ESCUELA DE TECNOLOGÍAS EN REDES Y TELECOMUNICACIONES

DESARROLLAR PRACTICAS DE LABORATORIO PARA LA MATERIA SEGURIDAD EN REDES DE LA CARRERA REDES Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE LAS AMÉRICAS

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Tecnóloga Redes y Telecomunicaciones.

Profesor Guía

ING. MARIO GARZÓN

Autora

SOFÍA CATALINA ANDRADE BONILLA

Año

2015

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

_____

Ing. Mario Garzón

171129660-6

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi (nuestra) autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

SOFÍA CATALINA ANDRADE BONILLA

172446084-3

AGRADECIMIENTOS

A la Universidad de las Américas,
Escuelas de Tecnologías,
Tecnología Redes y Telecomunicaciones,
por ser una entidad forjadora de
profesionales con deseos de servir
a la sociedad con calidad moral y técnica.
A mis padres, hermanos, familiares y amigos
por siempre estar presentes de una
u otra forma apoyándome, dándome su tiempo
y ánimo para seguir cumpliendo
mis metas profesionales.
Al Ing. Mario Garzón G. Tutor de Tesis,
por haber confiado en mi persona,
por su apoyo, por su tiempo,
paciencia y por los conocimientos
brindados desinteresadamente
durante la elaboración de este proyecto.

RESUMEN

El presente proyecto tiene como objetivo diseñar y elaborar once prácticas de laboratorio para los estudiantes que tomen la asignatura “Seguridad en Redes” de la Carrera Redes y Telecomunicaciones.

Estas prácticas se llevaran a cabo con la ayuda profesional del docente asignado por la Universidad de las Américas y también por los equipos proporcionados.

Los resultados se verán reflejados en las evaluaciones tomadas a los estudiantes a través de hojas de laboratorio.

ABSTRACT

This project aims to design and develop eleven practical laboratory for students taking the course "Network Security" Career Networking and Telecommunications.

These practices are carried out with the professional help of teachers assigned by the University of the Americas and also by the equipment provided.

The results will be reflected in the assessments made to students through laboratory sheets.

ÍNDICE

INDICE DE FIGURAS

INDICE DE TABLAS

1. CAPITULO I

LABORATORIO 1 “Auditoría de hardware y software, WinAudit”

1.1. INTRODUCCIÓN

El presente laboratorio 1, se refiere a la recopilación de información de un computador para la seguridad del mismo y del usuario, se lo realizará mediante una auditoría con la herramienta Winaudit.

1.2. DESCRIPCIÓN DE LOS EQUIPOS

- Software free Winaudit
- Computador
- Sistema Operativo Windows

1.3. MATERIALES

- Computador
- Sistema Operativo Windows 7

1.4. OBJETIVO GENERAL

Conocer los elementos que se encuentran instalados en un computador mediante una auditoría con Winaudit.

1.5. OBJETIVOS ESPECÍFICOS

- Realizar un análisis de las características del computador en hardware y software.
- Determinar los materiales en hardware y software necesarios.
- Desarrollar el laboratorio.
- Verificar el correcto funcionamiento del laboratorio N°1.
- Evaluar y aprobar el laboratorio.

1.6. TRABAJO PREPARATORIO

Antes de realizar la práctica, el estudiante tiene que conocer los temas que a continuación se describen:

1.6.1. Winaudit

Winaudit es un programa gratuito, multilenguaje que no precisa instalación, permite realizar un exhaustivo análisis o auditoría a un equipo con sistema Windows, recaba una gran cantidad de información del mismo. (1)

1.6.2. Tipos de Discos Duros

- **Disco Duro SAS**

Se emplea en servidores, pueden conectarse hasta 6 ó 7 metros de distancia, y, ofrecer el servicio hasta 24 computadoras. (2)

- **Disco Duro SCSI**

Es una interface a nivel de sistema que está diseñado para aplicaciones de propósito general, permite que se conecten hasta siete dispositivos a un único controlador. El SCSI-1 tiene un ancho de bus de 8 bits, después se incluyó características muy destacadas como la posibilidad de conectar hasta siete dispositivos de todo tipo como discos, cintas, escaners, etc. (3)

- **Disco Duro IDE, ATA Y PATA**

IDE= Componente Electrónico Integrado

ATA= Tecnología Avanzada de Contacto

PATA= Tecnología Paralela Avanzada

El disco duro tiene 40 conectores, la velocidad de transferencia es de 66, 100,133 Megabyte por segundo, se puede conectar un máximo de 2 dispositivos por conector de bus. (4)

- **Disco Duro SATA 2**

La diferencia con el SATA es que trabaja a 300Megabytes/segundo. (5)

- **Disco Duro de Estado Sólido**

También conocidos como SSD. En este caso no se usan discos giratorios sino matrices de transistores. Cada transistor se encarga de guardar una unidad de información. No existen partes móviles, con lo cual el acceso a la información es más rápido, son más resistentes a golpes, consumen menos, no hacen ruido. El único problema es que son más caros. (6)

1.6.3. Tecnología Hot Swap

Hot Swap se refiere a la posibilidad de cambiar periféricos u otros componentes de un equipo en "caliente", es decir, cuando éste se encuentra encendido y sin necesidad de interrumpir la conexión con el sistema operativo o la aplicación con la que se está trabajando. (7)

1.6.4. Tipos de RAM

- **DRAM:** Dinamic-RAM, o RAM DINAMICA, es la primera generación de memorias ram y por tanto la más lenta. Usada hasta la arquitectura 386, su velocidad típica es de 80 ó 70 nanosegundos (ns), tiempo que utiliza para el intercambio de información. Por esa razón la memoria de 70 ns es más rápida que la de 80 ns. Físicamente, aparece en forma de DIMMs o de SIMMs, siendo estos últimos de 30 contactos. (8)
- **EDO:** EDO-RAM, Extended Data Output-RAM. Evoluciona de la DRAM; permite recibir nuevos datos mientras los anteriores están saliendo, se vuelve una memoria más rápida. Muy común en la arquitectura Pentium MMX y AMD K6, con velocidad de 70, 60 ó 50 ns. Se instala sobre todo en SIMMs de 72 pines, aunque existe en forma de DIMMs de 168 pines. (9)

- **SDRAM:** Sincronic-RAM. Funciona de manera sincronizada con la velocidad de la placa. Se presenta en forma de DIMMs de 168 pines; es utilizada en procesadores Pentium II, de menos de 350 MHz, y Celeron. (10)
- **DDR2:** DDR-2 proviene de ("Dual Data Rate 2"), lo que traducido significa transmisión doble de datos segunda generación (este nombre es debido a que incorpora dos canales para enviar y además recibir los datos de manera simultánea): son un tipo de memorias DRAM (RAM de celdas construidas a base de capacitores), las cuales tienen los chips de memoria en ambos lados de la tarjeta y cuentan con un conector especial de 240 terminales para ranuras de la tarjeta principal (Motherboard). También se les denomina DIMM tipo DDR2, debido a que cuentan con conectores físicamente independientes por ambas caras como el primer estándar DIMM.(71)
- **DDR3:** DDR-3 proviene de ("Dual Data Rate 3"), lo que traducido significa transmisión doble de datos tercer generación: son el mas moderno estándar, un tipo de memorias DRAM (RAM de celdas construidas a base de capacitores), las cuales tienen los chips de memoria en ambos lados de la tarjeta y cuentan con un conector especial de 240 terminales para ranuras de la tarjeta principal (Motherboard). También se les denomina DIMM tipo DDR3, debido a que cuentan con conectores físicamente independientes por ambas caras como el primer estándar DIMM. Este tipo de memoria cuenta en su gran mayoría de modelos con disipadores de calor, debido a que se sobrecalientan. (72)
- **PC100:** o SDRAM de 100 MHz. Evoluciona de SDRAM para procesadores de Pentium II, de más de 350 MHz. (11)

1.6.5. Puerto USB

Es un puerto que sirve para conectar periféricos a una computadora. Fue creado en 1996 por siete empresas: IBM, Intel, Northern Telecom, Compaq,

Microsoft, Digital Equipment Corporation y NEC; de esta manera se fue dejando atrás los antiguos puertos paralelo y serial aumentando la velocidad de trabajo de los dispositivos a 12 mbps en promedio hasta 480mbps en la actualidad. Los equipos de Windows se adaptaron rápidamente a esta nueva tecnología, a lo que más tarde se sumaron los aparatos Macintosh. (12)

1.7. MODO DE TRABAJO

- Abrir Winaudit

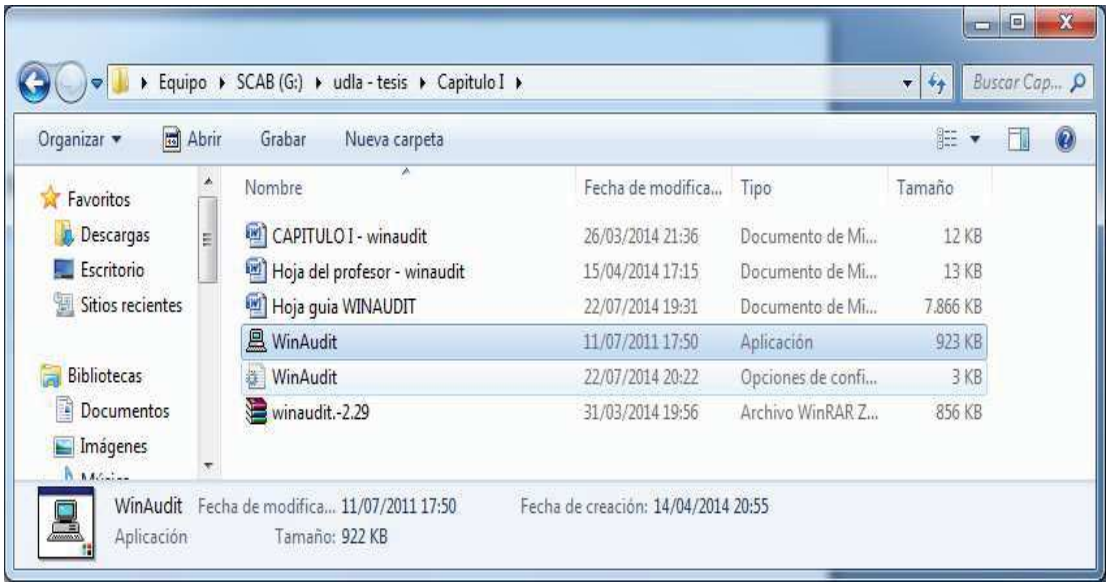


Figura 1. Ejecución WinAudit

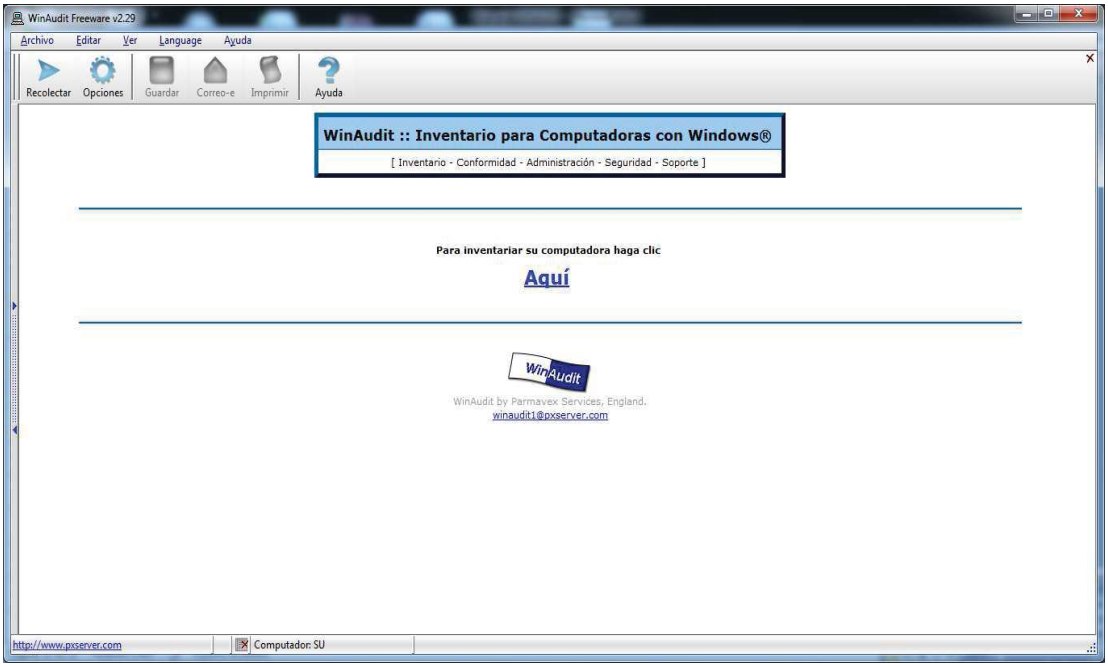


Figura 2. Ventana principal de WinAudit.

- Elegir la opción “Inventariar su computadora”.

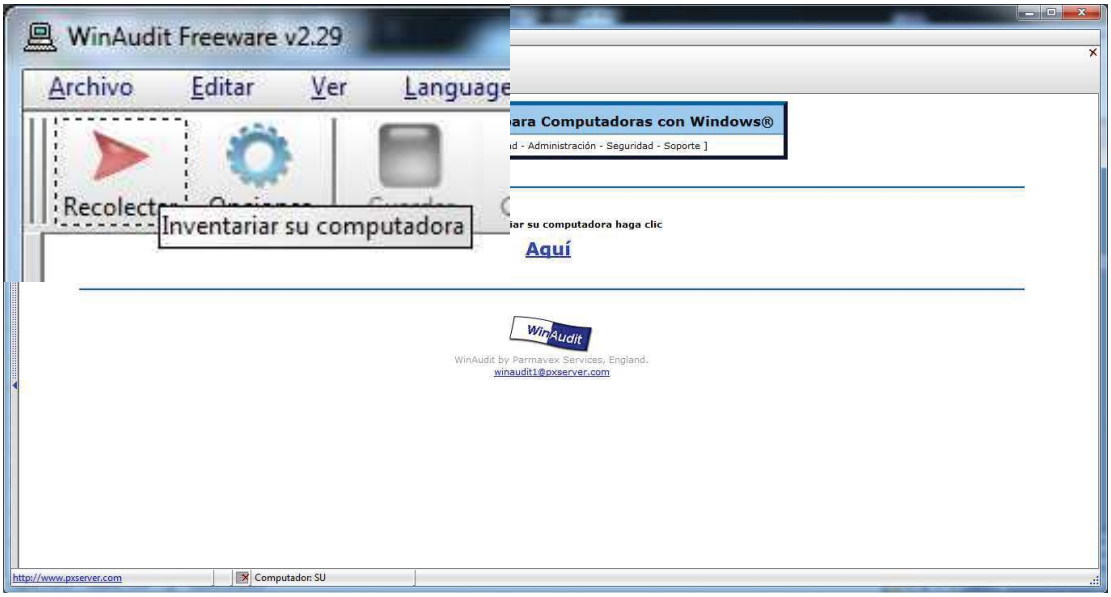


Figura 3. “Inventariar su computadora”.

- Esperar el resultado del inventario.

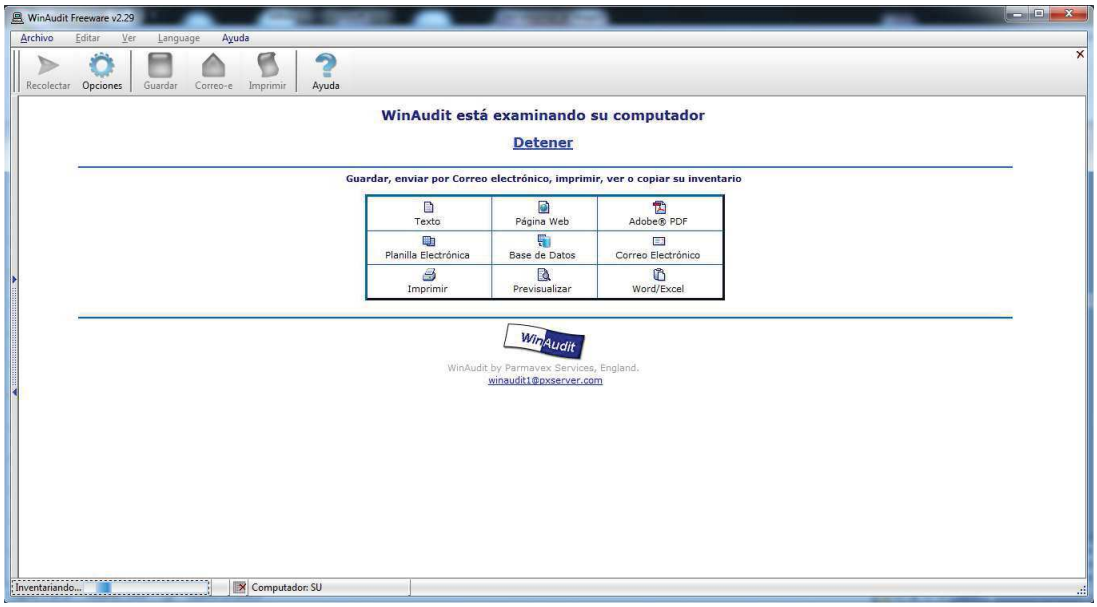


Figura 4. Proceso de inventario.

- Resultados obtenidos al finalizar el proceso.

Figura 5. Resultados.

Entre los resultados obtenidos se puede observar la siguiente información:

- Vista General

Vista General

Item	Value
Computer Name	SU
Domain Name	WORKGROUP
Site Name	
Roles	Workstation, Server
Description	
Operating System	Microsoft Windows 7 Ultimate 32-Bit
Manufacturer	Hewlett-Packard
Model	HP G42 Notebook PC
Serial Number	CNF112CVZQ
Asset Tag	
Number Of Processors	1
Processor Description	AMD Athlon(tm) II P360 Dual-Core Processor, 2294MHz
Total Memory	1792MB
Total Hard Drive	465GB
Display	@monitor.inf,%pnpmonitor.devicedesc%;Monitor PnP genérico, 13.9" (31cm x 17cm)
BIOS Version	HPQOEM - 3
User Account	SUSI
System Uptime	0 Days, 0 Hours, 35 Minutes
Local Time	2014-08-18 20:07:50

Figura 6. Información general del equipo inventariado.

- Discos Físicos

Discos Físicos

Hitachi HTS545050B9A300 ATA Device

Item	Value
Disk Number	1
Capacity	476937MB
Disk Type	Fixed hard disk media
Manufacturer	Hitachi
Model	Hitachi HTS545050B9A300 ATA Device
Serial Number	3131333038304250344735373751314 54a35564b
Firmware Revision	
Controller Rank	Primary
Master/Slave	Master
Total Cylinders	60801
Total Heads	255
Sectors Per Track	63
Buffer Size	
SMART Supported	
SMART Enabled	
SMART Self Test	

Figura 7. Muestra toda la información sobre los discos físicos que posee el computador.

- Baseboard

Baseboard

Item	Value
Board Number	1
Manufacturer	Hewlett-Packard
Product	1444
Version	69.37
Serial Number	PX210011Z07ACT
Asset Tag	Base Board Asset Tag
Features	Replacable
Board Type	Mother Board

Figura 8. Información de la placa principal del equipo.

1.8. TIEMPO ESTIMADO DE LA PRÁCTICA

Una sesión de clase.

1.9. ACTIVIDADES PARA LOS ALUMNOS

Elaborar un informe de la práctica realizada.

1.10. EVALUACIÓN

1. ¿Qué es auditoria de hardware?
2. ¿Cuántas particiones posee el equipo?
3. ¿Qué tipos de puertos se encontró en el equipo?
4. ¿Cuál es la versión del BIOS?
5. ¿Con que tipo de procesador cuenta el equipo?

2. CAPITULO II

LABORATORIO 2 “Identificación del tipo de archivos con notepad, notepad++ (extensión cambiada)”

2.1. INTRODUCCIÓN

En el laboratorio 2 se identifica las correctas extensiones de los archivos con la ayuda de los editores de texto bloc de notas y notepad++.

2.2. DESCRIPCIÓN DE LOS EQUIPOS

- Software free Notepad++
- Computador
- Sistema Operativo Windows

2.3. MATERIALES

- 1 archivo de imagen.
- 1 archivo de sonido extensión mp3.
- 1 archivo de sonido extensión wmv.
- 1 archivo de extensión DLL.
- 1 archivo de extensión exe.
- 1 archivo de extensión cab.

2.4. OBJETIVO GENERAL

Identificar si el tipo de extensión corresponde a la cabecera a través de la inspección del elemento con notepad++.

2.5. OBJETIVOS ESPECÍFICOS

- Utilizar correctamente el editor de texto notepad++.
- Desarrollar el laboratorio con los equipos especificados.
- Verificar el correcto funcionamiento del laboratorio N°2.
- Evaluar y aprobar el laboratorio.

2.6. TRABAJO PREPARATORIO

Previamente el estudiante tiene que conocer los temas que a continuación se describen:

2.6.1. Bloc de notas

El bloc de notas es un editor de texto gratuito incluido en todas las versiones del sistema Windows desde 1985. Es una aplicación básica, sencilla y rápida. Generalmente graba los archivos en formato ".txt", un formato que no tiene etiquetas ni estilos. (13)

2.6.2. Notepad++

Es un editor de texto y de código fuente libre con soporte para varios lenguajes de programación. Se parece al Bloc de notas, puede editar texto sin formato y de forma simple; no obstante, incluye opciones más avanzadas que pueden ser útiles para usuarios expertos como desarrolladores y programadores.

Se distribuye bajo los términos de la Licencia Pública General de GNU.(14)

2.6.3. Archivos del Sistema

Son los archivos necesarios para el funcionamiento interno del Sistema Operativo así como de los diferentes programas que trabajan en él. No está recomendado moverlos, editarlos o variarlos de ningún modo debido a que pueden afectar al buen funcionamiento del sistema.(15)

ACA --> Microsoft Agent Character

ACG --> Vista previa de Microsoft Agent

ACS --> Microsoft Agent Character

DLL --> Librería, extensión de aplicación

EXE --> Aplicación

CAT --> Catálogo de seguridad

CER --> Certificado de seguridad

CFG --> Configuraciones

CHK --> Fragmentos de archivos recuperados

CHM --> Ayuda HTML compilado

CMD --> Secuencia de comandos de Windows NT

CNF --> Velocidad de marcado

COM --> Aplicación MS-DOS

CPL --> Extensión del Panel de control

CRL --> Lista de revocaciones de certificados

CRT --> Certificado de seguridad

SYS --> Archivo de sistema

THEME -->Tema de Windows

TMP -->Archivo temporal

TTC -->Fuente True Type

2.6.4. Archivos de Audio

Los archivos de audio son todos los que contienen sonidos (no solo música). Las diferentes extensiones atienden al formato de compresión utilizado para convertir el sonido real en digital. (16)

MP1 -->Winamp, VLC, wmplayer

MP2 -->Winamp. VLC, wmplayer

MP3 -->Winamp, VLC, wmplayer

MTM -->Winamp, VLC, wmplayer

OGG -->Winamp, VLC, wmplayer

WMA -->Winamp, VLC, wmplayer

WMV --> Windows Media

MP3: Hoy por hoy es el formato más extendido para la compresión de música en Internet. La alta calidad lograda en su pequeño tamaño lo hace el favorito de la mayoría de los usuarios para comprimir música y compartirla en red.

OGG: Este formato es totalmente abierto y libre de patentes. Tan profesional y de calidad como cualquier otro pero con todos los valores del movimiento Open Source.

2.6.5. Archivos de Video

Los formatos de video no sólo contienen imágenes sino también el sonido que los acompaña. Es bastante habitual que al intentar visualizar un vídeo no se pueda ver la imagen aunque si se escucha el sonido. Esto se debe a que el formato de compresión utilizado en ellos no puede ser reconocido por el ordenador, siempre se ha de tener actualizados los códecs de cada uno de los formatos. (17)

ASF --> Windows Media

AVI -->BSPlayer

BIK --> RAD Video Tools

DIV --> DivX Player

MOV--> QuickTime

MOVIE --> (mov)

MP2V --> (mpeg)

MP4 --> (MPEG-4)

WMV --> Windows Media

AVI: El formato de video más extendido en Internet es el AVI.

MOV: Es el formato standard de video de Macintosh y es altamente utilizado en vídeos para reproducir en páginas web (trailers, publicidad...).

MPEG: siglas de "Moving Pictures Experts Group" también se encuentra como MPG.

2.6.6. Archivos Comprimidos

Los formatos de compresión son de gran utilidad a la hora del almacenamiento de Información ya ocupan el menor espacio posible y reúne muchos ficheros en uno sólo. (18)

R0... -->WinRAR

RAR-->WinRAR

TAR -->IZarc / WinRAR

TBZ -->IZarc / WinRAR

XXE -->IZarc / WinRAR

ZIP-->WinZIP

ZOO -->IZarc

RAR: Formato de compresión muy efectivo, cuenta con uno de los mejores programas de compresión/descompresión soportando prácticamente todos los formatos, no sólo el propio. Las extensiones R00, R01, R02, etc., pertenecen también a este formato cuando el comprimido se divide en varias partes.

ZIP: Es otro software muy utilizado; soportado por la amplia mayoría de los programas extractores por ser de los más extendidos es el más conocido para el público en general.

2.6.7. Imágenes

Poco hay que decir de las imágenes y de sus formatos salvo que cada uno de ellas utiliza un método de representación y que algunas ofrecen mayor calidad que otras. También cabe destacar que muchos programas de edición gráfica utilizan sus propios formatos de trabajo con imágenes. (19)

AIS -->ACDSeeSecuencias de imagen

BMP -->XnView / ACDSee

BW -->XnView / ACDSee

EMF -->XnView / ACDSee

GBR -->The Gimp

GIF -->XnView / ACDSee

GIH -->The Gimp

ICO -->Icono

JPE -->XnView / ACDSee

JPEG -->XnView / ACDSee

JPG -->XnView / ACDSee

RLE -->XnView / ACDSee

SGI -->XnView / ACDSee

TGA -->XnView / ACDSee

TIF -->XnView / ACDSee

BMP: Extensión que nace del nombre de este formato BitMaP o Mapa de Bits, gran calidad pero tamaño excesivo no suele ser muy utilizado en Internet por su carga lenta.

JPEG: También se ve como JPE y sobre todo como JPG es uno de los más extendidos, por su compresión y calidad, en páginas webs para logotipos y cabeceras.

GIF: Este formato cuenta con características que lo hacen ideal para el uso en páginas web, como es la posibilidad de darle un fondo transparente o insertarle movimiento.

2.6.8. Texto

Dentro de los documentos de texto se diferencia entre el texto plano y el texto enriquecido. Los primeros sencillamente guardan caracteres por ejemplo: los txt y log, y los segundos en los que se pueden asignar: un tamaño, fuente, color, etc., como es el caso de los archivos doc.(20)

DOC --> Microsoft Word

DIZ --> Bloc de notas / WordPad

DOCHTML --> HTML de Microsoft Word

EXC -->Bloc de notas / WordPad

PDF --> Adobe Acrobat

RTF --> Microsoft Word

SCP --> Bloc de notas / WordPad

TXT --> Bloc de notas / WordPad

WRI --> Write

DOC: Documentos de texto enriquecidos (posibilidad de asignar formato a las letras) está especialmente extendido por ser el habitual de uno de los programas más utilizados, el Microsoft Word.

TXT: Formato de texto plano, habitual para registros.

2.7. MODO DE TRABAJO

- Descargarse un archivo .png

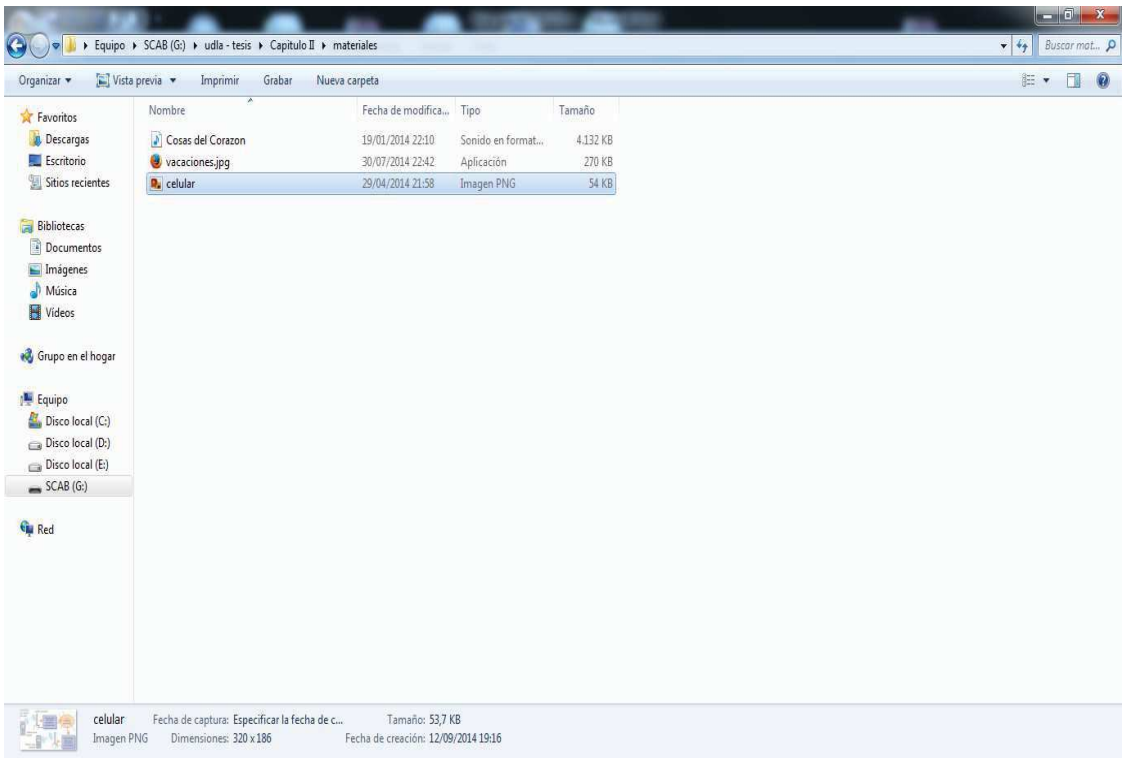


Figura 9. Ubicación del archivo .png.

- Ubicar el archivo .png y abrirlo con notepad++

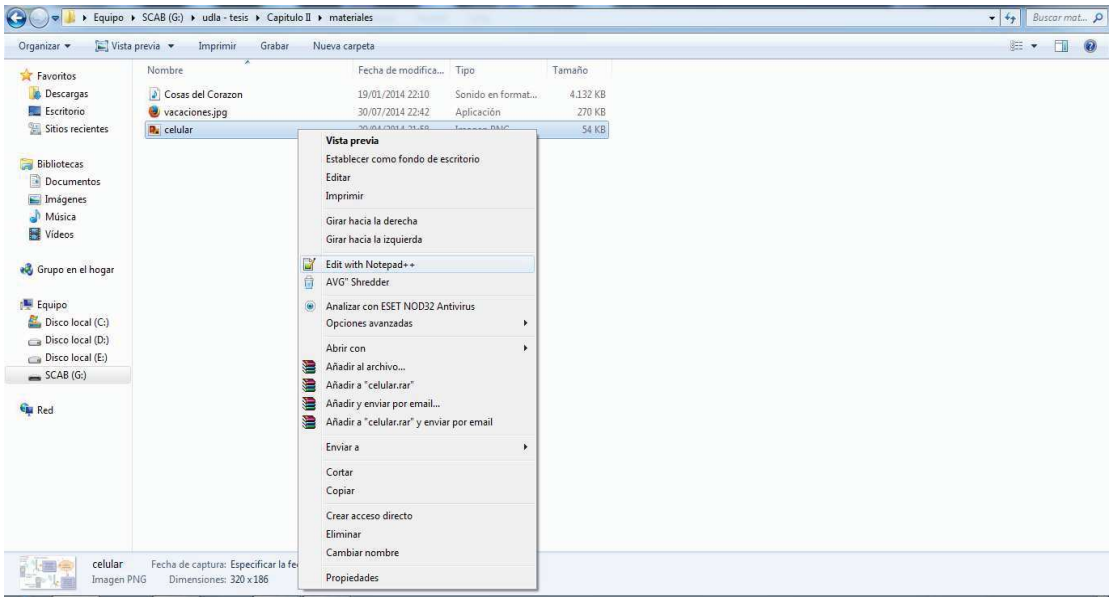


Figura 10. Archivo abierto con notepad++

- Una vez abierto con notepad++ identificar la cabecera del archivo.

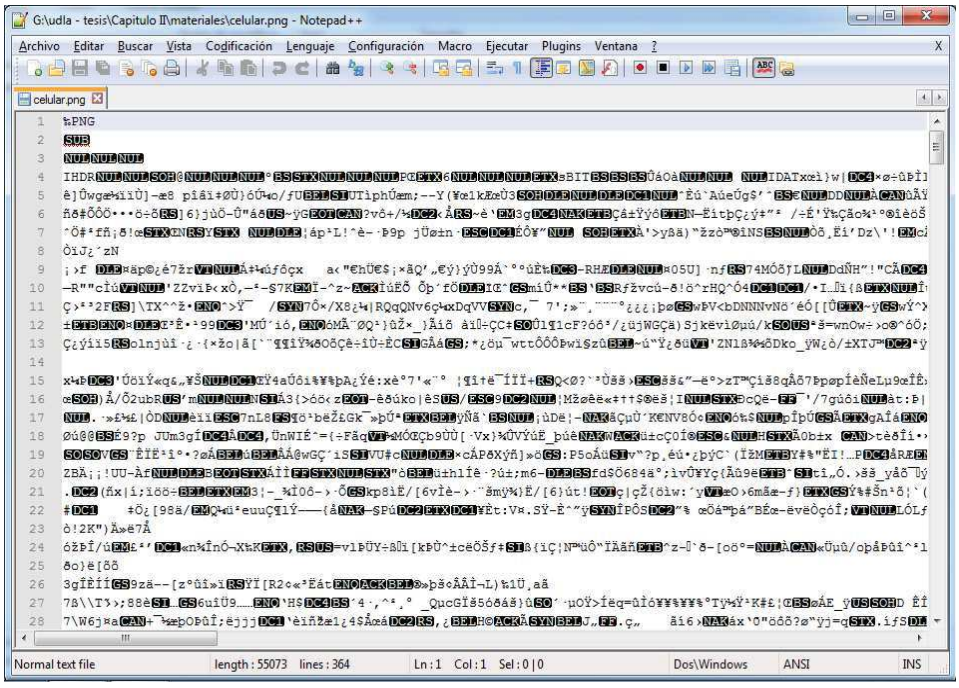


Figura 11. La cabecera %PNG es la cabecera correcta del archivo .png esto quiere decir que es una imagen confiable.

2.8. TIEMPO ESTIMADO DE LA PRÁCTICA

Una sesión de clase.

2.9. ACTIVIDADES PARA LOS ALUMNOS

Realizar un informe del laboratorio.

2.10. EVALUACIÓN

1. ¿Qué es una extensión?
2. ¿Cuál es la diferencia de un archivo .png y .exe?
3. ¿Qué es una cabecera?
4. Mencione 5 tipos de extensiones que son ejecutables
5. ¿Qué es un archivo con la extensión .bat?

3. CAPITULO III

LABORATORIO 3 “Análisis de archivos críticos, Sysinspector”

3.1. INTRODUCCIÓN

En el presente laboratorio 3 se conocerá los pasos a seguir para identificar los archivos confiables, críticos, procesos, conexiones de red entre otros elementos que se encuentran en un computador, mediante un análisis con Sysinspector.

3.2. DESCRIPCIÓN DE LOS EQUIPOS

- Software Free Sysinspector
- Computador
- Sistema Operativo Windows 7

3.3. MATERIALES

- Computador
- Sistema Operativo Windows.

3.4. OBJETIVO GENERAL

Identificar archivos confiables y determinar los cambios en el transcurso del tiempo.

3.5. OBJETIVOS ESPECÍFICOS

- Conocer previamente el trabajo preparatorio.
- Determinar los materiales en hardware y software necesarios.
- Desarrollar el laboratorio.
- Evaluar y aprobar el laboratorio.

3.6. TRABAJO PREPARATORIO

Previamente el estudiante debe conocer los temas que a continuación se describen:

3.6.1. SysInspector

ESET SysInspector es una herramienta de diagnóstico gratuita para sistemas basados en Windows, examina el sistema operativo y captura detalles de cada proceso en ejecución, contenido de registros, elementos de inicio y conexiones de red. Una vez creada la captura instantánea del sistema, ESET SysInspector aplica heurística para asignar el nivel de riesgo para cada objeto registrado. Su intuitiva interfaz gráfica le permite al usuario deslizarse fácilmente a través de extensos volúmenes de información, usando una barra de desplazamiento que agrupa objetos de colores particulares por el nivel de riesgo para un examen más detallado. ESET SysInspector es un recurso útil para cualquier experto en tecnología informática. (21)

3.6.2. Procesos del Sistema

La gran mayoría de los programas crean procesos que le permiten iniciarse con el sistema operativo. Los recursos disponibles en un sistema operativo son limitados y entre mas procesos se inicien con el mismo mas largo será el tiempo necesario para el arranque.(22)

- **Winlogon.exe.-** Se encarga de validar la identidad de un usuario en el sistema. Es un proceso esencial que no debería ser terminado. (23)
- **Csrss.exe.-**Es el Client Server Run time Subystem se inicia por SMSS. Es un subsistema esencial que debe estar siempre activo. Este administra la consola de Windows, crea y destruye threads y administra algunas porciones del entorno 16 bits virtual DOS. (24)
- **Svchost.exe.-** Es un proceso genérico que hace de host para otros procesos que corren desde DLL. (25)

3.6.3. Archivo Hosts

HOSTS (sin extensión alguna), es un archivo utilizado por Windows para asociar nombres de dominio con direcciones IP. Si este archivo existe en c:\windows\ (Windows 95, 98 y Me), o en \system32\drivers\etc\ (Windows NT, 2000 y XP), el sistema lo examina antes de hacer una consulta a un servidor

DNS, no necesariamente debe existir en todos los sistemas. Algunos malwares modifican el archivo HOSTS para que el usuario no pueda ingresar a algunos sitios (generalmente para impedir la actualización de antivirus u otro software de seguridad), o para que sea redirigido a sitios falsos. (26)

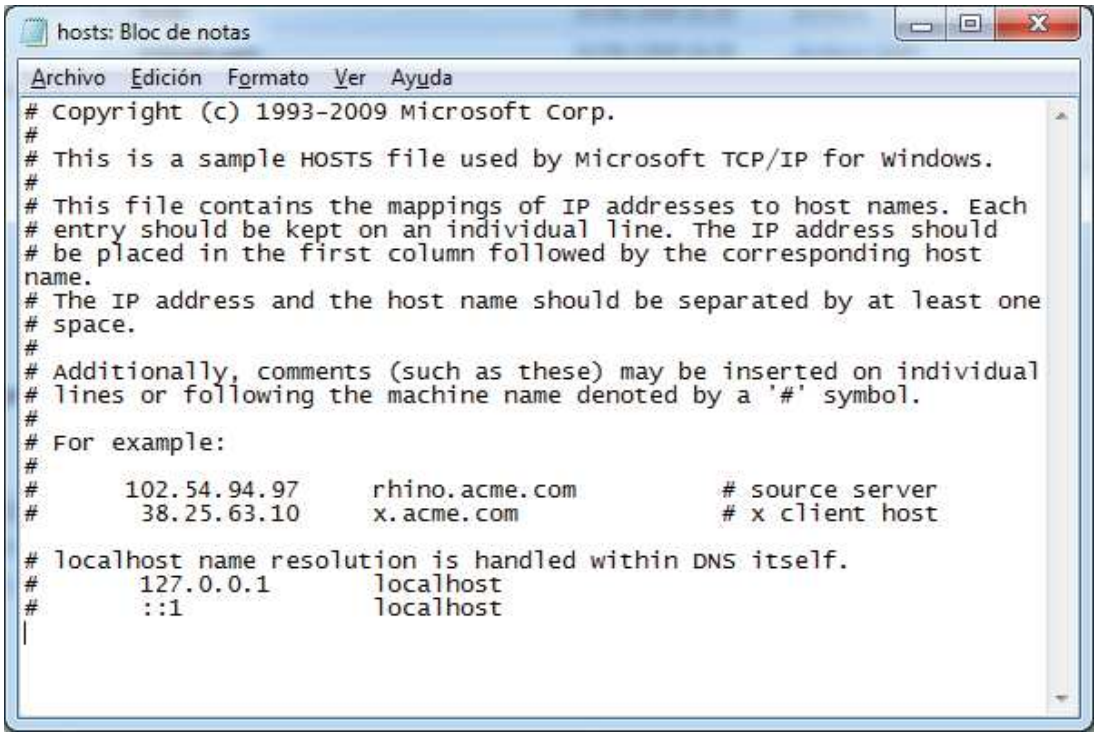


Figura 12. Archivo host por defecto de Windows 7.

3.6.4. Archivos Legítimos.

- **alg.exe**: Acrónimo de *Application Layer Gateway*. Se trata en realidad de un servicio que posibilita la conexión de diferentes protocolos a través de *Internet Connection Sharing* (ICS) e *Internet Connection Firewall* (ICF). Se encuentra alojado en la carpeta system32. (27)
- **lsass.exe**: Acrónimo de *Local Security Authority Subsystem Service*, se trata de un proceso netamente relacionado con una la seguridad en Windows, encargándose de los mecanismos de autenticación como parte de la capa de seguridad a nivel local. Se encuentra alojado en la carpeta system32. (28)

- **explorer.exe**: Representa al Explorador de Windows. Es la interfaz gráfica de la shell de Windows que posibilita la visualización de la barra de tareas, el administrador de archivos, el menú inicio y el escritorio del sistema. Se encuentra en la carpeta windows. (29)
- **ctfmon.exe**: Se trata de un proceso no crítico que forma parte de la Suite de Ofimática de Microsoft (MS Office) y se activa cada vez que se ejecuta una de sus aplicaciones (Word, Excel, PowerPoint, etc.) . El mismo se encuentra alojado en la carpeta system32 (30)
- **dllhost.exe**: Conocido como *Microsoft DCOM DLL Host Process*, este proceso se encarga de controlar todas aquellas aplicaciones basadas en Librerías de Enlaces Dinámicos (DLL). Se encuentra alojada en la carpeta system32. (31)

3.6.5. Malwares

Malware es la abreviatura de "*Malicious software",* término que engloba a todo tipo de programa o código informático malicioso, cuya función es dañar un sistema o causar un mal funcionamiento. (70)

- **Adware**

Programa malicioso que se instala en el sistema usualmente sin conocimiento del usuario cuyo fin es la descarga y/o visualización de publicidades no solicitadas, desplegadas por lo general a través de pantallas emergentes. (32)

- **Backdoor**

Tipo de troyano que permite el acceso al sistema infectado y su control remoto. El atacante puede entonces eliminar o modificar archivos, ejecutar programas, enviar correos masivamente o instalar herramientas maliciosas. (33)

- **Botnets**

Red de equipos infectados por códigos maliciosos que son controlados por un atacante de modo transparente al usuario, disponiendo de sus recursos para que trabajen de forma conjunta y distribuida. Cada sistema infectado, al que

suele llamarse zombi, interpreta y ejecuta las órdenes emitidas. Ofrece a los delincuentes una fuente importante de recursos que pueden trabajar de manera conjunta y distribuida. Mayormente se utilizan para el envío de spam, el alojamiento de material ilegal o la realización ataques de denegación de servicio distribuido. (34)

- **Bootkit**

Tipo de malware que se clasifica dentro de los rootkit. Se aloja en el inicio original del sistema operativo con el fin de obtener acceso total a las funciones de la computadora antes que finalice la carga del mismo. Un ejemplo de esta clase de malware es Stoned, el primer Bootkit capaz de afectar a la versión preliminar de Windows 8. (35)

- **Crack**

Parche que modifica una aplicación para activar su licenciamiento de manera gratuita y eliminar las restricciones de su uso, no respetando lo indicado en su licencia de uso. (36)

- **DDoS**

Ataque distribuido de denegación de servicio, por sus siglas en inglés "*DistributedDenial of Service*". Ampliación del ataque DoS que se lleva a cabo generando un gran flujo de información desde varios puntos de conexión, por lo general a través de una botnet. El ataque se realiza a través del envío de determinados paquetes de datos al servidor, de forma tal de saturar su capacidad de trabajo y forzar que el servicio deje de funcionar. (37)

- **Downloader**

Troyano cuya función es la descarga e instalación de archivos dañinos o más variantes de malware en el sistema infectado de la víctima. (38)

- **Gusanos**

Programa malicioso que cuenta con la capacidad de auto-reproducción, al igual que los virus, pero con la diferencia que no necesita de un archivo anfitrión -

archivo que aloja una porción de código malicioso- para la infección. Generalmente modifica el registro del sistema para ser cargado cada vez que el mismo es iniciado. Suelen propagarse a través de dispositivos USB o vulnerabilidades en los sistemas. El surgimiento de este tipo de amenaza puede ubicarse a finales de los años ’80, más precisamente en el año 1988, cuando apareció el gusano Morris, considerado el primero de su especie. (39)

- **Hoax**

En español, “bulo”. Correo electrónico o mensaje en redes sociales con contenido falso o engañoso que se distribuye en cadena debido a su temática impactante que parece provenir de una fuente fiable o porque el mismo mensaje pide ser reenviado. Es muy común que se anuncien potentes amenazas informáticas, la noticia del cierre de algún servicio web o se solicite ayuda para personas enfermas. El objetivo de este tipo de engaños suele ser recolectar direcciones para el envío de spam, generar incertidumbre entre los receptores o simplemente diversión. (40)

- **Ingeniería Social**

Conjunto de técnicas utilizadas para engañar a un usuario a través de una acción o conducta social. Consiste en la manipulación psicológica y persuasión para que voluntariamente la víctima brinde información o realice algún acto que ponga a su propio sistema en riesgo. Suele utilizarse este método para obtener contraseñas, números de tarjetas de crédito o pin, entre otros. (41)

- **Keylogger**

En español, “registrador de teclas”. Tipo de software que registra las teclas pulsadas en un sistema para almacenarlas en un archivo o enviarlas a través de Internet. Suele guardar contraseñas, números de tarjeta de crédito u otros datos sensibles. En la actualidad se pueden encontrar versiones más nuevas de esta herramienta fraudulenta capaces de realizar capturas de pantalla cuando se registra un clic, haciendo que estrategias de seguridad como el uso del teclado virtual sean obsoletas. (42)

- **Pharming**

Tipo de ataque que permite redireccionar un nombre de dominio a una dirección IP distinta de la original. El objetivo de este ataque consiste en dirigir al usuario a una página web falsa a pesar de que éste ingrese la dirección url correcta. El ataque suele realizarse sobre servidores DNS (en inglés, "*Domain Name System*") globales o en un archivo ubicado en el equipo víctima (*pharming* local). (43)

- **Phishing**

Ataque que se comete mediante el uso de Ingeniería Social con el objetivo de adquirir fraudulentamente información personal y/o confidencial de la víctima, como contraseñas y/o detalles de la tarjeta de crédito. Para efectuar el engaño el estafador, Conocido como phisher, se hace pasar por una persona o empresa de confianza utilizando una aparente comunicación oficial electrónica como correos electrónicos, sistemas de mensajería instantánea o incluso llamadas telefónicas. Los casos de phishing más comunes toman como objetivo de ataque a clientes de grandes entidades financieras y suelen contener algún tipo de amenaza de interrupción del servicio u otras consecuencias indeseables, si las instrucciones que indican no se realizan. (44)

- **Rogue**

Programa que simula ser una solución antivirus o de seguridad, generalmente gratuita, pero que en realidad es un programa dañino. Este tipo de ataque comienza con la muestra de ventanas de advertencia, llamativas y exageradas, acerca de la existencia de software malicioso en el sistema. De esta manera se instiga al usuario a la descarga de una falsa aplicación de seguridad (con la finalidad de instalar malware en la computadora) o a su compra (obteniendo el correspondiente crédito económico). (45)

- **Rootkit**

Herramienta diseñada para ocultar el acceso y control de un atacante a un sistema informático. Encubre archivos, procesos y puertos abiertos que

habilitan el uso arbitrario del equipo, vulnerando de manera directa las funciones del sistema operativo. Está programada para intentar evadir cualquier aplicación de seguridad, haciéndose imperceptible al analizar los procesos en ejecución. (46)

- **Spam**

Correo no deseado o correo basura enviado de forma masiva por un remitente desconocido, ya sea en formato de texto o con contenido HTML. Es utilizado, por lo general, para envío de publicidad, aunque también se lo emplea para la propagación de códigos maliciosos. Sirve también como puerta para cometer scam o phishing. Representa un riesgo para la seguridad y tiene efectos secundarios, como el impacto negativo en la productividad del personal por la lectura de los mismos y el aumento del consumo de recursos (ancho de banda, procesamiento, etc.). A su vez, puede manifestarse en comentarios de foros, blogs o en mensajes de texto. Inicialmente, el spam fue utilizado para enviar mensajes en formato de texto. Sin embargo, con la creación de filtros antispam se comenzaron a identificar este tipo de mensajes, y posteriormente, el spam evolucionó a correos con imágenes o contenido HTML. (47)

- **Spyware**

Aplicación espía que recopila información sobre los hábitos de navegación, comportamiento en la web u otras cuestiones personales de utilización del sistema del usuario sin su consentimiento. Posteriormente, los datos son enviados al atacante. No se trata de un código malicioso que dañe al ordenador, sino que afecta el rendimiento del equipo y la privacidad de los usuarios. Sin embargo, en algunos casos se producen pequeñas alteraciones en la configuración del sistema, especialmente en las configuraciones de Internet o en la página de inicio. (48)

- **Troyanos**

Programa malicioso que simula ser una aplicación indefensa. Se instala y ejecuta como un software legítimo pero realiza tareas maliciosas sin conocimiento del usuario. A diferencia de los gusanos y virus, no tiene

capacidad de replicarse a sí mismo. Los troyanos pueden ser utilizados para muchos propósitos, entre los que se encuentran el acceso remoto al equipo que permite que el atacante pueda conectarse remotamente al mismo, el registro de todo lo escrito y el robo de contraseñas e información del sistema. El nombre de esta amenaza proviene de la leyenda del caballo de Troya. (49)

- **Virus**

Programa malicioso creado para producir algún daño en el ordenador, desde mensajes molestos en pantalla y la modificación o eliminación de archivos hasta la denegación completa de acceso al sistema. Tiene dos características particulares: pretende actuar de forma transparente al usuario y tiene la capacidad de reproducirse a sí mismo. Requiere de un anfitrión -archivo que aloja una porción de código malicioso- para alojarse, tal como un archivo ejecutable, el sector de arranque o la memoria de la computadora. Al ser ejecutado, se produce el daño para el que fue concebido y luego se propaga para continuar la infección de otros archivos. (50)

3.7. MODO DE TRABAJO

- Abrir el software Sysinspector
- Comprobar los archivos seguros (VERDE).

