen ser objeto de ataques, y los que pertenezcan a terceros o que con frecuencia abran archivos arbitrarios descargados de la Web (lectores de PDF, Office, multimedia…).

3.2.4 Seguridad de los datos

La seguridad de los datos supone el último de los bastiones dentro del concepto de seguridad en profundidad por capas. Se centra específicamente en el cifrado de la información que un atacante pretende sustraer, convirtiéndose ésta en inútil para él. Estudiaremos el cifrado con contraseñas, cifrado EFS en profundidad y hablaremos de la figura del agente recuperador.

3.2.4.1 Proteger documentos

Los documentos *Word, Excel y Power Point* permiten añadirles una serie de medidas de seguridad como habilitar la opción de sólo lectura, añadirle una firma digital y cifrado con contraseña, entre otros, como observamos en la Figura 3-71.

Figura 3-71 Seguridad de Word

Si poseemos un programa para comprimir archivos, como los de tipo RAR (para archivos ZIP consistiría en el mismo proceso), podemos añadirle al archivo comprimido una contraseña para evitar que sea accedido por parte de alguien no autorizado (Figura 3-72).

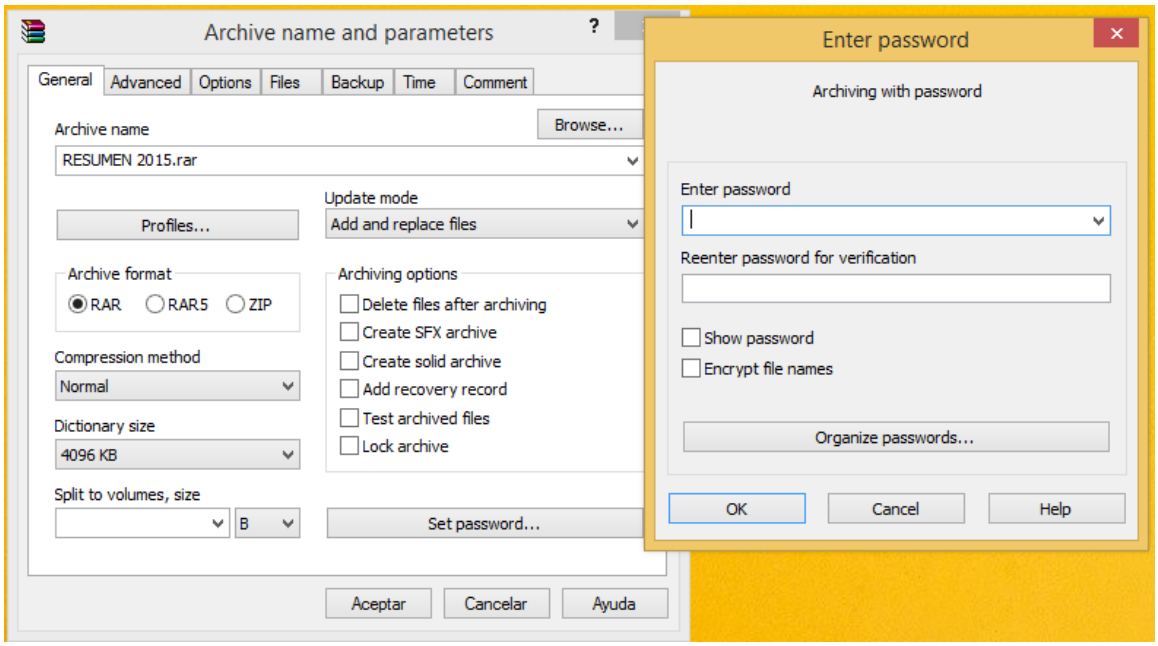

Figura 3-72 Estableciendo contraseña a un archivo RAR

3.2.4.2 Cifrado EFS

Se trata de la forma nativa de cifrado de datos de Microsoft para NTFS y trabaja con una combinación de criptografía simétrica y asimétrica (utiliza cifrados y claves), permitiendo a cada usuario proteger sus propios archivos, independientemente de sus permisos.

Debemos explicar que los grandes volúmenes no se suelen cifrar con criptografía asimétrica, ya que sería computacionalmente costoso. En su lugar, se cifran primero los datos con un método simétrico y, posteriormente, se le aplica una contraseña. Esta contraseña es cifrada a su vez con la clave pública del usuario, para evitar tener que memorizar la contraseña. Por último, esa clave pública se valida por un certificado.

Como hemos comentado, EFS crea certificados digitales para cifrar y descifrar con claves públicas y privadas, y utiliza claves simétricas para agilizar el proceso. Por cada fichero se usa una única clave para cifrar y descifrar. En la Figura 3-73 podemos ver un esquema que ejemplifica el funcionamiento básico de EFS.

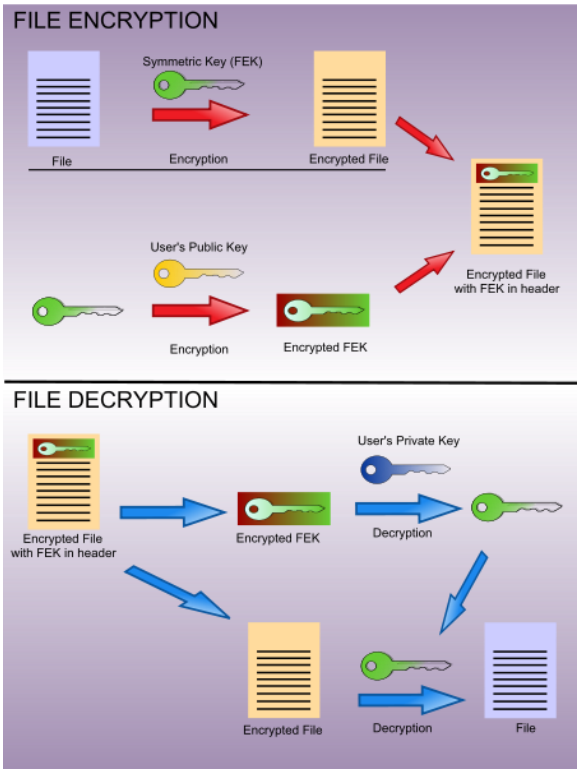

Figura 3-73 Funcionamiento básico de EFS

Esta clave (FEK o *File Encryption Key)* se almacena con el fichero cifrado y se encripta, a su vez, con la clave pública del usuario (estas claves públicas y privadas, junto con los certificados del usuario, se generan de manera automática y transparente la primera vez que ciframos un archivo).

Pinchando con el botón derecho del ratón > Avanzados, podemos acceder al menú y seleccionar un archivo o carpeta que queramos que se cifre, o una carpeta que sea directorio para almacenar archivos cifrados. Importante citar que los archivos que ya estuvieran dentro de una carpeta definida de este modo no se cifrarían automáticamente (Figura 3-74).