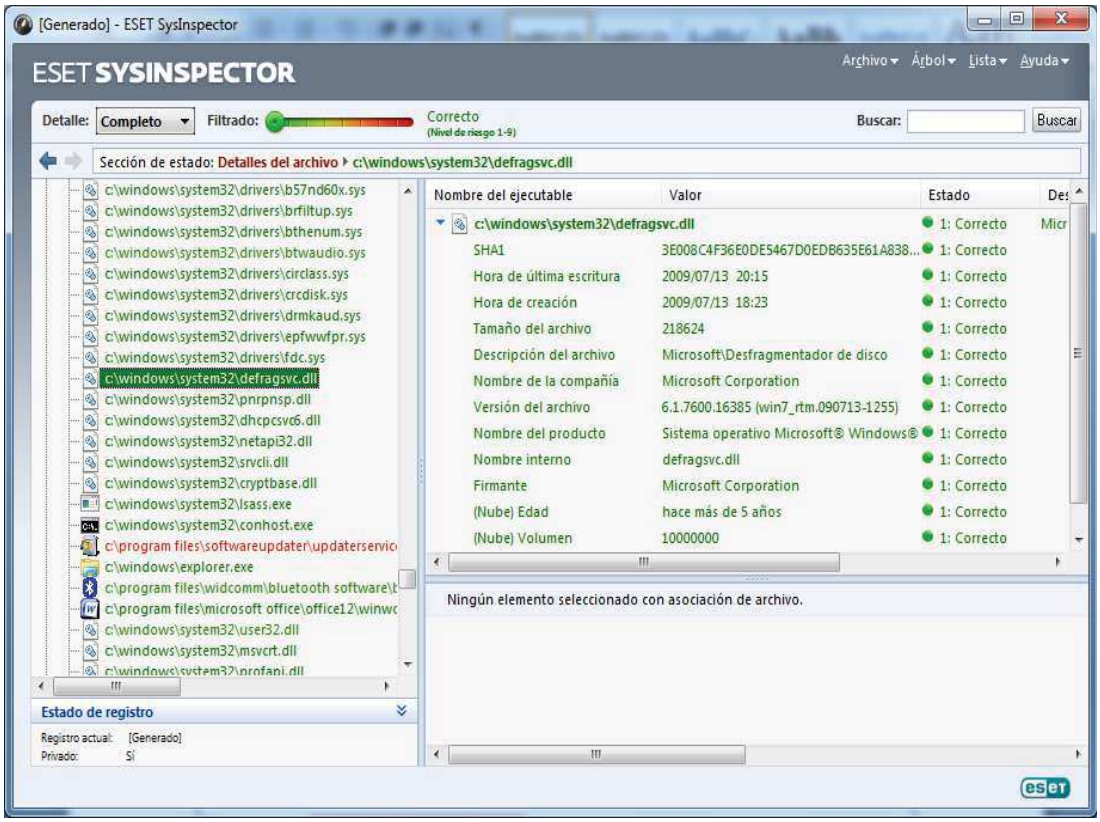


Figura 13. Archivos con un nivel de riegos de 1-9.

- Comprobar los archivos desconocidos (NARANJA).

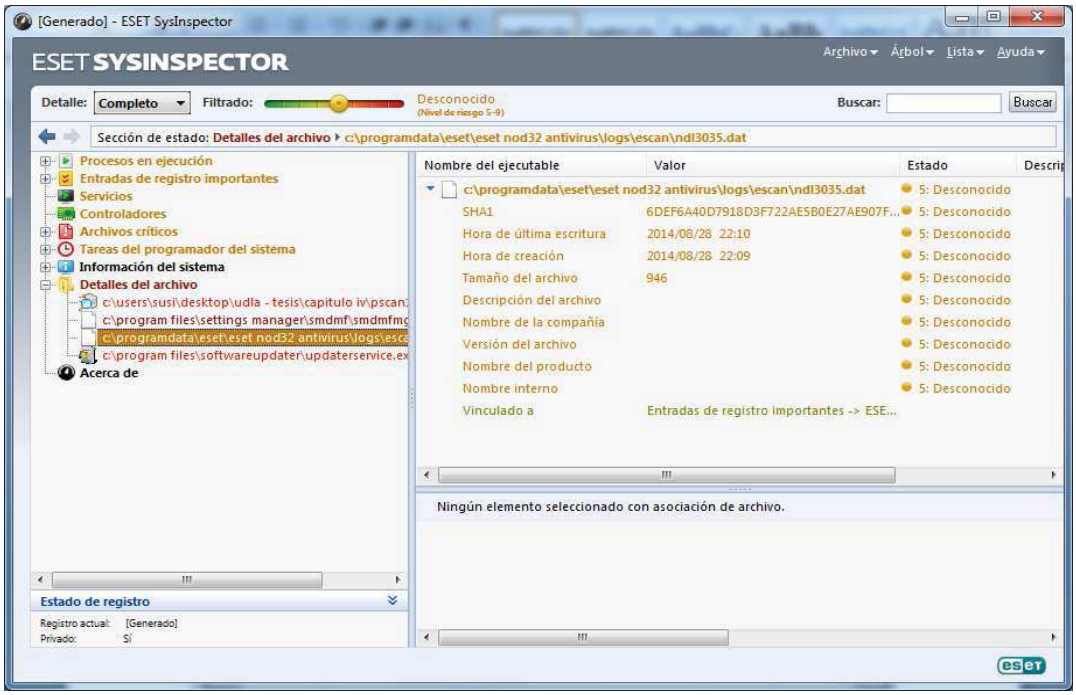


Figura 14. Archivos con un nivel de riesgo 5-9

- Comprobar los archivos inseguros (ROJO).

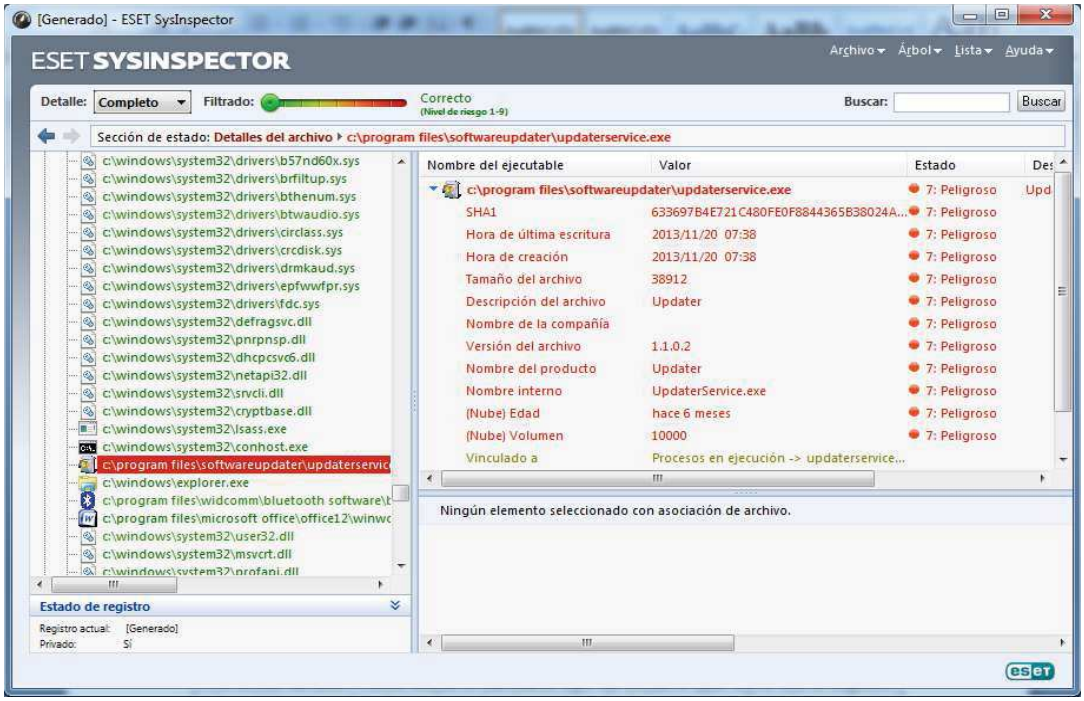


Figura 15. Archivos con un nivel de riego 9.

3.8. TIEMPO ESTIMADO DE LA PRÁCTICA

Una sesión de clases.

3.9. ACTIVIDADES PARA LOS ALUMNOS

Realizar un informe del laboratorio.

3.10. EVALUACIÓN

1. ¿Qué es un malware?
2. ¿Cuáles son los archivos críticos?
3. ¿Para qué sirve el sha1?
4. ¿Cuál es el proceso para filtrar el proceso Microsoft?
5. ¿Con que formato se guarda un resultado de Sysinspector si deseamos enviarlo por correo?

4. CAPITULO IV

LABORATORIO 4 “Verificación y análisis de conexión del PC, netstat.”

4.1. INTRODUCCIÓN

En el presente laboratorio 4 se conocerá un comando poco utilizado pero muy eficiente para adquirir información acerca de la red que posee un computador.

4.2. DESCRIPCIÓN DE LOS EQUIPOS

- Computador
- Sistema Operativo Windows

4.3. MATERIALES

- Computador
- Sistema Operativo Windows 7

4.4. OBJETIVO GENERAL

Identificar los puertos abiertos en un computador mediante el comando “netstat”.

4.5. OBJETIVOS ESPECÍFICOS

- Identificar, conocer y detectar las conexiones establecidas entre nuestro PC y la red Internet.
- Conocer el funcionamiento de las opciones de netstat.
- Determinar el estado del puerto 25.

4.6. TRABAJO PREPARATORIO

Previamente el estudiante tiene que conocer los temas que a continuación se describen:

4.6.1. Netstat

Netstat es una herramienta de línea de comandos, incluida en todos los sistemas operativos Windows, permite monitorear y estar al tanto de todas las conexiones establecidas entre una PC y el mundo exterior.

Con el comando NETSTAT al introducir las órdenes que permite ver, conocer, detectar e identificar las conexiones activas establecidas con el exterior, tanto entrantes como salientes, su origen y dirección IP de procedencia, saber los puertos que tenemos abiertos a la escucha, ver e identificar las conexiones entrantes e intrusiones de red en nuestra PC, saber si se tiene programas que establezcan contacto con un host remoto, etc.

Toda esa información y más, se puede obtener usando el comando NETSTAT con distintas opciones o modificadores. (51)

NETSTAT devuelve una serie de parámetros que indican el estado en que se encuentran las conexiones, son los siguientes:

Tabla 1. Parámetros de netstat.

LISTENING:	El puerto está abierto escuchando en espera de una conexión.
ESTABLISHED:	La conexión ha sido establecida.
CLOSE_WAIT:	La conexión sigue abierta, pero el otro extremo, comunica que no se continuará enviando información.
TIME_WAIT:	La conexión ha sido cerrada, pero no se elimina de la tabla de conexión por si hay algo pendiente de recibir.
LAST_ACK:	La conexión se está cerrando.
CLOSED:	La conexión ha sido cerrada completamente.

4.6.2. Puerto

Un puerto es un punto de acceso entre computadoras para el uso de servicios y flujo de datos entre equipos.

4.6.3. Asignaciones predeterminadas.

Existen miles de puertos (codificados en 16 bits, es decir que cuenta con 65536 posibilidades). Es por ello que la IANA (Internet Assigned Numbers Authority [Agencia de Asignación de Números de Internet]) desarrolló una aplicación estándar para ayudar con las configuraciones de red.

- Los puertos del 0 al 1023 son los "puertos conocidos" o reservados. En términos generales, están reservados para procesos del sistema (daemons) o programas ejecutados por usuarios privilegiados. Sin embargo, un administrador de red puede conectar servicios con puertos de su elección.
- Los puertos del 1024 al 49151 son los "puertos registrados".
- Los puertos del 49152 al 65535 son los "puertos dinámicos y/o privados".

A continuación se indican algunos de los puertos conocidos más utilizados:

Tabla 2. Puertos y asignaciones

Puerto	Servicio o aplicación
21	FTP
23	Telnet
25	SMTP
53	Sistema de nombre de dominio
63	Whois
70	Gopher
79	Finger
80	HTTP
110	POP3
119	NNTP

Por lo tanto, un servidor (un equipo conectado que ofrece servicios como FTP, Telnet, etc.) cuenta con números de puerto fijos a los cuales el administrador de red conecta los servicios. Entonces, los puertos del servidor generalmente se encuentran entre 0 y 1023 (rango de valores relacionado con servicios conocidos).

Del lado del cliente, el sistema operativo elige el puerto entre aquéllos que están disponibles de forma aleatoria. Por lo tanto, los puertos del cliente nunca incluirán los puertos que se encuentran entre 0 y 1023, ya que este rango de valores representa a los *puertos conocidos*. (52)

4.6.4. Puerto TCP/IP

El TCP / IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa. (53)

4.7. MODO DE TRABAJO

- Abrir la ventana ejecutar con las teclas “Windows + R”.
- Abrir la consola CMD

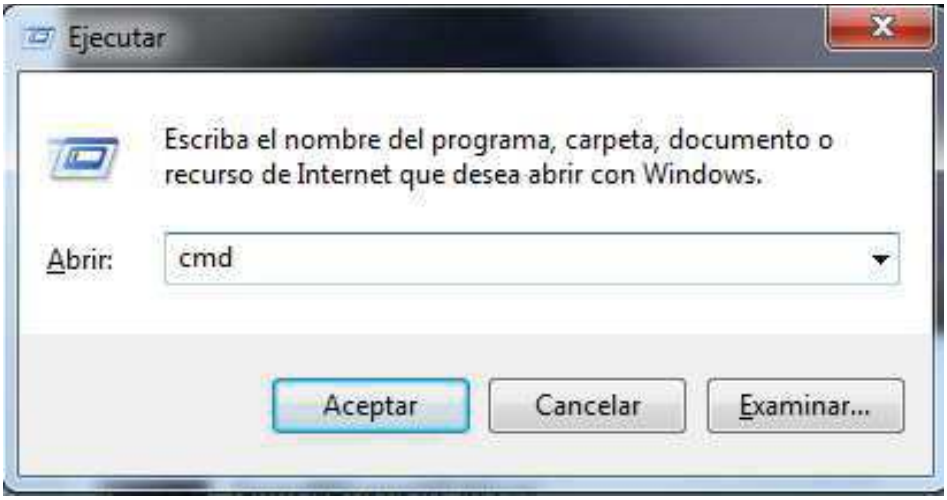


Figura 16. Consola de Windows (CMD).

- Para conocer los comandos que posee netstat introducir en la consola “netstat –h”.

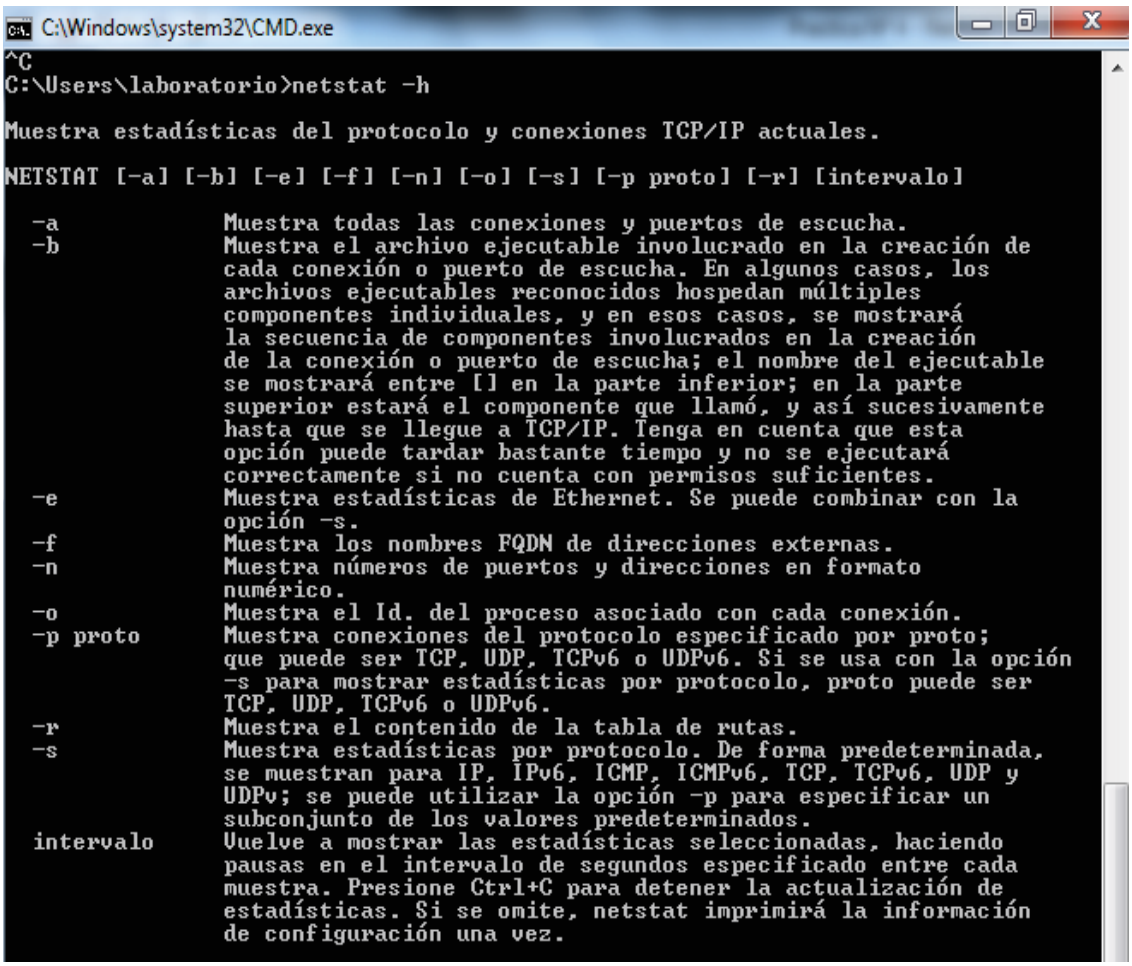


Figura 17. Información de los comandos netstat.

- Netstat –a: muestra todas las conexiones y los puertos en escucha del computador.

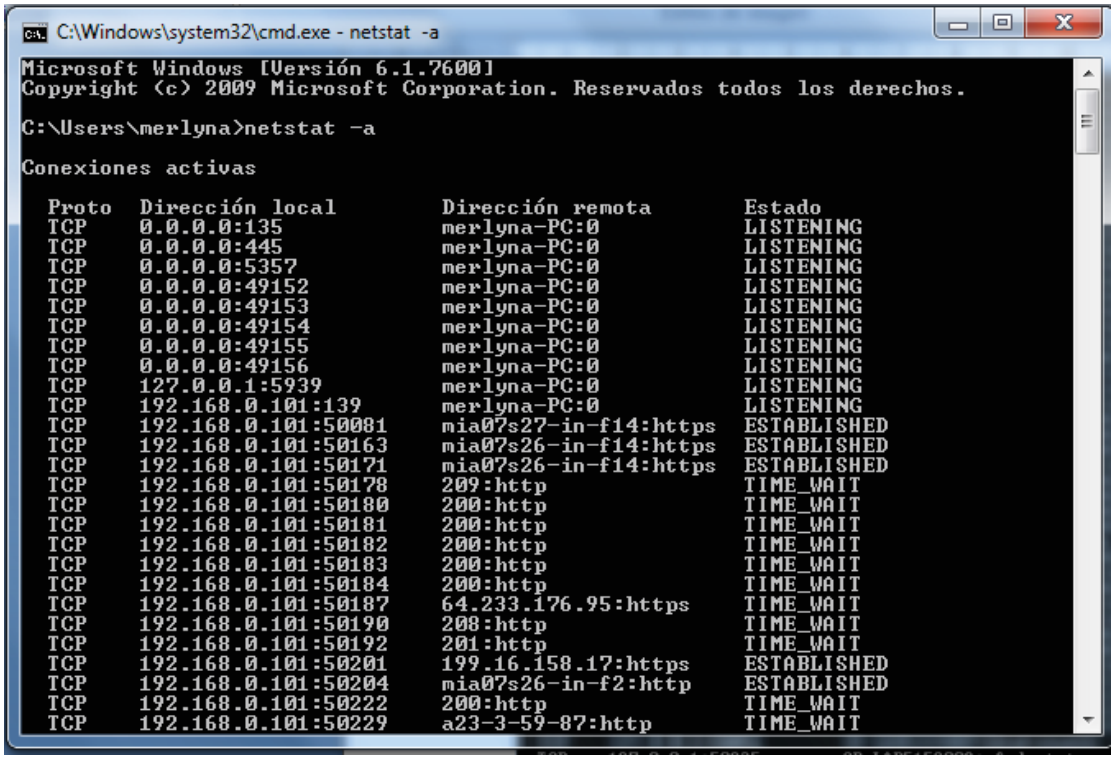


Figura 18. Información Puertos.

- Netstat -e: muestra las estadísticas Ethernet.

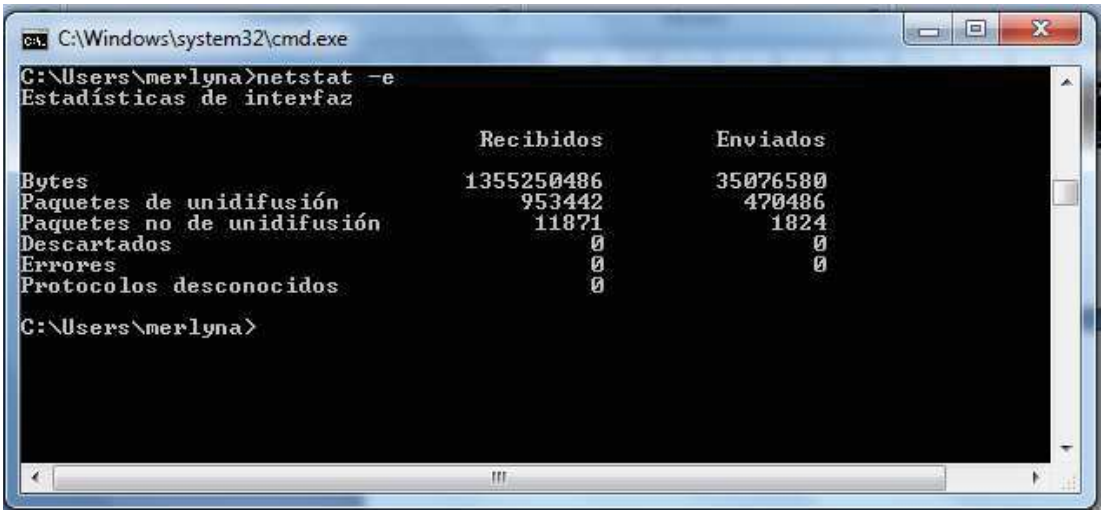


Figura 19. Estadísticas Ethernet

- Netstat –n: muestra las direcciones y los números de puerto en forma numérica, sin resolución de nombres.

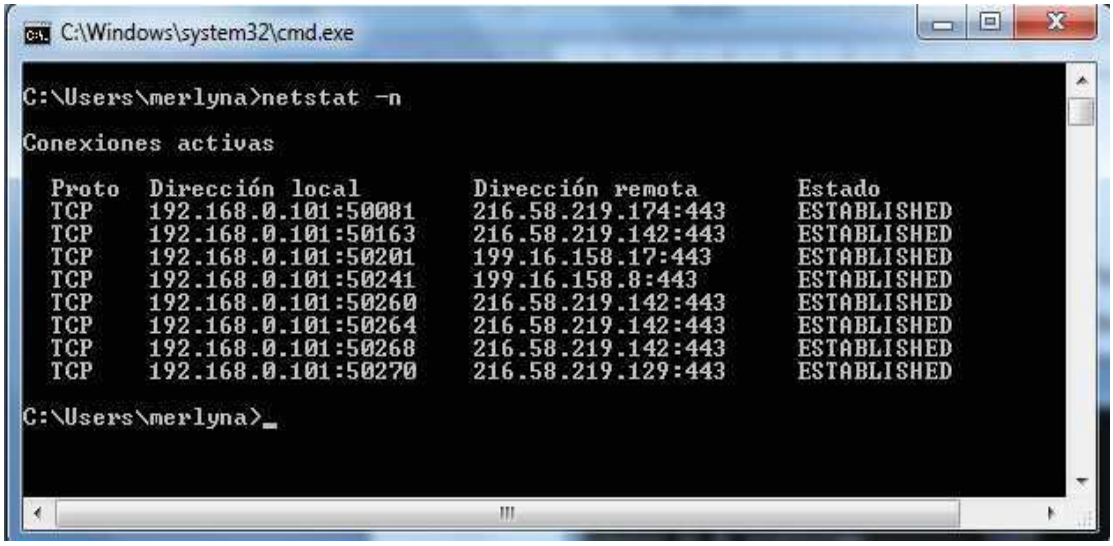


Figura 20. **Direcciones y números de puertos en forma numérica.**

- Netstat –o: Indica el número del proceso asignado a la conexión.

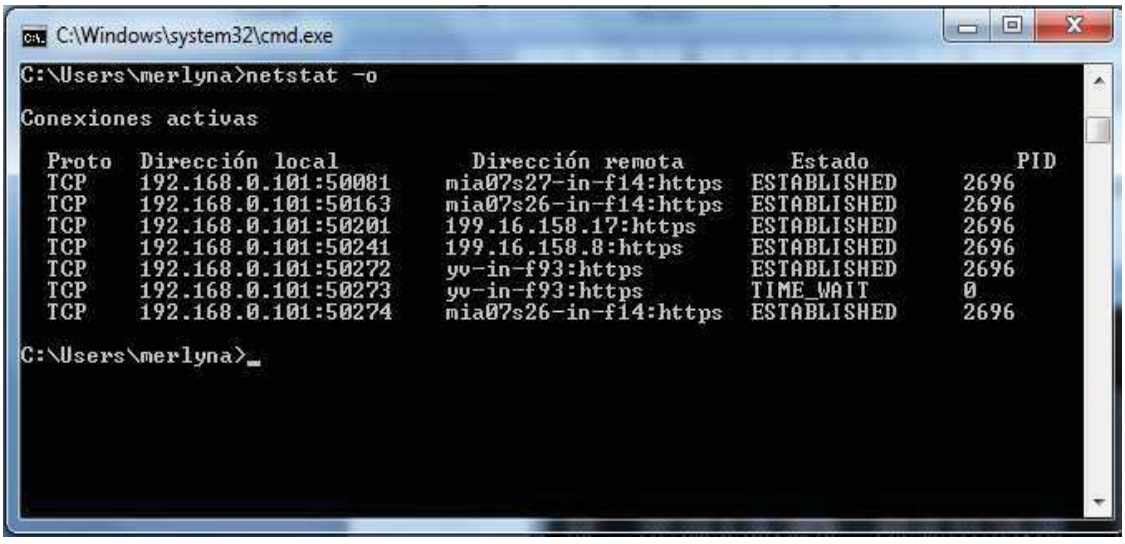


Figura 21. Número de procesos asignados a la conexión.

- Netstat –p seguido del nombre del protocolo (TCP, UPD o IP): muestra la información relacionada con el protocolo especificado.

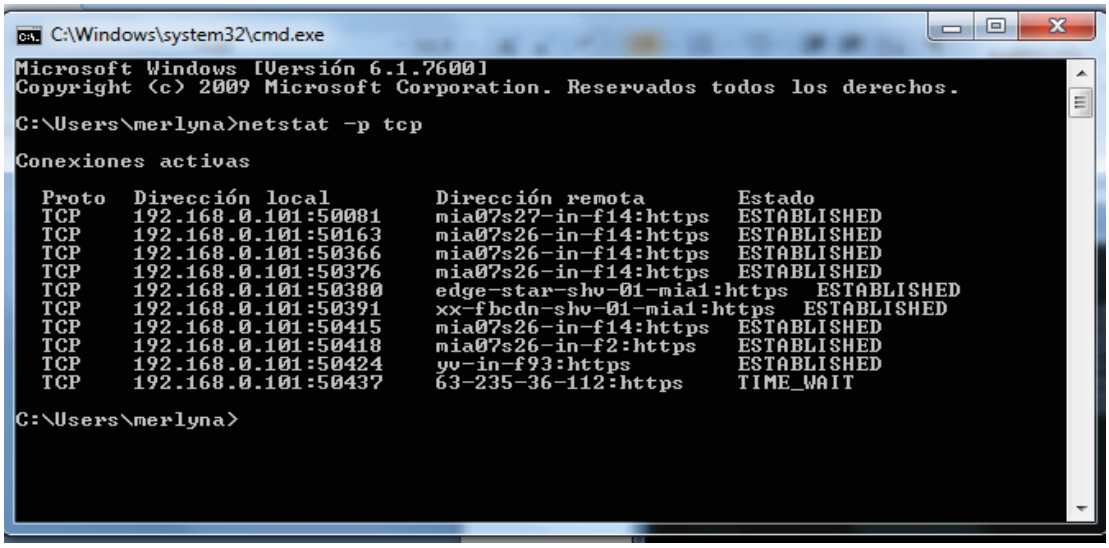


Figura 22. Información del protocolo TCP.

- Netstat –r: muestra la tabla de enrutamiento.

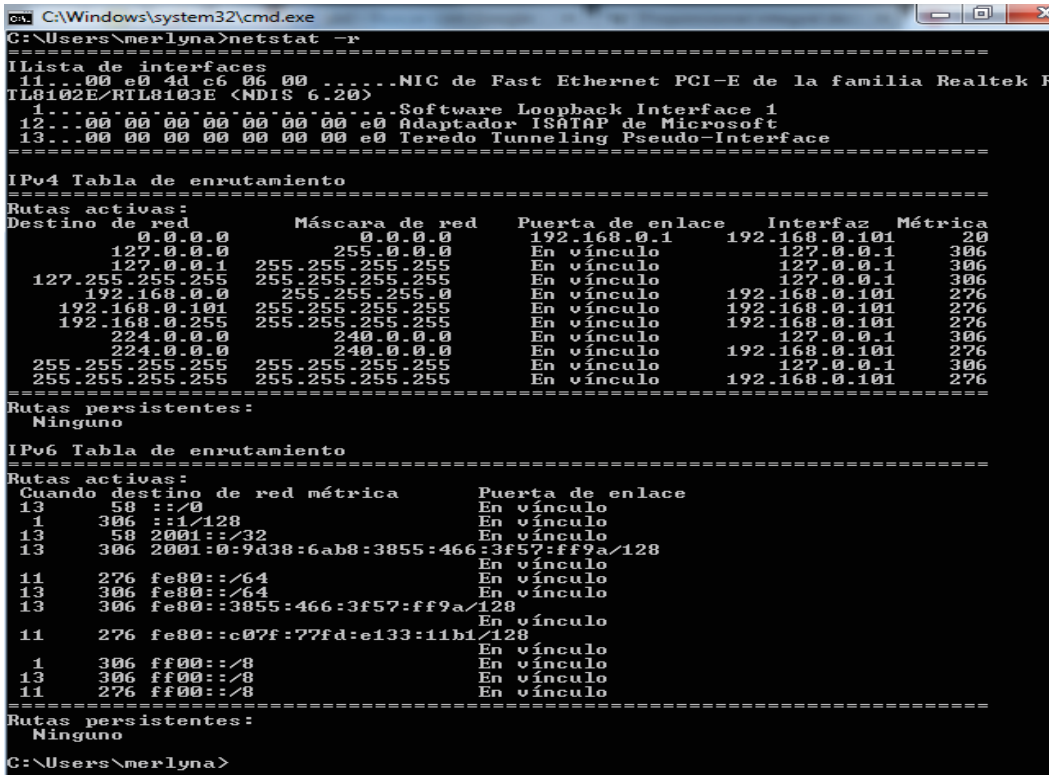


Figura 23. Tabla de enrutamiento.

- Netstat –s: muestra las estadísticas detalladas para cada protocolo.

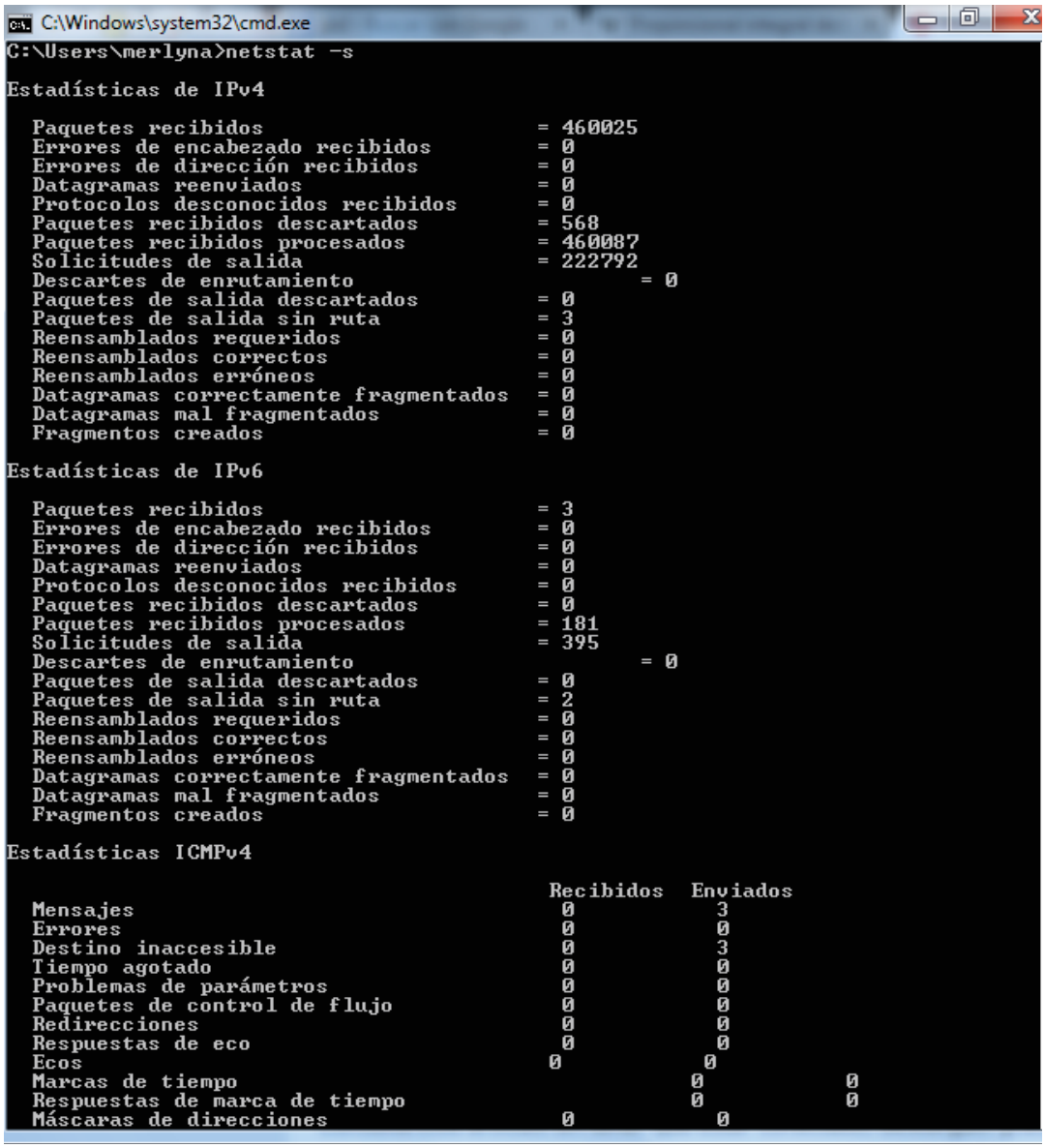


Figura 24. Detalles de cada protocolo.

4.8. TIEMPO ESTIMADO DE LA PRÁCTICA

Una sesión de clase.

4.9. ACTIVIDADES PARA LOS ALUMNOS

Realizar un informe de la práctica.

4.10. EVALUACIÓN

1. ¿Qué formato se obtiene con el comando netstat –aon?
2. ¿Para qué sirve el puerto 3389?
3. Describa brevemente como se identifica si un puerto se encuentra abierto o cerrado.
4. ¿Qué significa el estado “TIME_WAIT”?
5. ¿Qué nos muestra el comando “netstat –e”?

5. CAPITULO V

LABORATORIO 5 “Captura y análisis de tráfico de red, WireShark”

5.1. INTRODUCCIÓN

En el siguiente laboratorio se aprenderá a capturar y analizar el tráfico de una red con la ayuda de la herramienta WireShark.

5.2. DESCRIPCIÓN DE LOS EQUIPOS

- Software free WireShark
- Computador
- Sistema Operativo Windows

5.3. MATERIALES

- Computador
- Sistema Operativo Windows 7

5.4. OBJETIVO GENERAL

Elaborar una práctica de laboratorio de Wireshark con los conocimientos previamente adquiridos y analizar el tráfico de una red.

5.5. OBJETIVOS ESPECÍFICOS

- Aprender el correcto funcionamiento del analizador Wireshark.
- Observar la captura de paquetes y otras funcionalidades a partir del análisis adquirido.
- Conocer la importancia de la herramienta Wireshark.

5.6. TRABAJO PREPARATORIO

Previamente el estudiante debe conocer los temas que a continuación se describen:

5.6.1. Wireshark

Wireshark es un analizador de red, configura la interfaz de red en un modo denominado "modo promiscuo" que puede capturar todo el tráfico que circula por la red. (54)

5.6.2. Características

- Captura de paquetes de datos en vivo de una interfaz de red.
- Muestra los paquetes con información de protocolo muy detallado.
- Permite guardar datos de paquetes capturados.
- Filtra paquetes en muchos criterios.
- Búsqueda de paquetes en muchos criterios.
- Colorea muestra de los paquetes en base a filtros. (55)

5.6.3. Protocolo ARP

El protocolo ARP es un protocolo estándar específico de las redes. Su status es electivo.

El protocolo de resolución de direcciones es responsable de convertir la dirección de protocolo de alto nivel (direcciones IP) a direcciones de red físicas (MAC). (56)

5.6.4. Protocolo DHCP

DHCP significa Protocolo de configuración de host dinámico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración en forma dinámica. Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es distribuir direcciones IP en una red. (57)

5.6.5. Protocolo HTTP

El protocolo HTTP (Protocolo de transferencia de hipertexto) es el protocolo más utilizado en Internet. El propósito del protocolo HTTP es permitir la

transferencia de archivos (principalmente, en formato HTML) entre un navegador (el cliente) y un servidor web localizado mediante una cadena de caracteres denominada dirección URL. (58)

5.6.6. Protocolo DNS

DNS (acrónimo de Domain Name System) es una base de datos distribuida y jerárquica, que almacena la información necesaria para los nombres de dominio. Sus usos principales son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico correspondientes para cada dominio. (59)

5.6.7. Protocolo FTP

El protocolo FTP es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. (60)

5.6.8. Protocolo UDP

El protocolo UDP (Protocolo de datagrama de usuario) ofrece a las aplicaciones un mecanismo para enviar datagramas IP en bruto encapsulados sin tener que establecer una conexión. (61)

5.7. MODO DE TRABAJO

- Iniciar el wizard de instalación. Hacer clic en “Next”. Luego seleccionar “I Agree” en el acuerdo de licencia de uso.

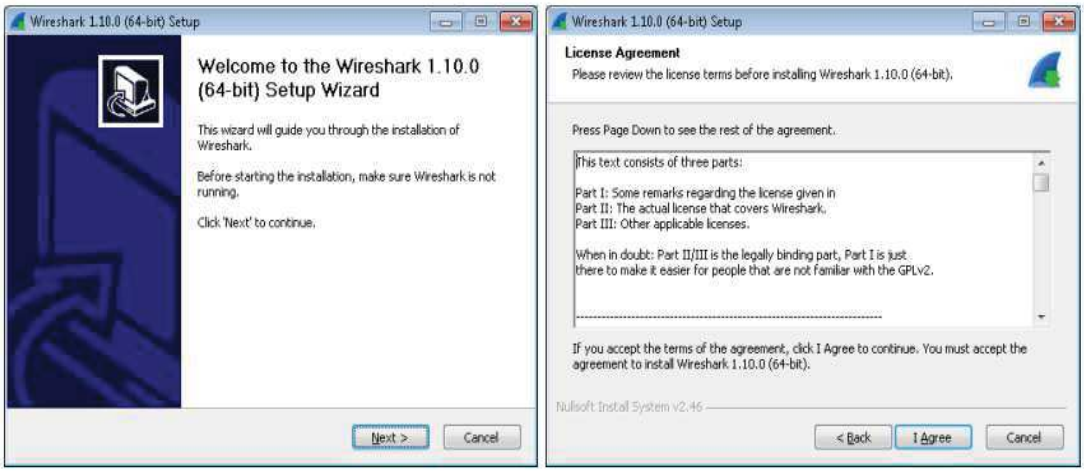


Figura 25. Licencia de Wireshark.

- Seleccionar todos los componentes a instalar y seleccionar las extensiones que se encuentran a continuación:

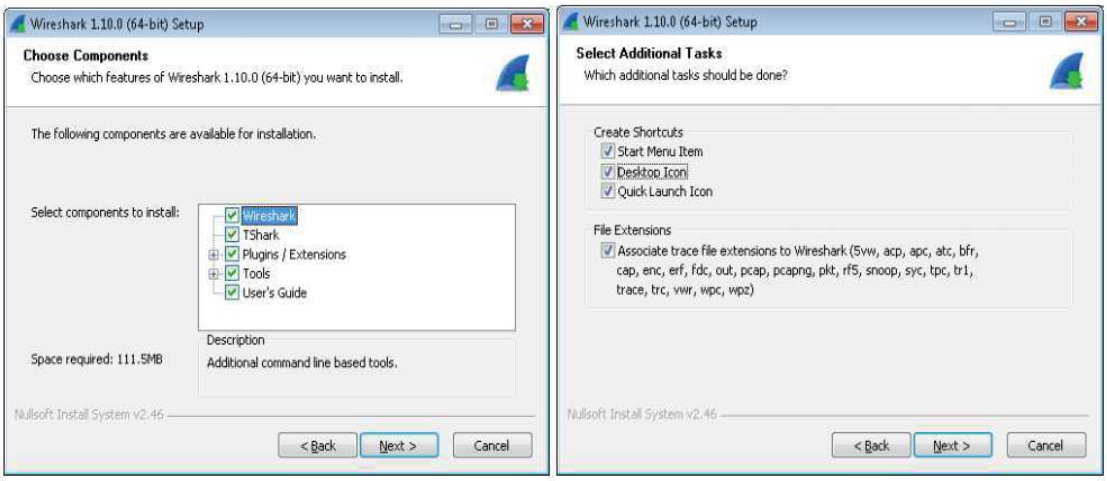


Figura 26. Ventana de instalación de Wireshark.

- Para el funcionamiento de Wireshark es necesaria la instalación de la librería WinPcap. Debido a esto, seleccionar su instalación si no está previamente instalado o si está instalada una versión anterior a la sugerida por el instalador.

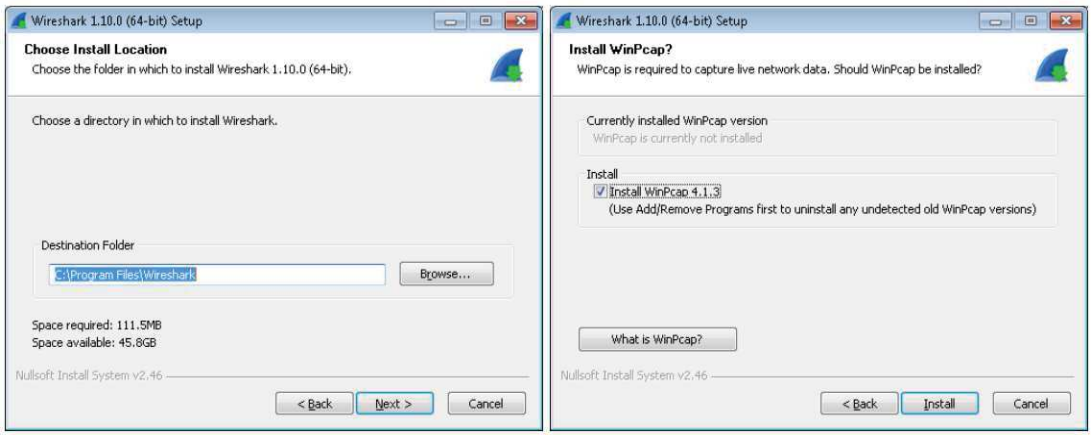


Figura 27. Ubicación e instalación de la librería WinPcap.

- Se inicia la instalación de algunos de los componentes de Wireshark y luego se muestra el wizard de instalación de la versión 4.1.3 de WinPcap.

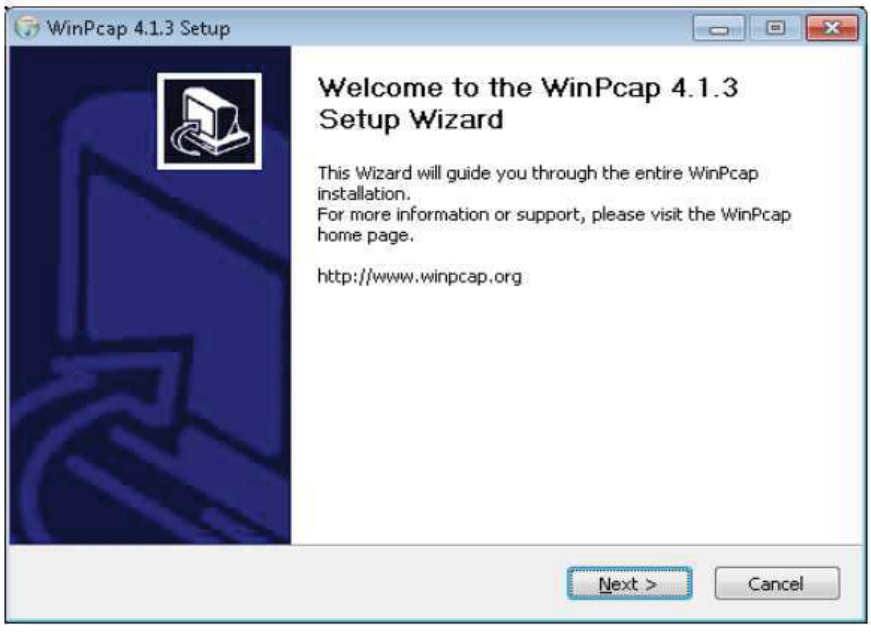


Figura 28. Setup de Wireshark.

- Aceptar las condiciones de la licencia de uso de WinPcap.

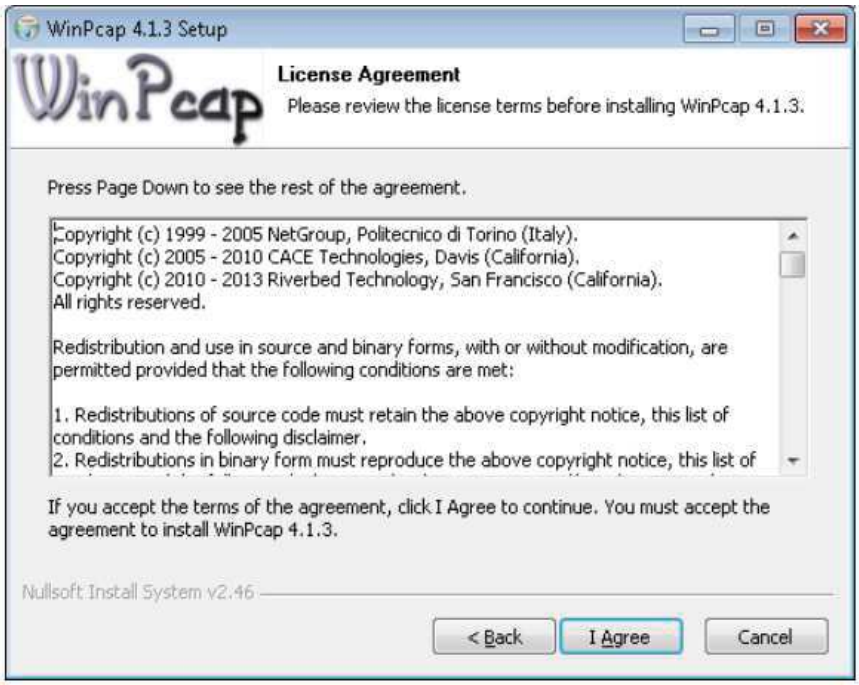


Figura 29. Licencia de WinPcap.

- Seleccionar la opción de iniciar automáticamente el driver de WinPcap al iniciar el sistema.

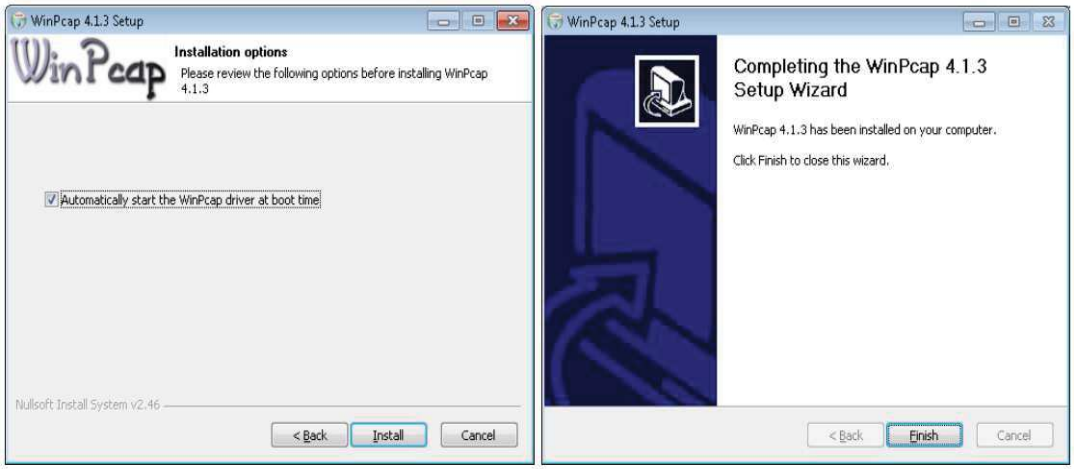


Figura 30. Setup de WinPcap.

- Cerrar la ventana de instalación e iniciar la aplicación.

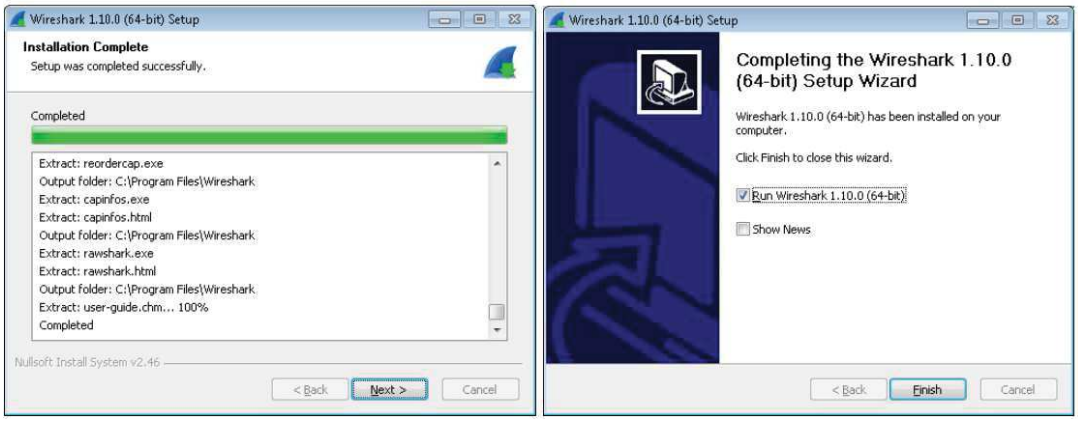


Figura 31. Instalación de WinPcap y finalización de instalación de Wireshark.

- Antes de comenzar la práctica, iniciar un servidor FTP

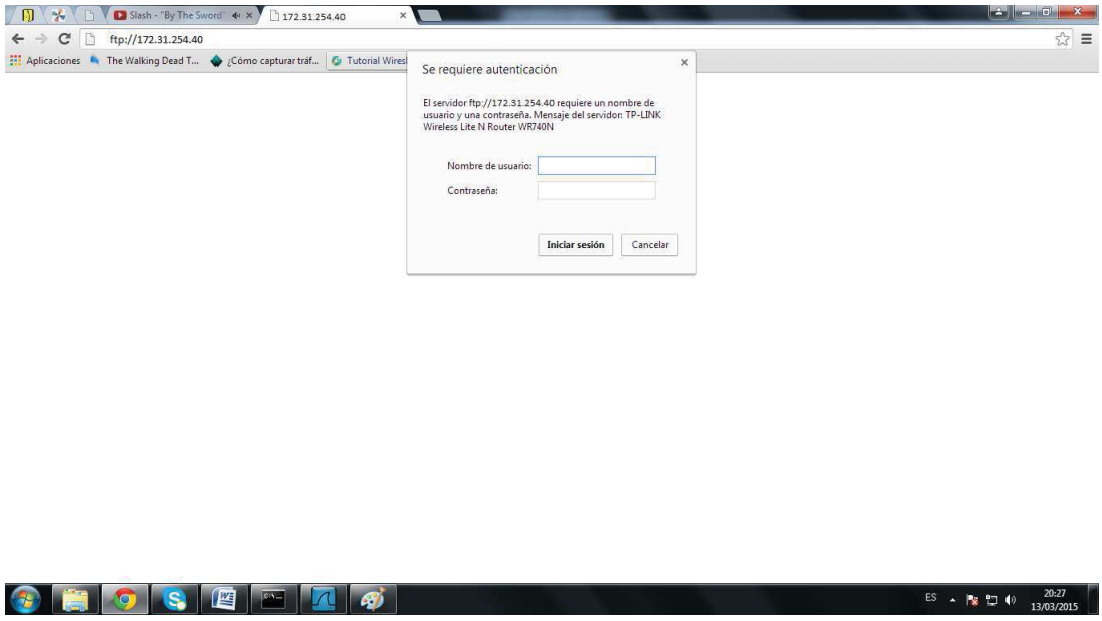


Figura 32. Servidor FTP

El servidor iniciado en este laboratorio tiene el siguiente nombre de usuario y contraseña:

Nombre de usuario: sofia

Contraseña: sofia

Una vez iniciado el servidor iniciar a capturar el tráfico de red con Wireshark

- Abrir Wireshark

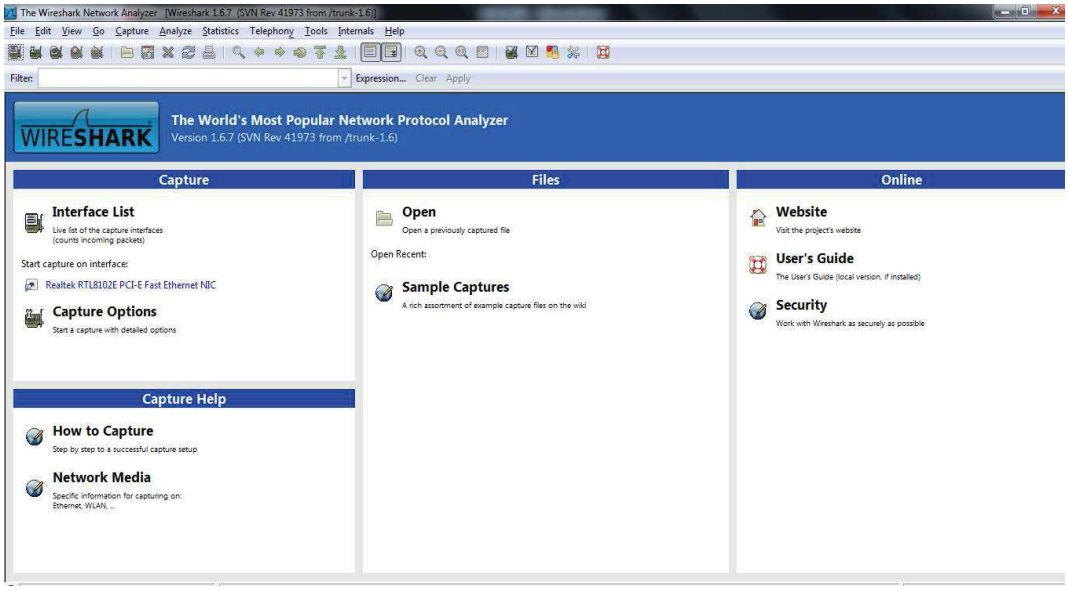


Figura 33. Wireshark.

- Clic en opción “Capture” – submenú “Interfaces”

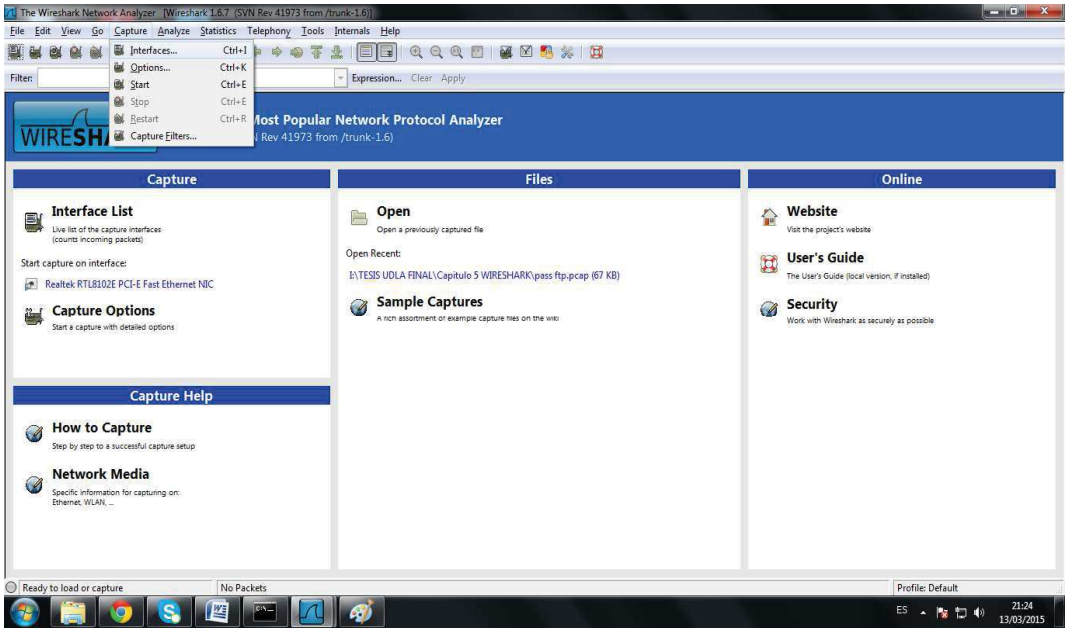


Figura 34. Ventana Wireshark. Menú Capture.

- Identificar la tarjeta de red y dar clic en “Start” para empezar a capturar el tráfico de red.

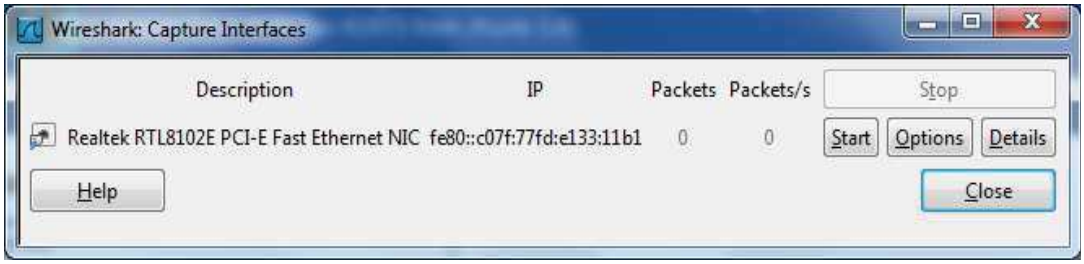


Figura 35. Interfaces

- Filtrar la captura de tráfico con: FTP

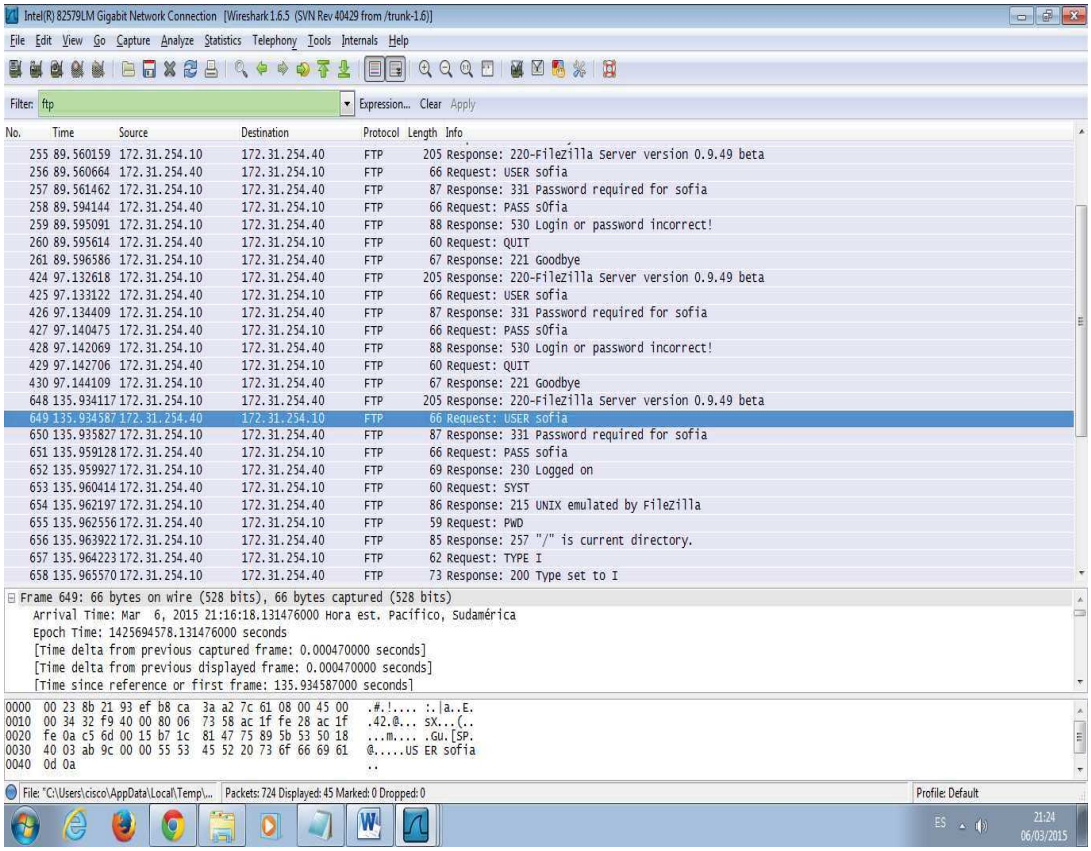


Figura 36. Tráfico de red capturado.

- Analizar la captura e identificar el nombre de usuario y contraseña que fueron asignadas para el servidor FTP.

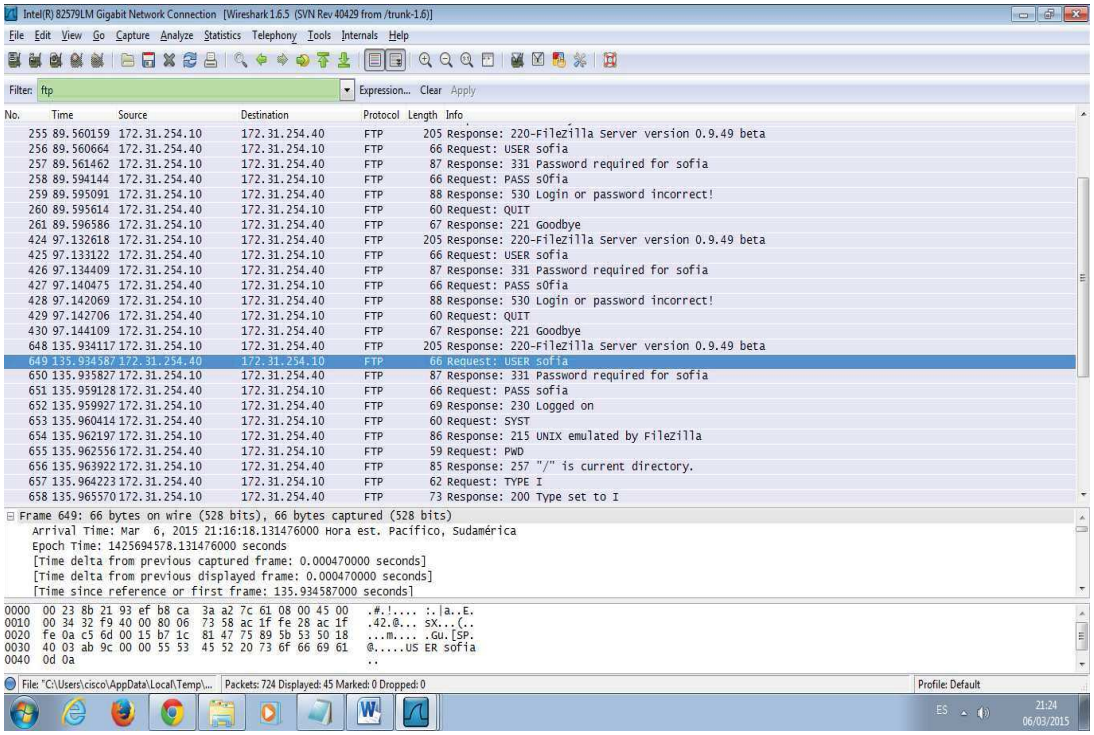


Figura 37.Identificación de contraseña en protocolo FTP

5.8. TIEMPO ESTIMADO DE LA PRÁCTICA

Una sesión de clase

5.9. ACTIVIDADES PARA LOS ALUMNOS

Realizar una descripción de 5 protocolos encontrados en el tráfico de red.

5.10. EVALUACIÓN

1. ¿Qué es Wireshark?
2. ¿Qué es un protocolo FTP?
3. ¿Porque es importante realizar frecuentemente capturas de tráfico de red?
4. ¿Para quése utiliza un analizador de red?
5. ¿Qué es un paquete de datos?

6. CAPITULO VI

LABORATORIO 6 “Escaneo de puertos abiertos por equipo, Advanced Port Scanner”

6.1. INTRODUCCIÓN

En el siguiente laboratorio se identificarán los puertos abiertos y cerrados en una red mediante la herramienta Advanced Port Scanner.

6.2. DESCRIPCIÓN DE LOS EQUIPOS

- Software Free Advanced Port Scanner.
- Computador
- Sistema Operativo Windows

6.3. MATERIALES

- Computador
- Sistema Operativo Windows 7

6.4. OBJETIVO GENERAL

Identificar posibles vulnerabilidades por una incorrecta configuración de firewall mediante el escáner de puertos.

6.5. OBJETIVOS ESPECÍFICOS

- Analizar los puertos abiertos y cerrados con una aplicación gráfica.
- Realizar un análisis de la red.
- Determinar los puertos comunes abiertos en los equipos.

6.6. TRABAJO PREPARATORIO

Previamente el estudiante debe conocer los temas que a continuación se describen:

6.6.1. Advanced Port Scanner

Advanced Port Scanner es una sencilla y reducida herramienta que realiza un examen completo de todos los puertos de conexión del sistema en unos segundos.

6.7. MODO DE TRABAJO

- Abrir la herramienta Advanced Port Scanner

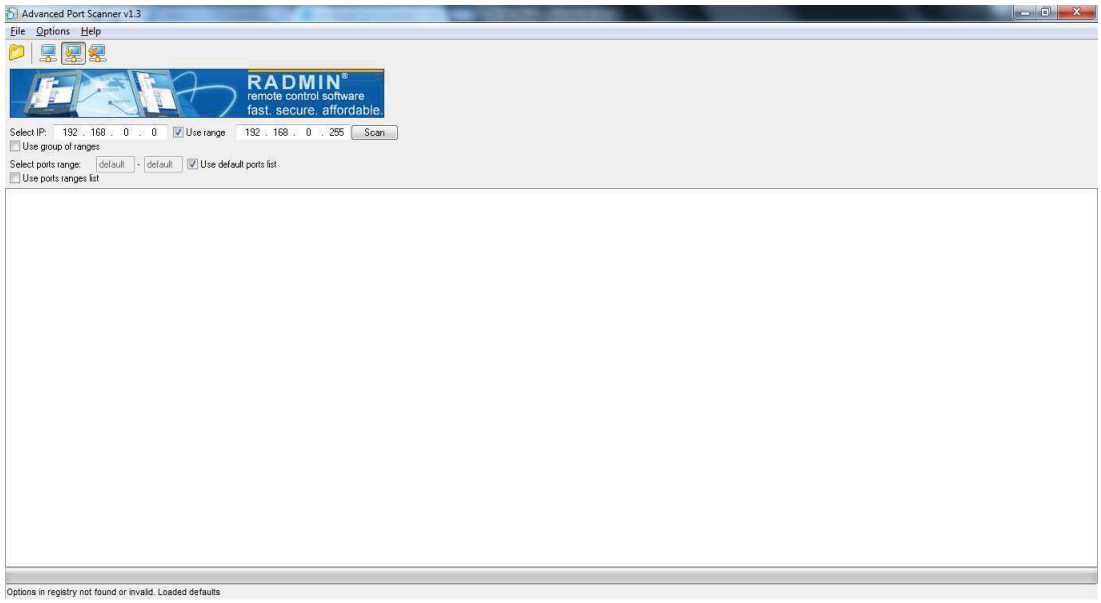


Figura 38. Ventana principal de Advanced Port Scanner.

- Indicar el rango de la IP y clic en el botón “Scan”.

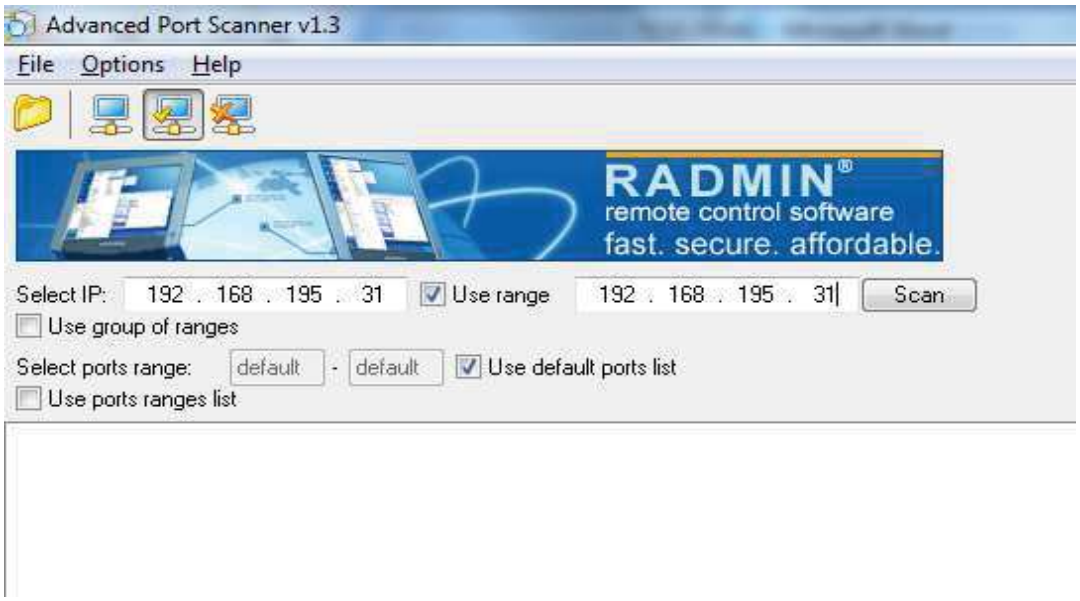


Figura 39. Asignación del rango IP.

- Una vez finalizado el scanner, analizar los puertos abiertos y cerrados.

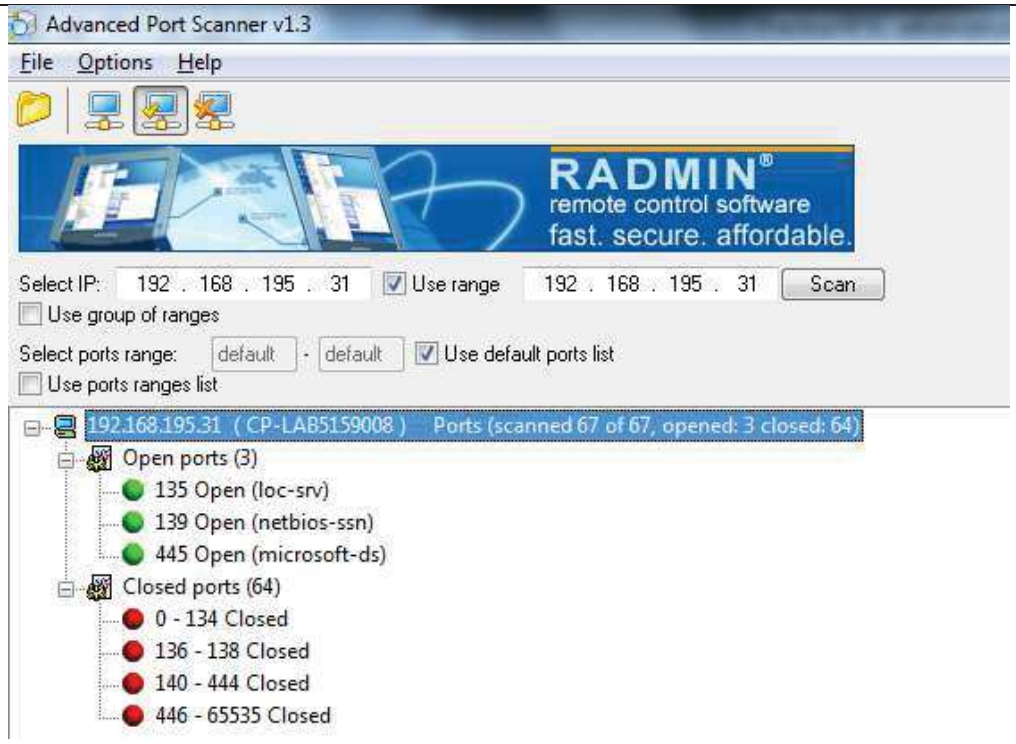


Figura 40. Identificación de puertos abiertos y cerrados.

6.8. TIEMPO ESTIMADO DE LA PRÁCTICA

Una sesión de clase.

6.9. ACTIVIDADES PARA LOS ALUMNOS

Realizar el scanner de puertos de una IP especifica.

6.10. EVALUACIÓN

1. ¿Cómo puedo bloquear puertos?
2. ¿Cuál es el rango de los puertos?
3. ¿Cómo escanear los puertos abiertos en una dirección pública?
4. ¿Porque no es recomendable utilizar los puertos por defecto?
5. Describa 3 puertos no utilizados frecuentemente.

7. CAPITULO VII

LABORATORIO 7 “Elaboración de contraseñas y verificación de complejidad”

7.1. INTRODUCCIÓN

En el siguiente laboratorio se elaborará y verificará una contraseña con un alto índice de complejidad para la seguridad del usuario.

7.2. DESCRIPCIÓN DE LOS EQUIPOS

- Computador
- Sistema Operativo Windows.

7.3. MATERIALES

- Computador
- Sistema Operativo Windows 7
- 5 contraseñas antiguas que fueron utilizadas en sistemas digitales

7.4. OBJETIVO GENERAL

Conocer e identificar los parámetros para la creación de una contraseña de máxima seguridad.

7.5. OBJETIVOS ESPECÍFICOS

- Conocer los tipos de contraseñas existentes.
- Examinar si las contraseñas utilizadas diariamente cuentan con un nivel de seguridad adecuado.
- Identificar cada uno de los caracteres alfanuméricos y especiales que pueden ser utilizados en la creación de una contraseña.

7.6. TRABAJO PREPARATORIO

Previamente el estudiante debe conocer los temas que a continuación se describen:

7.1.1. Contraseña

Una Contraseña o Clave personal, también denominada con su anglicismo Password, es un código o combinación de caracteres, utilizado como medida de seguridad y cuyo objeto es el de proteger el “acceso no autorizado” a un recurso determinado. (62)

7.1.2. Parámetros de una contraseña

Una contraseña segura:

- Tiene ocho caracteres como mínimo.
- No contiene el nombre de usuario, el nombre real o el nombre de la empresa.
- No contiene una palabra completa.
- Es significativamente diferente de otras contraseñas anteriores.
- Está compuesta por caracteres de cada una de las siguientes cuatro categorías:

Tabla 3. Categorías de caracteres permitidos para una contraseña. (63)

Categoría de caracteres	**Ejemplos**
Letras mayúsculas	A, B, C
Letras minúsculas	a, b, c
Números	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Símbolos del teclado (todos los caracteres del teclado que no se definen como letras o números) y espacios	¡”#$%&/(()

7.1.3. Tipos de contraseñas

- **Cadenas de caracteres**

Las contraseñas son cadenas de caracteres, números y símbolos. Tener acceso a un teclado proporciona un método para introducir este tipo de passwords. Las contraseñas pueden ir de las más sencillas, como los tres números para acceder a ciertas plazas de garaje, hasta las más complicadas combinaciones de caracteres, números y símbolos que se recomienda emplear para proteger la información más sensible. (64)

- **Cadenas de caracteres más un token**

En el siguiente nivel, los passwords requieren una cadena de caracteres, números y símbolos más un token o ficha de algún tipo. Por ejemplo los cajeros automáticos. Para acceder a éstos se necesita una tarjeta y un número personal identificativo o PIN. Se consideran más robustos ya que si un usuario pierde u olvida alguno de los dos requerimientos el acceso será denegado. (65)

- **Password biométricos**

Consisten en utilizar alguna característica física no reproducible, como las huellas digitales o el aspecto de la cara, para permitir el acceso. Un ejemplo es el escáner de retina en el cual el interior del ojo se fotografía para la posterior identificación del sujeto. La retina contiene un patrón único de distribución de vasos sanguíneos fácilmente apreciable y que se puede utilizar para la identificación del individuo. Los passwords biométricos son los que se consideran más sofisticados y más seguros de todos los passwords. Sin embargo, un password que se pueda transportar en el dedo o en el ojo no tiene porqué ser más seguro que uno transportado en la cabeza si el software está bien configurado. (66)

7.7. MODO DE TRABAJO

- Ingresar a la pag. Web http://www.passwordmeter.com/ y comprobar el nivel de las contraseñas creadas.

Ejemplo 1: Udla1

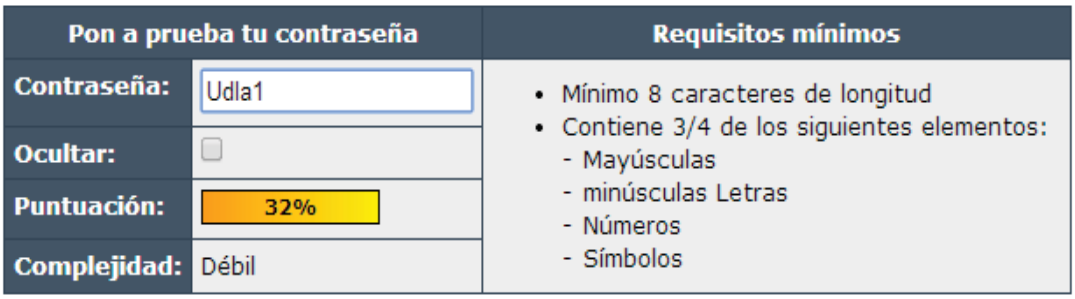


Figura 41. Contraseña con un nivel de seguridad bajo.

Ejemplo 2: UdelasAmericas

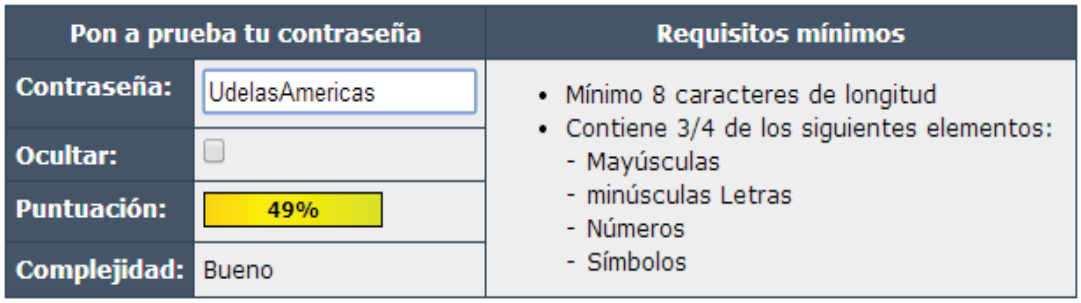


Figura 42. Contraseña con un nivel de seguridad medio.

Ejemplo 3: #uD1a2014.

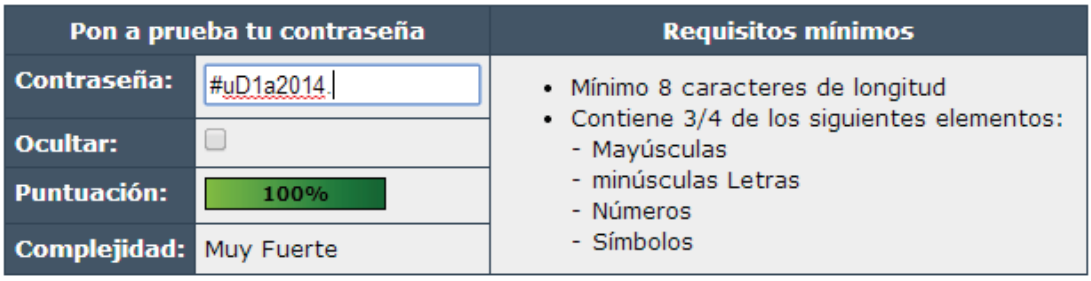


Figura 43. Contraseña con un nivel de seguridad alto

7.8. TIEMPO ESTIMADO DE LA PRÁCTICA

Una sesión de clase.

7.9. ACTIVIDADES PARA LOS ALUMNOS

Crear 6 contraseñas

N° contraseñas	Nivel de segurida
2	Baja
2	Media
2	Alta

7.10. EVALUACIÓN

1. ¿Qué es una contraseña?
2. ¿Cuál es el tiempo recomendado para cambiar las contraseñas?
3. Escriba tres contraseñas que considere seguras
4. ¿Qué es una contraseña biométrica?
5. ¿Qué tipos de caracteres se puede utilizar en una contraseña?

8. CAPITULO VIII

LABORATORIO 8 “Elaboración de Certificados de seguridad, llave pública y privada”

8.1. INTRODUCCIÓN

En el siguiente laboratorio se generará un certificado de seguridad, llave pública y privada mediante la herramienta Gpg4win.

8.2. DESCRIPCIÓN DE LOS EQUIPOS

- Computador
- Sistema Operativo Windows

8.3. MATERIALES

- Computador
- Software Gpg4win
- Sistema Operativo Windows 7

8.4. OBJETIVO GENERAL

Crear y certificar una llave pública.

8.5. OBJETIVOS ESPECÍFICOS.

- Conocer los beneficios de tener una llave priva y pública
- Crear y utilizar una llave pública y privada
- Exportar y certificar una llave pública.

8.6. TRABAJO PREPARATORIO

Previamente el estudiante debe conocer los temas que a continuación se describen:

8.6.1. Llave pública y privada

El siguiente ejemplo se explicará brevemente como funciona una llave pública y privada.

“Digamos que tengo que enviar una información importante pero no puedo confiar en el mensajero. Por lo tanto, escribo mi mensaje en un papel, lo meto en una caja de metal, le pongo un candado y lo envío. La caja llega a su destino sin problema, pero el destinatario no puede leerla, pues no puede abrir el candado. Si le envío la llave, aunque sea por otro medio -otro mensajero-, puede verse que hay un nivel de riesgo, al comprometer la seguridad de la llave, confiándola a extraños. Así funciona el ciframiento convencional.

Cambiemos ahora un poco la situación. Digamos ahora que el destinatario me envía previamente un candado, abierto. Es *su* candado, yo no puedo abrirlo si se cierra, pues la llave solamente la tiene él. La llave permanecerá segura en su poder. Recibo el candado, escribo mi mensaje, lo meto en la caja y cierro la caja con el candado que recibí. A partir de ese momento, ni yo mismo, que escribí el mensaje, puedo ya verlo. Está protegido por el candado. Envío la caja y el destinatario la abre con su llave. Así funciona la llave pública y privada. La llave pública es el candado y su pareja es la llave de metal (llave privada) que lo abre. Por supuesto, esta pareja debe ser fabricada una para la otra.

La versión criptográfica es un par de secuencias de caracteres, que usadas por un programa adecuado pueden cifrar y descifrar un texto. La llave pública solamente puede cifrar. La llave privada puede descifrar o hacer las dos cosas, aunque esto último no es tan importante. Yo recibo la llave pública de mi destinatario y con ella cifro la información que le enviaré. Una vez cifrada, yo mismo no puedo ver la información. Envío esta información, en un correo por ejemplo, el destinatario la recibe y la descifra con su llave privada.

No hay peligro en publicar las llaves públicas porque son precisamente para eso. Y están diseñadas de manera que es muy difícil -casi imposible con la tecnología actual- deducir una llave privada de una pública. Y claro, ambas llaves deben ser generadas previamente, como un par correspondiente, igual que el candado y su llave.” (67)

8.7. MODO DE TRABAJO

- Descargar el Software Gpg4win del siguiente link: http://www.gpg4win.org/
- Instalar el software GNU Privacy Assistant – Key Manager

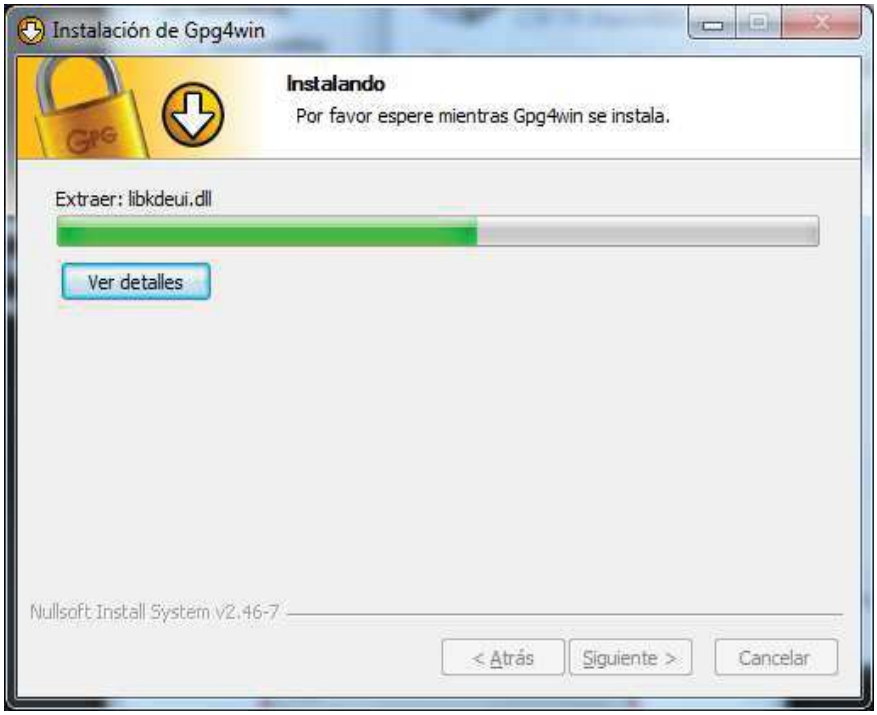


Figura 44. Instalación de GNU Privacy Assistant – Key Manager

- Una vez abierto GNU, crear una llave o clave privada.

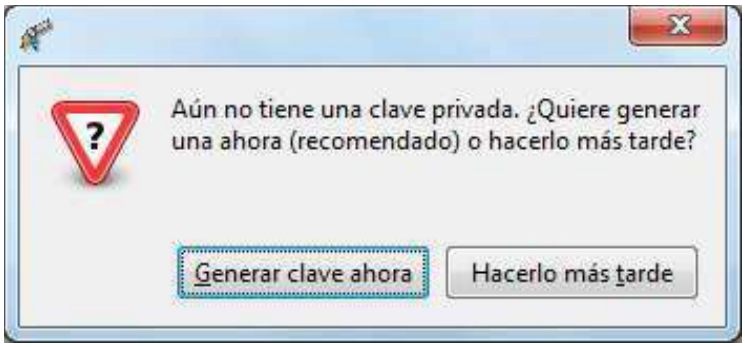


Figura 45. Generación de Clave

- Introducir el nombre de usuario

Figura 46. Nombre de usuario.

- Ingresar el mail del usuario

Figura 47. Mail de usuario.

- Elegir “Crear copia de seguridad” (recomendado)

Figura 48. Copia de seguridad

- Crear una contraseña: Ud1a20l5

Figura 49. Contraseña

- Volver a repetir la contraseña.

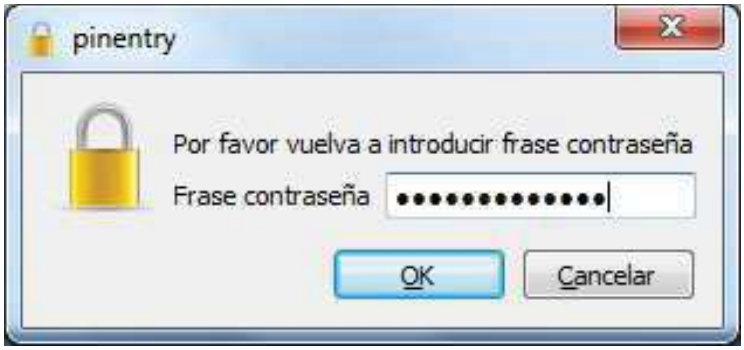


Figura 50. Repetición de contraseña.