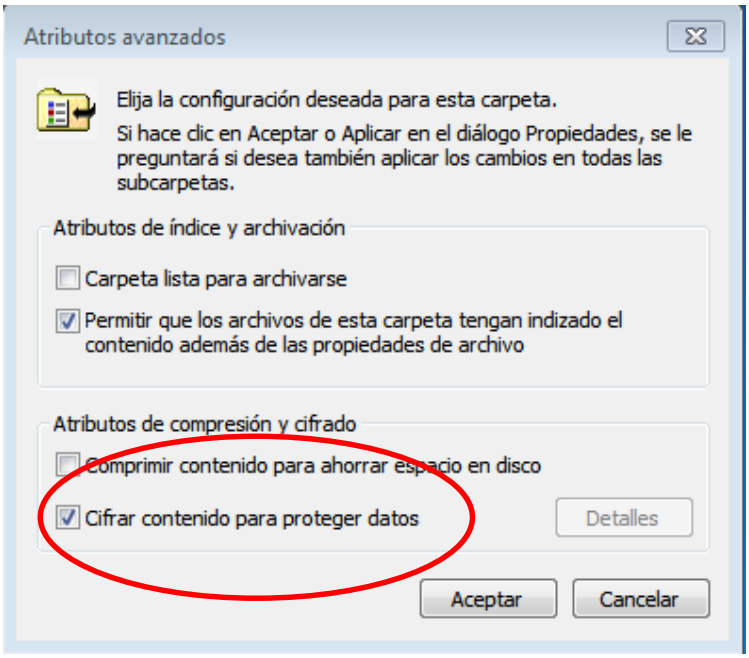

Figura 3-74 Opciones de cifrado EFS

Una vez realizado este cambio, el usuario tendrá disponibles los archivos para manipularlos cuando acceda con su contraseña. Cualquier otro que inicie sesión o explore el disco con otro sistema operativo arrancado desde un dispositivo removible, verá los datos como ilegibles o inaccesibles, asegurando así la inaccesibilidad de los mismos por terceros.

Debemos entender que los certificados que se generan utilizan el SID del usuario, por lo que son únicos por máquina. Si se corrompe el equipo o se borra el usuario, no se podrá recuperar el contenido cifrado (independientemente de que creemos un usuario con el mismo nombre). La solución es crear copias de seguridad de los archivos PFX (*Personal Information Exchange).*

Para realizar una copia de seguridad general del certificado de usuario con la clave privada (que servirá para recuperar cualquier archivo cifrado con EFS), seguiremos los siguientes pasos:

certmgr.msc > Personal > Certificados > Botón derecho > Todas las tareas > Exportar > Elegir con clave privada.

Se creará un fichero PFX que contendrá el certificado con la clave pública y privada, capaces de descifrar todas las FEK que posee cada archivo cifrado (Figura 3-75).

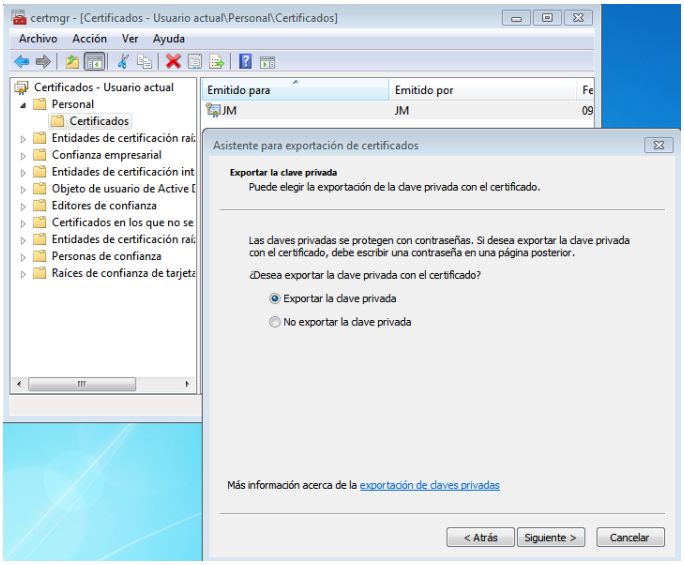

Figura 3-75 Creando una capa de seguridad de certificados con clave privada

A la hora de importarlo, se nos da la opción de añadir una medida más de seguridad denominada *Habilitar protección segura de clave privada*. Esto hará que se nos avise y se pida una contraseña cada vez que una aplicación utiliza la clave privada. Pero existe un inconveniente: no se podrá volver a exportar el PFX.

Si nos encontráramos en la situación de querer exportar el nuevo PFX, debemos generar nuevos certificados y volver a cifrar todo con los nuevos, y podremos proceder a exportar de nuevo y realizar copias de seguridad.

3.2.4.3 Agente de recuperación

En el caso de que queramos aplicar cifrados EFS en un entorno empresarial, necesitamos una figura que pueda recuperar cualquier dato cifrado. Esto será necesario para no tener que depender de que todos los usuarios realicen copias de seguridad de sus certificados, y por si un empleado borra su usuario por accidente o deja un puesto de trabajo con información cifrada.

Windows, una vez se cree este *Agente recuperador*, que pertenecerá al grupo de administradores, cifrará todo archivo, además de con el certificado del usuario que está cifrando, con el certificado del *Agente recuperador*.

Para crearlo, escribiremos *Cipher /R:CertificadoAgenteRecuperacion* en la consola de Windows a la que se accede desde la barra de búsqueda. Escribiremos la contraseña que elijamos y se crearán dos archivos: uno con extensión .CER (público y sin clave privada) y otro con extensión .PFX, como vemos en la Figura 3-76.

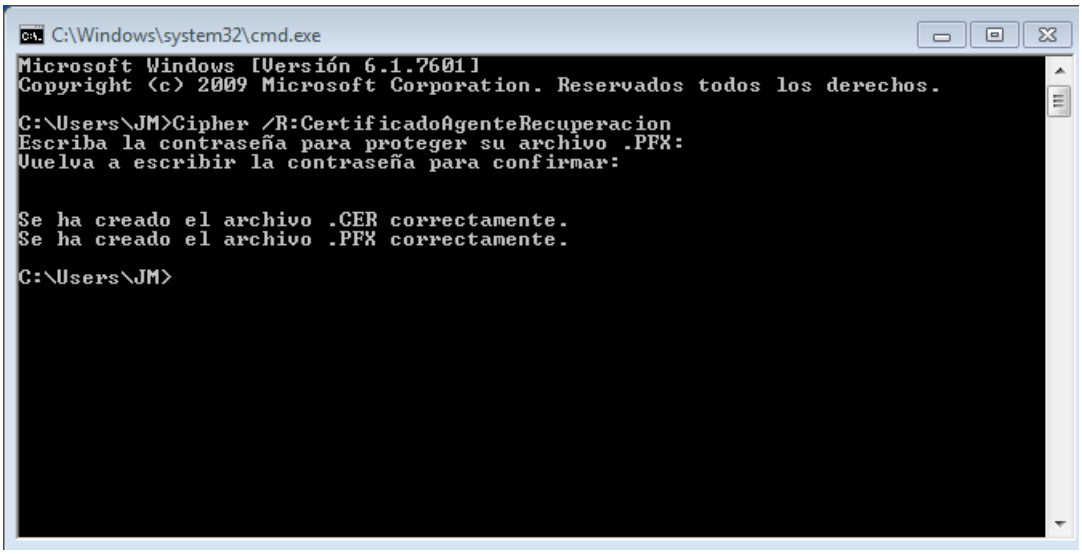

Figura 3-76 Creación del certificado del Agente de Recuperación

El archivo .CER se utilizará para cifrar todas las claves que se utilicen para encriptar los archivos con este certificado. Importante tener en cuenta que esta medida se aplica a los archivos cifrados después de la creación del Agente.