- Elegir la carpeta donde se guardará el archivo con la copia de seguridad de las llaves generadas

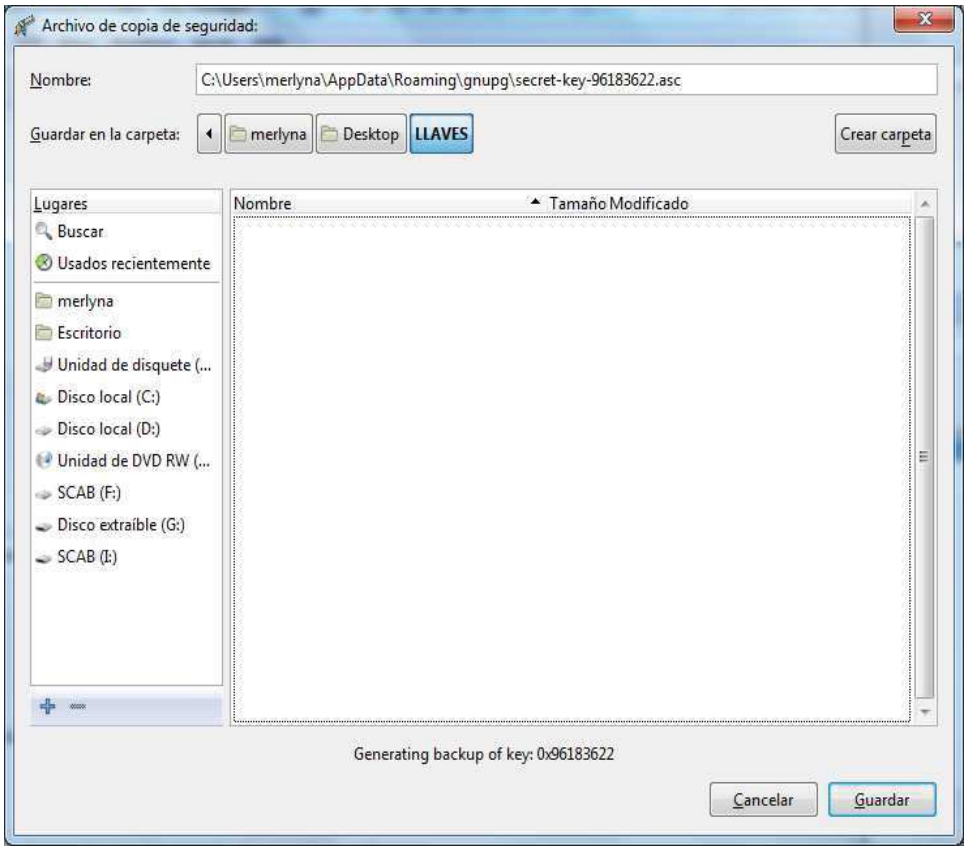


Figura 51. Carpeta para guardar copia de seguridad.

- La llave privada ha sido creada.

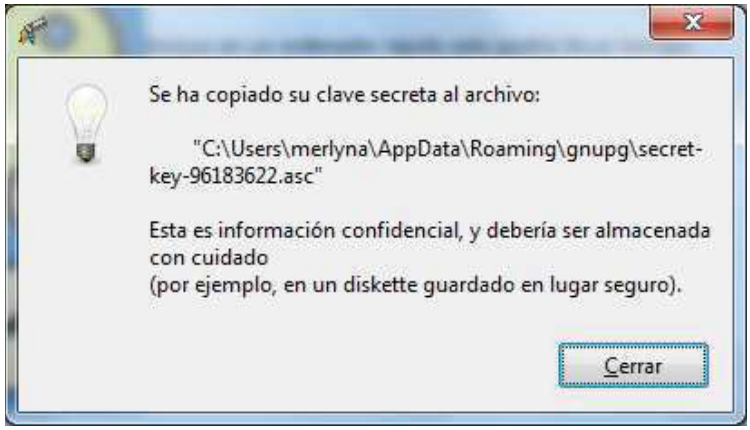


Figura 52. Mensaje de creación de llaves.

- Verificar información introducida.

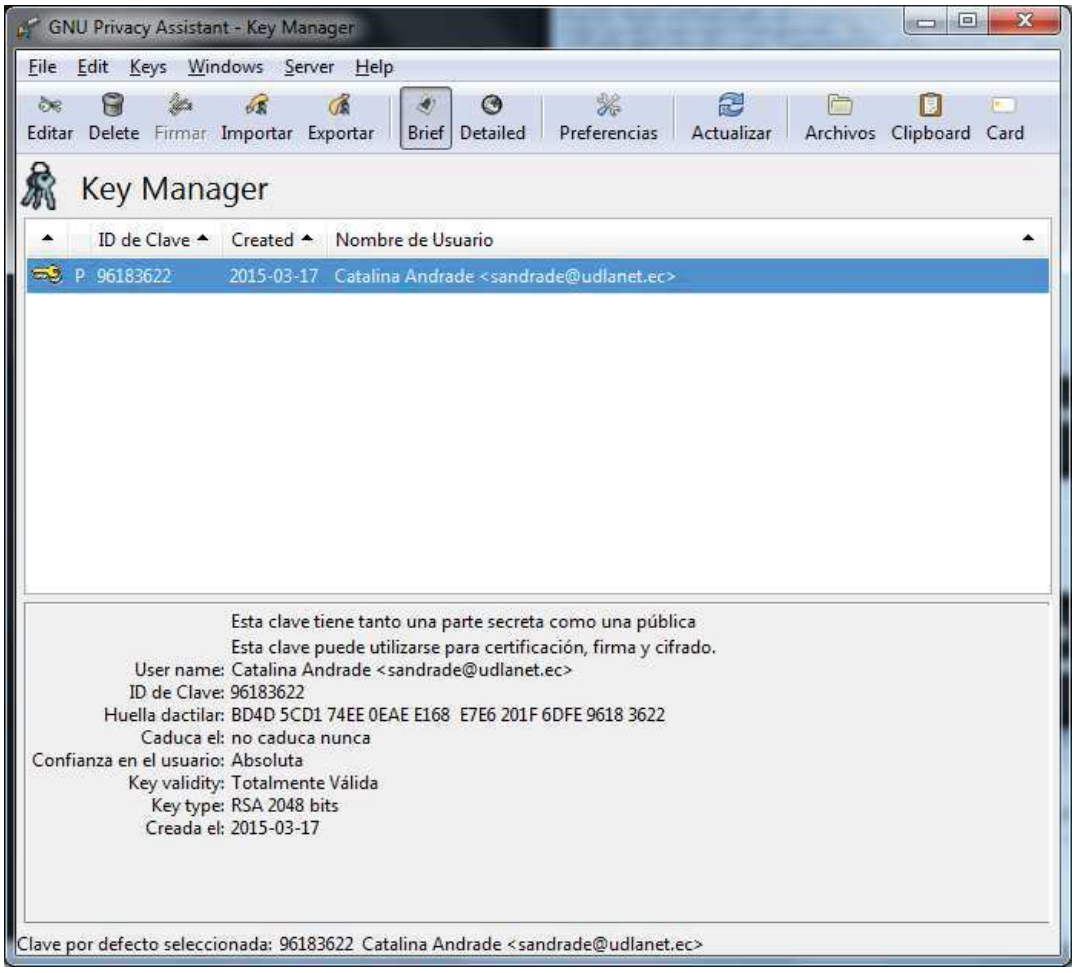


Figura 53. Información del usuario creado.

- Para exportar la llave pública, seleccionar el usuario y dar clic en la opción “Exportar”

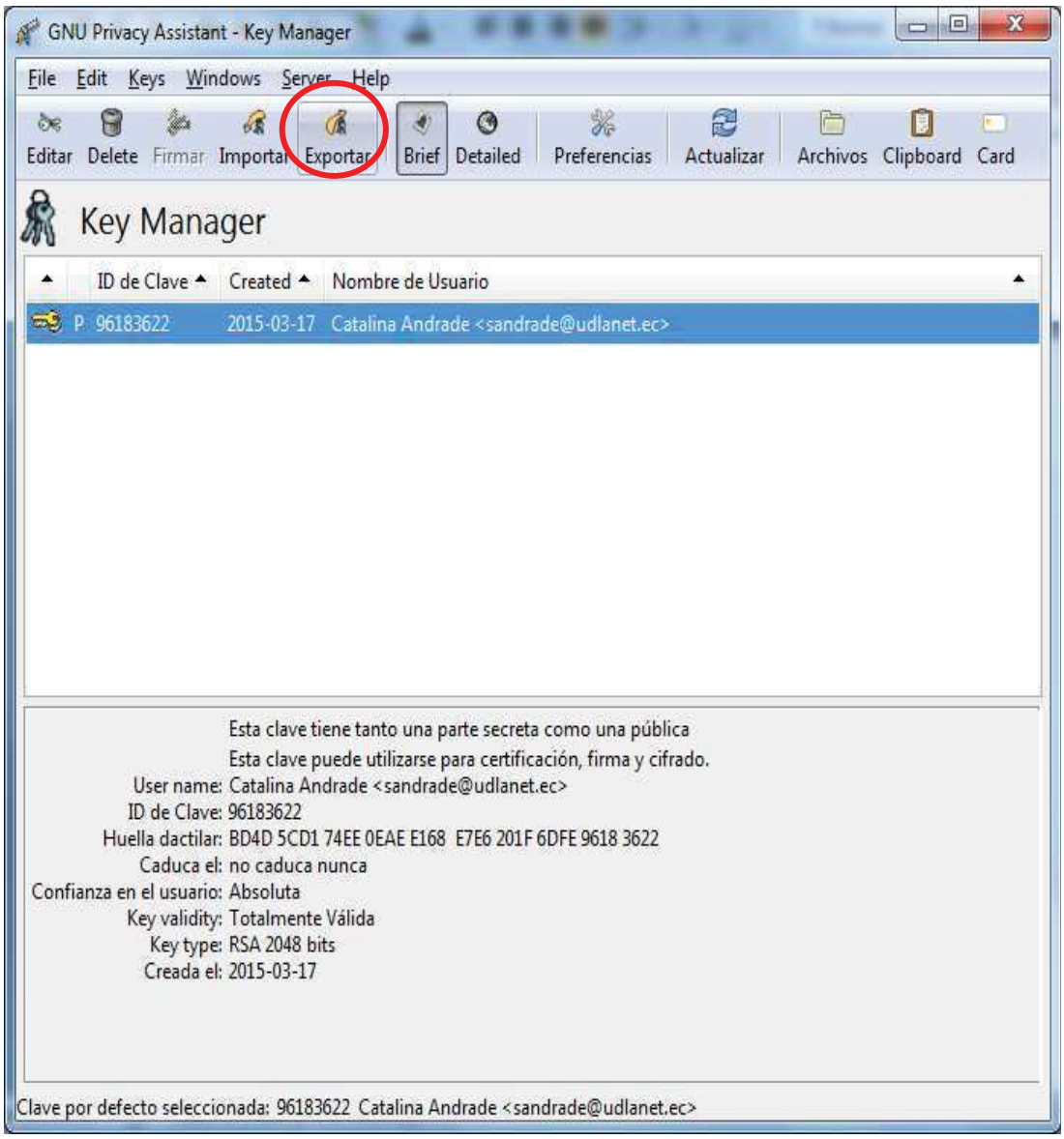


Figura 54. Exportar usuario.

- Especificar la ubicación donde se guardará el archivo con la información de la llave pública.

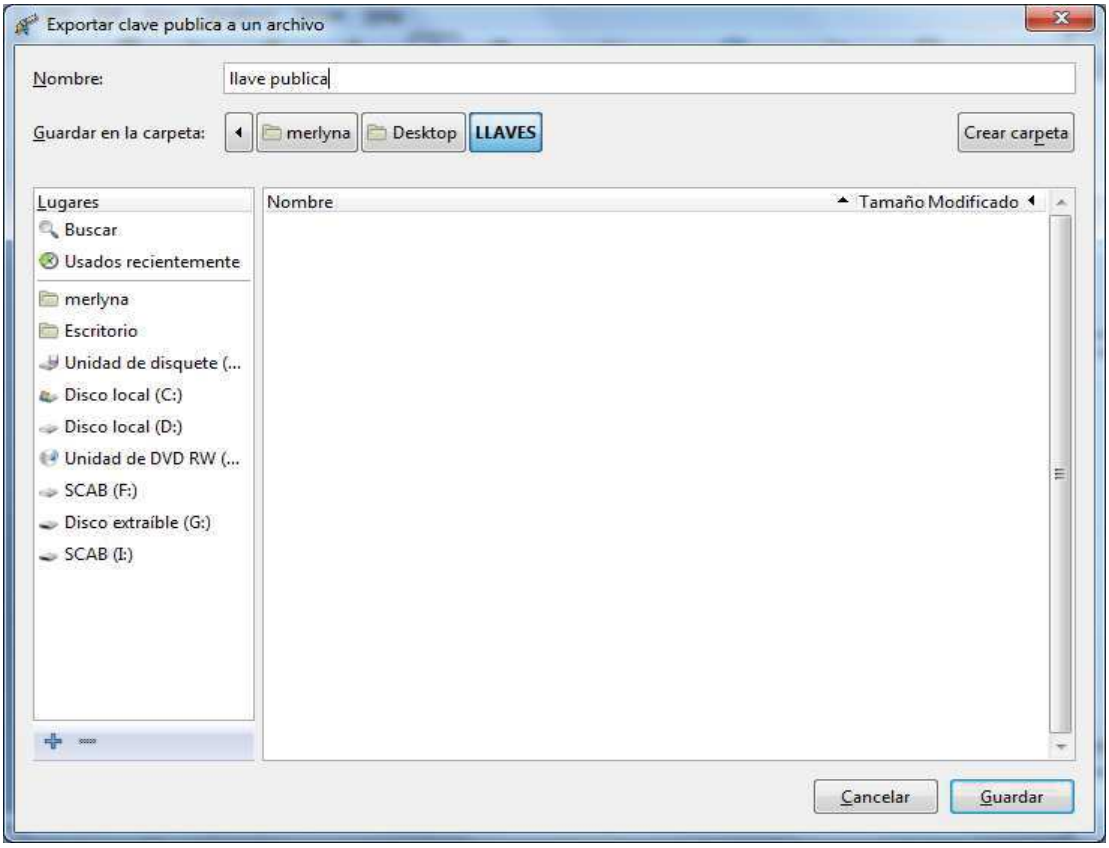


Figura 55. Ubicación donde se guardará la información de la llave pública.

- Clic en guardar y si se realizo correctamente todos los pasos se tendrá el documento en la dirección señalada.

Figura 56. Mensaje indicando la ruta donde se exportó la llave pública.

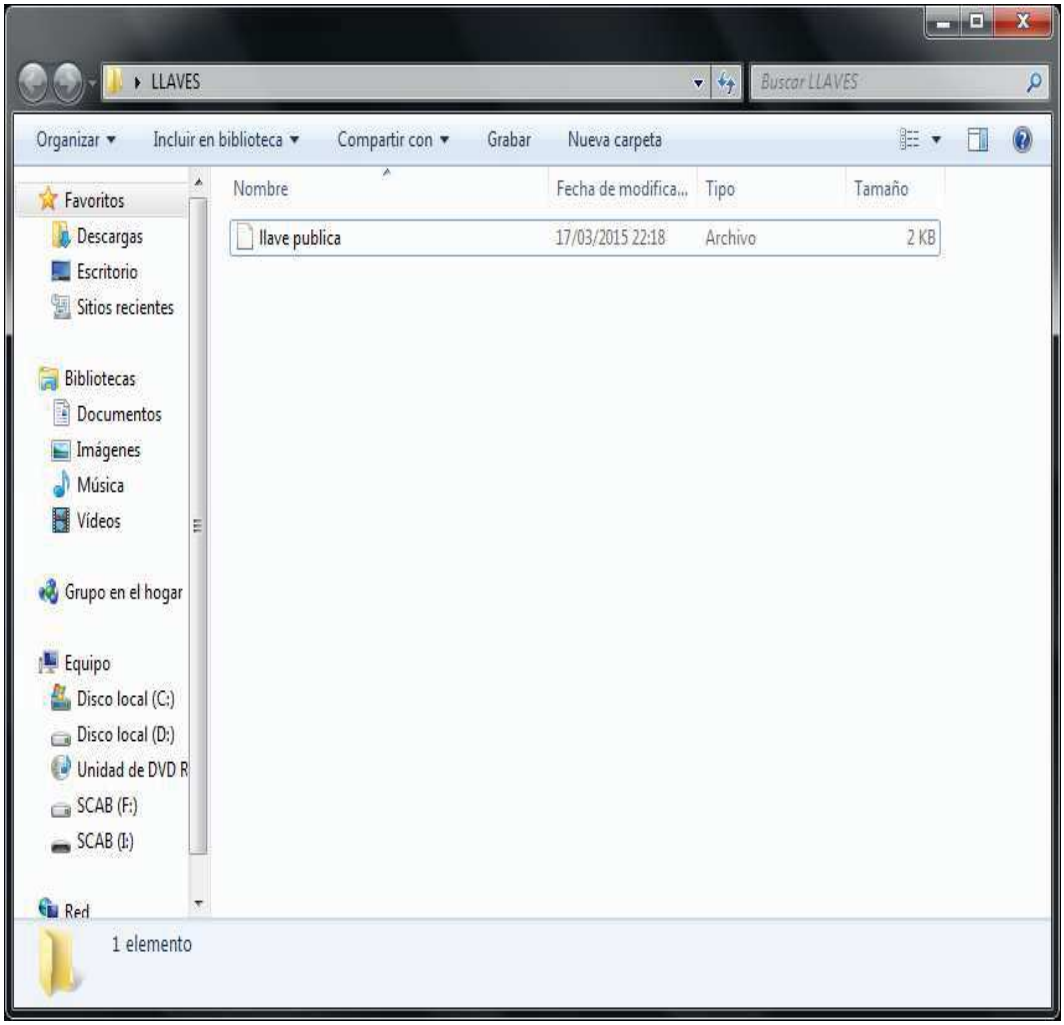


Figura 57. Archivo “llave pública”.

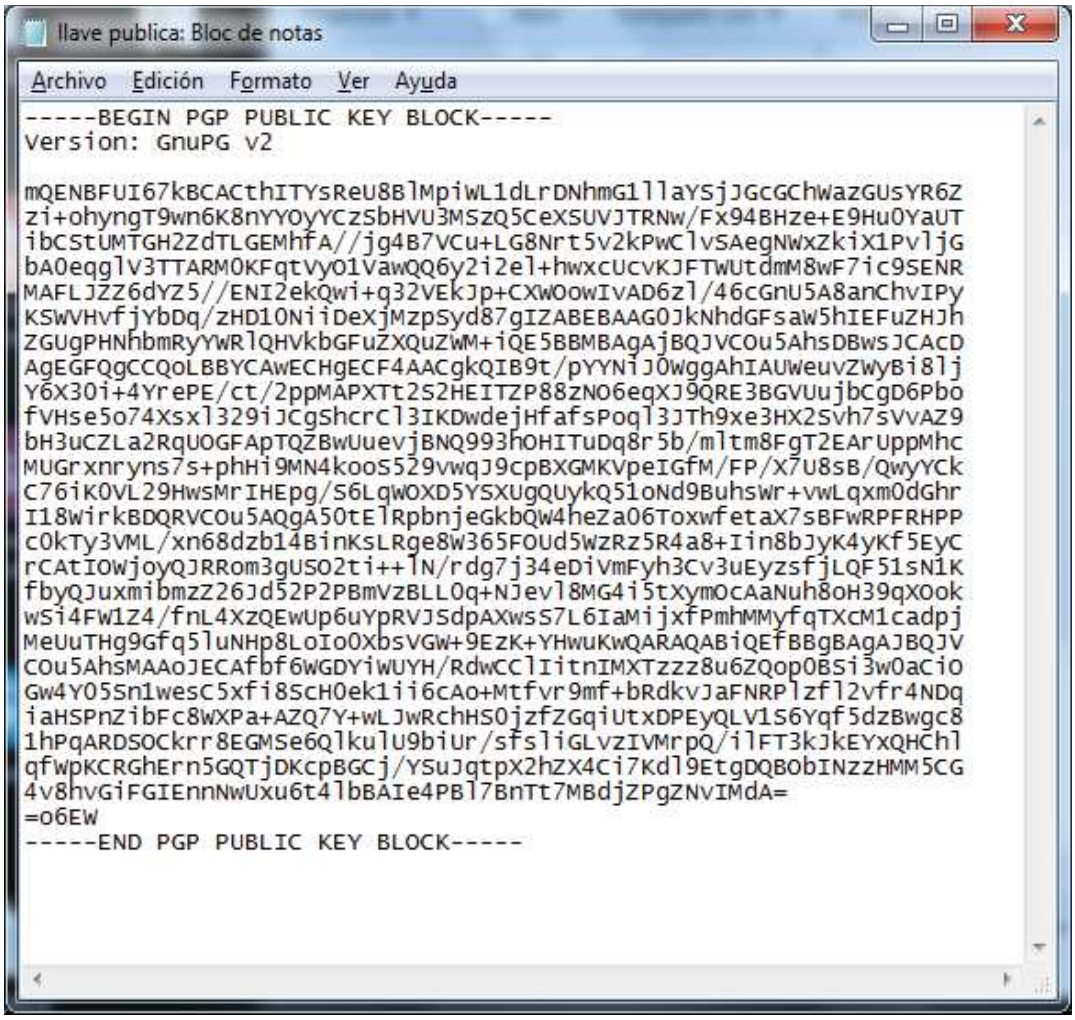


Figura 58. Archivo "llave pública" encriptado.

- Una vez ubicado el archivo de la llave pública, enviar por medio del correo electrónico a la persona que se le asignará permiso de confidencialidad.

Figura 59. Envío por correo electrónico.

- Descargar el archivo, abrir la herramienta “Kleopatra”, clic en “Import Certificates”.

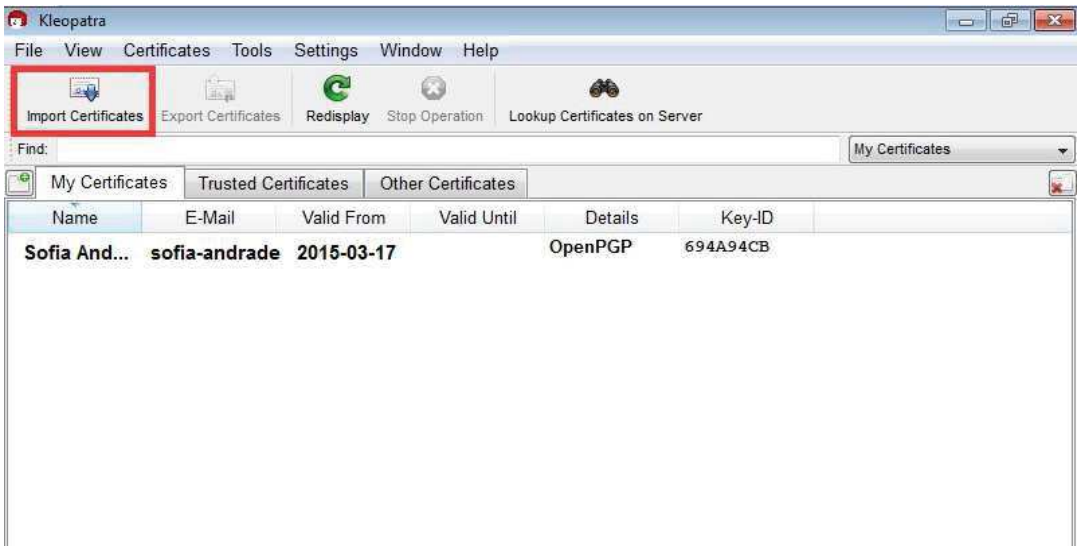


Figura 60. Import Certificates.

- Importar el archivo “llave pública”

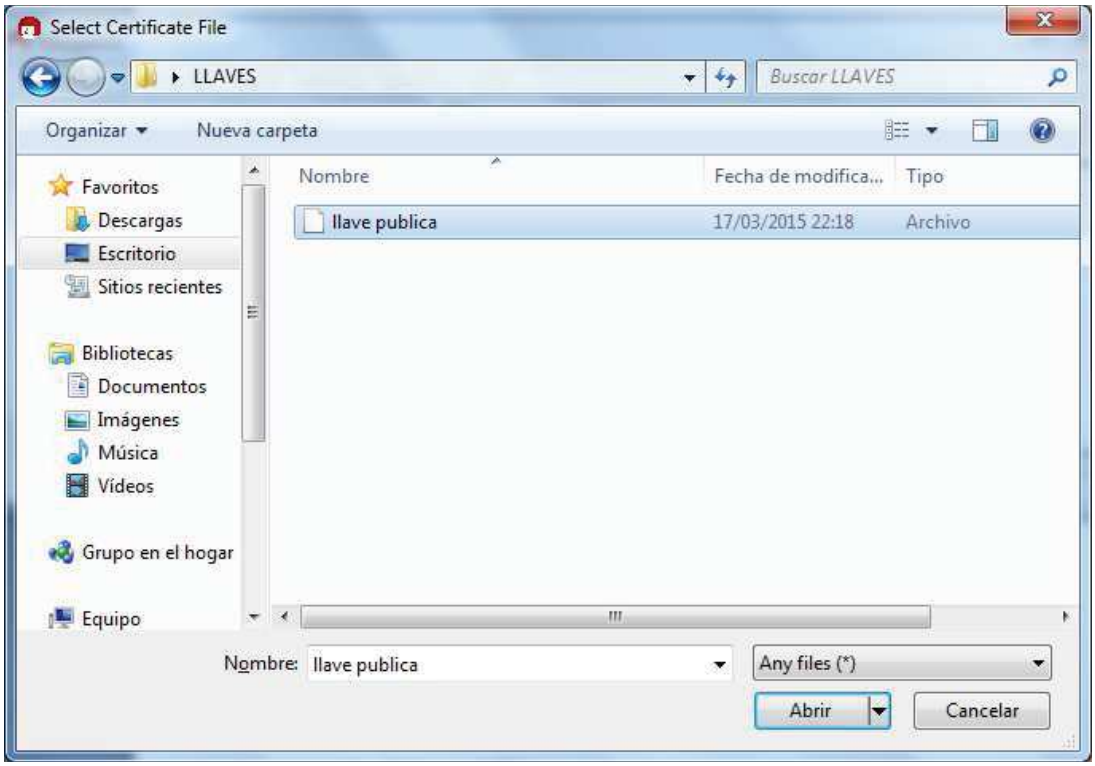


Figura 61. Ubicación del archivo “llave pública”

- La “llave publica” ha sido importada

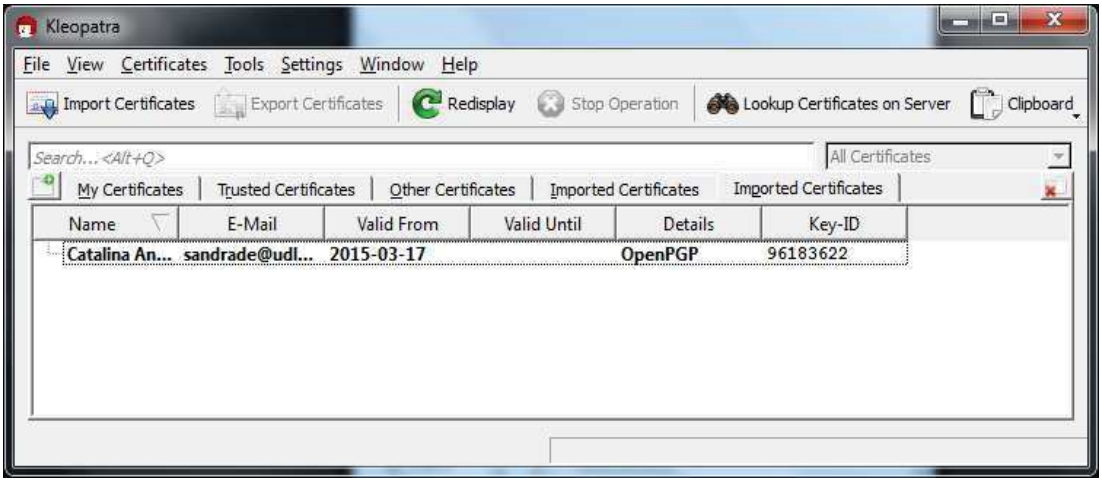


Figura 62. Herramienta “Kleopatra”

- Para firmar la llave pública, clic derecho en el usuario y elegir la opción “Certify Certicate”

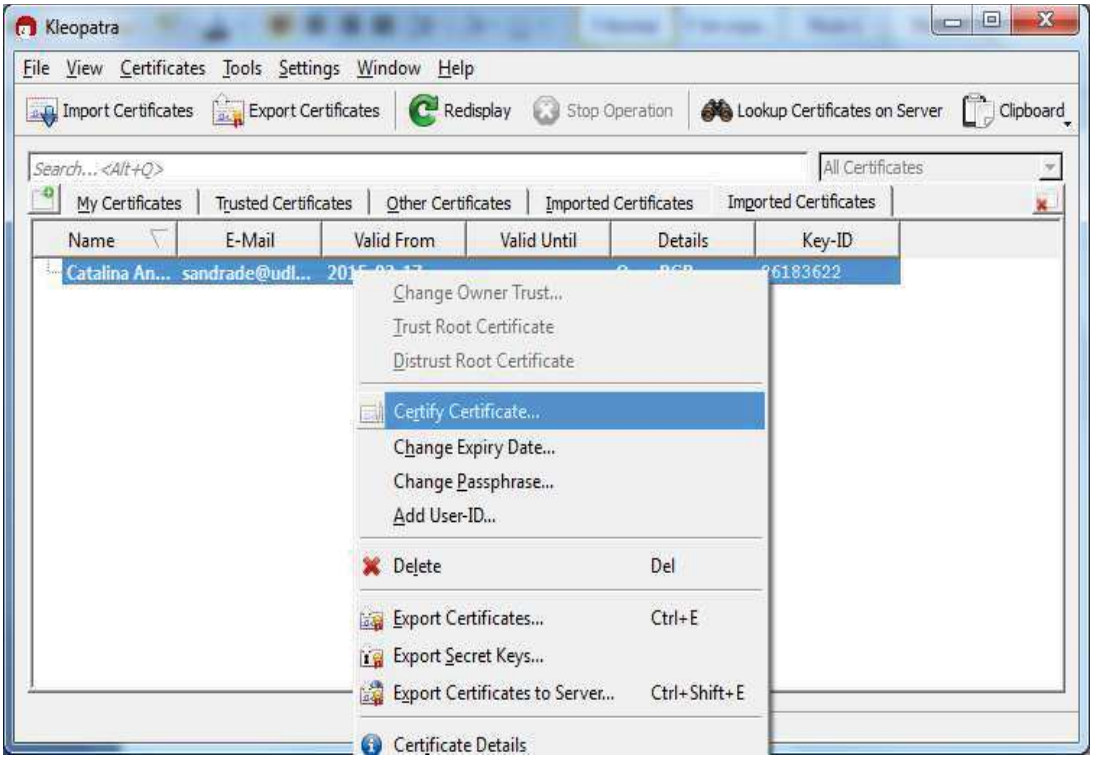


Figura 63. Certificación del usuario.

- Elegir el usuario y habilitar la opción “I have verified the finger print”

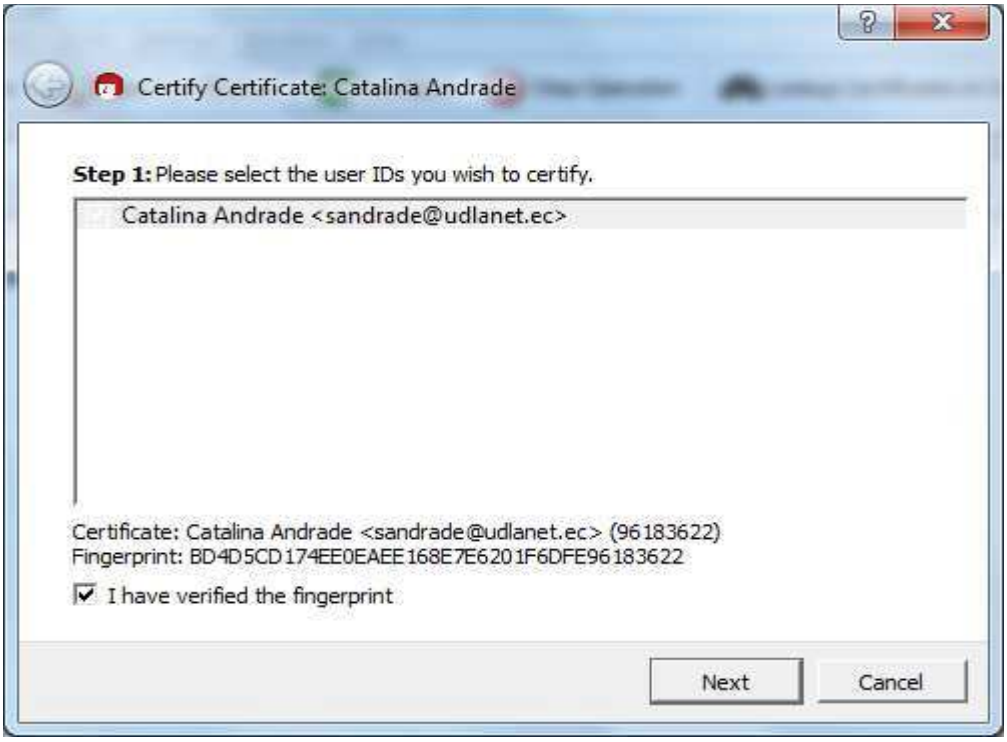


Figura 64. Otorgar derechos de certificación.

- Escoger la opción que indica que se “certificará por mí”.

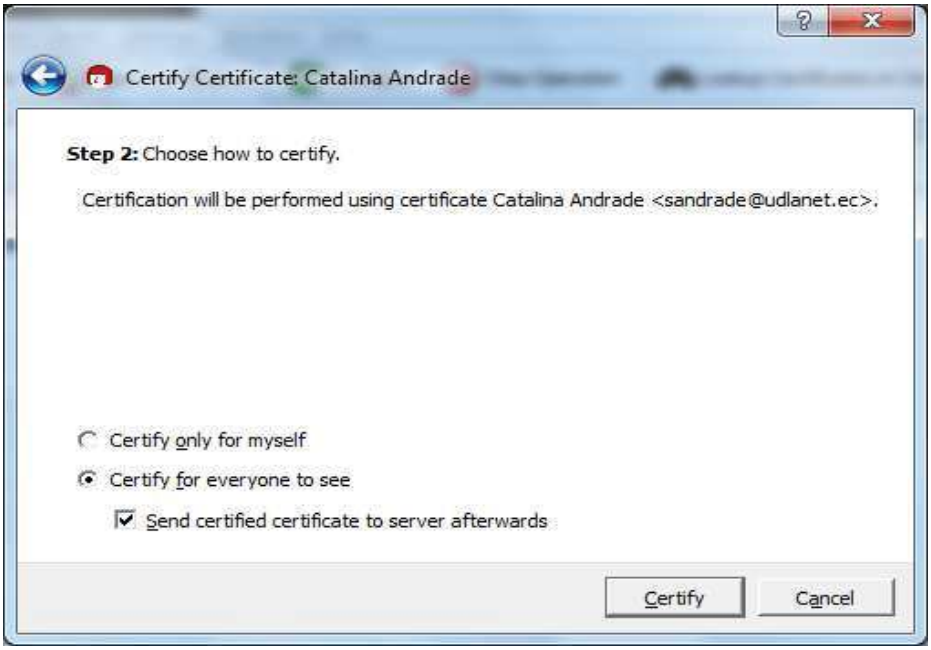


Figura 65. Usuario Certificado.

8.8. TIEMPO ESTIMADO DE LA PRÁCTICA

Una sesión de clase

8.9. ACTIVIDADES PARA LOS ALUMNOS

Crear una llave pública y certificarla para que otro usuario tenga permiso de confidencialidad.

8.10. EVALUACIÓN

1. ¿Qué es una llave pública y privada?
2. ¿Porque es importante crear una llave pública?
3. ¿Con que extensión se crea el archivo de una llave pública?
4. ¿Porque es importante tener una copia de seguridad de la llave pública?
5. ¿Cómo funciona una llave pública y privada?

9. CAPITULO IX

LABORATORIO 9 “Encriptación de información, CRYPTAINER LE y DeCypherIT”

9.1. INTRODUCCIÓN

En el siguiente laboratorio se conocerá la importancia de encriptar la información mediante la herramienta Cryptainer Le.

9.2. DESCRIPCIÓN DE LOS EQUIPOS

- Computador
- Sistema Operativo Windows.

9.3. MATERIALES

- Computador
- Software Cryptainer Le
- Software DeCypherIT
- Sistema Operativo Windows 7

9.4. OBJETIVO GENERAL

Encriptar y desencriptar un archivo con la ayuda de los software Cryptainer Le y DeCypherIT

9.5. OBJETIVOS ESPECÍFICOS.

- Encriptar un archivo mediante un software grafico.
- Conocer los beneficios que tiene encriptar un archivo.

9.6. TRABAJO PREPARATORIO

Previamente el estudiante debe conocer los temas que a continuación se describen:

9.6.1. Cryptainer Le

Cryptainer LE es un programa gratuito de encriptación que crea múltiples unidades encriptadas y protegidas por claves de acceso.

9.6.2. DeCypherIT

DeCypherIT es una utilidad gratuita que permite desencriptar los archivos encriptados generados por Cryptainer y Secure IT

9.7. MODO DE TRABAJO

- Descargar el Software Cryptainer Le y DeCypherIT del siguiente link: http://www.cypherix.es/downloads.htm
- Instalar los software Cryptainer Le y DeCypherIT
- Abrir Criptayner Le
- Crear un nuevo volumen.

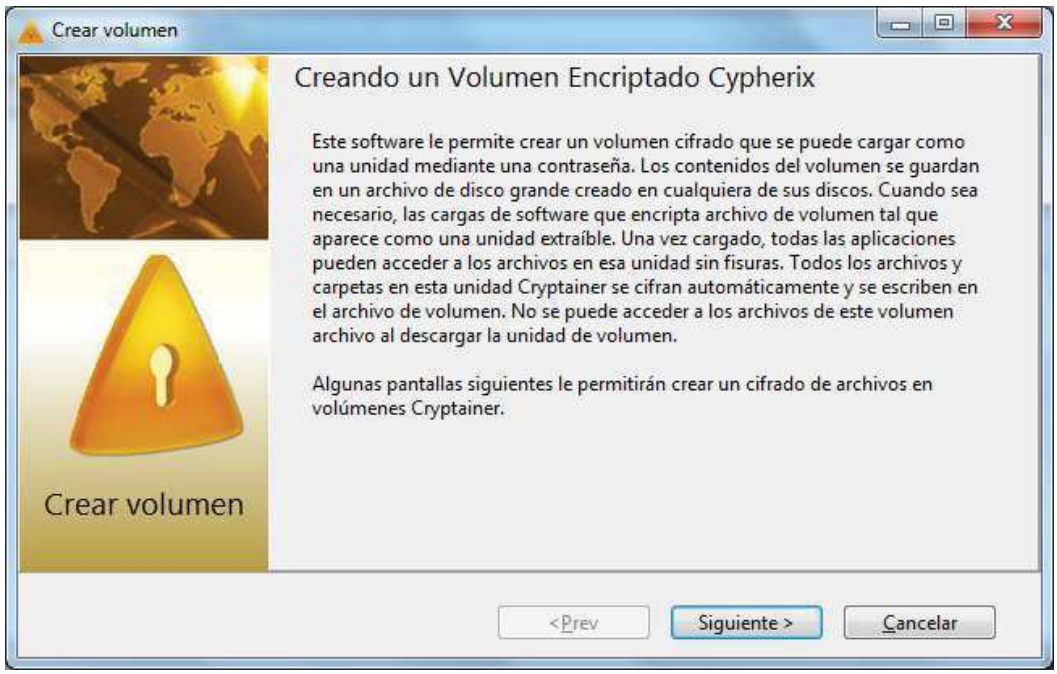


Figura 66. Creación de un volumen.

- Especificar un nombre y tamaño para el nuevo volumen

Figura 67. Tamaño y etiqueta de volumen.

- Escoger una ubicación

Figura 68. Nombre del archivo de volumen y ubicación.

- Elegir una contraseña. Ejemplo: Ud1a20l5

Figura 69. Contraseña del volumen y algoritmo de encriptado.

- Elegir la primera opción.

Figura 70. Formato de Volumen.

- Una vez ingresado la información, proceder a crear un volumen encriptado.

Figura 71. Creación del volumen.

- Para terminar la creación del volumen, formatear el volumen.

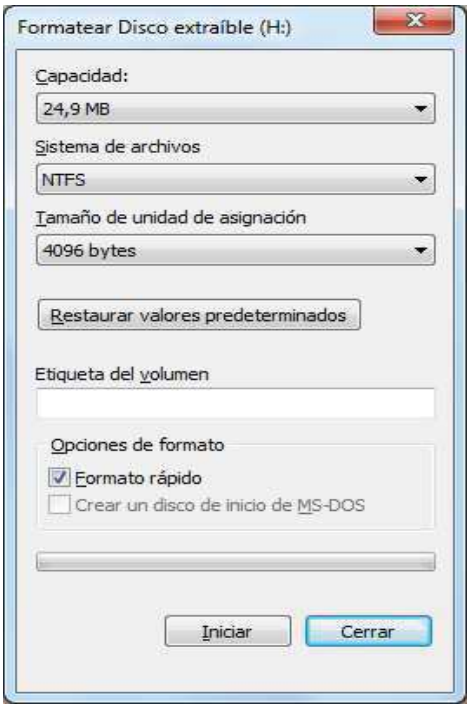


Figura 72. Formateo del volumen creado.

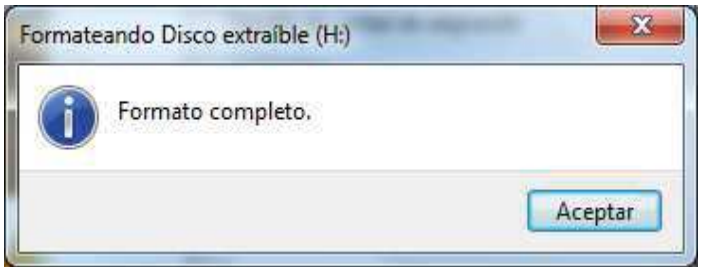


Figura 73. Mensaje de formato completo.

- Una vez creado el volumen, dirigirse a Cryptainer, Menú “Archivo” y escoger la opción “Cargar Volumen Cryptainer”

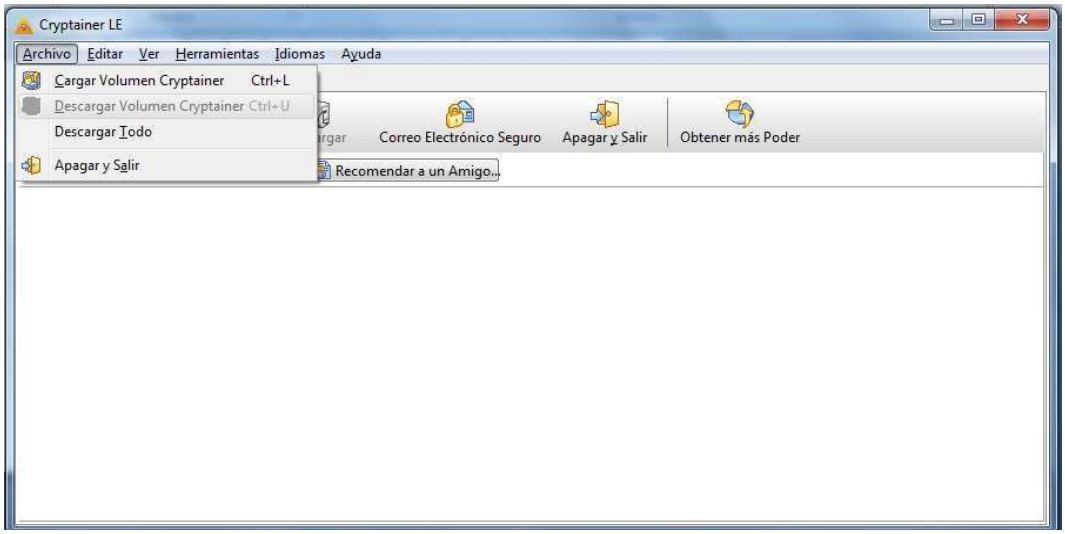


Figura 74. Ventana para cargar un volumen encriptado.

- Introducir la contraseña establecida: Ud1a20l5

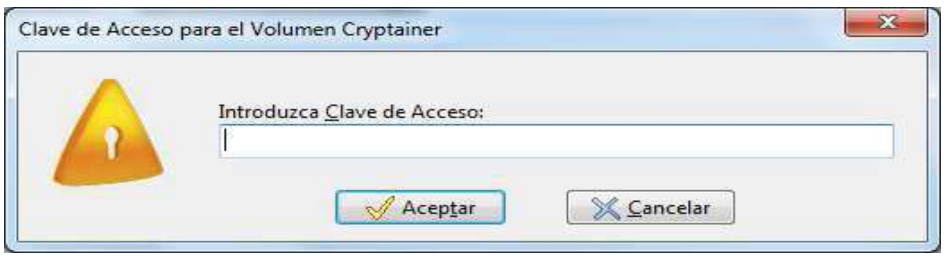


Figura 75. Solicitud de contraseña.

- Una vez descargado nuestro volumen podremos hacer uso de él

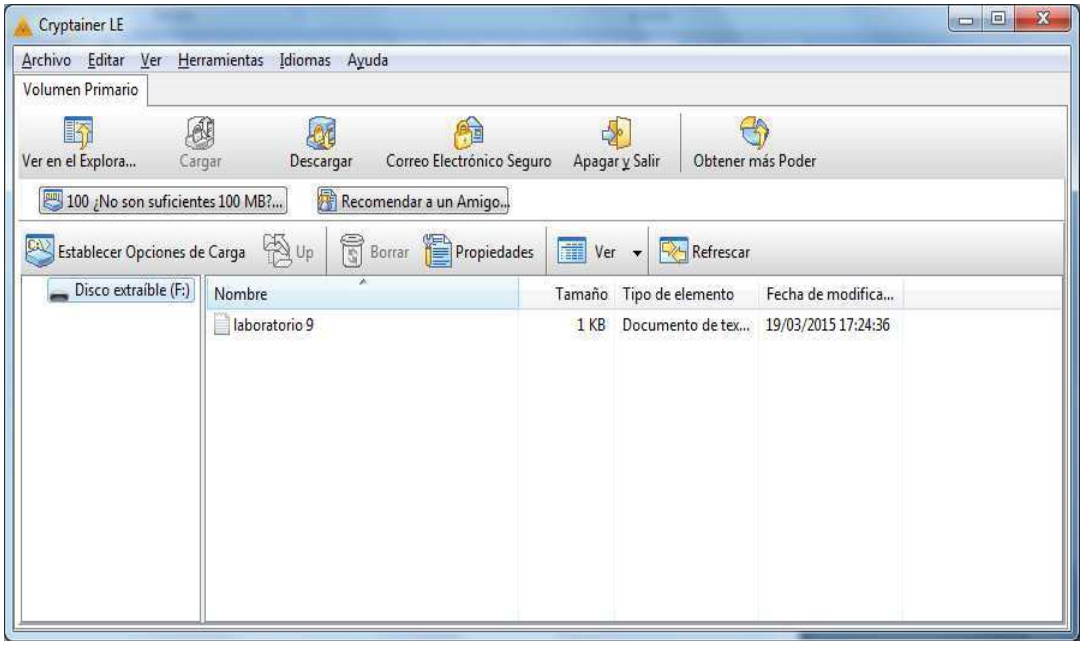


Figura 76. Volumen desencriptado.

9.7.1. Encriptar un archivo

- Herramientas <"Encriptar un archivo para enviar por correo electrónico">

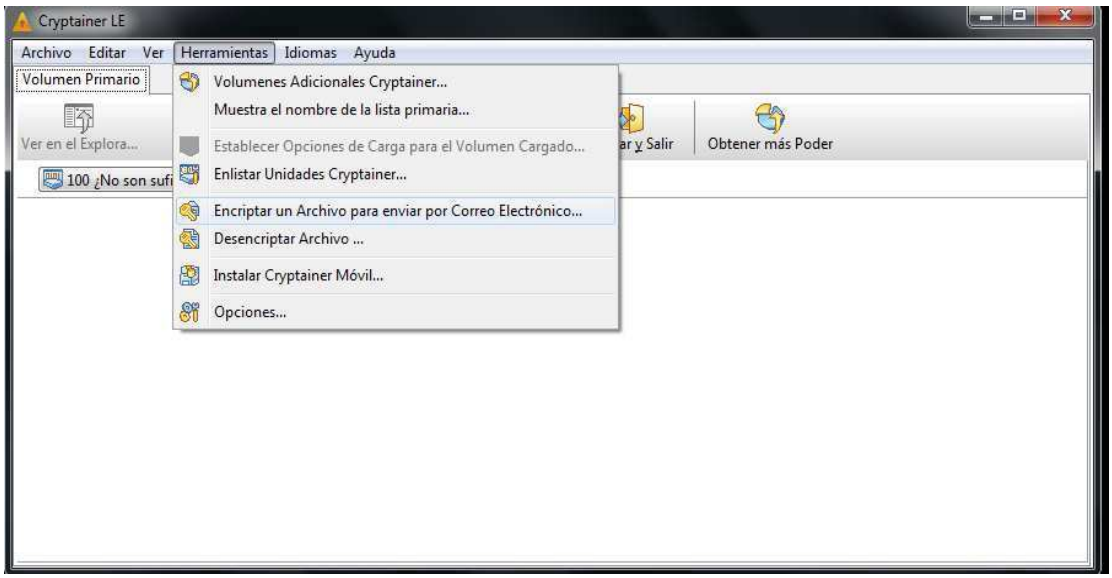


Figura 77. Ventana para enviar un archivo encriptado por e-mail.

- Elegir archivo a encriptar

Figura 78. Ubicación de archivo hacer encriptado.

- Establecer una contraseña

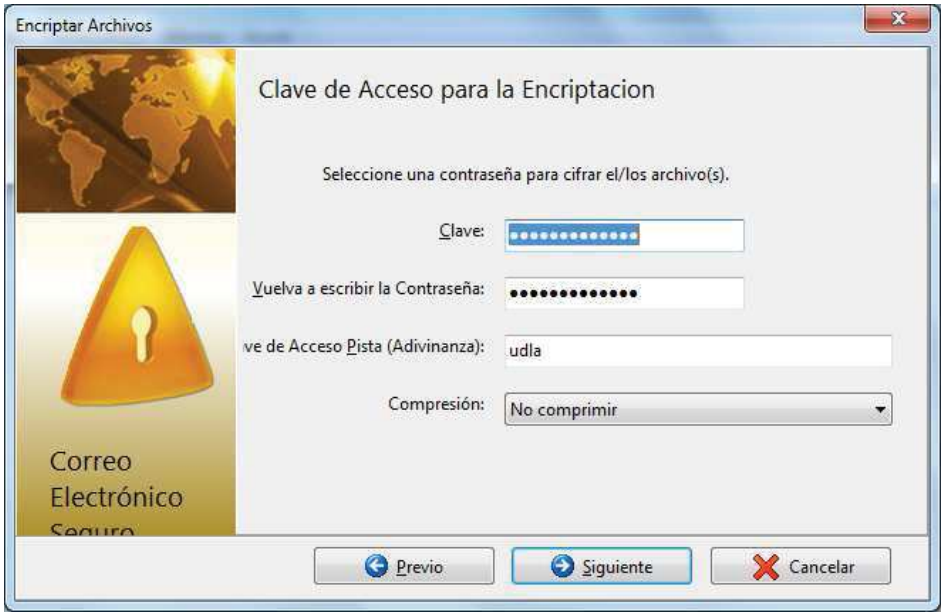


Figura 79. Clave de acceso para la encriptación.

- Indicar ubicación donde se va a guardar el archivo.

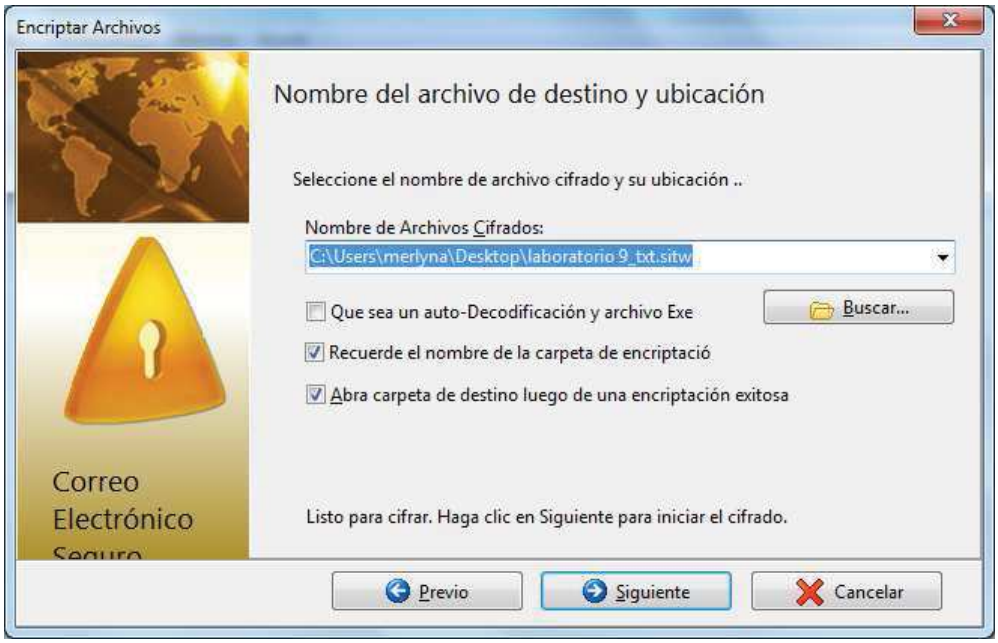


Figura 80. Nombre del archivo de destino y ubicación.

- El archivo ha sido encriptado.

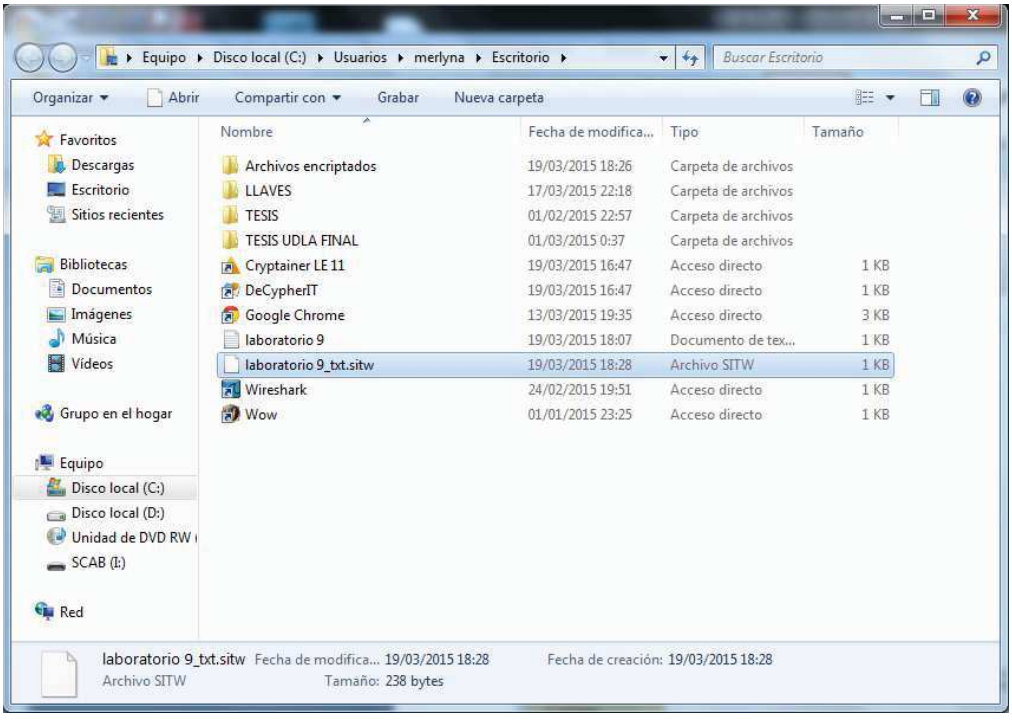


Figura 81. Archivo encriptado.

9.7.2. Desencriptar un archivo

- Herramientas <Desencriptar Archivo>

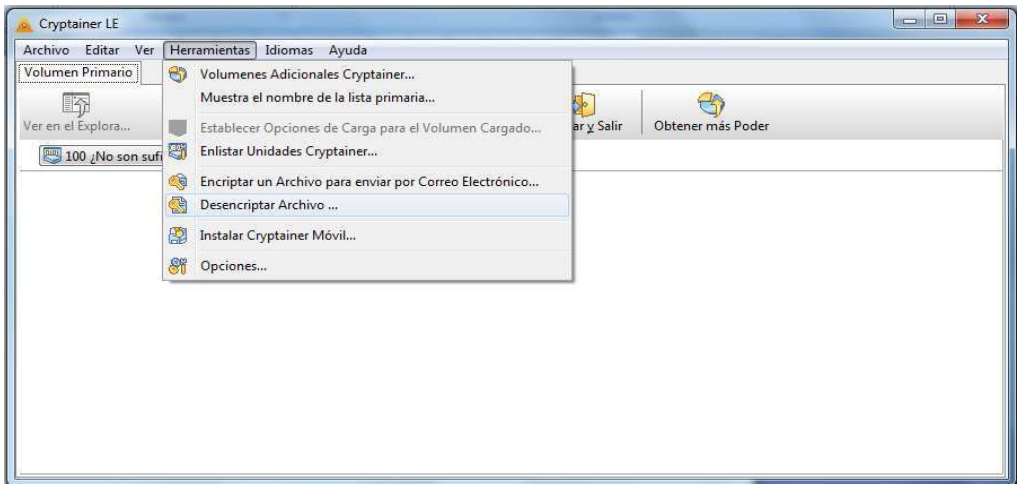


Figura 82. Desencriptar un archivo.

- Ubicar archivo encriptado

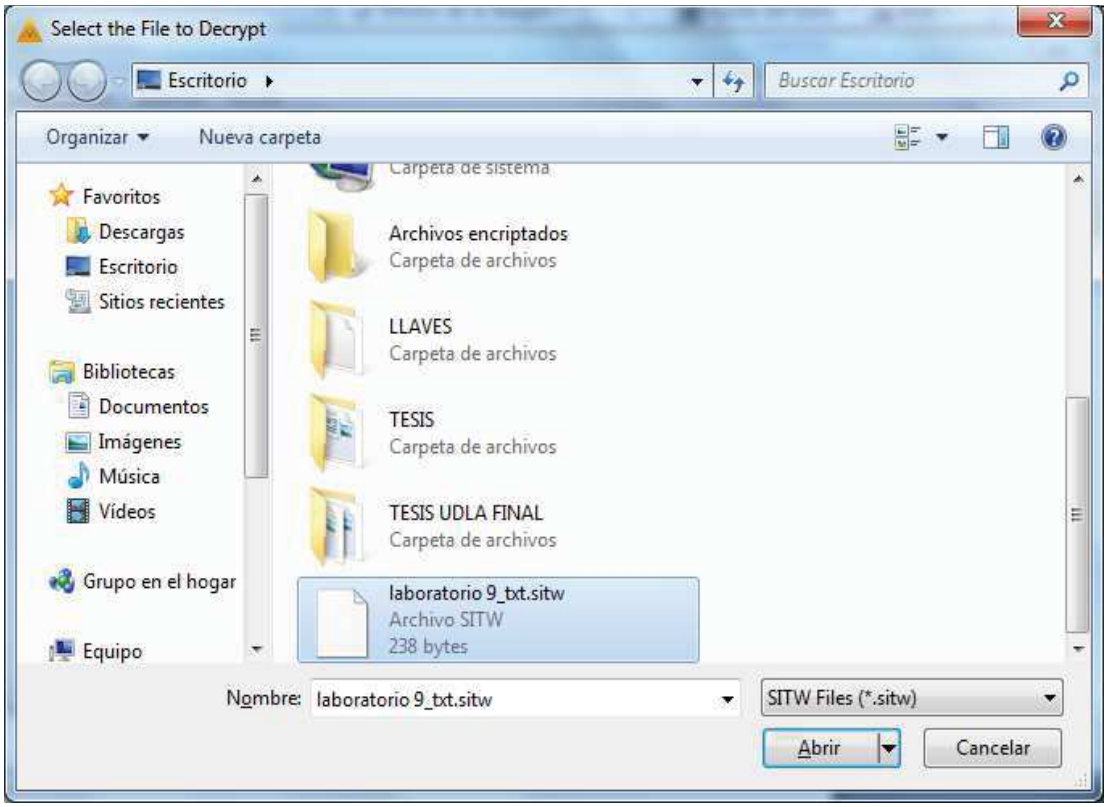


Figura 83. Ubicación del archivo encriptado.

- Introducir contraseña que fue asignado al archivo.

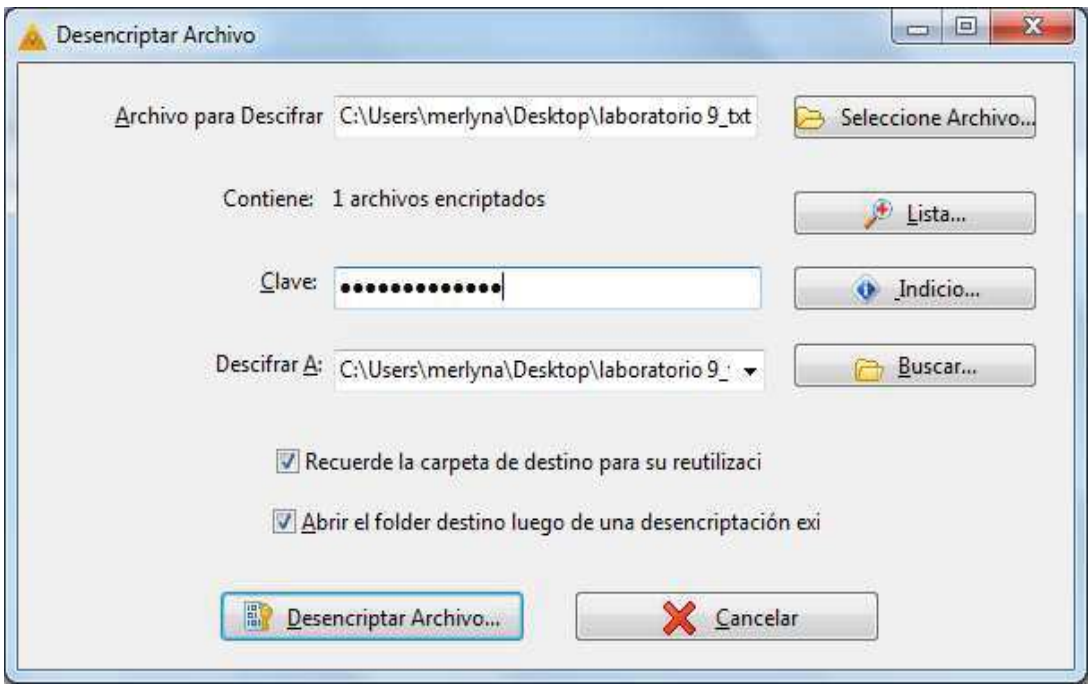


Figura 84. Introducción de contraseña

- Si no se tiene una carpeta específica para archivos desencriptados, proceder a crearla o aceptar y se creará automáticamente.

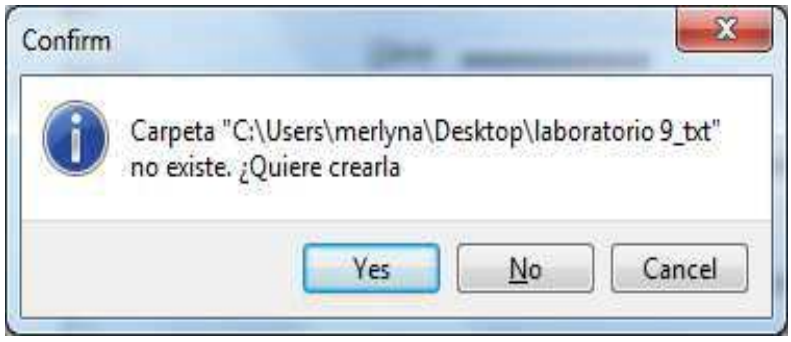


Figura 85. Creación de carpeta para archivos desencriptados.

- El archivo ha sido desencriptado.

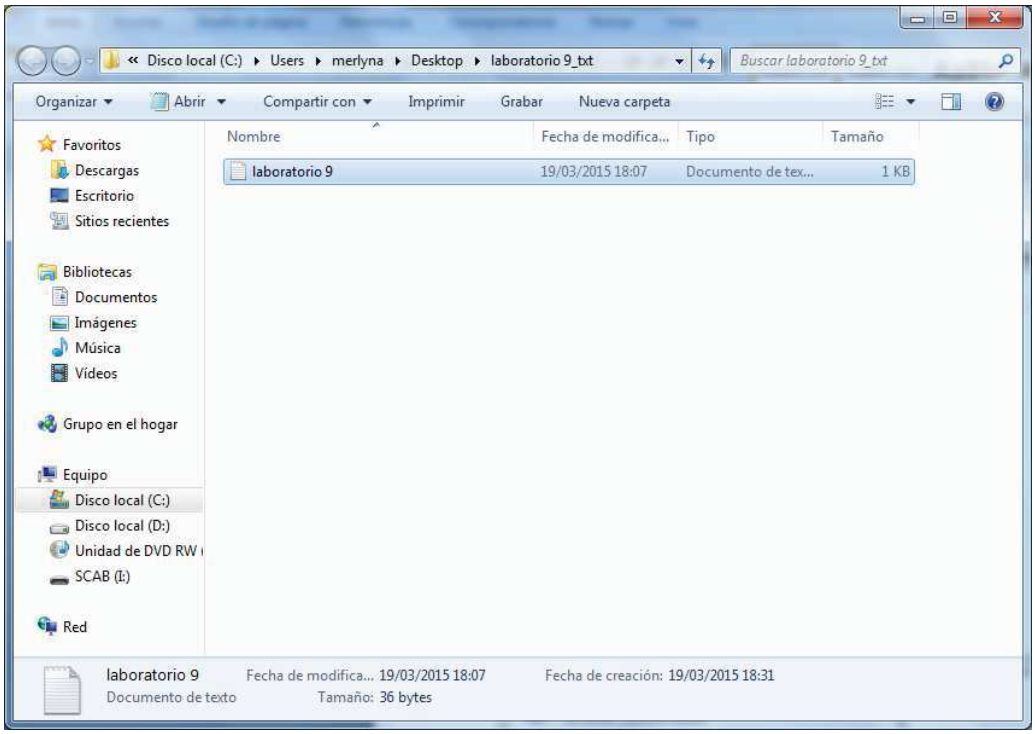


Figura 86. Archivo desencriptado.

- Abrir el archivo.

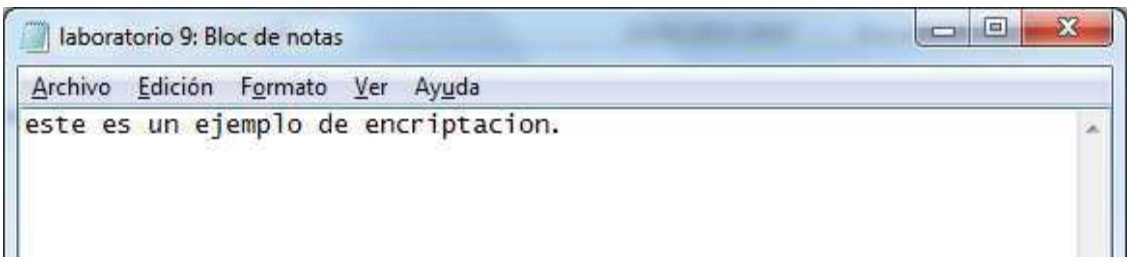


Figura 87. Archivo desencriptado abierto.

9.8. TIEMPO ESTIMADO DE LA PRÁCTICA

Una sesión de clase

9.9. ACTIVIDADES PARA LOS ALUMNOS

Crear un volumen, un archivo, encriptarlos y al archivo enviarlo por mail a otro estudiante para que proceda a desencriptarlo.

9.10. EVALUACIÓN

1. ¿Para qué sirve el software Cryptainer Le?
2. ¿Porque es importante encriptar volúmenes (discos)?
3. ¿Cómo funcionan las llaves públicas y privadas?
4. ¿Cómo se visualiza un archivo encriptado?
5. ¿Cuál es el objetivo principal de Cryptainer Le?

10. CAPITULO X

LABORATORIO 10 “Configuración de firewall software. Windows”

10.1. INTRODUCCIÓN

En el laboratorio se conocerá los pasos para una correcta configuración de un cortafuegos o firewall.

10.2. DESCRIPCIÓN DE LOS EQUIPOS

- Computador
- Sistema Operativo Windows.

10.3. MATERIALES

- Computador
- Firewall Windows.
- Sistema Operativo Windows 7

10.4. OBJETIVO GENERAL

Configurar correctamente un firewall de Windows.

10.5. OBJETIVOS ESPECÍFICOS

- Conocer la importancia y funcionamiento de un firewall.

10.6. TRABAJO PREPARATORIO

Previamente el estudiante debe tener conocimiento de los temas que a continuación se describen:

10.6.1. Firewall

Un firewall es software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.

Un firewall puede ayudar a impedir que hackers o software malintencionado (como gusanos) obtengan acceso al equipo a través de una red o de Internet. Un firewall también puede ayudar a impedir que el equipo envíe software malintencionado a otros equipos. (68)

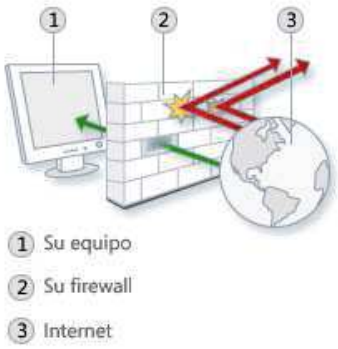


Figura 88. Funcionamiento de un Firewall

10.7. MODO DE TRABAJO

- Abrir Panel de control

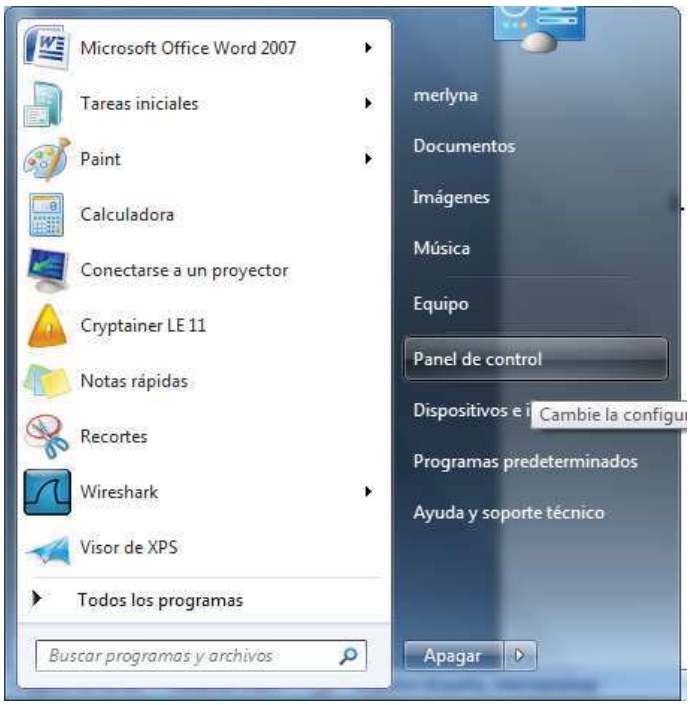


Figura 89. Panel de control

- Ir a la opción “Sistema y Seguridad”.

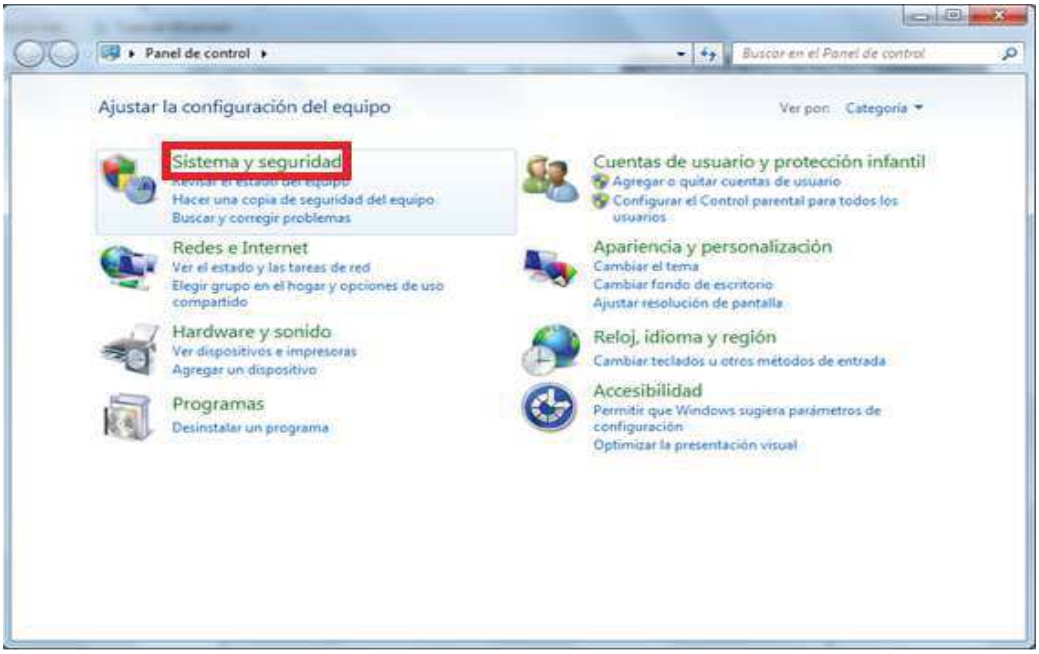


Figura 90. Sistema y Seguridad

- Ir a “Firewall de Windows”.

Figura 91. Firewall de Windows

- Comprobar la seguridad en redes domésticas y redes públicas.

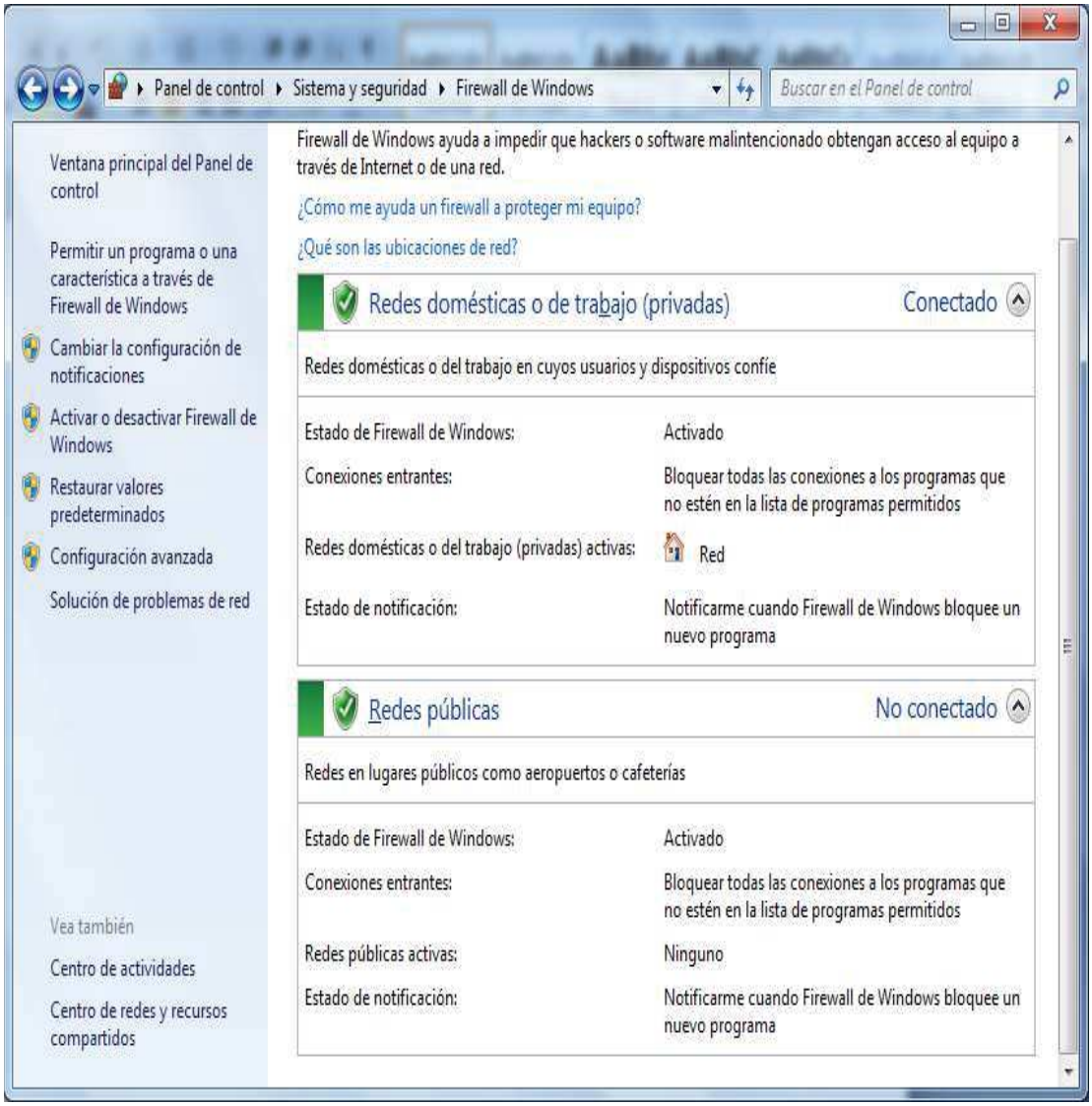


Figura 92. Redes domésticas y redes públicas.

10.7.1. Activar o desactivar Firewall

- Dirigirse a la opción “Activar o desactivar Firewall de Windows” y analizar las opciones.

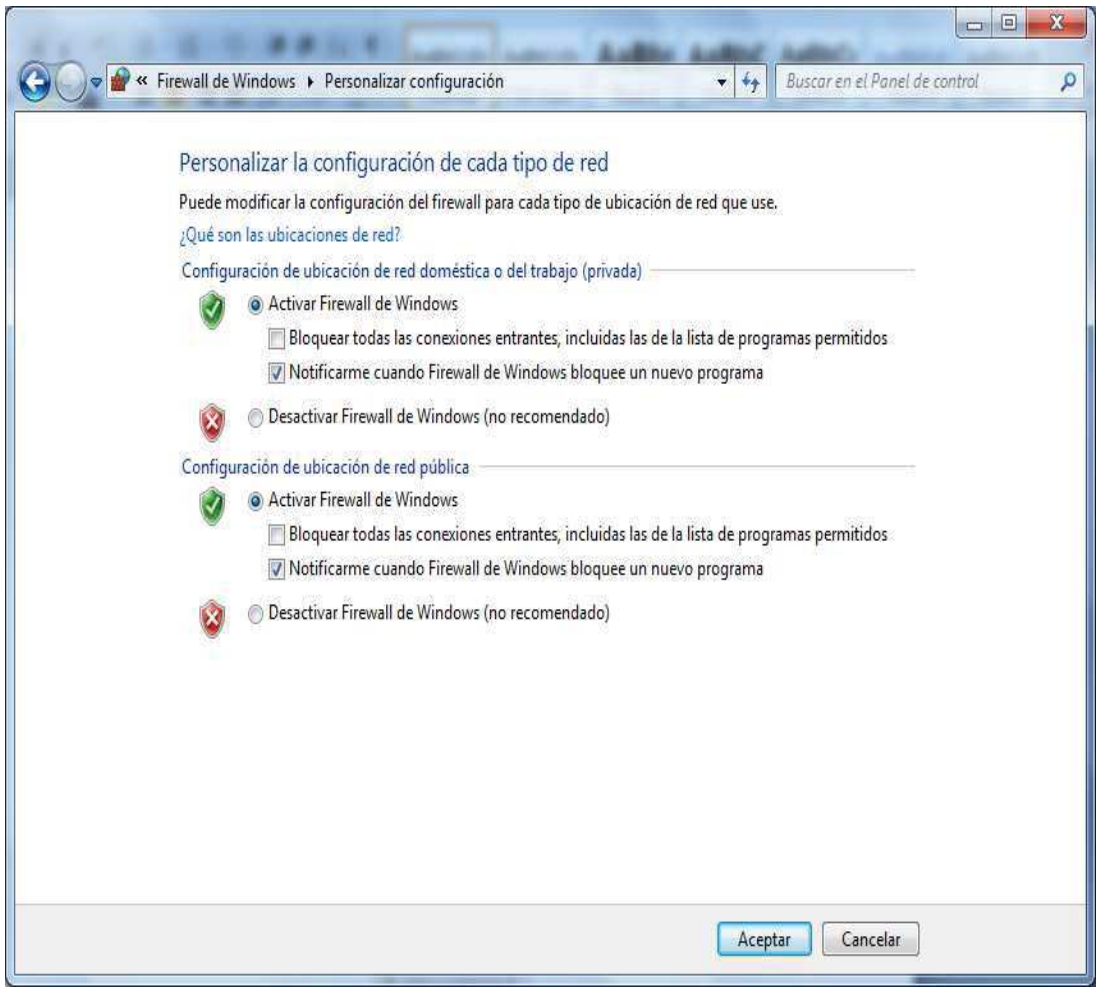


Figura 93. Activar o desactivar Firewall de Windows.

10.7.2. Configuración Avanzada.

Creación de reglas.

- Dirigirse a la opción “Configuración Avanzada”

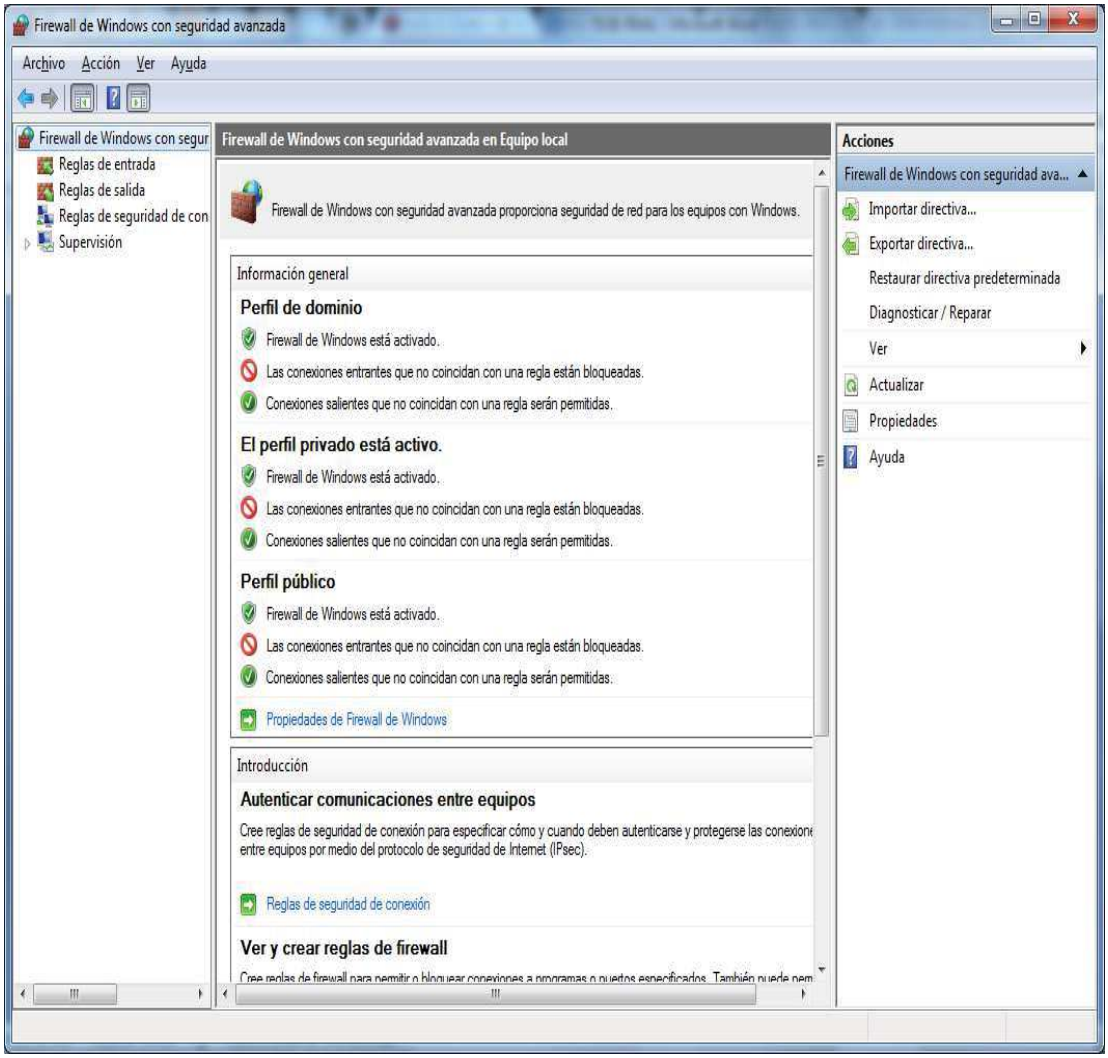


Figura 94. Configuración Avanzada de Firewall.

- Opción “Reglas de entrada” y al lado derecho opción “Nueva regla”.

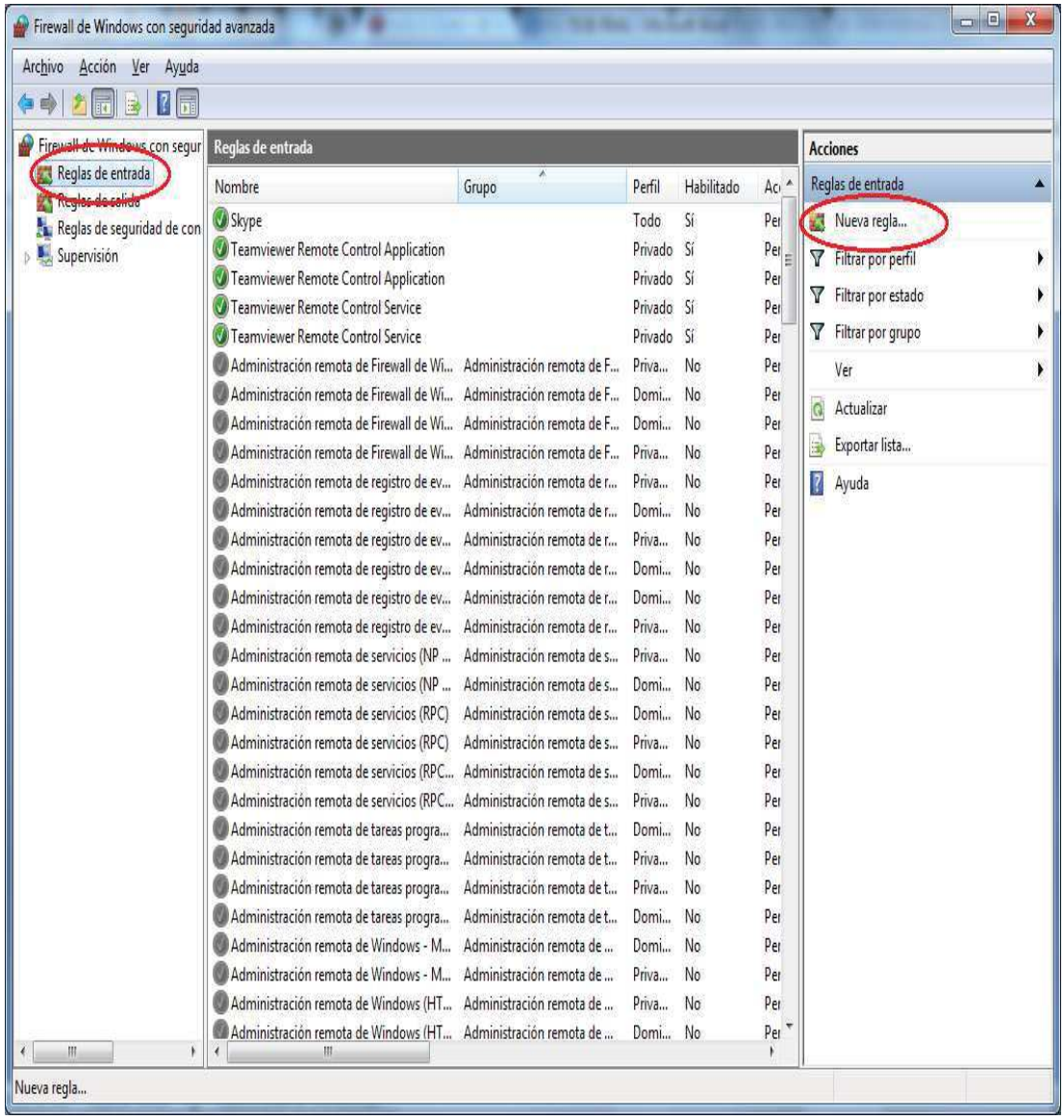


Figura 95. Creación de nuevas reglas.

- Escoger el tipo de regla a escoger, en esta práctica se realizará por puerto.

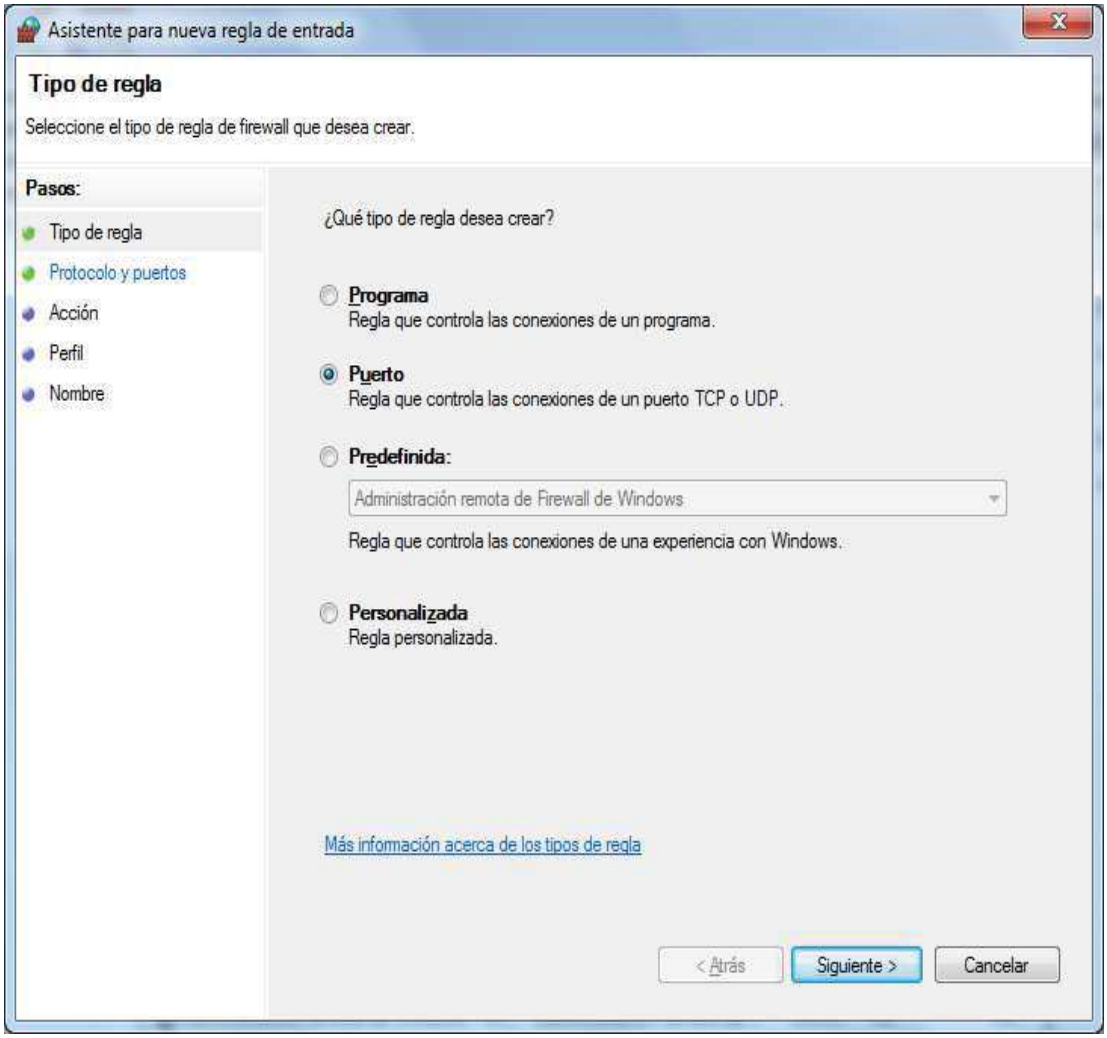


Figura 96. Tipo de regla que se va a crear.

- Elegir un tipo de protocolo y el número de puerto a bloquear.

Figura 97. Tipo de protocolo y puerto para establecer en la regla a crear.

- Elegir una acción, este caso lo vamos a bloquear.