Ahora debemos actualizar los datos de cifrado con el comando *Cipher /U* y posteriormente importar el certificado y definirlo en el sistema como *Agente de recuperación*.

Para ello, acudimos a *secpol.msc* > Directivas de clave pública > Sistema de cifrado de archivos (EFS) > Botón derecho > Agregar agente de recuperación > Elegimos el generado con *Cipher /R* (Figura 3-77).

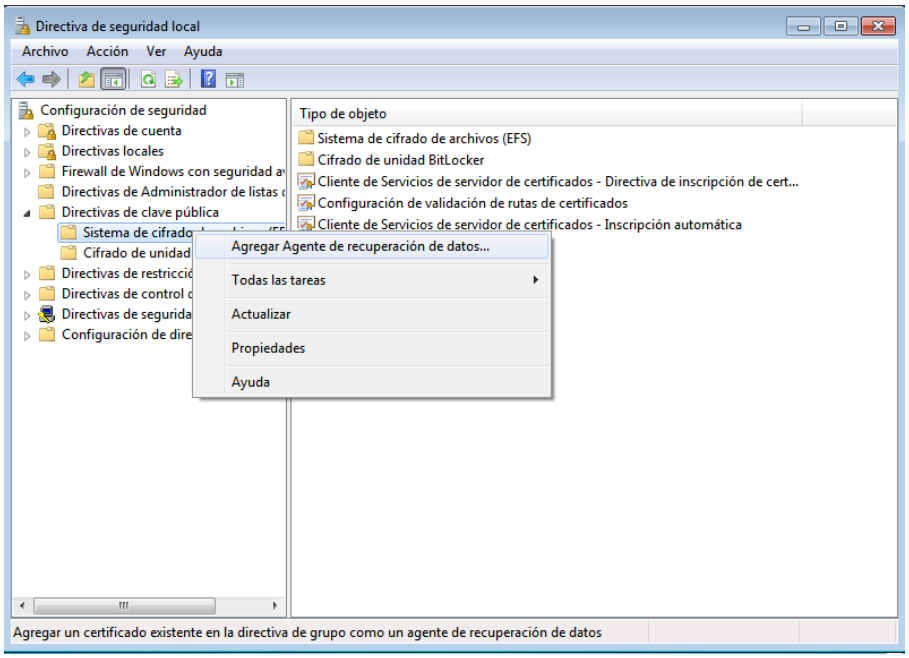

Figura 3-77 Agregando Agente de Recuperación al sistema de cifrado

Para realizar la recuperación de archivos cifrados, se deberá importar en otro equipo el fichero .PFX generado y, desde ahí, descifrar los archivos.

Como último apunte, es conveniente recordar que la clave del usuario es la que permite descifrar el certificado que, a su vez, se utiliza para descifrar la contraseña de cada archivo. Por esta razón, debemos tomar medidas como proteger el usuario con una contraseña robusta, aplicar medidas de seguridad de contraseñas comentadas anteriormente, bloquear la sesión cuando se deja el equipo, etc.

3.2.4.4 Ocultar unidades disco

La seguridad no trata sólo de cifrar, sino también de ocultar. Esta medida sencilla podría evitar que ciertos volúmenes del disco se mostrasen a los demás.

En caso de que no deseemos que aparezca una unidad de disco, podemos ocultarla a la vista accediendo a *gpedit.msc* > Configuración Usuario > Plantillas Administrativas > Componentes de Windows > Explorador de Windows > Ocultar estas unidades especificadas de mi PC (Figura 3-78).

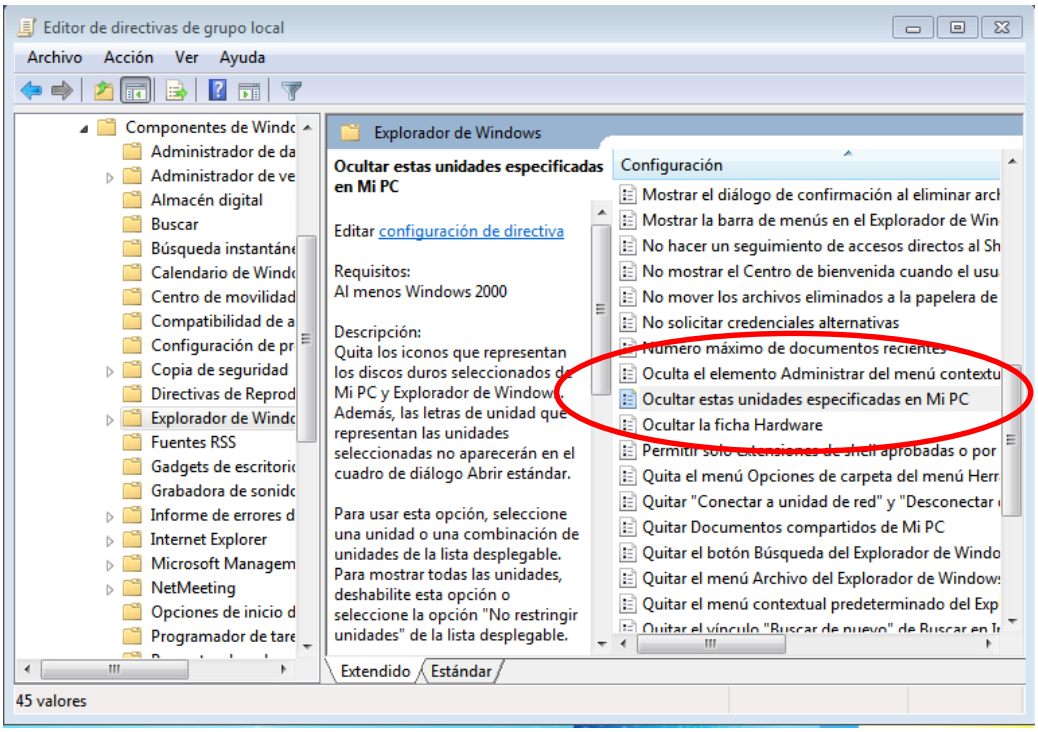

Figura 3-78 Ocultar unidades de disco

3.2.5 Seguridad en dispositivos removibles

La cantidad de información que manejamos y traspasamos, hace, en ocasiones, necesaria la utilización de dispositivos de memoria extraíbles. En ellos, por un lado, podemos tener información sensible que debemos proteger si el dispositivo se extravía, o, por otro lado, pueden transmitirnos un *malware* que se ejecuta en el sistema y lo infecta en cuanto lo conectamos al equipo. Por ello, debemos aplicar una serie de medidas de seguridad que reduzcan la probabilidad de que esto ocurra.

3.2.5.1 Reproducción automática

Es sabido que la gran mayoría de infecciones que ocurren al insertar un disco extraíble o memoria USB se deben a que el usuario utiliza la reproducción automática que aparece al reconocer el sistema un dispositivo removible.

Esta acción sigue las instrucciones de un archivo *Autorun.inf*, que es el utilizado por el *malware* de un atacante para propagarse por el equipo. Para desactivar esa opción, y seleccionar a qué unidades se le aplica el cambio, realizaremos lo siguiente:

Configuración Equipo > Plantillas Administrativas > Componentes Windows > Directivas de reproducción automática > Desactivar Reproducción Automática (Figura 3-79).

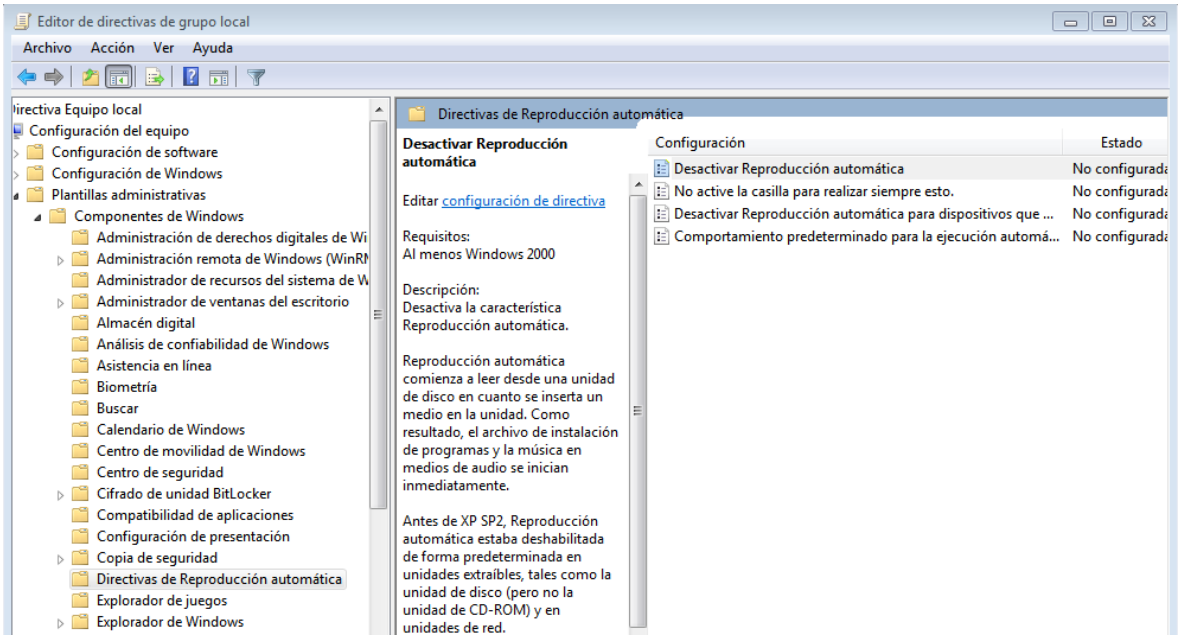

Figura 3-79 Inhabilitar la reproducción automática en dispositivos removibles

Tras deshabilitar esta opción, es recomendable siempre analizar en búsqueda de virus antes de acceder al contenido del dispositivo.

3.2.5.2 Cifrado de datos

En el caso de tener que transportar información clasificada o sensible en dispositivos removibles, es conveniente cifrarla para que, en caso de perder el disco de memoria o que sea objeto de robo, la información está protegida.

En caso de disponer de Windows 7 *Ultimate* o *Enterprise*, podemos optar por cifrar los USBs con *BitLocker To Go* [26] [27].

3.2.6 Borrado y recuperación

Las amenazas a la seguridad no siempre vienen del exterior, a veces, las creamos nosotros mismos con el uso incorrecto del equipo o con ciertas acciones erróneas. Borrar un archivo por completo (y no lo que creemos que es borrar cuando vaciamos la papelera de reciclaje) y evitar que permanezca en la memoria del equipo o recuperar un archivo importante que eliminamos por accidente, son medidas necesarias para mantener seguro nuestro PC.

3.2.6.1 Borrado

Cuando creemos estar borrando un fichero, realmente no es así, simplemente el S.O. no lo muestra más. Aun así, la información que éste contiene todavía se encuentra repartida por el disco duro y no se borrará completamente hasta que ese espacio sea sobrescrito por otra información. Esa información podría ser recuperada por un atacante y utilizada para obtener datos sensibles personales o profesionales.

Como herramienta para borrar realmente un archivo, reemplazando los bytes de memoria que ocupa el fichero por otros valores, tenemos *SDelete* [28], que afirma no ser posible recuperar lo ya borrado.

Como buena práctica, tenemos que borrar de manera regular el espacio libre del disco duro, esperando a ser reutilizado, ya que podría contener información sensible que puede ser recuperada. Para ello, utilizamos la opción "-c" del *SDelete* (Figura 3-80) o el comando *cipher /w: c:*\.

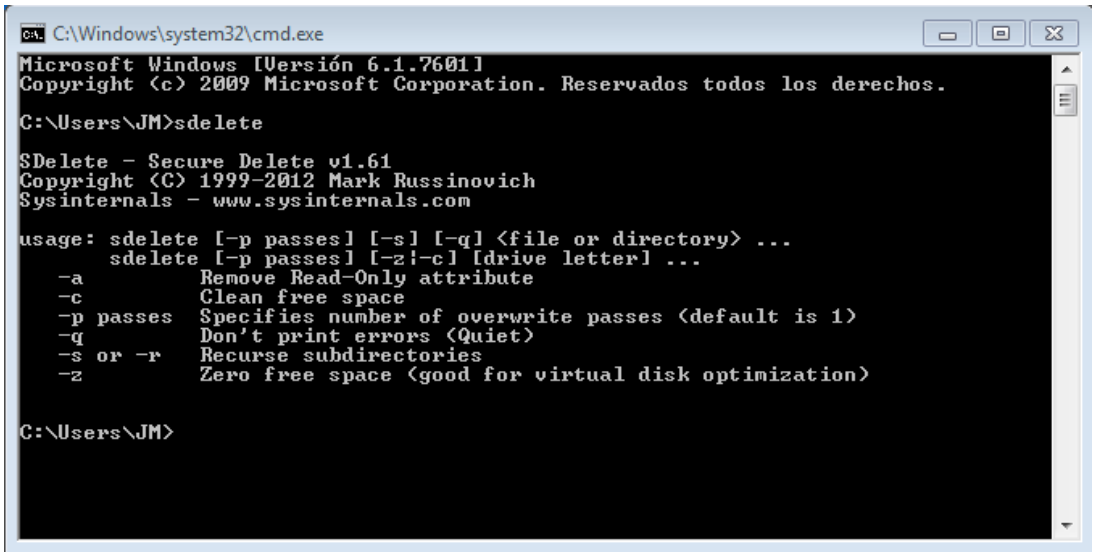

Figura 3-80 Opciones de ejecución de *SDelete*

3.2.6.2 Recuperación

En caso de querer recuperar información borrada por accidente, podemos acudir al programa *Recuva* [29] (Figura 3-81) que posee una interfaz sencilla que nos permite ver los archivos borrados recientemente y elegir recuperarlos.