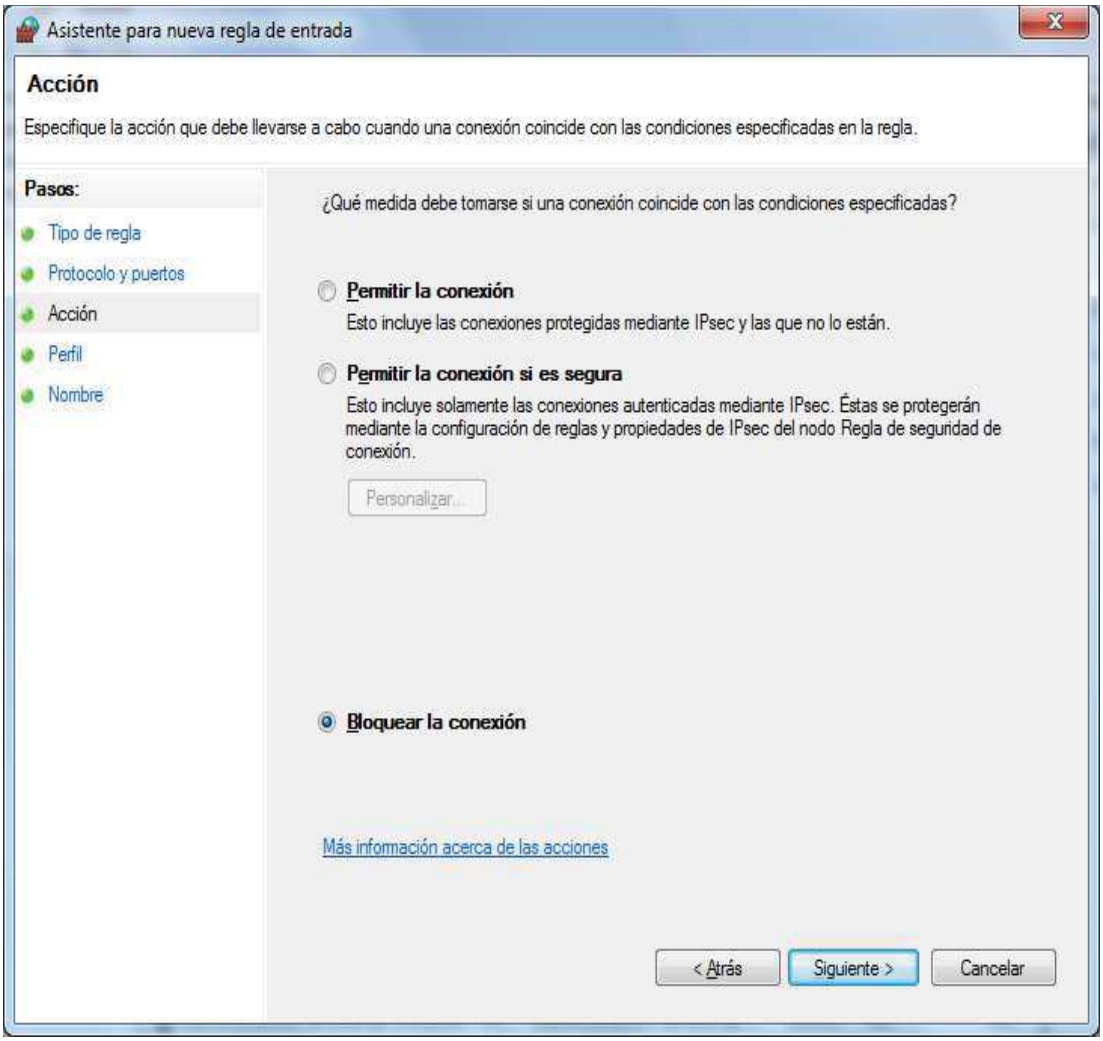


Figura 98. Acción para establecer en la regla.

- Elegir un tipo de perfil donde se bloqueará el puerto, en este caso elegimos los tres perfiles.

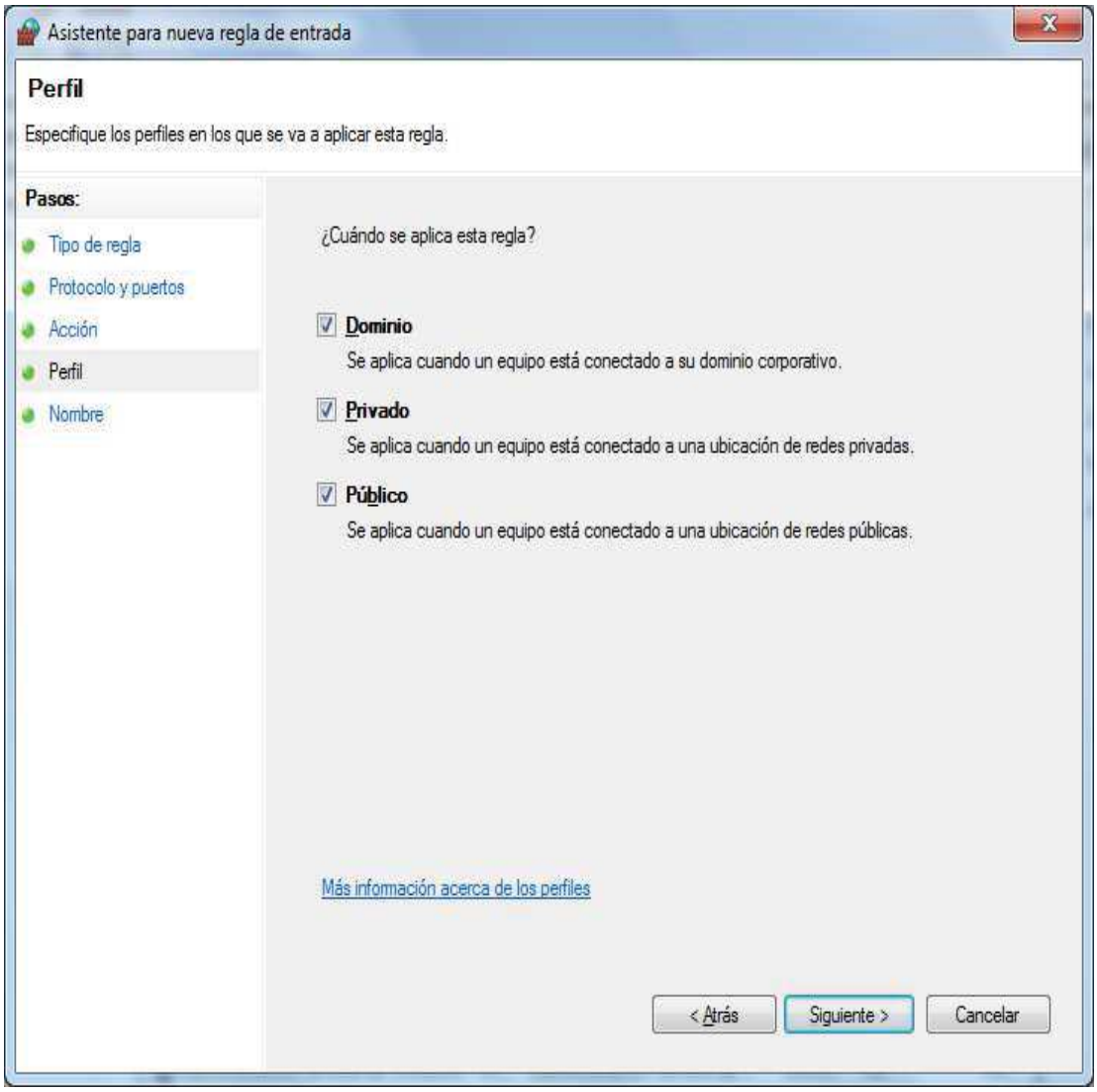


Figura 99. Perfiles para aplicar en la regla.

- Escribir el nombre de la regla que se creará.

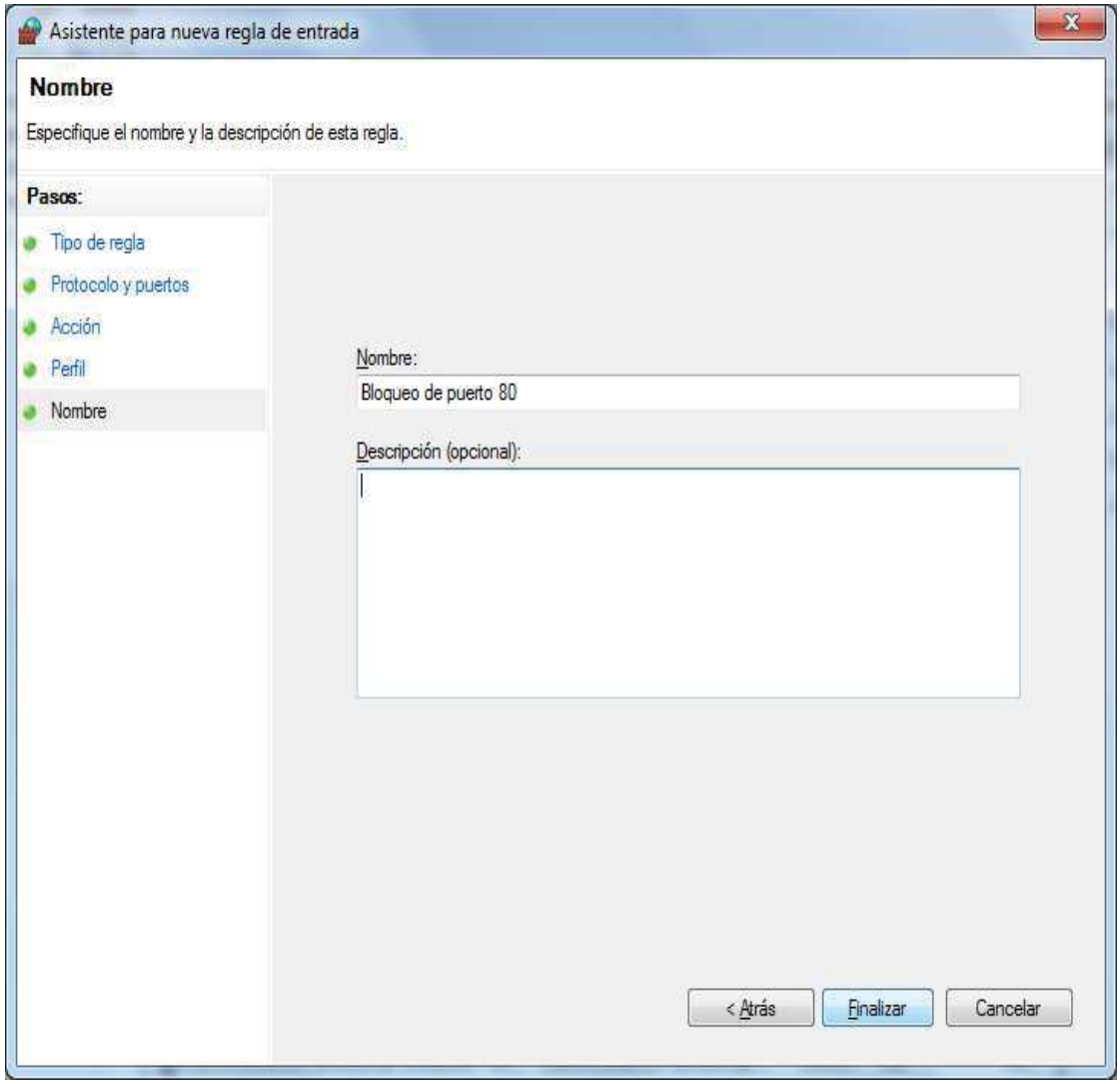


Figura 100. Nombre de la regla.

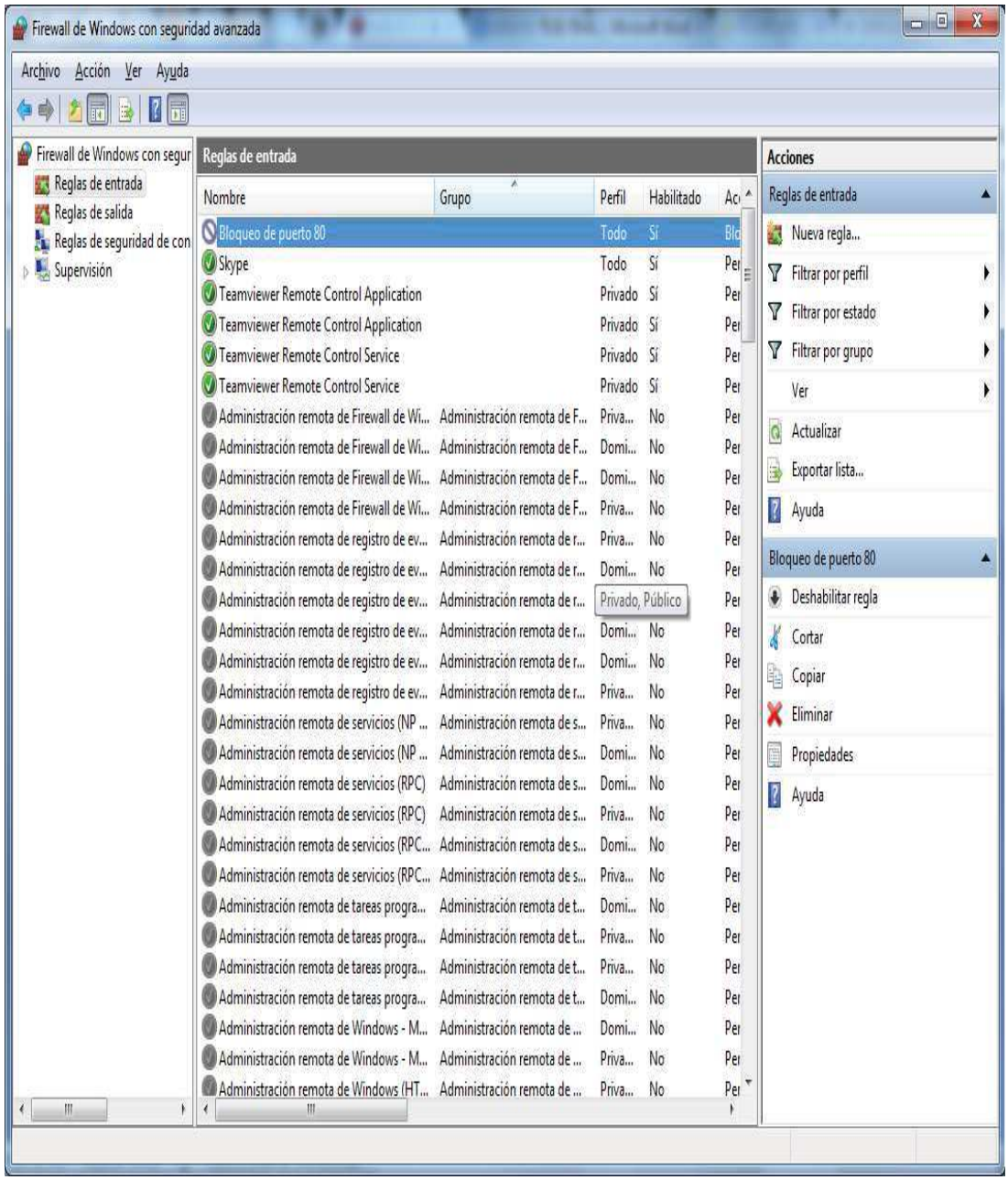


Figura 101. Regla de bloqueo del puerto 80, creada.

- Una vez bloqueado el puerto no se permitirá la navegación.

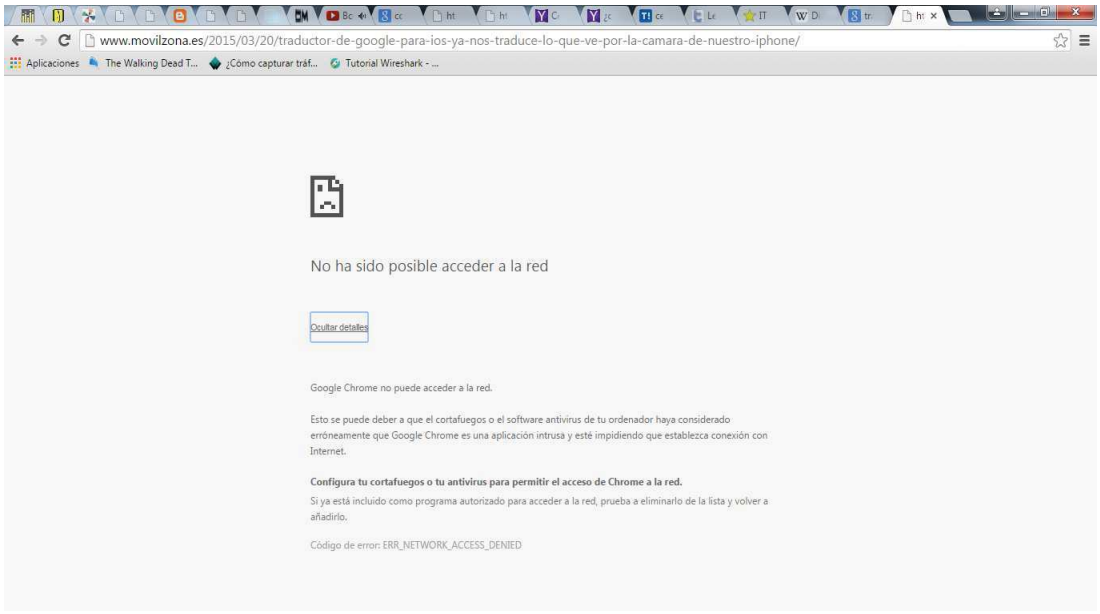


Figura 102. Navegación bloqueada.

10.8. TIEMPO ESTIMADO DE LA PRÁCTICA

Una sesión de clase.

10.9. ACTIVIDADES PARA LOS ALUMNOS

Realizar un informe sobre la importancia de activar un cortafuegos o Firewall.

10.10. EVALUACIÓN

1. ¿Qué un Firewall?
2. ¿Cómo funciona un Firewall?
3. ¿Cuáles son los objetivos de utilizar un firewall?
4. ¿Indique los pasos para activar Firewall en Windows?
5. Realice un esquema de un firewall

11. CAPITULO XI

LABORATORIO 11 “Configuración VPN por software, openvpn.”

11.1. INTRODUCCIÓN

En el siguiente laboratorio se conocerá los pasos para crear una red virtual privada.

11.2. DESCRIPCIÓN DE LOS EQUIPOS

- Computador
- Sistema Operativo Windows.

11.3. MATERIALES

- Computador
- Software openvpn.
- Sistema Operativo Windows 7

11.4. OBJETIVO GENERAL

Configurar correctamente VPN, mediante la herramienta openvpn.

11.5. OBJETIVOS ESPECÍFICOS

- Conocer los beneficios de configurar una red virtual privada.
- Aprender a utilizar comandos para la creación de vpn.
- Investigar los comandos utilizados en la configuración de vpn.

11.6. TRABAJO PREPARATORIO

Previamente el estudiante debe conocer los temas que a continuación se describen:

11.6.1. VPN

Una red VPN (red privada virtual) es una red privada construida dentro de una infraestructura de red pública, como por ejemplo Internet. Las empresas pueden usar una red VPN para conectar de manera segura oficinas y usuarios remotos por medio de un acceso a Internet económico suministrado por un tercero, en lugar de a través de enlaces WAN dedicados o enlaces de acceso telefónico de larga distancia. (69)

11.7. MODO DE TRABAJO

- Descargar software Openvpn del siguiente link: https://openvpn.net/index.php/open-source/downloads.html
- Descargar Windows Vista and Later bits. (Investigar los bits del computador).

Downloads

OpenVPN 2.3.6 -- released on 2014.12.01 (Change Log)

This release fixes a critical *denial of service vulnerability* in OpenVPN servers (CVE-2014-8104). The vulnerability can only be exploited by *authenticated clients*. Also note that confidentiality and authenticity of traffic are *not* affected. More information about this vulnerability is available on the Trac wiki. This release includes a few other fixes and enhancements. A full list of changes is available here

Windows installers I002 and I602 bundle OpenSSL 1.0.1l, which fixes the FREAK vulnerability. The impact of the vulnerability on OpenVPN is discussed in detail in the Wiki. Windows installers I003 and I603 bundle OpenSSL 1.0.1m that fixes several security vulnerabilities, one of which (CVE-2015-0286) is likely to affect OpenVPN also.

If you find a bug in this release, please file a bug report to our Trac bug tracker. In uncertain cases please contact our developers first, either using the openvpn-devel mailinglist or the developer IRC channel (#openvpn-devel at irc.freenode.net). For generic help take a look at our official documentation, wiki, forums, openvpn-users mailing list and user IRC channel (#openvpn at irc.freenode.net).

Source Tarball (gzip)	openvpn-2.3.6.tar.gz	GnuPG Signature
Source Tarball (xz)	openvpn-2.3.6.tar.xz	GnuPG Signature
Source Zip	openvpn-2.3.6.zip	GnuPG Signature
Installer (32-bit), Windows XP and later	openvpn-install-2.3.6-I003-i686.exe	GnuPG Signature
Installer (64-bit), Windows XP and later	openvpn-install-2.3.6-I003-x86_64.exe	GnuPG Signature
Installer (32-bit), Windows Vista and later	openvpn-install-2.3.6-I603-i686.exe	GnuPG Signature
Installer (64-bit), Windows Vista and later	openvpn-install-2.3.6-I603-x86_64.exe	GnuPG Signature

Figura 103. Ventana Downloads de Openvpn.

- Seleccionar todos los componentes.

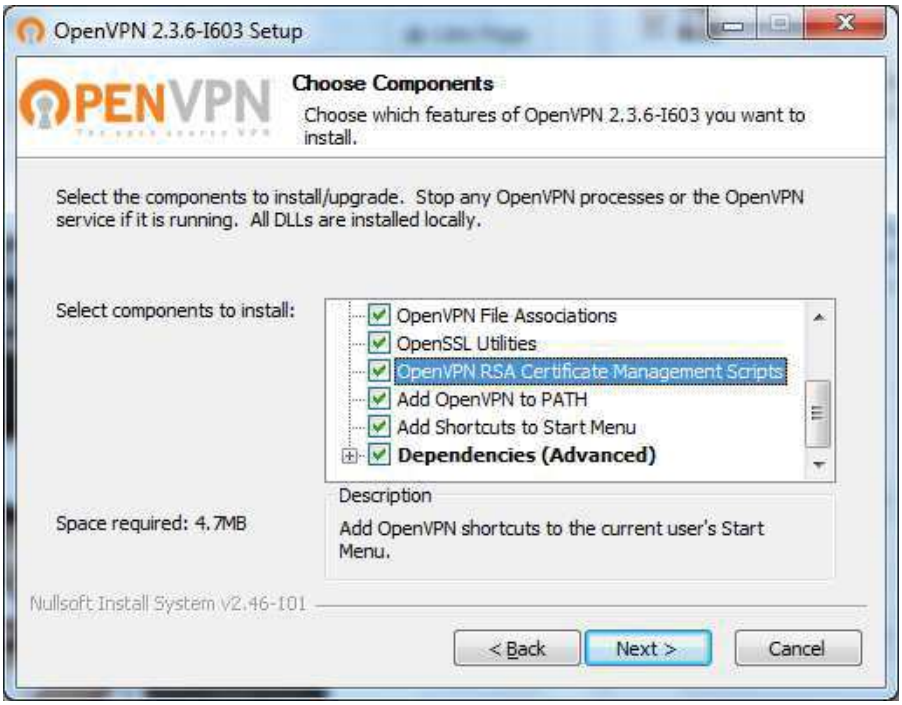


Figura 104. Componentes de instalación.

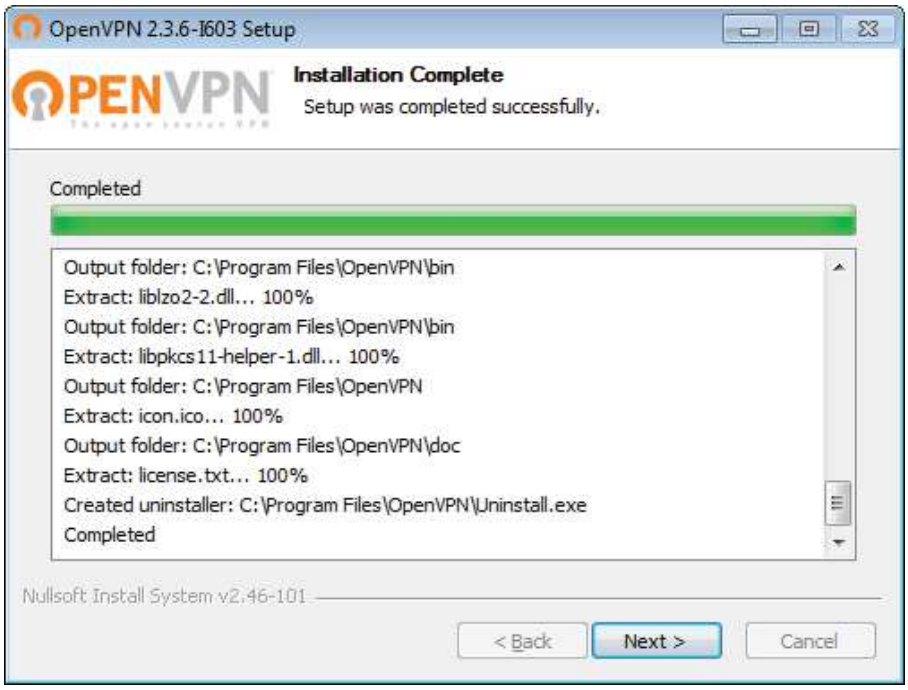


Figura 105. Instalación de Openvpn.

- Identificar la carpeta “openvpn” en donde fue instalado, abrir la carpeta “easy-rsa” y modificar con notepad u otro editor de texto el archivo “vars.bat.sample.”

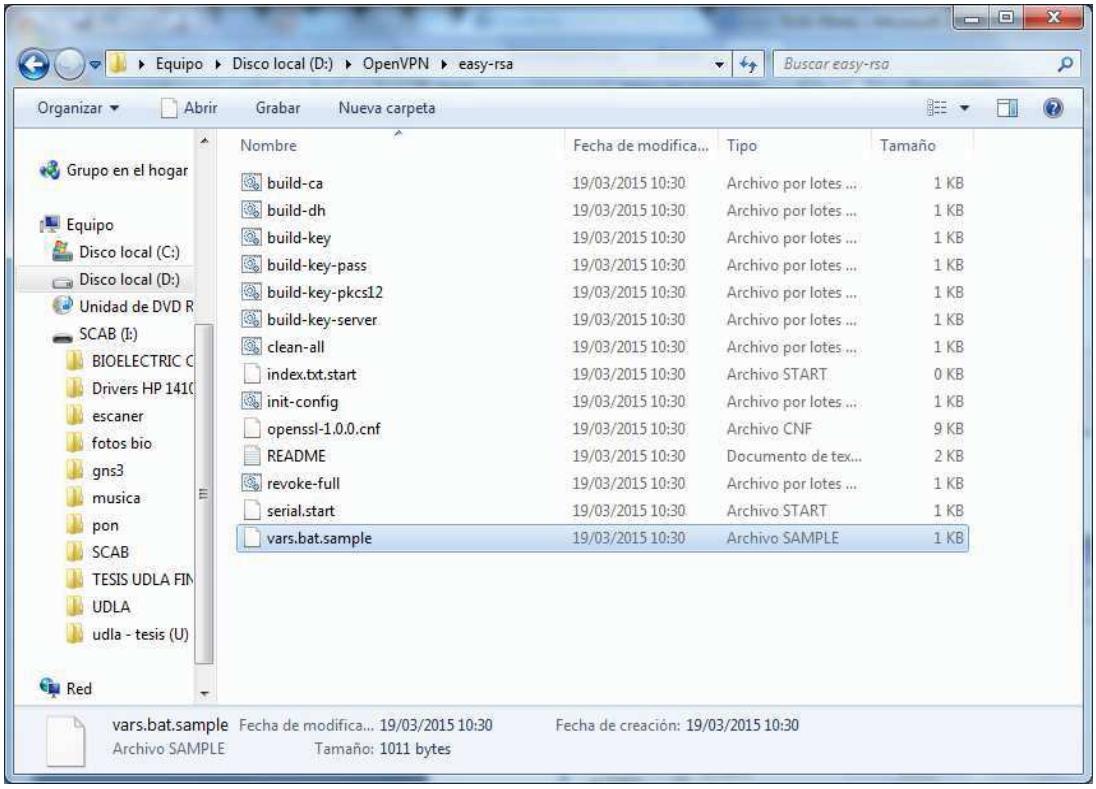


Figura 106. Ubicación archivo “vars.bat.sample”

- Modificar el siguiente texto como se muestra a continuación:

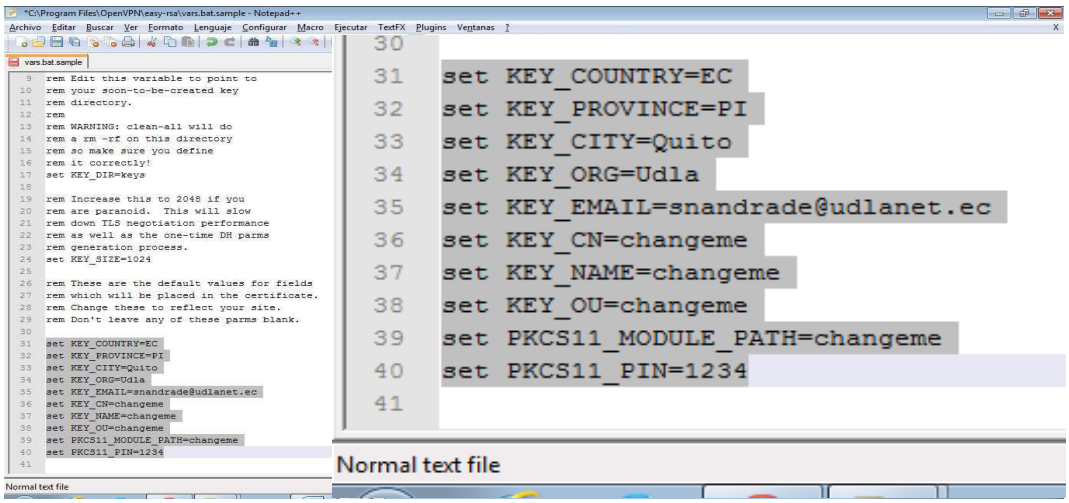


Figura 107. Archivo “vars.bat.sample”.

- Guardar el archivo y cambiar el nombre a “vars.bat”
- Abrir una consola de Windows y copiar la ruta de ubicación del archivo “vars.bat”.

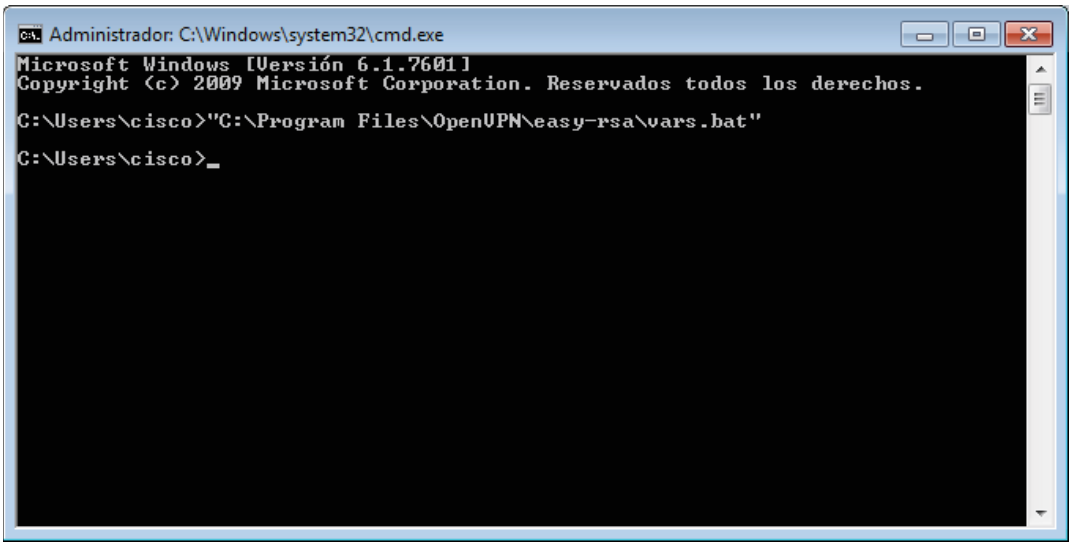


Figura 108. Vars.bat “Cargar los parámetros de configuración VPN”

- Ubicar el archivo “Clean-all” y copiar a consola.

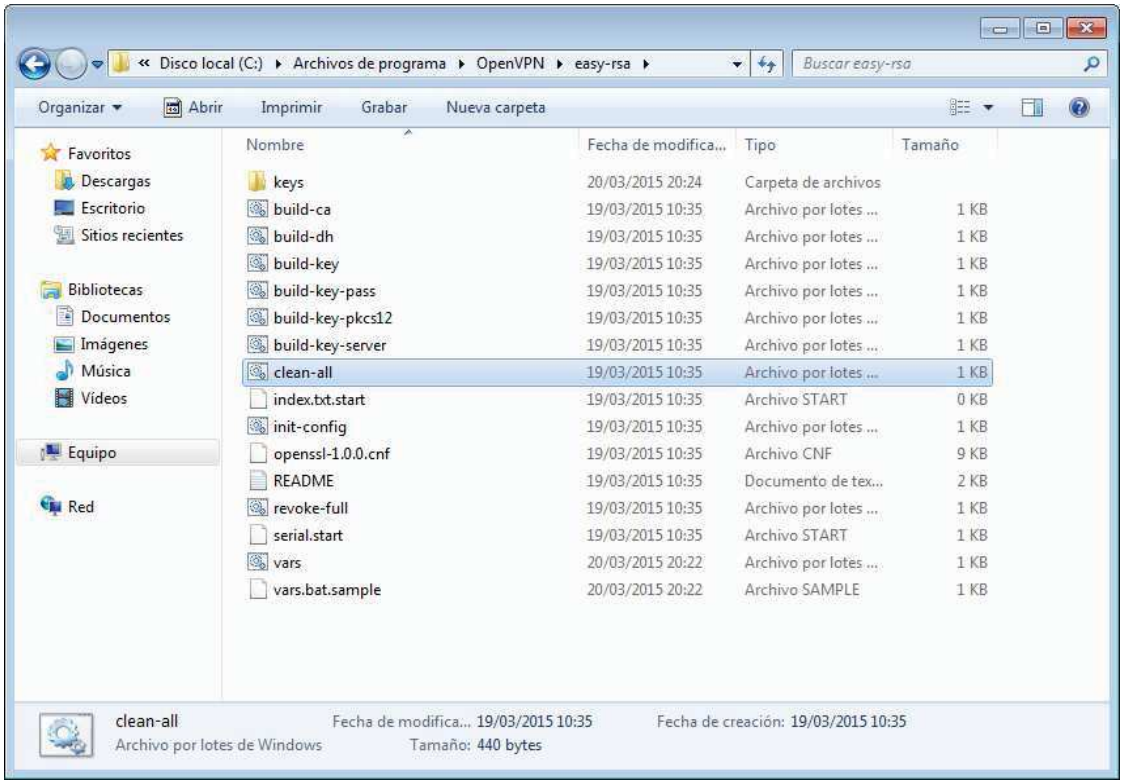


Figura 109. Archivo “Clean-all”

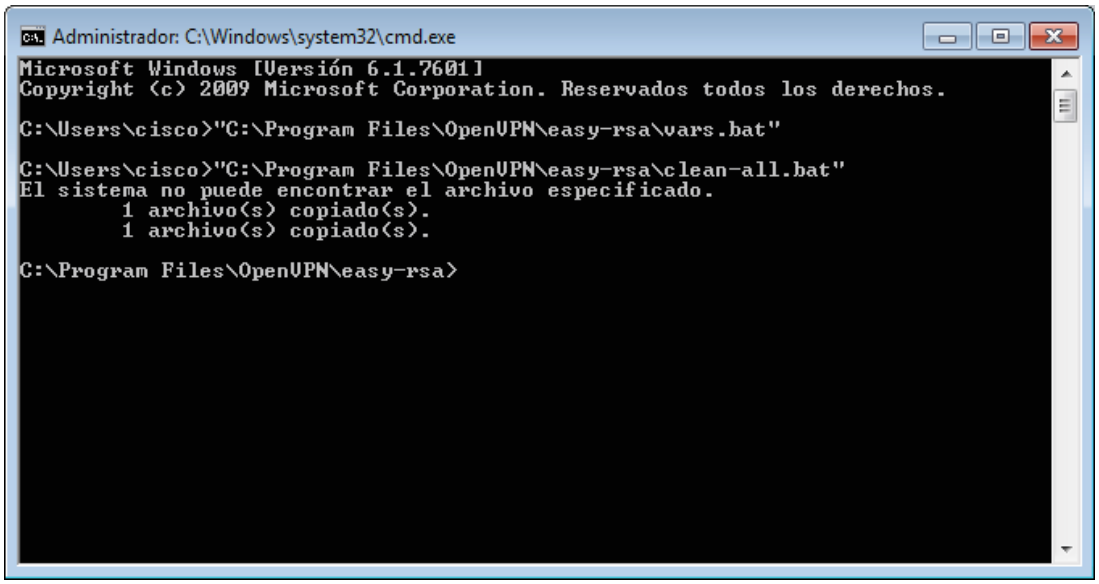


Figura 110. Clean-all.bat: creará la carpeta "keys" y posteriormente limpiará parámetros anteriores.

- Ubicar el archivo "build-key" y copiar a la consola

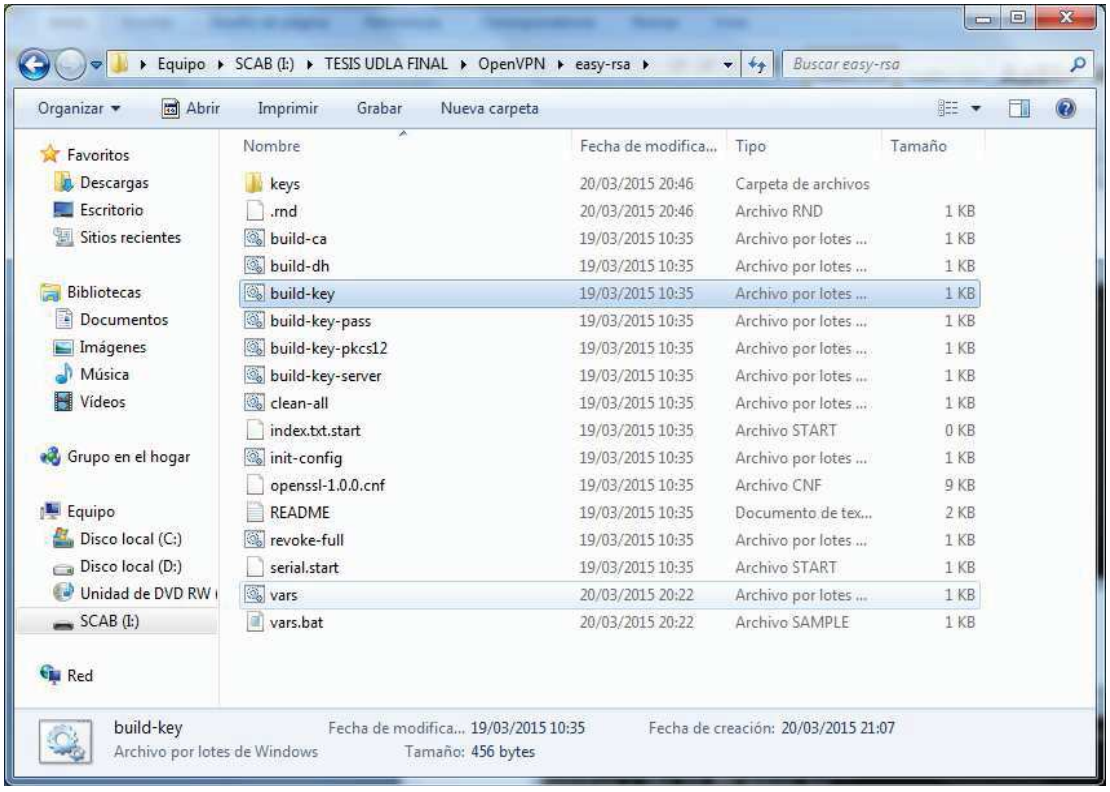


Figura 111. Ubicación archivo "build-key".

- Ubicar el archivo “build-ca” y copiar a la consola, esto generará un certificado de seguridad.

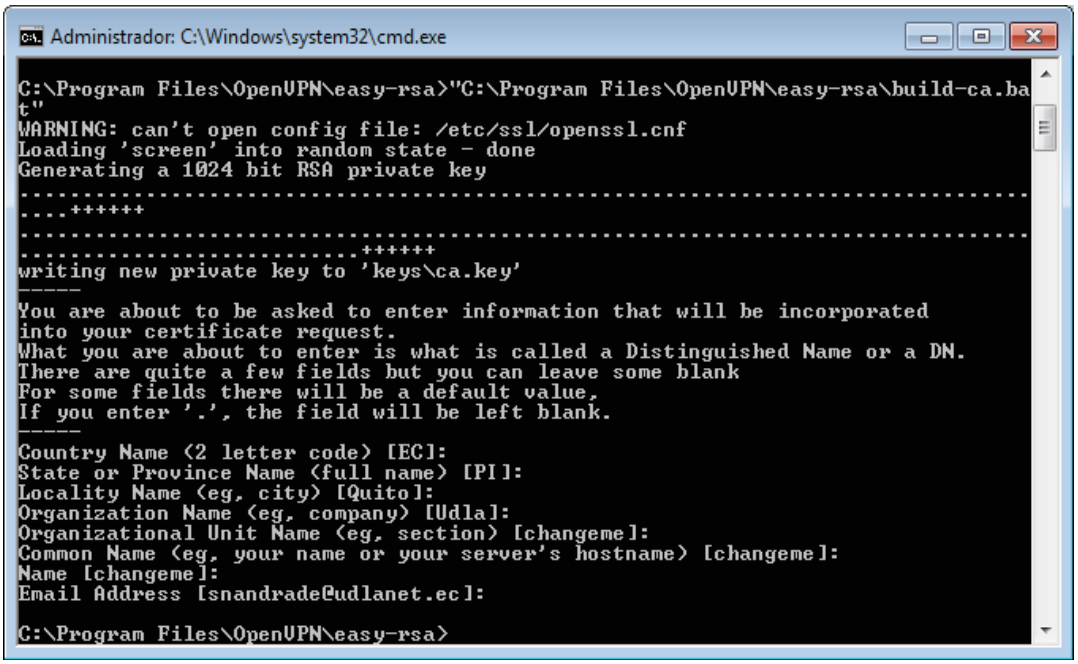


Figura 112. “Build-ca.bat” Genera certificado de seguridad.

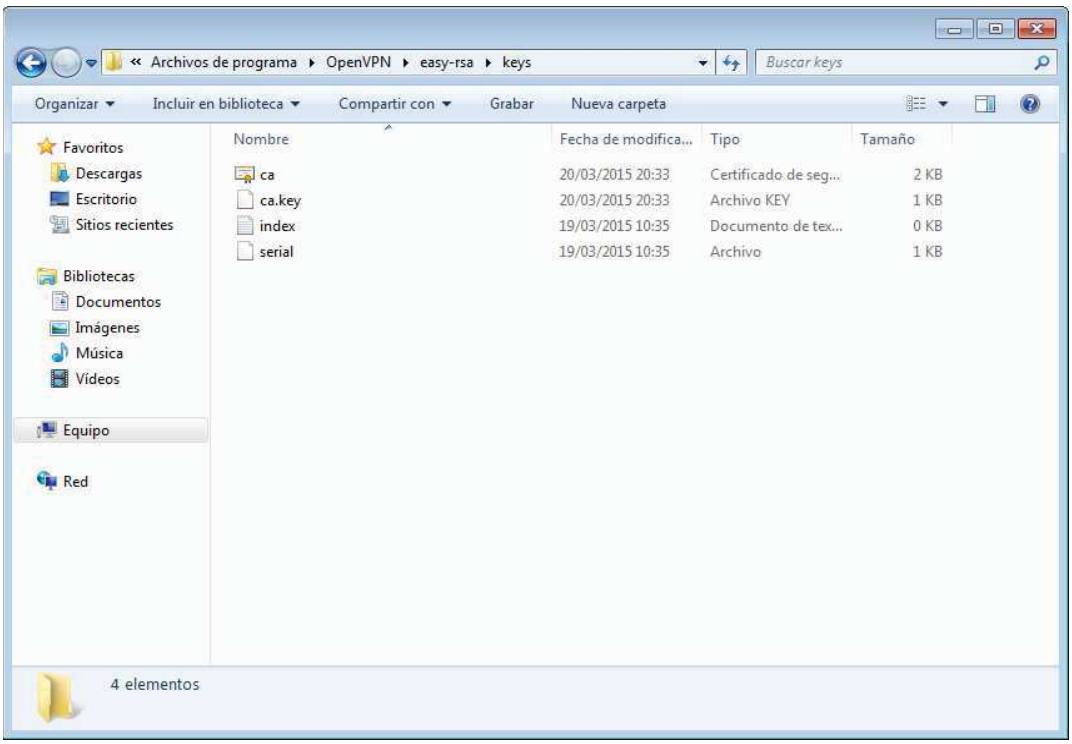


Figura 113. Certificado de seguridad creado.

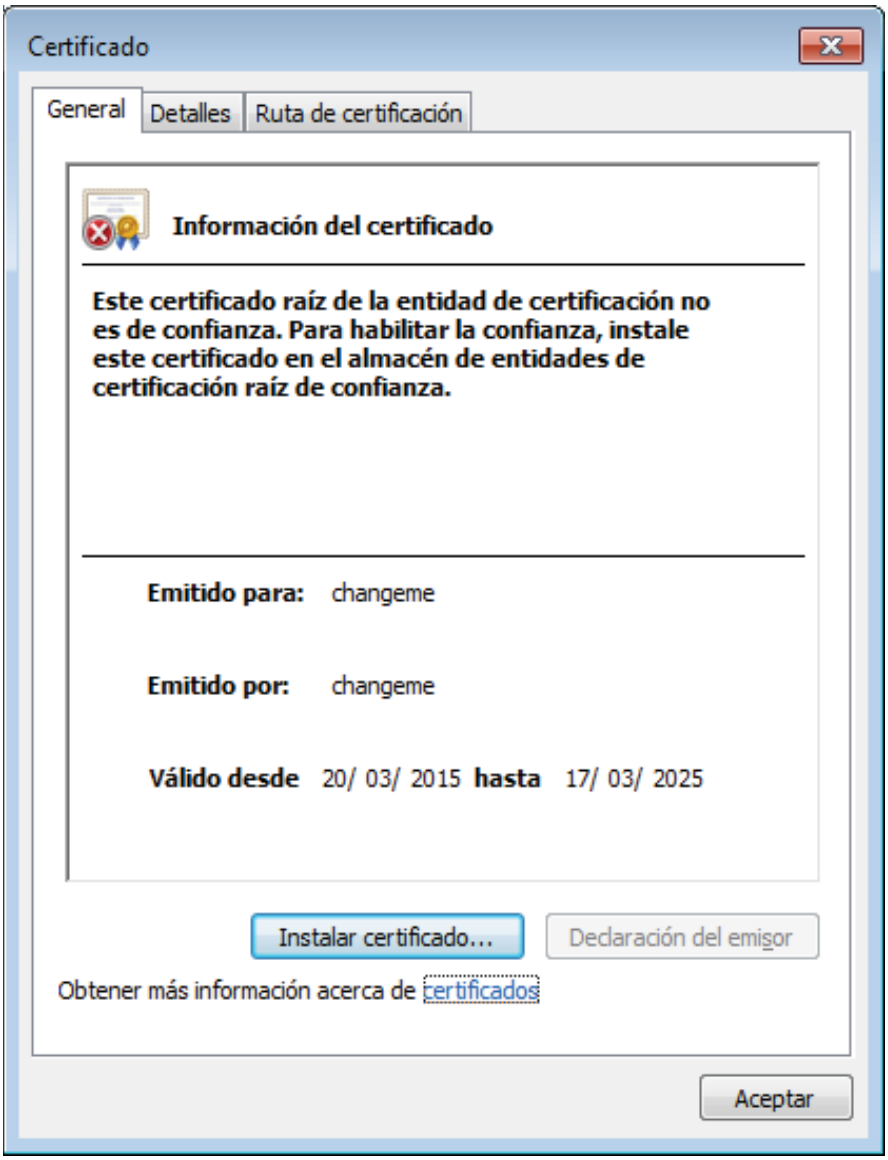


Figura 114. Información de Certificado de seguridad.