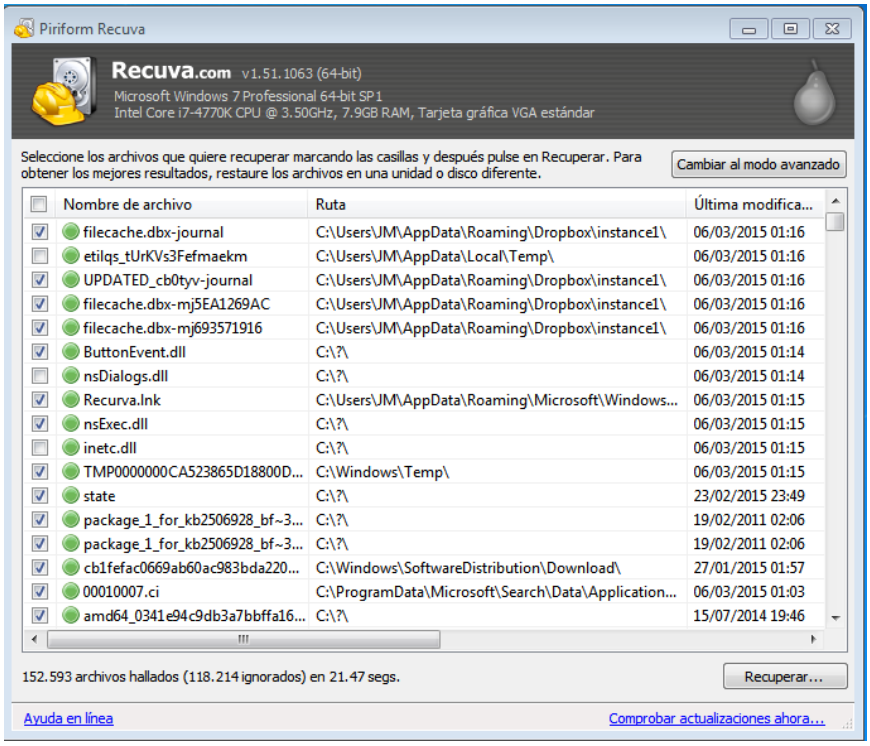

Figura 3-81 Interfaz de *Recuva*

En la Figura 3-82 vemos que nos ofrece una serie de opciones útiles como ordenar los archivos por naturaleza, elegir las áreas donde buscar, opción *escaneo profundo* para no obviar ningún archivo, etc., a la hora de recuperar datos perdidos.

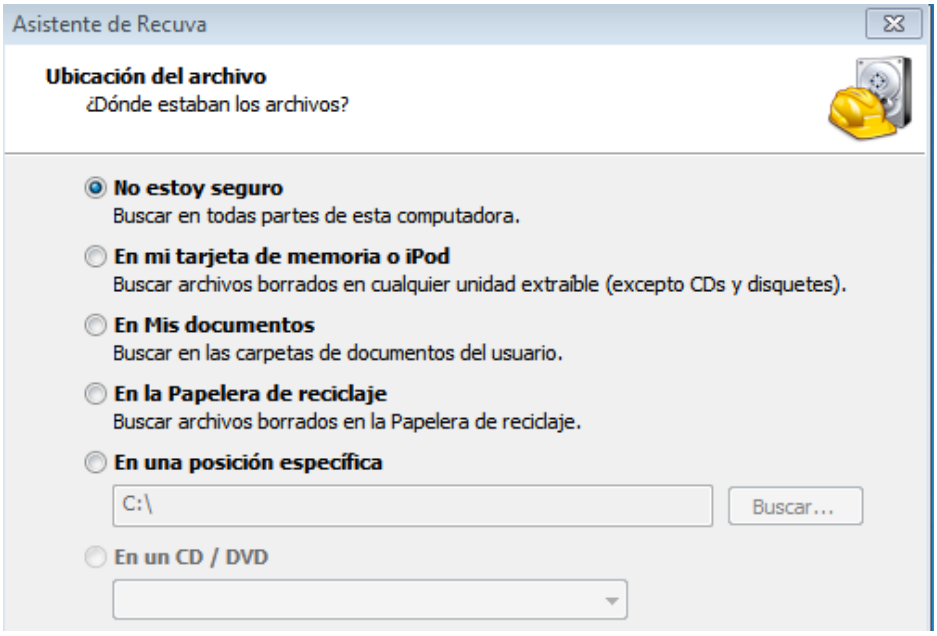

Figura 3-82 Asistente de *Recuva*

4 RESULTADOS

4.1 Descripción del contenido

En este capítulo procedemos a presentar e interpretar los resultados obtenidos tras todas las pruebas anteriores realizadas. Para facilitar la lectura y aplicación de todas las medidas descritas en el apartado anterior, optamos por presentar la Tabla 4-1 que recoge y refleja, por niveles y capas, todas las recomendaciones y cambios necesarios para dar seguridad a nuestro equipo.

Las medidas en sí estarán dotadas de un color que indique su grado de importancia a la hora de aplicarlas con el objetivo de aumentar en mayor o menor medida la seguridad del ordenador.

El código de colores será:

- Rojo: Gran impacto en el nivel de seguridad.
- Amarillo: Impacto medio en el grado de seguridad.

4.2 Tabla con medidas a aplicar

Nivel de aplicación	Medida de seguridad	Finalidad de la medida o medio para aplicarla
Seguridad física	Crear una contraseña de la BIOS	Contraseña para arrancar el sistema
	Establecer un orden de arranque del sistema	Evitar cualquier arranque que no sea desde el S.O.
	Desactivar opciones inseguras en BIOS	*Wake on Lan*, *Password Bypass*, micrófono, cámara, módem, etc.
	Activar TPM en BIOS	Seguridad de *hardware*
	Aplicar contraseña a HD	El usuario no debe suspender ni hibernar el equipo
	Herramienta Bitlocker (*Enterprise o Ultimate)*	Cifrar disco duro con contraseña
	Activar DEP en BIOS	Evitar ejecución de código de *sólo lectura*

Seguridad del S.O.	Parchear *offline*	Drivers de fábrica junto con *WSUS Offline*	
		Aplicación MBSA	Verificar falta de actualizaciones del sistema
	Mantener S.O. Actualizado	*Windows Update* de Panel de Control	
	Inicio de sesión	Activar *requerir Ctrl+Alt+Supr*	Evitar ataque con GINA
	Malware de arranque	Aplicar a ciertos registros sensibles el modo *sólo lectura*	Registro *Run*
			Registro *Winlogon*
		Comprobar ausencia de ejecutables tipo *troyano.exe* tras *userinit*	
		Herramienta *WinLockLess*	Negar creación o modificación de subramas
	Desactivar teclas especiales	Evitamos ataques a través de su activación	
	Programa *MSConfig*	Control de servicios y aplicaciones de terceros y usuarios	
	Usuarios	Utilizar cuentas separadas para administrar y para uso normal	Evitar que un atacante tenga permisos de administrador
		No crear usuarios locales sino de dominio	Controlamos credenciales de manera más segura
		Comprobar que el UAC está activado	Hace uso responsable de permisos
		Modificar el UAC para que aplique el modo *Notificarme siempre*	Más restrictivo por el hecho de informarnos en cada uno de los cambios que realicen
		Cambios en las *plantillas de seguridad*	Activar el *Modo aprobación del administrador*
			Activar *Detectar instalaciones de aplicaciones y pedir confirmación de elevación*