11.7.1. Creación del Servidor.

- Ubicar el archivo “build-key-server” en la carpeta easy-sra.

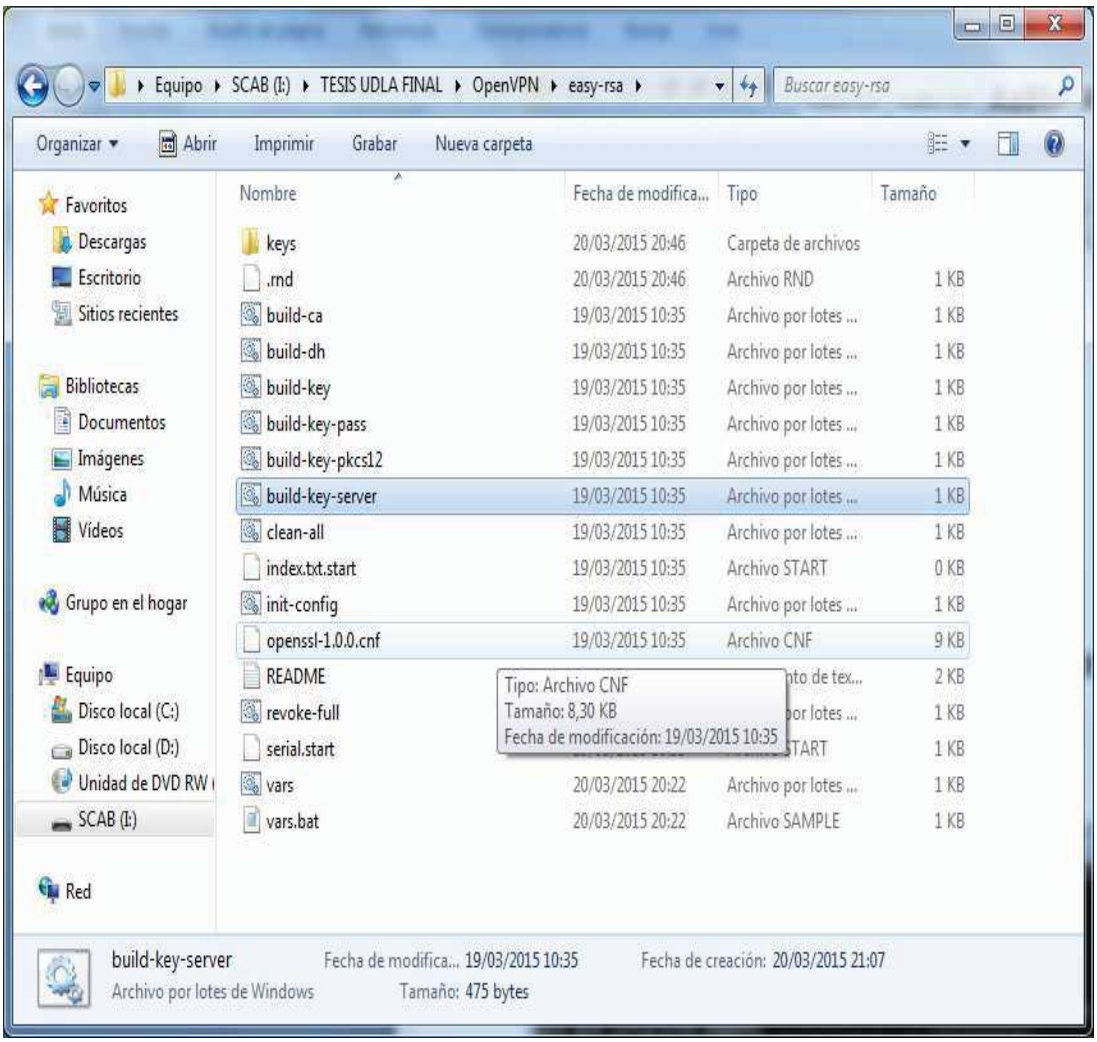


Figura 115. Ubicación del archivo “build-key.server”.

- Abrir una consola de Windows y copiar el archivo “build-key-server”, para crear un servidor.
- Asignar un nombre para el servidor.

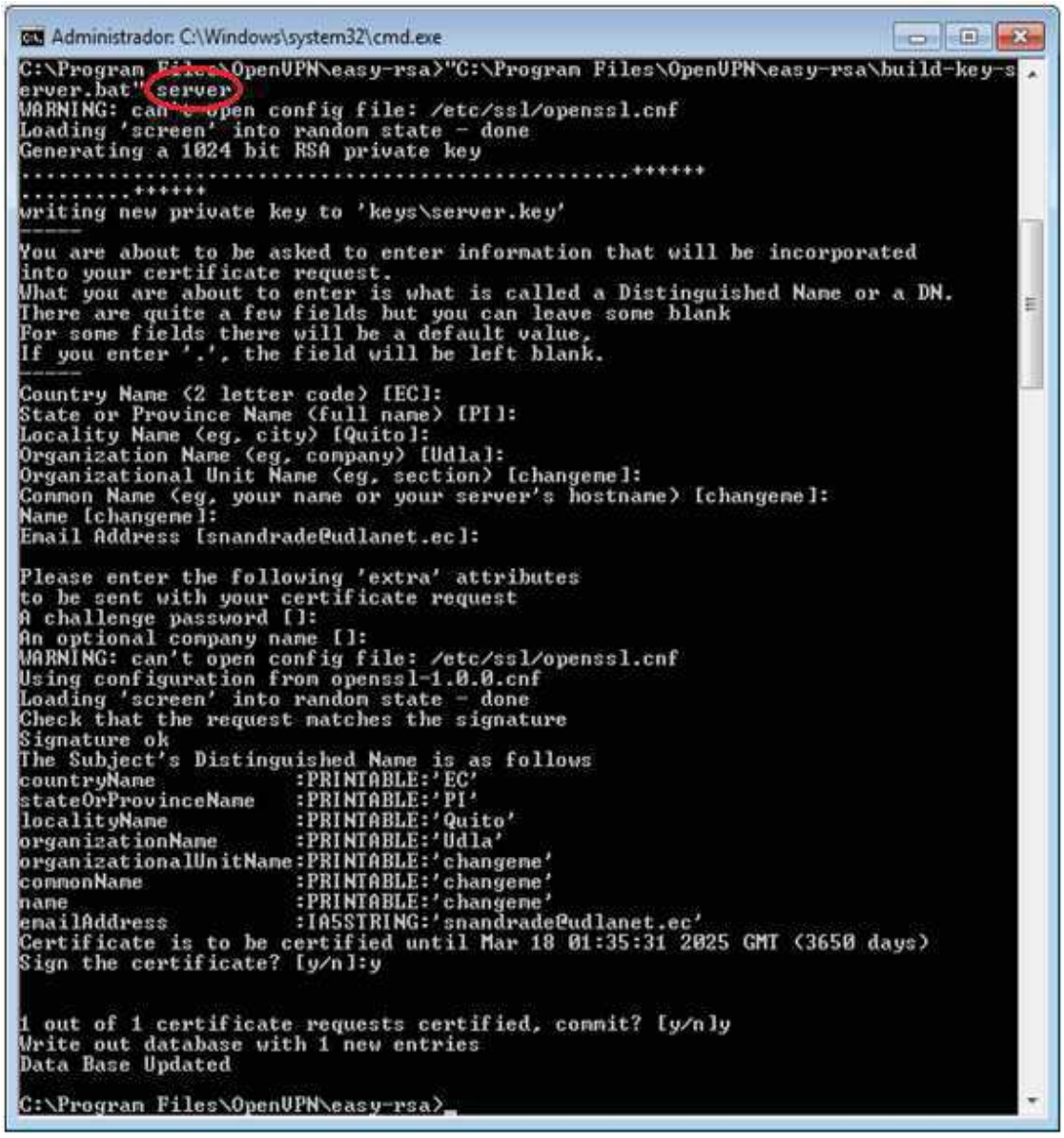


Figura 116. Creación y certificación del servidor “server”.

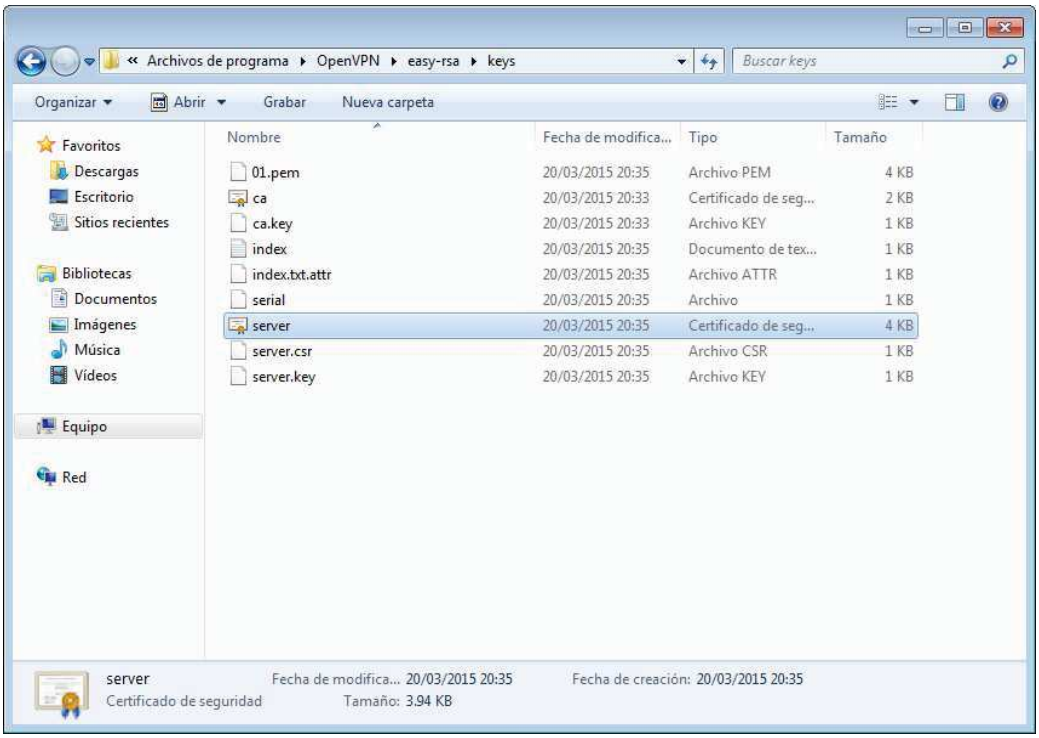


Figura 117. Creación del servidor "server".

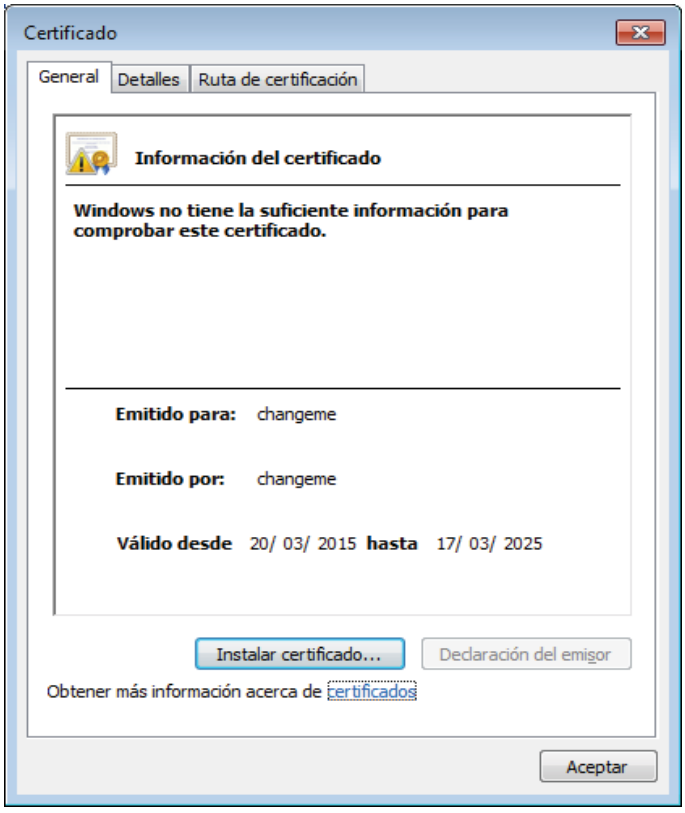


Figura 118. Certificado de seguridad del servidor "server".

- Ubicar el archivo “build-dh”, y copiarlo a la consola de Windows para generar el intercambio de claves.

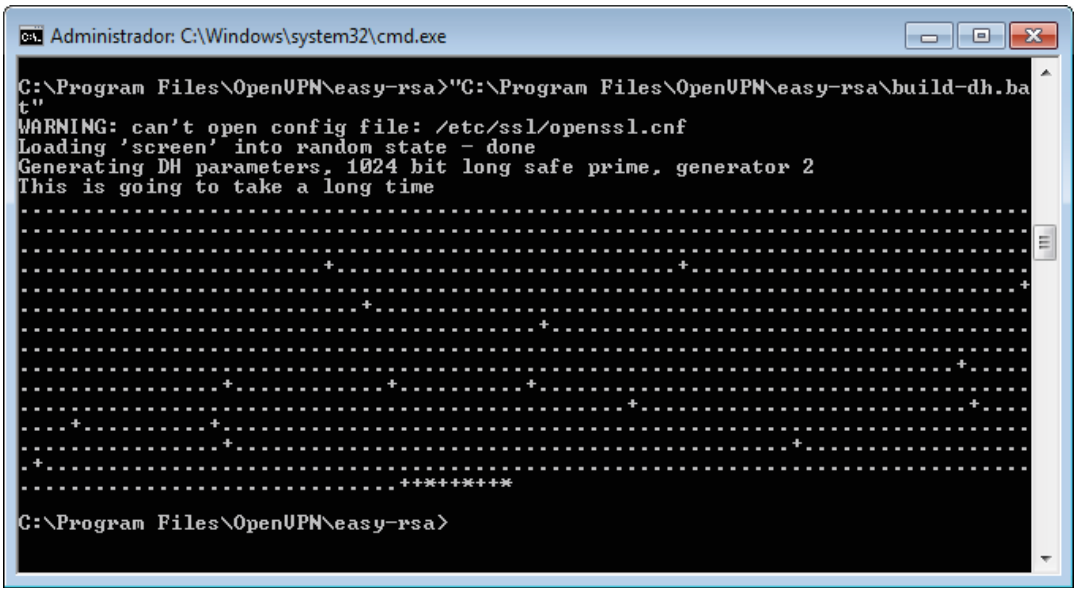


Figura 119. Build-dh.bat: generación de intercambio de claves.

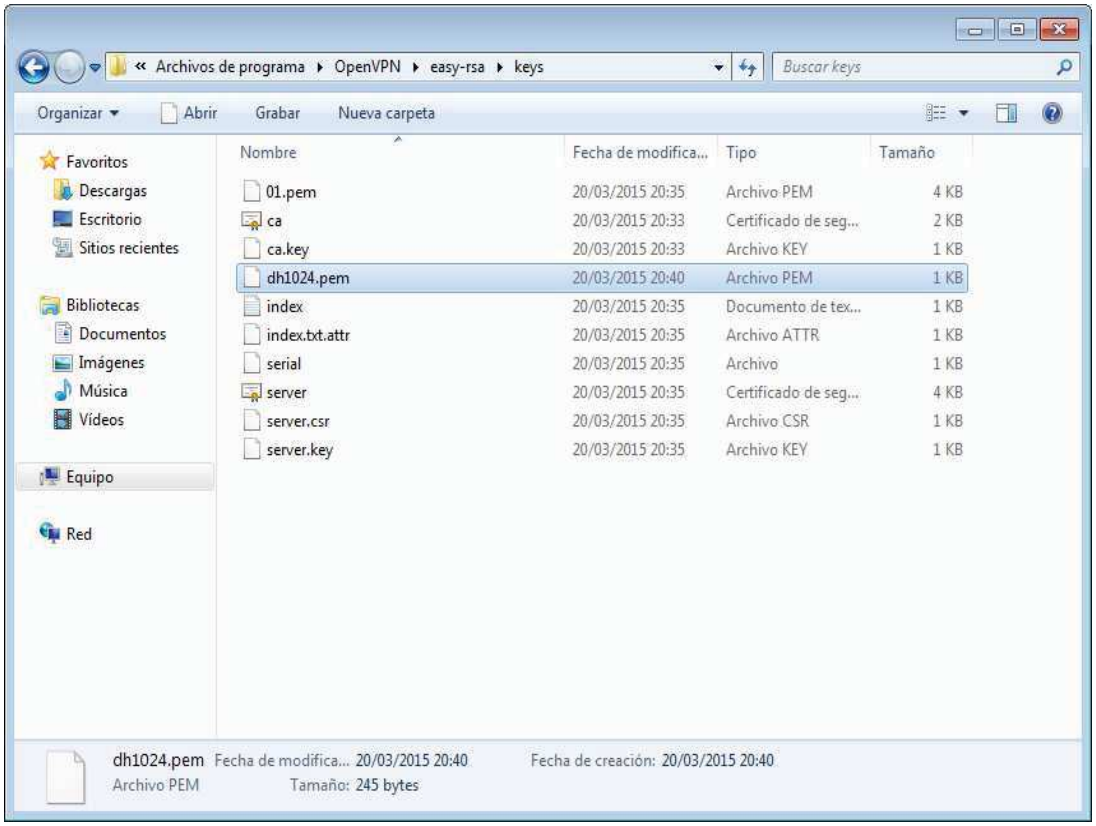


Figura 120. Archivo “dh1024.pem” creado cn comando “build-dh.bat”

11.7.2. Creación de Clientes

- Ubicar el archivo “build-key.bat” y copiarlo a la consola para la creación de un cliente o usuario.

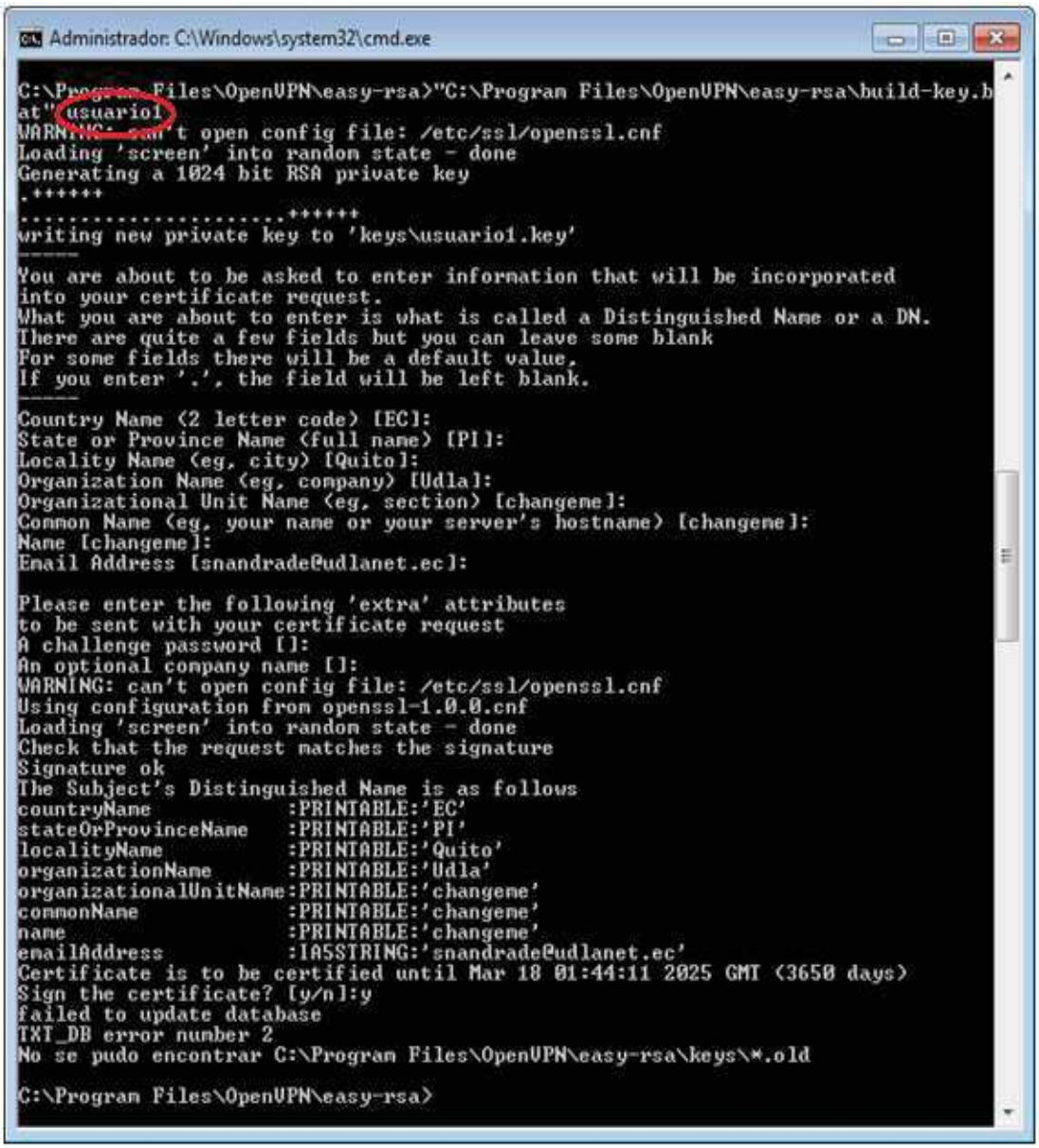


Figura 121. Creación usuario1

- Asignar un nombre. “Usuario1”
- Ubicar el archivo “build-key.bat” y copiarlo a la consola para la creación de un cliente o usuario.
- Asignar un nombre. “Usuario2”

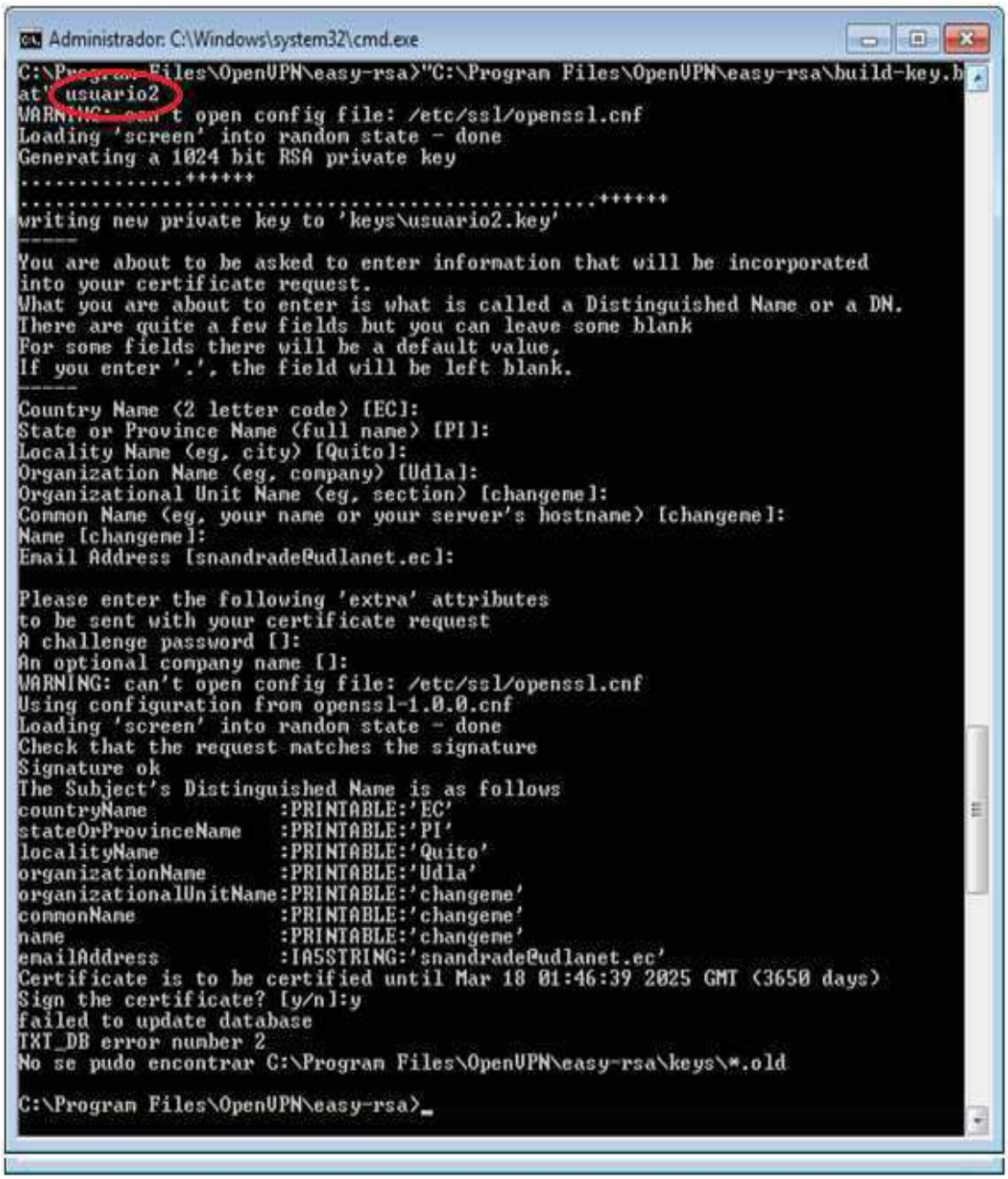


Figura 122. Creación usuario2.

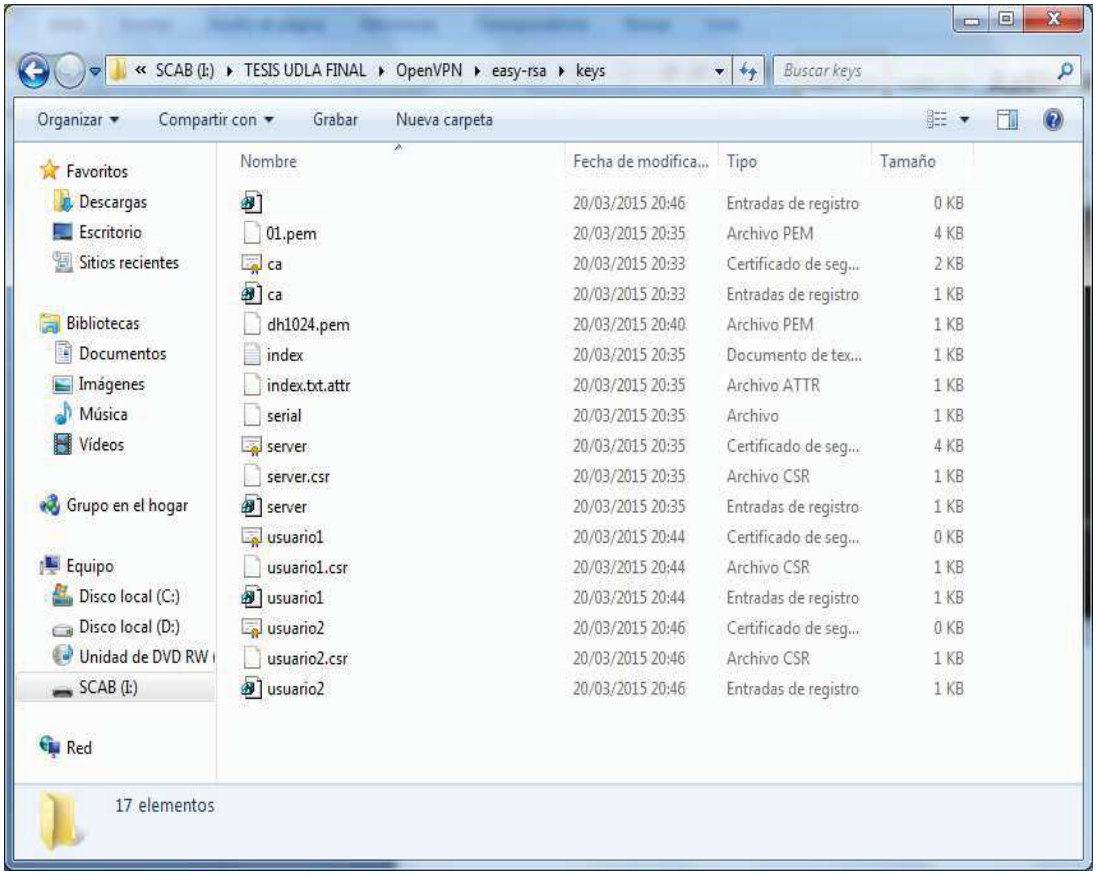


Figura 123. Servidor y clientes creados con sus respectivos certificados.

11.8. TIEMPO ESTIMADO DE LA PRÁCTICA

Una sesión de clase

11.9. ACTIVIDADES PARA LOS ALUMNOS

Realizar una red virtual privada y comprobar su correcto funcionamiento.

11.10. EVALUACIÓN

1. ¿Qué es openvpn?
2. ¿Qué es una vpn?
3. ¿Con que objetivo se configura una vpn?
4. ¿Cómo funciona una vpn?
5. ¿Cómo se comprueba que está funcionando correctamente una vpn?

12. CAPITULO XII

Conclusiones y Recomendaciones

12.1. Conclusiones

La tecnología se ha desarrollado eficazmente de tal forma que en la actualidad la internet se convirtió en una herramienta indispensable para el campo profesional, estudiantil y social, sin embargo según avanza la tecnología, se han desarrollado varios tipos de amenazas informáticas las cuales ponen en peligro a los usuarios de ser víctimas de robos virtuales, suplantación de identidad, fraudes, pérdida de información, etc. Pero a pesar de dichas amenazas existen soluciones que se pueden tomar en cuenta para disminuir el riesgo de ser víctimas de la delincuencia virtual.

En este proyecto se han diseño y desarrollado once prácticas de laboratorio para el aprendizaje del estudiante que tomará la asignatura “Seguridad en Redes” de la Carrera Redes y Telecomunicaciones de la Universidad de las Américas.

Es importante indicar que los once laboratorios realizados en este proyecto de tesis, son una pequeña muestra de todos los métodos que se tiene para protegerse de las amenazas virtuales que existen en la actualidad.

Como se pudo observar el diseño y desarrollo de las once prácticas de laboratorio indican lo fácil que es proteger una red de las amenazas virtuales y además los estudiantes estarán adquiriendo los conocimientos necesarios para la asignatura “Seguridad en Redes”.

Los laboratorios se desarrollaron con software específicos y actualizados para el uso extendido en las aulas de la Universidad de las Américas.

12.2. Recomendaciones

Se recomienda a la Universidad de las Américas dar mantenimiento preventivo y correctivo, periódicamente a los equipos de los diferentes laboratorios para el funcionamiento adecuado al momento de realizar las prácticas.

De igual forma, se recomienda al profesor fijado para dictar la asignatura “Seguridad en Redes”, realizar una pequeña introducción con sus respectivos temas de la práctica que va a realizar.

A los estudiantes ir previamente preparados con el laboratorio que van a realizar, ya sea con los materiales o temas a investigar.

Se recomienda evaluar cada laboratorio realizado para verificar el porcentaje de conocimientos obtenidos en cada clase dictada.

13. Referencias

1. ALEGSA. Definición de Bloc de Notas. Recuperado el 30 de julio del 2014 de:http://www.alegsa.com.ar/Dic/bloc%20de%20notas.php#sthash.08ZFe4qe.dpuf(13)
2. Anónimo. File Transfer Protocol. Recuperado del 26 de septiembre del 2014 de : http://es.wikipedia.org/wiki/File_Transfer_Protocol (60)
3. Anónimo. El protocolo UDP. Recuperado el 27 de septiembre del 2014 de: http://neo.lcc.uma.es/evirtual/cdd/tutorial/transporte/udp.html (61)
4. Anónimo. Qué es una Contraseña. Consejos de empleo. Recuperado el 10 de octubre del 2014 de: https://basicoyfacil.wordpress.com/2008/10/21/que-es-una-contrasena-consejos-de-empleo/ (62)
5. Anónimo. Tipos de contraseñas. Recuperado el 20 de octubre del 2014 de: https://sites.google.com/a/iiconcepcion.edu.ar/uso-preventtivo-sobre-internet/tipos-de-contrasenas (64) (65) (66)
6. Anónimo. ARP. Recuperado el 03 de septiembre del 2014 de: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/arp.html(56)
7. Anónimo. Procesos de Windows. Recuperado el 11 de agosto del 2014 de http://es.kioskea.net/faq/582-procesos-de-windows (23) (24) (25)
8. Anónimo. Puerto/Puertos TCP/IP. Recuperado el 23 de agosto del 2014 de http://es.kioskea.net/contents/272-puerto-puertos-tcp-ip (52)
9. Anónimo. DHCP. Recuperado el 05 de septiembre del 2014 de: http://es.kioskea.net/contents/261-el-protocolo-dhcp(57)
10. Anónimo. HTTP. Recuperado el 05 de septiembre del 2014 de: http://es.kioskea.net/contents/264-el-protocolo-http (58)
11. Anónimo. Sugerencias para crear una contraseña segura. Recuperado el 13 de octubre del 2014 de: http://windows.microsoft.com/es-419/windows-vista/tips-for-creating-a-strong-password (63)

12. Anónimo. Trucos Windows. Eliminar Malware. Recuperado el 11 de agosto del 2014 de https://www.trucoswindows.net/procesos/eliminar-malware/ (22)
13. Anónimo. ¿Qué es un Firewall?. Recuperado el 30 de Octubre del 2014 de: http://windows.microsoft.com/es-xl/windows/what-is-firewall#1TC=windows-7 (68)
14. Anónimo. ¿Qué es ESET SysInspector? Recuperado el 10 de agosto del 2014 de:http://kb.eset.es/business/soln762 (21)
15. Anónimo. Glosario. Recuperado el 20 de agosto del 2014 de:http://www.welivesecurity.com/la-es/glosario/ (32) (33) (34) (35) (36) (37) (38) (39) (40) (41) (42) (43) (44) (45) (46) (47) (48) (49) (50)
16. Anónimo. Seguridad. VPN. Recuperado el 5 noviembre del 2014 de: http://www.cisco.com/web/ES/solutions/es/vpn/index.html (69)
17. Anónimo. Memoria DDR2 – DDR3. Recuperado el 25 de mayo del 2015 de: http://www.informaticamoderna.com/Memoria_DDR3.htm (71) (72)
18. Barrios, J. Introducción al protocolo DNS. Recuperado el 15 de septiembre del 2014 de: http://www.alcancelibre.org/staticpages/index.php/introduccion-protocolo-dns (59)
19. Castro, J. Informe final de prácticas profesionales. Recuperado el 04 de mayo del 2014 http://es.slideshare.net/JosCastroR/informe-final-deprcticasprofesionales (1)
20. Chávez, J. Protocolo TCP / IP. Recuperado el 30 de agosto del 2014 de: http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml#ixzz3Ub7xS7Sw (53)
21. Echeverria, G. Morán, C. Memorias Ram. Recuperado el 25 de julio del 2014 de: http://www.monografias.com/trabajos11/memoram/memoram.shtml#ixzz3A8jocOlc (8) (9) (10) (11)
22. Jorge. Procesos legítimos y nativos del sistema operativo II. Recuperado el 11 de agosto del 2014 de

http://www.welivesecurity.com/la-es/2009/05/18/procesos-legitimos-nativos-sistema-operativo-ii/ (27) (28) (29) (30) (31)

23. Juarez, G. ¿Cómo funcionan las llaves públicas y privadas? Recuperado el 25 octubre del 2015 de: http://www.alcancelibre.org/article.php/20070620210641855 (67)
24. Krall, C. Notepad++, editor gratuito con ventajas para programar en diversos lenguajes (HTML, CSS, JavaScript, PHP...). Recuperado el 30 de julio del 2014 de:http://www.aprenderaprogramar.com/index.php?option=com_content&view=article&id=205:notepad-editor-gratuito-con-ventajas-para-programar-en-diversos-lenguajes-html-css-javascript-php&catid=57:herramientas-informaticas&Itemid=179 (14)
25. Lucía. Tipos de Discos Duros. Recuperado El 21 de junio del 2014 de http://partesdelacomputadora.info/tipos-de-discos-duros/ (2)
26. Manosalvas, C. Protocolos, Análisis de Tráfico y Simulaciones de Red. Recuperado el 02 de septiembre del 2014 de:http://www.monografias.com/trabajos93/protocolos-analisis-trafico-y-simulaciones-red/protocolos-analisis-trafico-y-simulaciones-red.shtml (54) (55)
27. Martín, J. Tipos de Discos Duros. Posteado el 07 de abril del 2012. Recuperado el 15 julio del 2014 de: http://equipotecnico.es/es/tutoriales-tecnicos-trucos-y-tecnicas/86-tipos-de-discos-duros.html (4) (5)
28. Martínez, O. Puertos USB en todos los sentidos. Recuperado el 25 de julio del 2014 de http://www.monografias.com/trabajos75/puertos-usb-todos-sentidos/puertos-usb-todos-sentidos.shtml#ixzz3A8m3LXRF (12)
29. NORFIPC. Ver, conocer, e identificar con NETSTAT las conexiones establecidas en el equipo. Recuperado el 20 de agosto del 2014 de: http://norfipc.com/redes/netstat-conocer-ver-conexiones-activas.html (51)
30. Osorio, J. Historia de los Discos Duros. Recuperado el 21 de junio del 2014 de http://www.monografias.com/trabajos37/discos-duros/discos-duros2.shtml#ixzz3QYQOsZ9e (3)

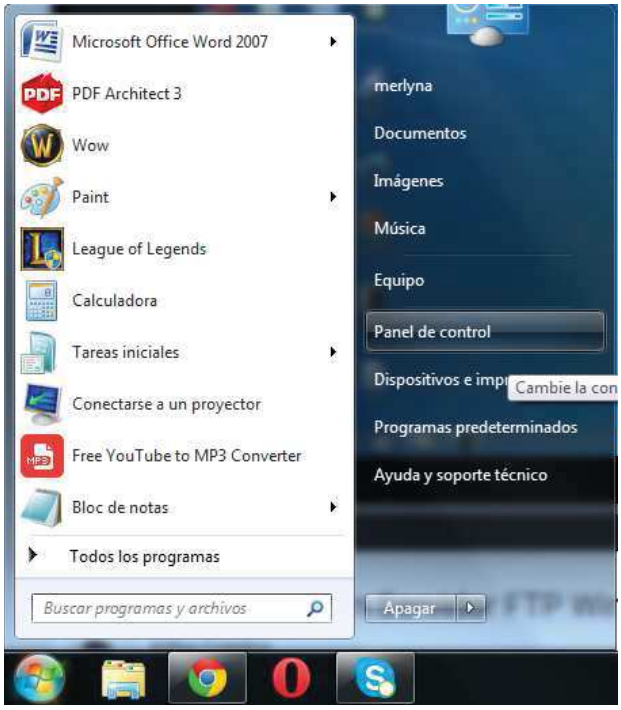
31. Padilla, C. Hot Swap (Inserción en caliente). Recuperado el 25 de julio del 2014 de http://www2.udec.cl/~cpadilla/hotswap.htm (7)
32. Redacción VSAntivirus. Sobre el archivo HOSTS en Microsoft Windows. Recuperado el 11 de agosto del 2014 de: http://www.vsantivirus.com/faq-hosts.htm (26)
33. Rivero, M. ¿Qué son los Malwares?. Recuperado el 5 de enero del 2015 de: https://www.infospyware.com/articulos/que-son-los-malwares(70)
34. Sánchez, A. Disco Duros, ¿Qué es y sus características?. Recuperado el 21 de julio del 2014 de:http://computadoras.about.com/od/conocer-mi-computadora/g/Disco-Duro.htm (6)
35. Vanesa. Tipos de extensiones. Recuperado el 10 de agosto del 2014 de:http://www.monografias.com/trabajos17/extensiones/extensiones.shtml (15) (16) (17) (18) (19) (20)

14. Anexos

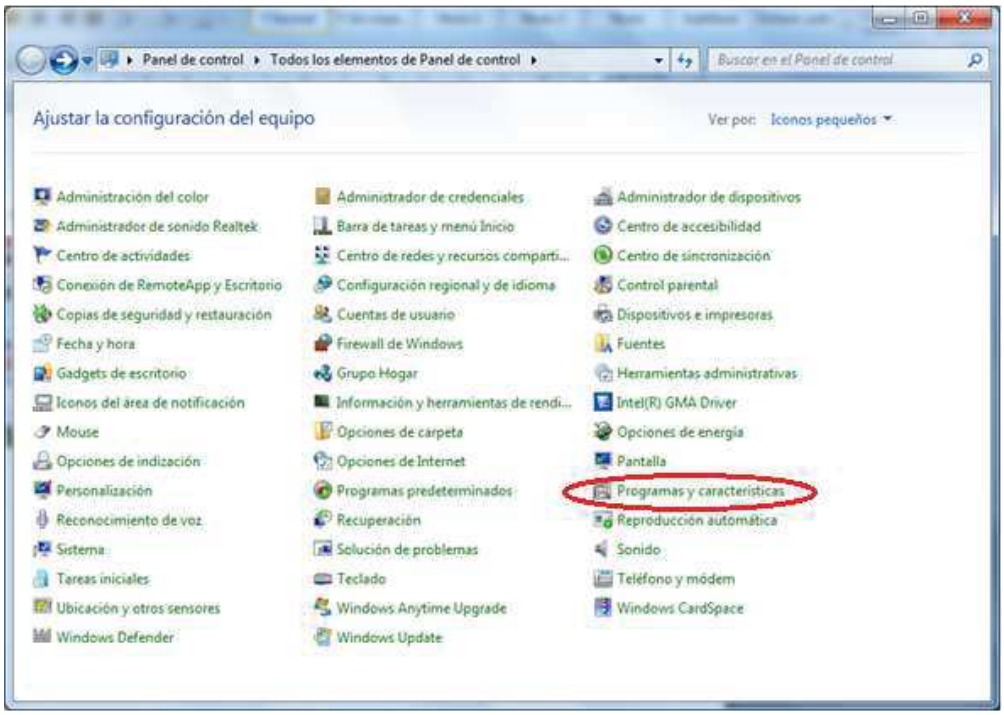
Anexo 1

Configuración de un servidor FTP en Windows 7

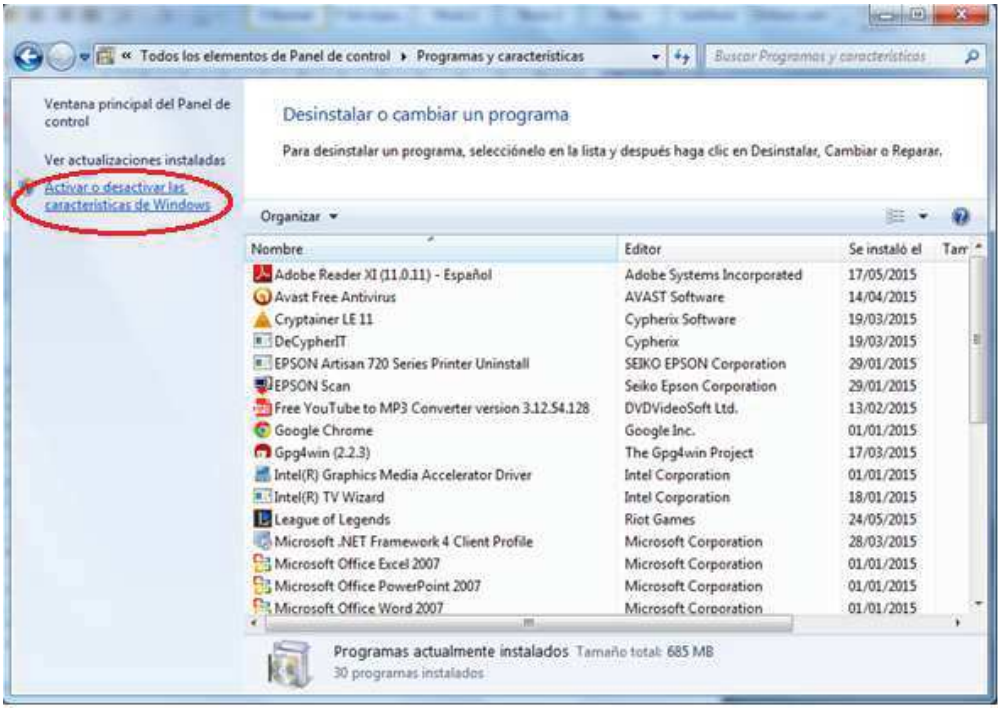
- Dirigirse al botón de Windows
- Abrir “Panel de Control”



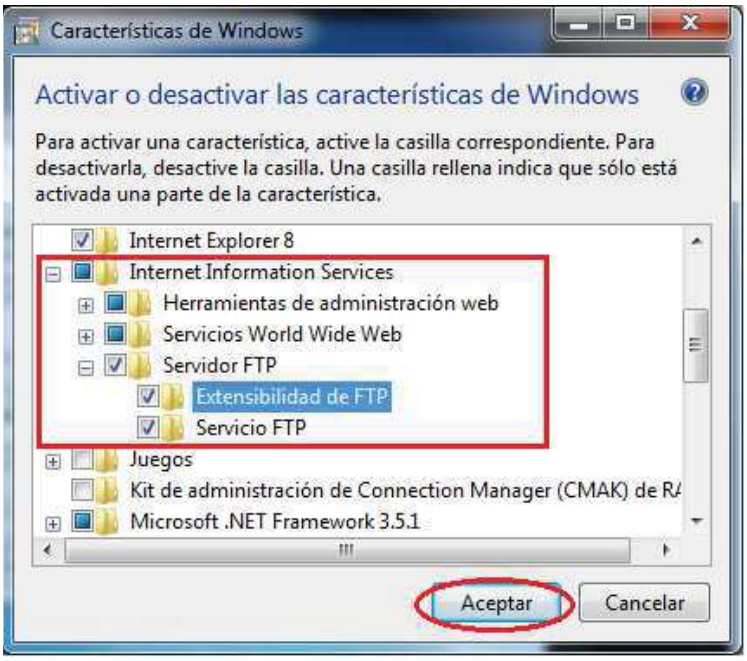
- Opción “Programas y Características”