Seguridad del S.O.	Usuarios	Cambios en las *plantillas de seguridad*	Activar *Obligar al usuario a introducir sus credenciales en el escritorio seguro*
		Cambios en *Directivas seguridad local*	Activar *Cambiar a escritorio seguro cuando se pida confirmación de elevación*
			Desactivar *Permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro*
		Deshabilitar *Enumerar las cuentas de administrador al realizar una elevación*	
		Habilitar *Requerir ruta de acceso de confianza para la entrada de credenciales*	
		Impedir modificación del *Panel de Control*	Evitamos cambios no deseados por usuarios/atacantes
		Deshabilitar la posibilidad de *compartir archivos* entre usuarios	
	Desactivar el *uso compartido de escritorio remoto*	Impedimos alteración del sistema a distancia	
	Mostrar archivos ocultos y extensiones de archivos	Comprobamos la existencia de archivos y la concordancia entre ellos y sus extensiones	
	Contraseñas	Evitar que los usuarios puedan *depurar programas*	Impedimos un volcado de *hashes*
		Utilizar más de 14 caracteres	Activamos exclusivamente NTLM
		Obligar a *Solicitar Contraseña tras hibernar o suspender el equipo*	Evitamos que se salte la contraseña un usuario que pretenda acceder, tras salir de la hibernación o suspensión
		No dejar la contraseña vacía	

Seguridad del S.O.	Contraseñas	Cambiar la que viene por defecto	Ya que son conocidas
		No utilizar *recordatorio de contraseña*	Disminuye la posibilidad de adivinar la contraseña
		No usar datos relacionados con la vida personal	Son fácilmente identificables
		Mezclar letras, números y símbolos	Aumentan dificultad y evitan ataques de diccionario
		No repetir caracteres	Disminuye la posibilidad de adivinar la contraseña
		No mantener patrón invariable	Disminuye la posibilidad de adivinar la contraseña
		No establecer una contraseña influenciada por la disposición de las teclas en el teclado	Disminuye la posibilidad de adivinar la contraseña
		Actualizar de manera regular las contraseñas	Disminuye la posibilidad de adivinar la contraseña
	Herramienta *Syskey*	Cifrado de contraseñas ya cifradas y añade *System Key*	
	Permisos y usuarios	Cambiar nombre de la cuenta de administrador y aplicarle una contraseña fuerte	Dificulta su identificación e intrusión
		Desactivar cuenta invitado	Cierra puertas de acceso a atacantes
		Gestionar un grupo de usuarios normales y otro de administradores	Reducimos probabilidad de que un *malware* tome posesión de la cuenta con privilegios
		Aplicación *MMC*	Gestión de usuarios y grupos
		Omitir comprobación de recorrido	Evitamos accesos a carpetas restringidas

Seguridad del S.O.	Permisos y usuarios	Eliminar ciertos permisos de usuarios	*Control total*
			Cambiar permisos
			Atravesar carpeta y ejecutar archivo
			Tomar posesión
		Modificar auditorías de seguridad en *Directivas de seguridad local*	*Apagar sistema de inmediato si no se pueden registrar las auditorías de seguridad*
			No permitir enumeraciones anónimas de cuentas y recursos compartidos SAM
			No permitir enumeraciones anónimas de cuentas SAM
			Permitir traducción SID – nombre anónimo
			Restringir acceso anónimo a canalizaciones con nombre y recursos compartidos
			No permitir almacenamiento de contraseñas y credenciales para la autenticación de la red
			Forzar protección con contraseñas seguras para claves de usuario almacenadas en el equipo
			Impedir *Instalación de controladores de impresora*
			Restringir *Cargar y descargar controladores de dispositivo*

Seguridad del S.O.	Permisos y usuarios	Modificar auditorías de seguridad en *Directivas de seguridad local*	Desactivar *Mostrar el último nombre usuario* o *Mostrar información del usuario cuando bloquee la sesión*
	Cortafuegos	Crear Reglas de entrada	Restringir puertos de acceso al ordenador
		Reglas salida	Restringir puertos de salida al ordenador
		Herramienta *FWRulez*	Facilita la creación de reglas de E/S
	Servicios	Controlar los que se ejecutan sin necesidad de usuario	
Seguridad del software	Firma criptográfica GPG	Aplicación *GnuPG*	Comprobar concordancia firmas
		Servidor *MIT*	Comprobar reputación de un usuario
		Comprobar veracidad a través de certificados	Rutas de certificación
		Actualizar certificados	Programa *MMC*
	Búsqueda infecciones	Herramienta *Microsoft Removal tool*	Eliminación *malware*
		Web *Virustotal*	Análisis archivo en búsqueda de *malware*
	Activación de DEP	A través de Windows	
		Comando *bcdedit*	
	Activación ASLR para randomizar el uso de memoria	Programa *Setdllcharacteristics*	
		Herramienta *Processexplorer*	
	Aplicación EMET	Combinación DEP, ASLR y SEHOP	
Seguridad de los datos	Cifrar documentos de diversos tipos para evitar su lectura o modificación	*Word, Excel, Power Point y RAR*	
	Cifrado EFS	Cifrado con claves públicas y privadas para añadir autenticación y veracidad	
		Crear copias de seguridad de las claves	

Seguridad de los datos	Cifrado EFS	Aumentar seguridad mediante la *Protección segura de clave privada*
	Creación *Agente recuperador*	Figura que permite reparar daños causados por cifrado incorrecto
	Ocultar unidades de disco	No mostrar ciertos volúmenes del sistema
Seguridad dispositivos removibles	Evitar reproducción automática	Evitamos la creación del archivo *autorun.inf* utilizado por el *malware*
	Cifrado Bitlocker To Go (*Ultimate o Enterprise)*	Cifrado de información contenida en dispositivo removible
Borrado y recuperación	Herramienta *Sdelete*	Borrado completo de datos
	Herramienta *Recuva*	Recuperación de información o archivos borrados

Tabla 4-1 Resumen de las medidas de seguridad a aplicar desarrolladas en el capítulo tres

Con este resumen, podemos, de manera rápida y esquemática, evaluar los distintos niveles en los que debemos aplicar seguridad y comprobar, una a una, todas las medidas desarrolladas en el tercer capítulo.

Podemos deducir cierta información de la tabla, como que el grueso de las medidas de seguridad se centran en la seguridad del S.O. o que medidas del tipo DEP o cifrado de datos son repetidas en diversas capas y son claves a la hora de conseguir un buen nivel de seguridad en nuestros equipos.

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones

Los objetivos propuestos al inicio del TFG consistían en elaborar, para alguien no experto en la materia, una guía de buenas prácticas que aglutinara una serie de recomendaciones, con el fin de definir un esquema de configuración segura para un equipo con sistema operativo Windows. Además de desarrollar dicha guía, se ha indicado paso a paso cómo aplicar las medidas citadas apoyándonos en capturas para facilitar su comprensión. Por tanto, el contenido de los capítulos tres y cuatro conforman la documentación que se pretendía generar al inicio de este TFG. De esta manera, se puede considerar haber cumplido todos los objetivos propuestos al comenzar el proyecto.

Una vez realizado el presente proyecto, junto con la investigación que ha conllevado, hemos adquirido una mayor conciencia en lo que respecta a la seguridad de nuestra información. Se han dado a conocer ataques e infecciones de *malware* que son más frecuentes de lo que pensábamos, y las medidas que tenemos a nuestro alcance para prevenirlos o combatirlos.

En lo que respecta a los experimentos llevados a cabo, debido al modelo de la BIOS instalada en el equipo de las pruebas, ciertas medidas citadas no podían ser aplicadas. Aun así se ha explicado cómo se debería proceder en caso de tener la posibilidad de llevarlas a cabo. Son las siguientes:

- Contraseña HD a través de la BIOS.
- Activar el modo *anti theft* en la BIOS.
- Desactivar la posibilidad de que se ejecute el *password bypass* en la BIOS.
- Impedir el uso de contraseñas *backdoor* de la BIOS.