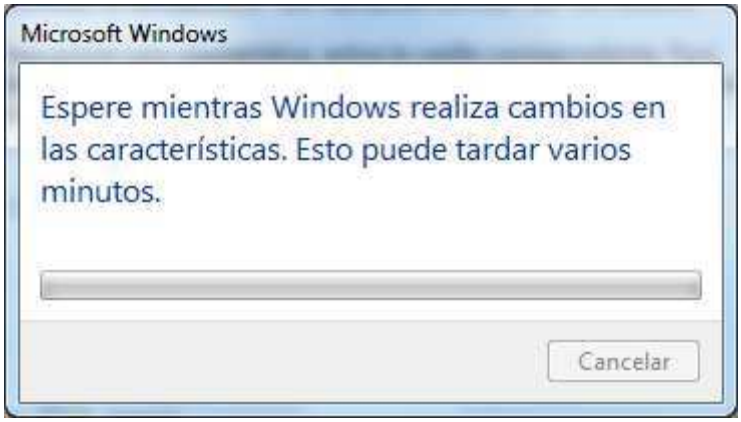
- Dirigirse a la parte izquierda superior de la ventana en la opción “Activar o desactivar las características de Windows”



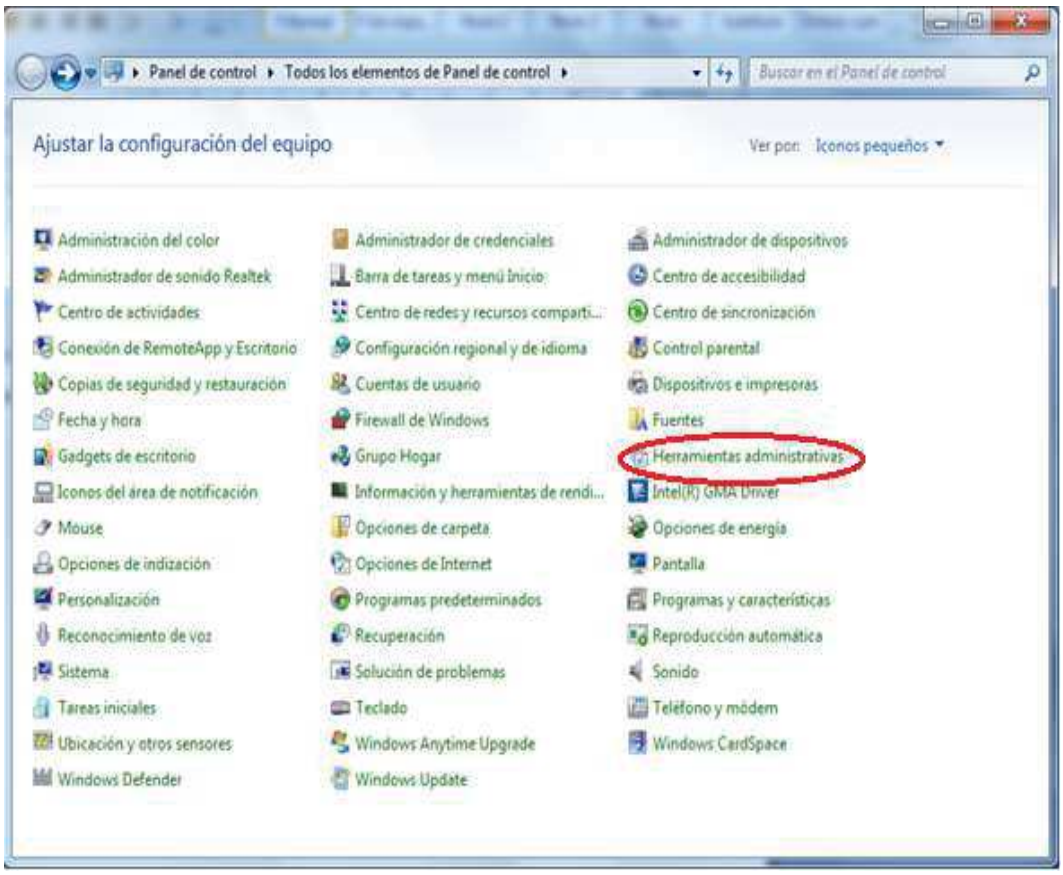
- Buscar la opción “Internet Information Services” y activar todos los servicios.
- Abrir la carpeta “Servidor FTP” y activar todas las opciones.
- Aceptar



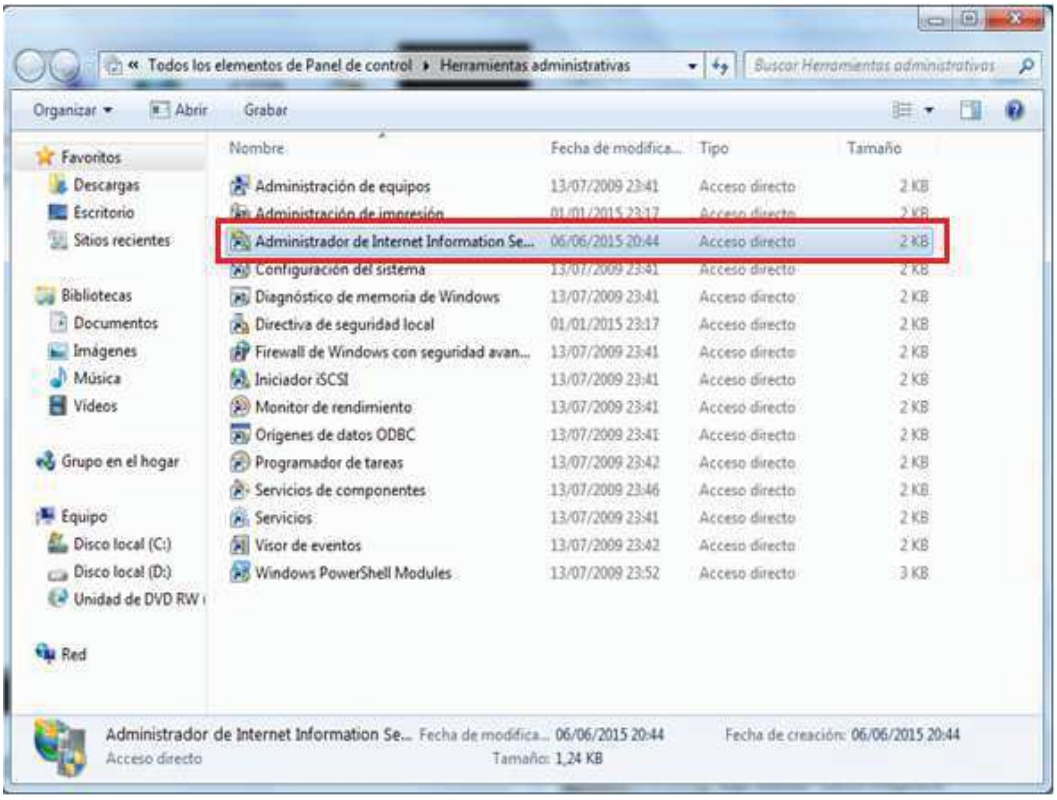
- Esperar que Windows guarde los cambios.



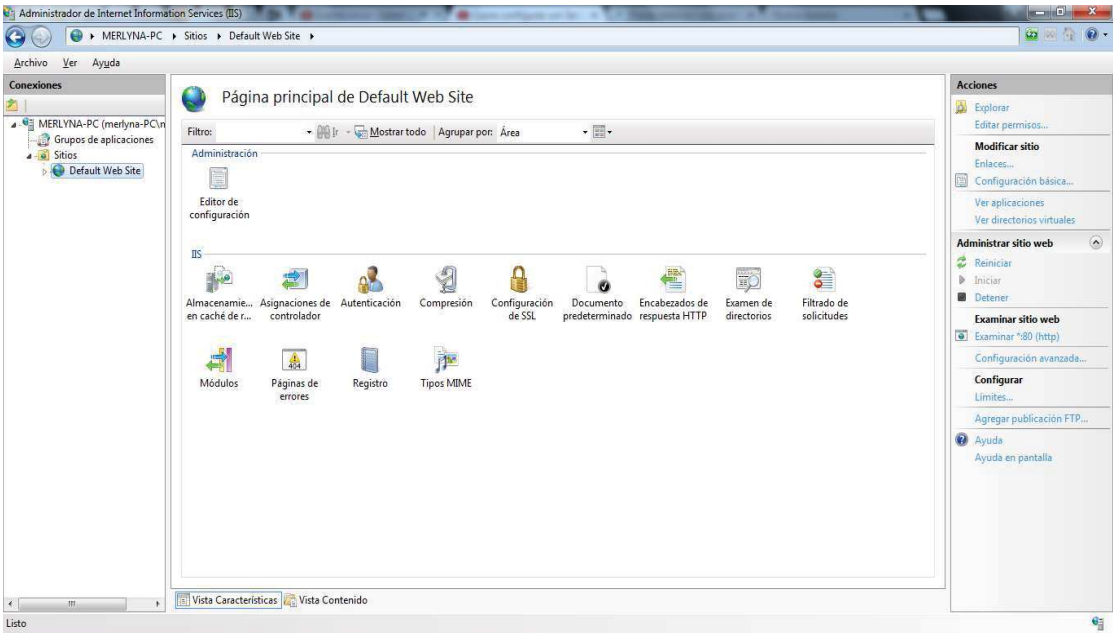
- Regresar a Panel de control
- Opción “Herramientas administrativas”



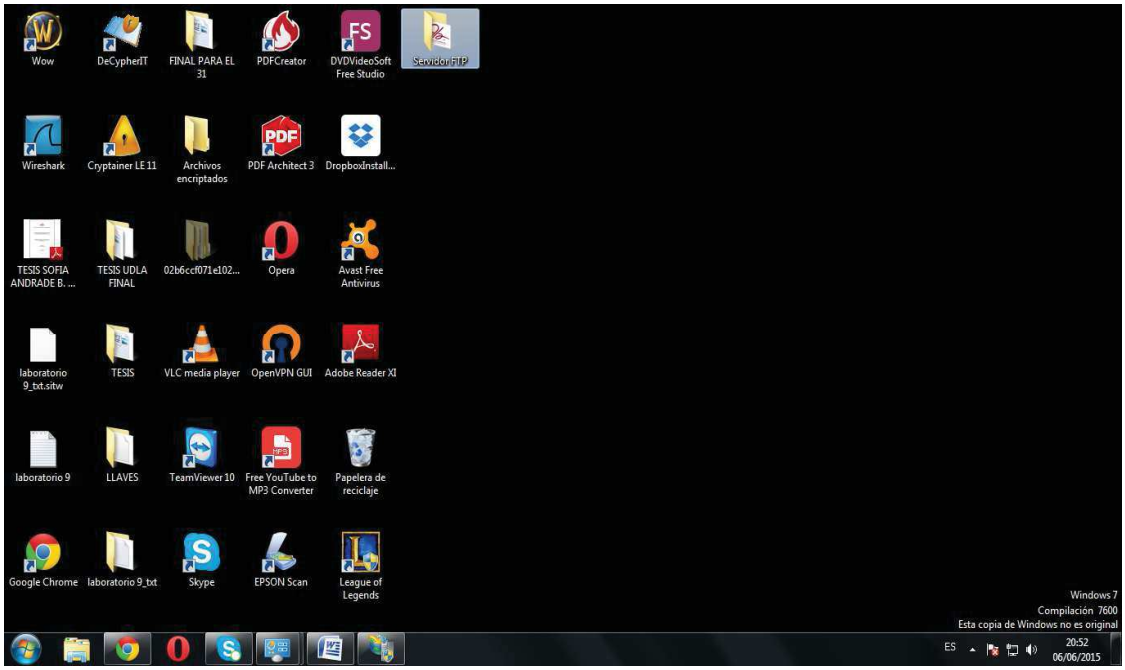
- Dirigirse a “Administrador de Internet Information Services”



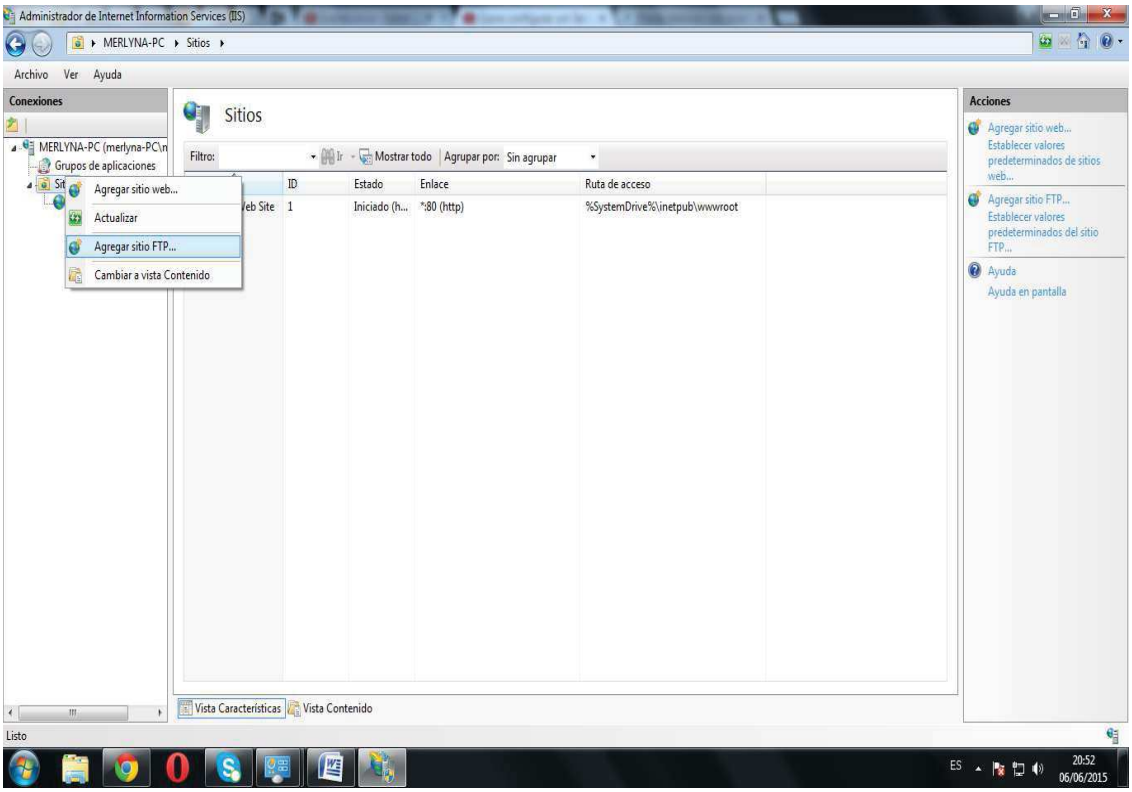
- Observar “Página Principal de Default Web Site”.



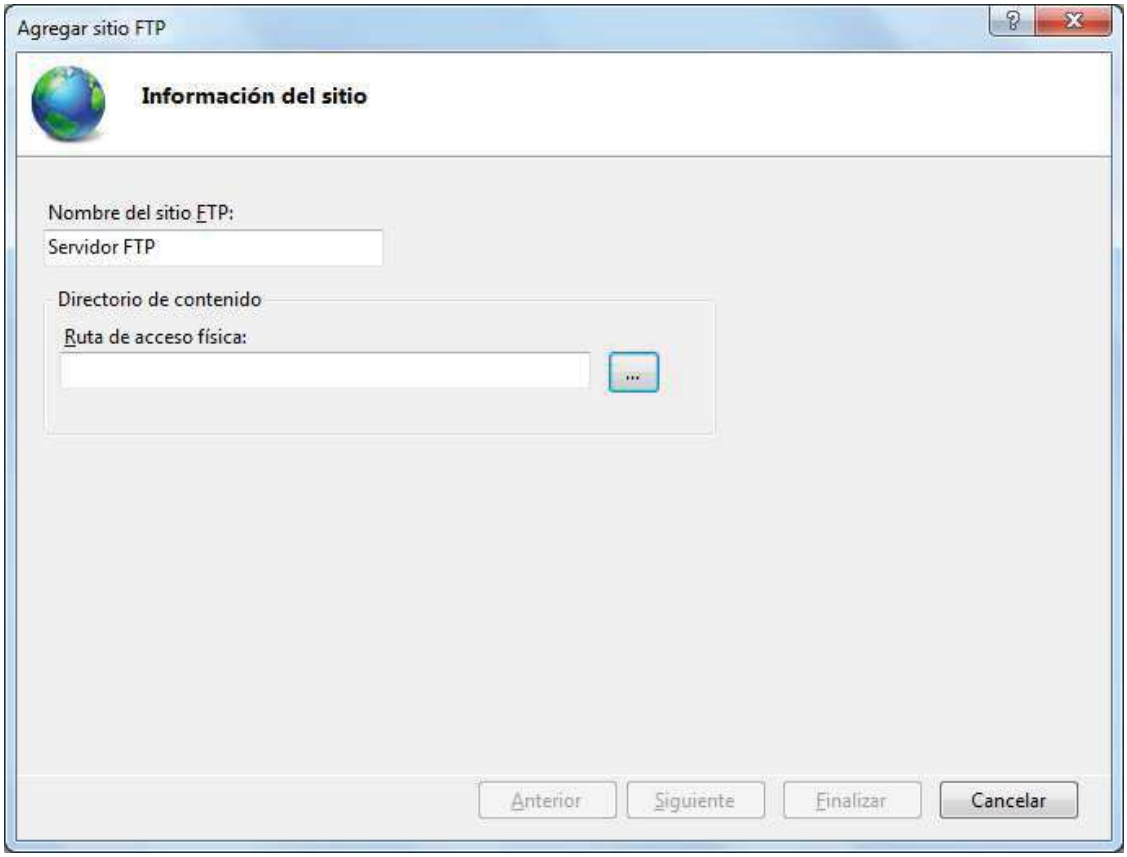
- Crear una carpeta “Servidor FTP” y guardar una imagen o documento dentro de ella.



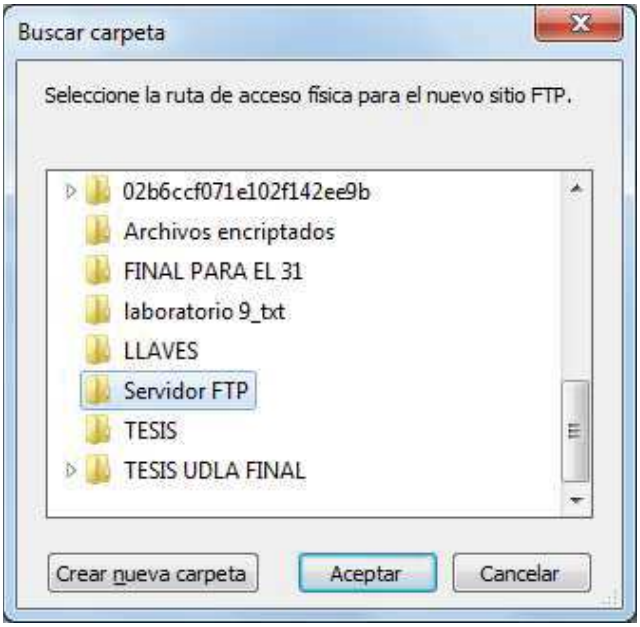
- Regresar a “Administrador de Internet Information Services”
- Dar clic derecho en “Sitios”
- Escoger “Agregar sitio FTP”



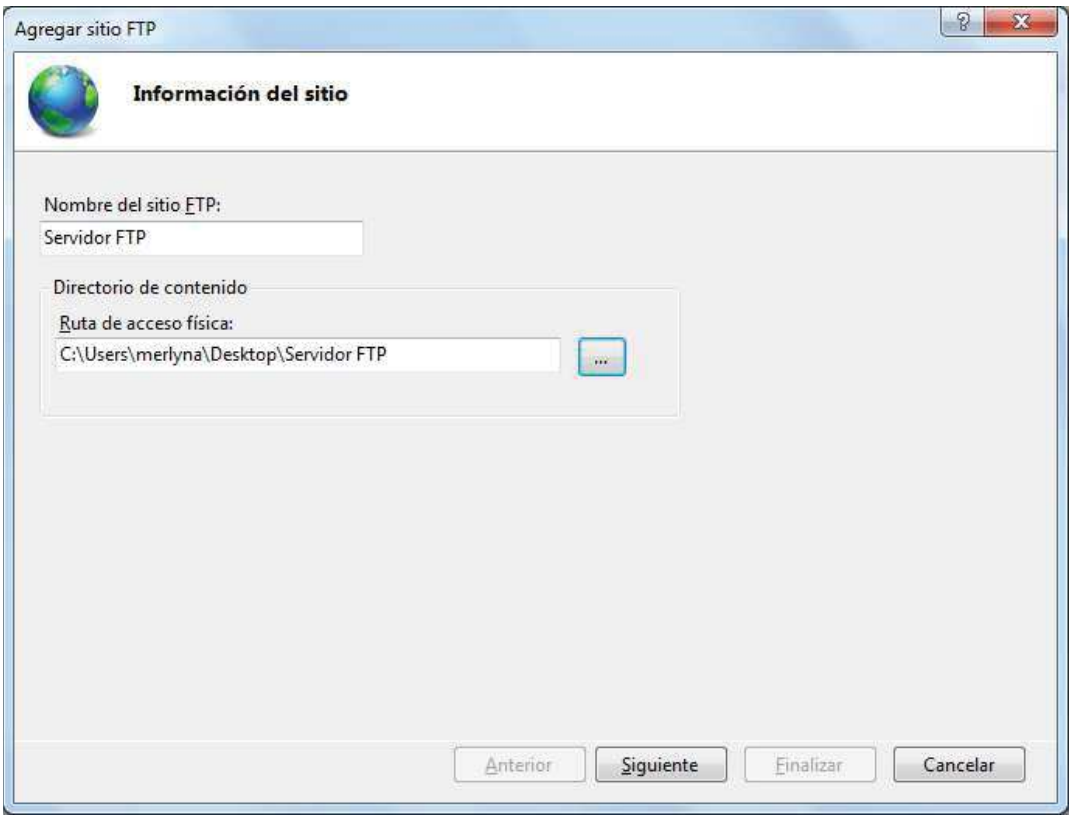
- En nombre del sitio FTP se asignará el mismo nombre de la carpeta que se creó en el escritorio en este ejemplo se llama: Servidor FTP.



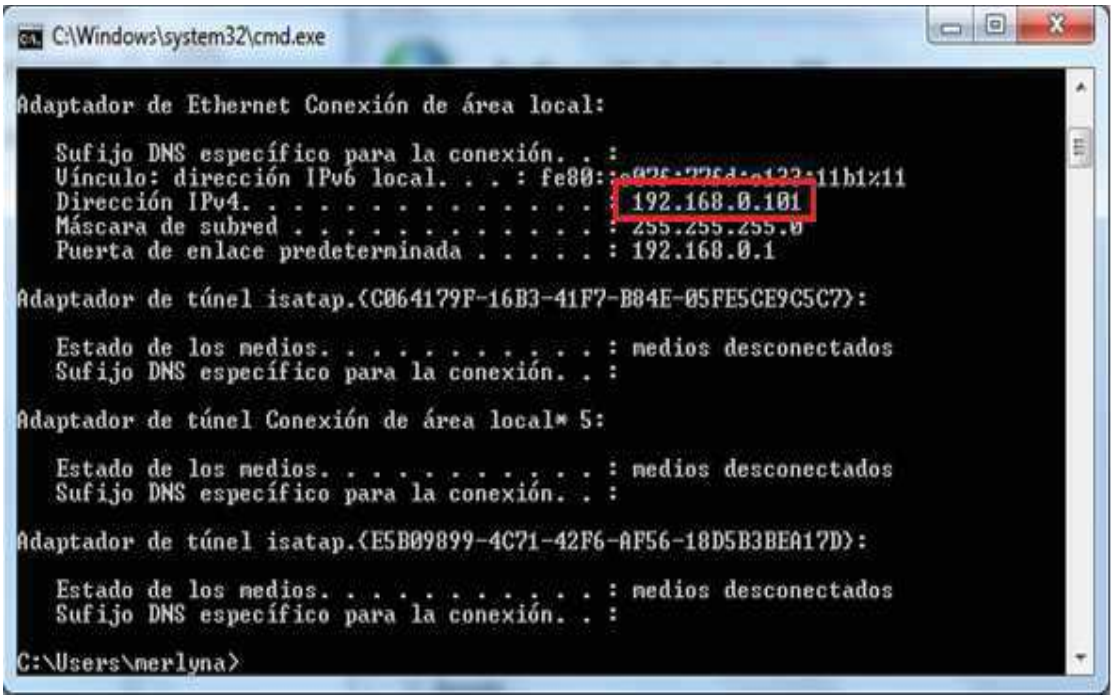
- En “ruta de acceso física” buscamos donde se encuentra la carpeta “Servidor FTP”, en este ejemplo se encuentra en el escritorio.
- Clic en Aceptar



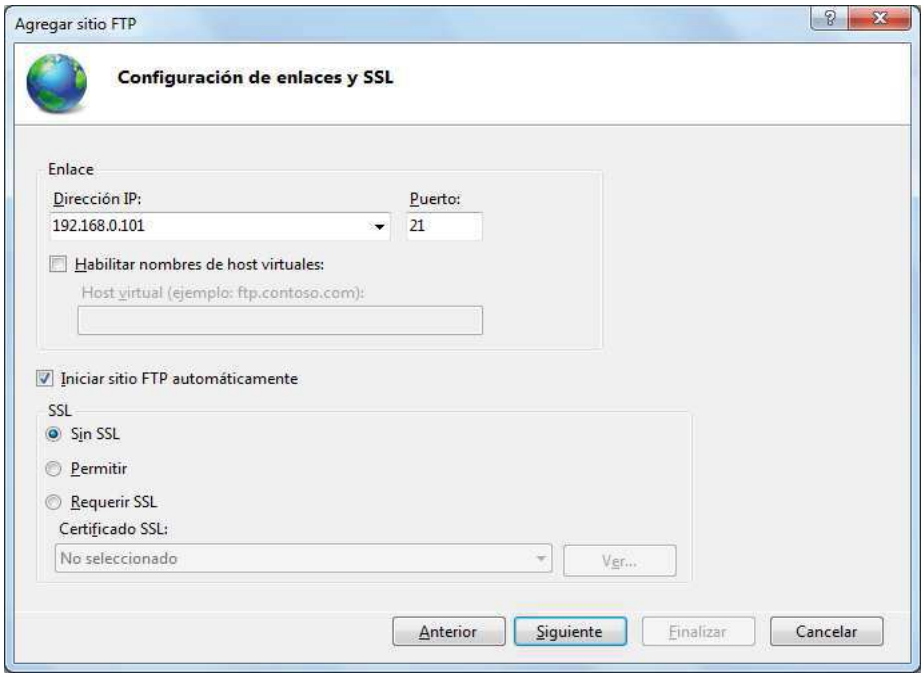
- Clic siguiente



- Para saber la dirección de IP de nuestra red abrimos un “Símbolo de Sistema” e introducimos el comando “ipconfig”.

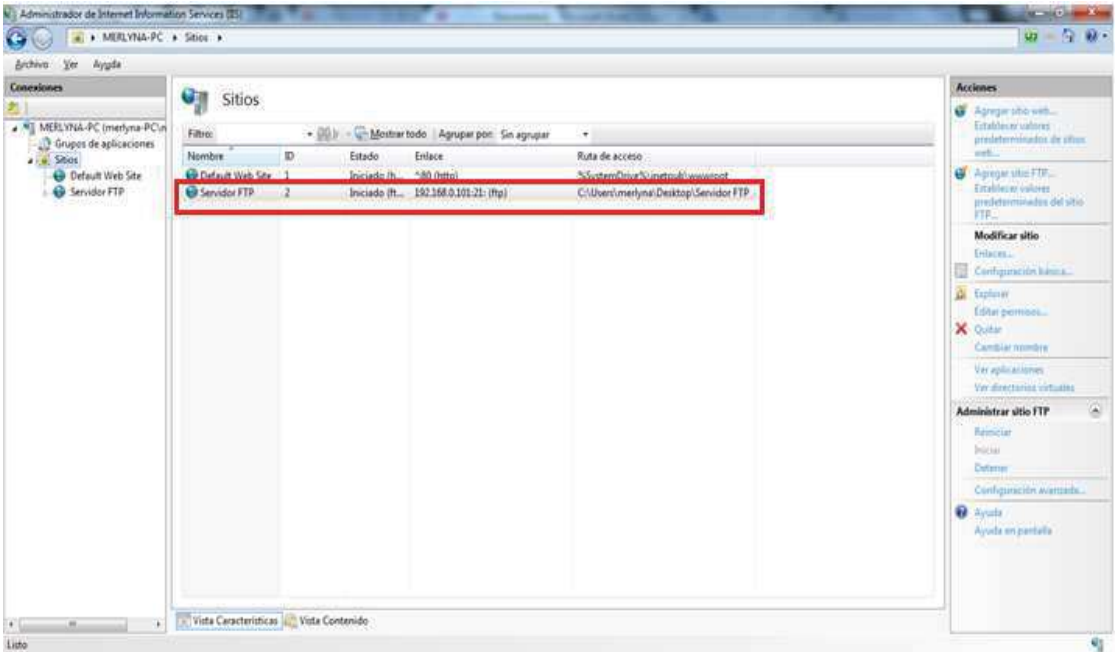


- Con el conocimiento de la dirección IP, regresar a la Configuración de enlaces y SSL e introducir los datos solicitados.
- Clic siguiente

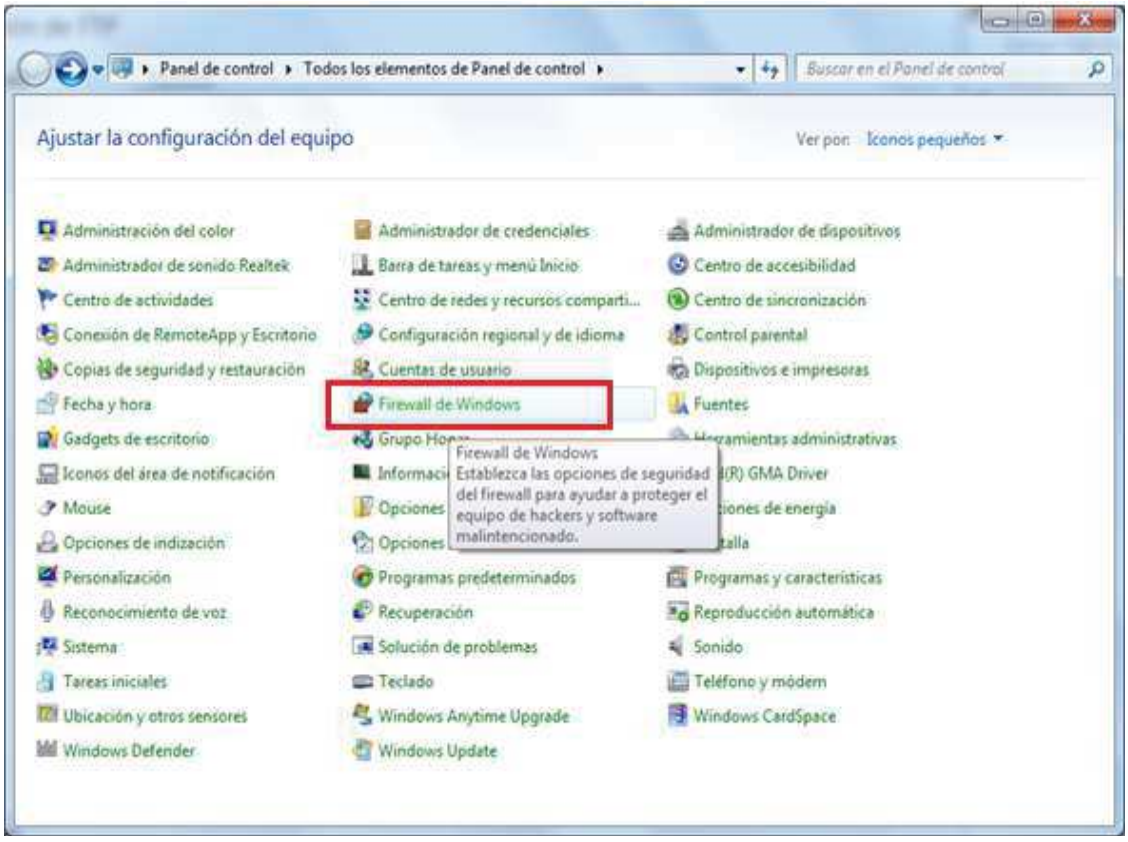


- Autenticación: Básica
- Autorización: Elegir usuarios especificados y escribir el nombre de un usuario creado en la computadora.
- Permisos: Leer – Escribir
- Clic Finalizar

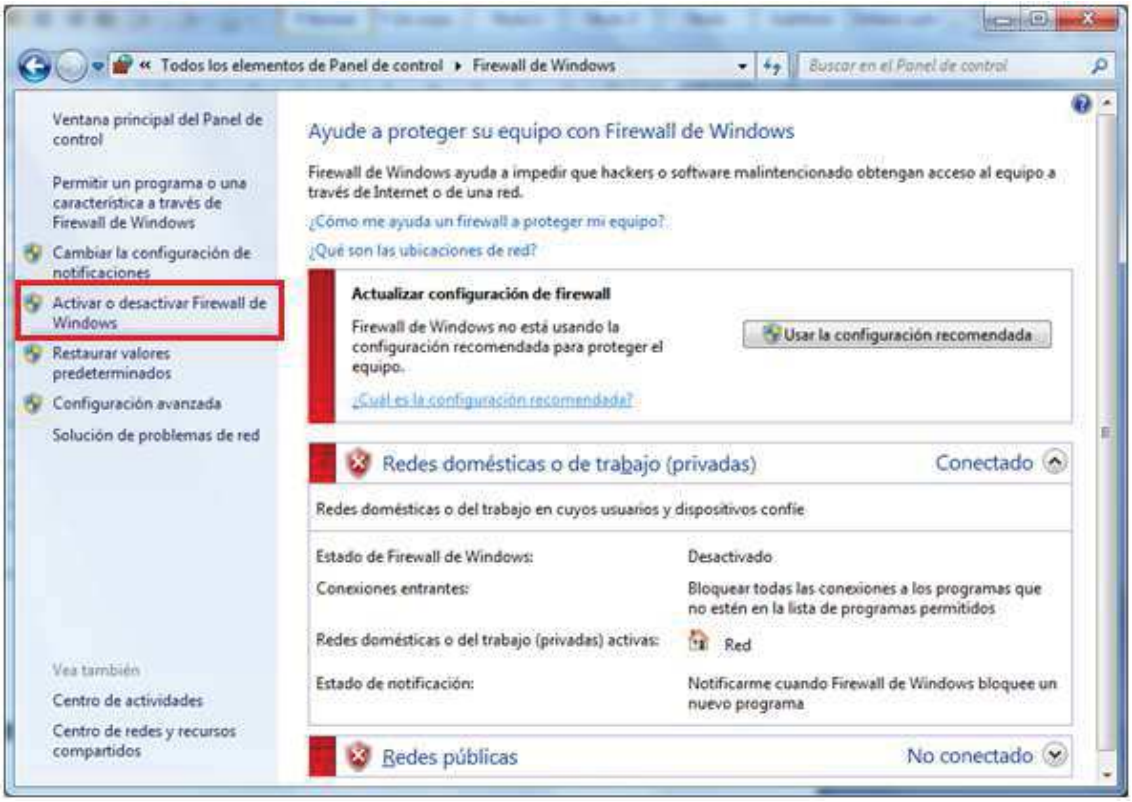
- Se ha creado el sitio “Servidor FTP”.



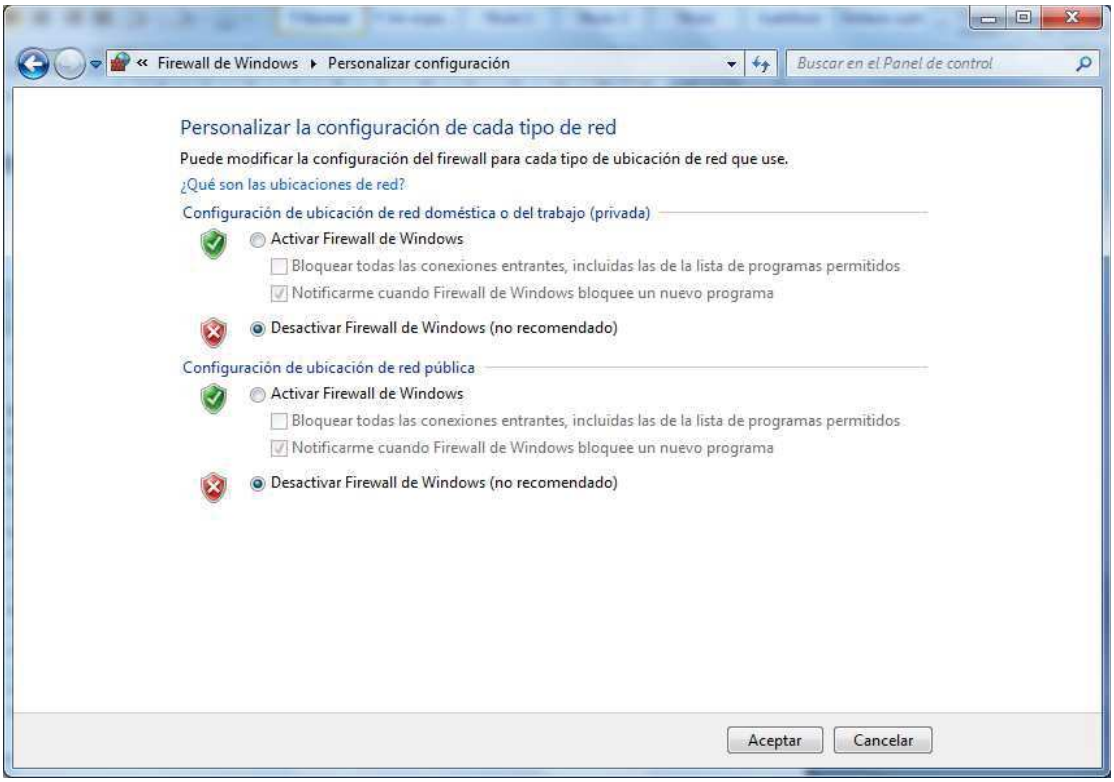
- Dirigirse a Panel de Control
- Opción “Firewall de Windows”.



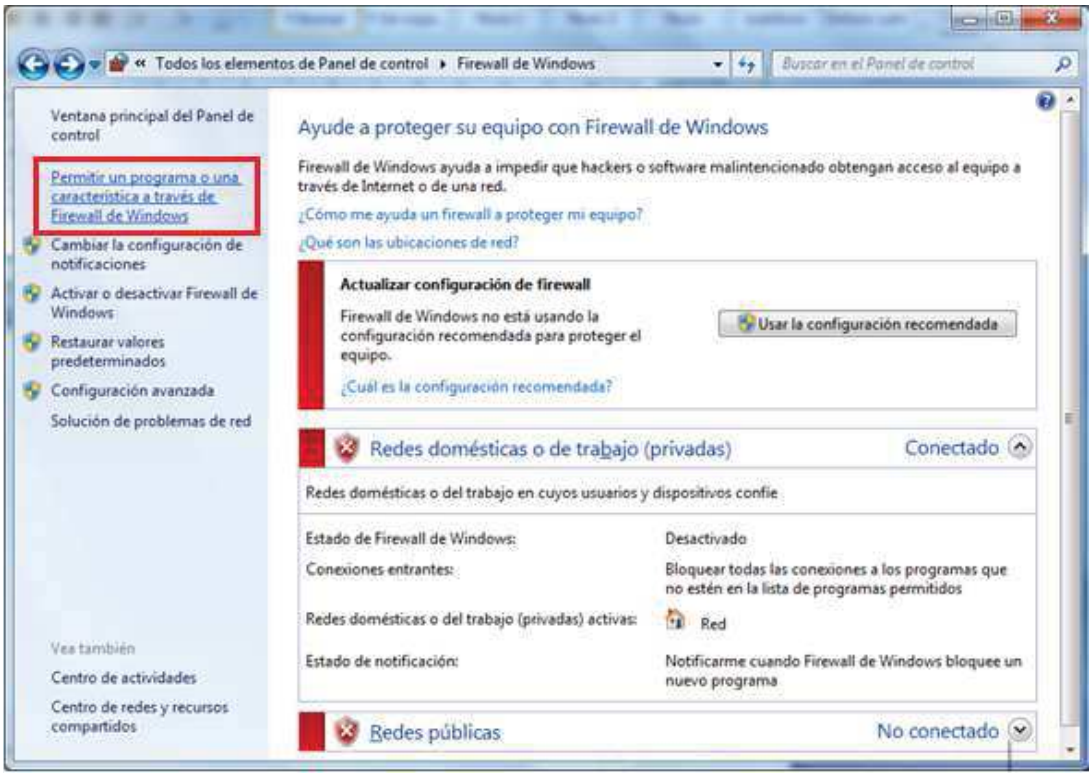
- Opción “Activar o desactivar Firewall de Windows”



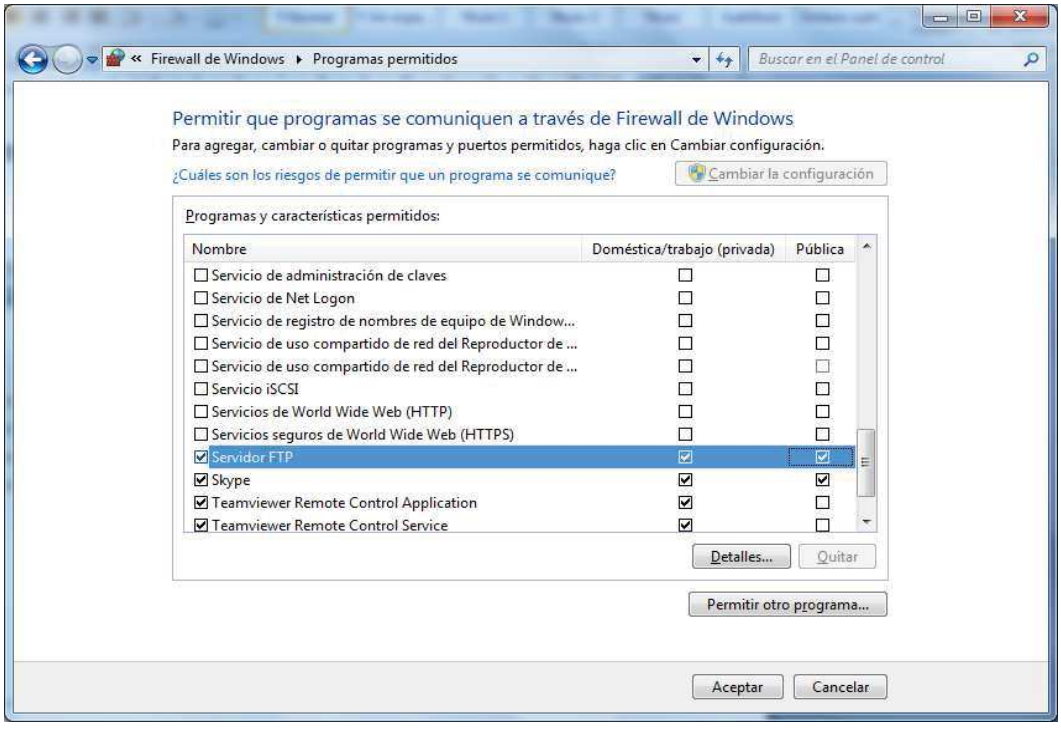
- Desactivar Firewall de Windows, tanto para la red privada como para la pública.



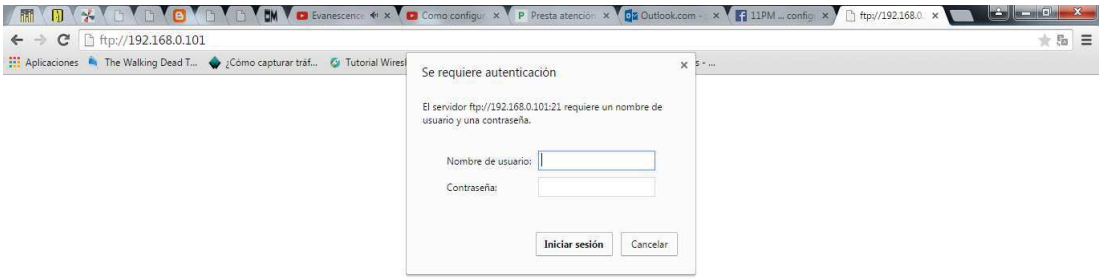
- Regresar a Firewall de Windows
- Elegir esta vez la opción “Permitir un programa o una característica a través de Firewall de Windows”



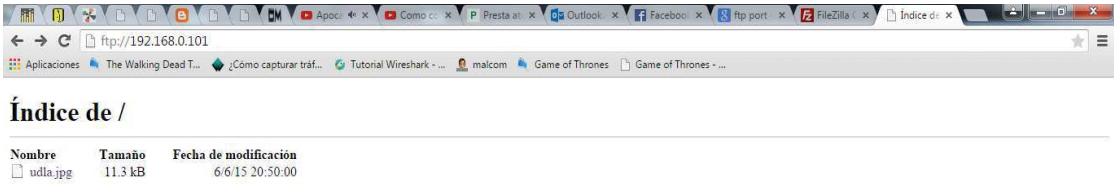
- Buscar “Servidor FTP” y activar las casillas privada y doméstica.
- Clic en aceptar para que se guarden los cambios.



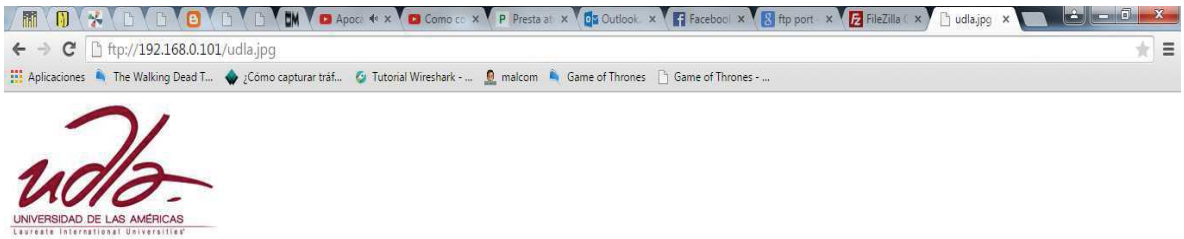
- Dirigirse a una navegador web e introducir la la dirección IP con que asigno al servidor FTP, antepuesto por ftp:///(dirección IP)
- Introducir el nombre de usuario, en este ejemplo fue “merlyna”.
- Contraseña: password del nombre de usuario en computadora.



- Verificar si el contenido de la carpeta “Servidor FTP” es igual al del contenido de la web.



- Abrir la imagen.



El servidor FTP ha sido configurado con éxito.