A mayores, debido a no poseer una versión de Windows 7 avanzada (*Ultimate o Enterprise)*, no pudimos instalar ni utilizar *Bitlocker* ni *Bitlocker To Go* para añadir seguridad a nuestro sistema. Aun así, se explica, de manera general, qué ventajas ofrece y cómo utilizarlos.

Por último, todas las pruebas pudieron realizarse tanto en el equipo como en la máquina virtual a excepción de las siguientes que, por razones de incompatibilidad o falta de parte *hardware* de *Virtualbox*, no pudieron llevarse a cabo en ésta:

- Medidas relacionadas con la BIOS.
- Ejecución del comando *bcdedit* para comprobar la activación del DEP (*nx*).
- La instalación del EMET.

Tras finalizar el presente trabajo, podemos afirmar haber tratado de manera clara y metódica, para un usuario de nivel medio, las diversas áreas del equipo en las que podemos incrementar la seguridad

para evitar ataques, infecciones, robos de información, etc. Además, se han incluido herramientas, aplicaciones y programas de ayuda para la prevención y/o recuperación de ataques, junto con imágenes y capturas de pantalla que asisten a comprender cómo utilizarlas.

5.2 Líneas futuras

Se presentan, a continuación, unas tareas para llevar a cabo en un futuro y profundizar en lo ya analizado y descubierto sobre recomendaciones de seguridad de un sistema. Como líneas futuras, se plantean las siguientes:

- **Simulación de ataques frecuentes o infecciones de *malware* al equipo o a la máquina virtual**. Sobre un equipo configurado según las indicaciones de este documento, se podría estudiar cómo simular ataques sobre éste con el fin de comprobar la efectividad de su configuración de seguridad. La consecución de este paso permitiría no sólo profundizar en el conocimiento de cómo funcionan los ataques perpetrados a los equipos, sino también, gracias a ello, saber aplicar de manera más lógica aún cambios en la configuración del ordenador que eviten intrusiones ajenas no deseadas.

- **Análisis de seguridad y riesgos de un equipo con la herramienta *EAR /PILAR*** [30] **del CCN.** Con el fin de analizar el nivel de seguridad adquirido en un equipo, al que se le han aplicado las medidas de seguridad descritas en la memoria, y los riesgos a los que está expuesto, se puede hacer uso de la herramienta *PILAR* del CCN. De esta manera podríamos profundizar en el conocimiento de la seguridad que las medidas nos proporcionan y saber qué áreas están más desprotegidas para concentrarnos en aumentarles la protección.

- **Estudio de recomendaciones que puedan exportarse a otros S.O**. Una vez finalizado el estudio de recomendaciones de seguridad de un S.O. Windows 7, se puede proceder a conocer las similitudes o diferencias que posee con otro S.O. como su sucesor Windows 8 u 8.1 o incluso uno más distinto como es Linux o Mac O.S. De esta manera, podríamos descubrir si la seguridad ha ido *in crescendo* conforme han avanzado los sistemas Windows o si otros S.O. del mercado poseen una mejor estructura segura en sus sistemas, lo que los convertiría en una posible mejor opción para ciertos organismos.

- **Estudio de recomendaciones que puedan exportarse a dispositivos móviles**. Por último, no podemos dejar de lado los dispositivos móviles, los cuales están arrasando con el aumento de su uso por parte de todos. Estas herramientas también se están utilizando, cada vez más, para gestionar información de toda índole, por lo que ser capaces de protegerlos debe convertirse en una prioridad de cualquier usuario que precie el valor de los datos que contienen. Los conceptos fundamentales adquiridos durante el estudio del trabajo nos permiten sentar las bases desde las que comenzar a investigar, estudiar y elaborar medidas de seguridad enfocadas, de manera específica, a los dispositivos móviles.

6 BIBLIOGRAFÍA

[1] «Norma IEC 17799» [En línea]. Available: http://www.shutdown.es/ISO17799.pdf. [Último acceso: 01 04 2015].

[2] «Web de estadísticas StatCounter (gráfico)» [En línea]. Available: http://gs.statcounter.com/#desktop-os-ww-monthly-201201-201501-bar. [Último acceso: 07 02 2015].

[3] «Web de estadísticas StatCounter (mapa)» [En línea]. Available: http://gs.statcounter.com/#desktop-os-ww-monthly-201501-201501-map. [Último acceso: 07 02 2015].

[4] «Normas ISO» [En línea]. Available: http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0025819#.VRwmEPmsWEs. [Último acceso: 01 04 2015].

[5] «PDF ISO-IEC 17799» [En línea]. Available: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf. [Último acceso: 07 02 2015].

[6] «*Riseupnet - Hacklab*» [En línea]. Available: https://we.riseup.net/hacklab_zam+asamblea/seguridad_informatica. [Último acceso: 07 02 2015].

[7] «Microsoft Tech.» [En línea]. Available: https://technet.microsoft.com/es-es/library/dd548337(v=ws.10).aspx. [Último acceso: 07 02 2015].

[8] J. Mieres, «*PDF Buenas prácticas en seguridad informática*» [En línea]. Available: http://www.welivesecurity.com/wp-content/uploads/2014/01/buenas_practicas_seguridad_informatica.pdf. [Último acceso: 07 02 2015].

[9] «PDF Doc. Estrategia Ciberseguridad Nacional» [En línea]. Available: http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf. [Último acceso: 07 02 2015].

[10] «Guías STIC CCN» [En línea]. Available: https://www.ccn.cni.es/index.php?option=com_content&view=article&id=6&Itemid=9.

[Último acceso: 07 02 2015].

[11] S. de los Santos, *Máxima Seguridad en Windows: Secretos Técnicos* (2ª Edición), Móstoles (Madrid): Informática64, 2012.

[12] «*Downloads Oracle VM VirtualBox*» [En línea]. Available: https://www.virtualbox.org/wiki/Downloads. [Último acceso: 26 02 2015].

[13] «Cómo usar *Bitlocker*» [En línea]. Available: http://windows.microsoft.com/es-es/windows7/products/features/bitlocker. [Último acceso: 01 03 2015].

[14] «*WSUS offline*» [En línea]. Available: http://download.wsusoffline.net/. [Último acceso: 01 03 2015].

[15] «MBSA» [En línea]. Available: https://technet.microsoft.com/es-es/security/cc184923.aspx. [Último acceso: 06 03 2015].

[16] «*WinLockLess*» [En línea]. Available: http://unaaldia.hispasec.com/2012/04/hispasec-presenta-winlockless.html. [Último acceso: 05 03 2015].

[17] «Grupos usuarios» [En línea]. Available: http://windows.microsoft.com/es-es/windows/user-groups#1TC=windows-7. [Último acceso: 07 03 2015].

[18] «*FWRulez*» [En línea]. Available: http://www.hispasec.com/#tools-tab. [Último acceso: 05 03 2015].

[19] «*GnuPG*» [En línea]. Available: https://www.gnupg.org/index.html. [Último acceso: 03 03 2015].

[20] «Servido PGP del MIT» [En línea]. Available: http://pgp.mit.edu/. [Último acceso: 03 03 2015].

[21] «*Removal Tool*» [En línea]. Available: http://www.microsoft.com/es-es/download/malicious-software-removal-tool-details.aspx. [Último acceso: 07 03 2015].

[22] «*Virustotal*» [En línea]. Available: https://www.virustotal.com/. [Último acceso: 03 03 2015].

[23] «*Setdll*» [En línea]. Available: http://blog.didierstevens.com/2010/10/17/setdllcharacteristics/. [Último acceso: 05 03 2015].

[24] «*Process explorer*» [En línea]. Available: https://technet.microsoft.com/es-es/sysinternals/bb896653.aspx. [Último acceso: 05 03 2015].

[25] «EMET» [En línea]. Available: http://www.microsoft.com/en-us/download/details.aspx?id=41138. [Último acceso: 05 03 2015].

[26] «*BitLock to go*» [En línea]. Available: http://www.techrepublic.com/blog/windows-and-office/secure-your-usb-drives-with-bitlocker-to-go-for-windows-7/. [Último acceso: 06 03 2015].

[27] «B2G» [En línea]. Available: http://windows.microsoft.com/es-es/windows7/what-is-the-bitlocker-to-go-reader. [Último acceso: 06 03 2015].

[28] «*SDelete*» [En línea]. Available: https://technet.microsoft.com/es-es/sysinternals/bb897443. [Último acceso: 05 03 2015].

[29] «*Recuva*» [En línea]. Available: http://www.piriform.com/recuva. [Último acceso: 05 03

2015].

[30] «Herramienta PILAR» [En línea]. Available: https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=1904:herramientas&catid=102:menus1rnivel&Itemid=172&lang=es. [Último acceso: 07 04 2015].

[31] «DEP» [En línea]. Available: http://www.windowstecnico.com/archive/2010/01/07/aslr-dep-la-lucha-contra-los-exploits.aspx. [Último acceso: 02 03 2015].

[32] «DLL» [En línea]. Available: http://support.microsoft.com/kb/815065/es. [Último acceso: 05 03 2015].

[33] «Dominio» [En línea]. Available: http://windows.microsoft.com/es-es/windows-8/join-domain-workgroup-homegroup. [Último acceso: 02 03 2015].

[34] «MMC» [En línea]. Available: http://windows.microsoft.com/es-es/windows-vista/what-is-the-microsoft-management-console-mmc. [Último acceso: 02 03 2015].

[35] «NTFS Microsoft» [En línea]. Available: http://windows.microsoft.com/es-es/windows-vista/comparing-ntfs-and-fat-file-systems. [Último acceso: 02 03 2015].

[36] «Servicios» [En línea]. Available: https://msdn.microsoft.com/es-es/library/d56de412(v=vs.110).aspx. [Último acceso: 07 03 2015].

[37] «*UAC Microsoft*» [En línea]. Available: http://windows.microsoft.com/es-es/windows/what-are-user-account-control-settings#1TC=windows-7. [Último acceso: 02 03 2015].

ANEXO I: GLOSARIO

- ACL (*Access Control List):* son las listas que definen los permisos que tiene un usuario, grupo o programa sobre un archivo.
- *Anti theft*: Anti robo.
- ASLR: *Address Space Layout Randomization* (aleatoriedad memoria RAM). El ASLR crea una aleatoriedad en la memoria para que, al cargar el sistema operativo, las librerías del sistema, que solo las debería usar el sistema, se posicionen en diferentes lugares de la RAM, haciendo complicado la creación de un *exploit*.
- BIOS: *Basic Input/Output System.*
- CCN: Centro Criptológico Nacional.
- Claves pública y privada: Este método consiste en que un usuario tiene una clave privada que es personal e intransferible y que sólo él conoce y posee. La clave pública, como su nombre indica, está accesible para todo el mundo. Están diseñadas a pares, lo que quiere decir que una complementa a la otra y no pueden funcionar con ningún otro par. Por ello cuando tenemos un archivo que el propietario ha firmado con su clave privada, que sólo él tiene, lo juntamos con la clave pública que podemos conseguir y así podemos comprobar que son correctas. Así podemos cerciorarnos que no es un archivo falso. La clave privada por lo tanto asegura al resto que somos quienes decimos ser (autenticación) mientras que si ciframos algo con nuestra clave pública, sólo nosotros con nuestra clave privada podemos descifrarlo (privacidad).
- DEP: *Data Execution Prevention* o Prevención de Ejecución de Datos. Con DEP se protege la zona de RAM, estableciendo cuando una zona de memoria contiene código ejecutable y cuando solo contiene código para variables. Evita la ejecución de código en áreas de la memoria reservadas para el almacenamiento de datos ya que cuando la memoria se declara como no ejecutable y un programa trata de ejecutar código desde esa memoria, Windows cierra el programa [31].
- DLL: *Dynamic Link Library* es una biblioteca que contiene el código y datos que pueden ser utilizados por más de un programa al mismo tiempo. Cada programa puede utilizar la funcionalidad contenida en este archivo DLL. Esto ayuda a promover la reutilización de código y el uso eficaz de la memoria [32].
- Dominio: Red de ordenadores sin necesidad de usuario local de cada ordenador [33].
- EFS: *Encrypting File System.*
- EMET: *Enhanced Mitigation Experience Toolkit.*
- *Exploit*: Permite aprovecharse de un descuido en la programación de alguna aplicación, permitiendo la inclusión de código malicioso, donde se esperaba la entrada de un dato por parte del usuario. Un *exploit* necesita que la zona de memoria destinada a las variables de un programa sea ejecutable para introducir en ella su código malicioso.
- FEK: *File Encryption Key.*
- *Firewall:* Cortafuegos.
- GINA: *Graphical Identification and Authenticacion* o pantalla de inicio de sesión.
- Hash: Firma almacenada resultante de la aplicación de un algoritmo a una clave de usuario introducida.
- HD: *Hard Drive* o Disco Duro.
- Kernel: Núcleo S.O.
- LM: *Lan Manager.*
- MMC (*Microsoft Management Console*): Hospeda y muestra herramientas administrativas creadas por Microsoft y por otros proveedores de software [34].

- NTFS o *New Technology File System*: Sistema de archivos subyacente en el software, necesario para poder almacenar datos (Versión mejorada del FAT 32 y FAT/FAT16 ya que en seguridad puede utilizar cifrado y permisos y restringir el acceso a archivos específicos) [35].
- NTLM: *NTLan Manager.*
- Perfil: Conjunto de reglas definidas por el usuario que se aplican a una tarjeta de red.
- PFX: *Personal Information Exchange.*
- PGP: *Pretty Good Privacy* o Privacidad Bastante Buena.
- SAM: *Security Account Manager* o administrador de cuentas de seguridad.
- SEHOP: *Structure Exception Handler Overwrite Protection.* Medio a través del cual impedimos que un atacante explote las vulnerabilidades de la SEH y la sobrescriba. Este método es utilizado por, aproximadamente, un 20% de los *exploits*.
- Servicios: permiten crear aplicaciones ejecutables de larga duración, en modo *background.* [36]
- SID: *Security Identifier* o identificador de seguridad de usuario.
- S.O.: Sistema operativo.
- STIC: Seguridad en las Tecnologías de Información y Comunicaciones.
- TPM: *Trusted Platform Module.*
- UAC: *User Account Control* o Control Cuentas Usuario. Notifica cuando los programas pretenden realizar cambios en el equipo que requieren permisos. Existen distintas configuraciones con distintos niveles de seguridad [37].
- WPAD: *Web Proxy Auto-Discover Protocol.*
- WSUS: *Windows Server Update Services.*