

LOS PELIGROS DEL ABRIR ARCHIVOS DESCONOCIDOS: CASO PRÁCTICO

Abrir o ejecutar un archivo desconocido en Windows puede ser peligroso debido a la posibilidad de que el archivo contenga software malicioso, como virus, troyanos o ransomware. Estos programas maliciosos pueden dañar tu computadora, robar información personal o incluso tomar el control de tu sistema.

Windows tiene medidas de seguridad para proteger a los usuarios, como advertencias al intentar abrir archivos de fuentes desconocidas. Sin embargo, la mejor protección es la precaución del usuario. Es importante solo abrir archivos de fuentes confiables y tener un software antivirus actualizado.

Recuerda, si no estás seguro de un archivo, es mejor no abrirlo. Siempre es mejor prevenir que lamentar.

El párrafo anterior fue creado usando la inteligencia artificial por Copilot con Bing Chat, acerca de los peligros de abrir o ejecutar un archivo desconocido para los usuarios de escritorio de Windows que son mayoría a nivel mundial.

Es una explicación general que seguramente muchos ya han leído hasta el cansancio pero que es difícil de cuantificar el daño que puede causar; a algunas personas que nunca les ha pasado algo así pueden incluso tener una idea de exageración, a los que les ha pasado, quizás fueron cosas leves que un buen técnico en computadoras pudo solucionar sin muchas complicación y unos pocos, que su campo no provenga de la informática y las ciencias computacionales, les ha pasado y han tenido que aprender dolorosamente estos peligros.

Es por ello que he realizado esta clase de la manera más práctica y simple posible, alejándome de los clásicos conceptos textos similares con la intención de llegar a la gran mayoría de usuarios Windows y puedan aplicar este ejemplo y dar a entender lo peligroso que puede llegar a ser el abrir o ejecutar un archivo desconocido; y mejorar su conocimiento y prácticas en la seguridad de su propia información sin tomarla a la ligera.

PASO 1. APRENDEREMOS A MOSTRAR U OCULTAR EXTENSIONES

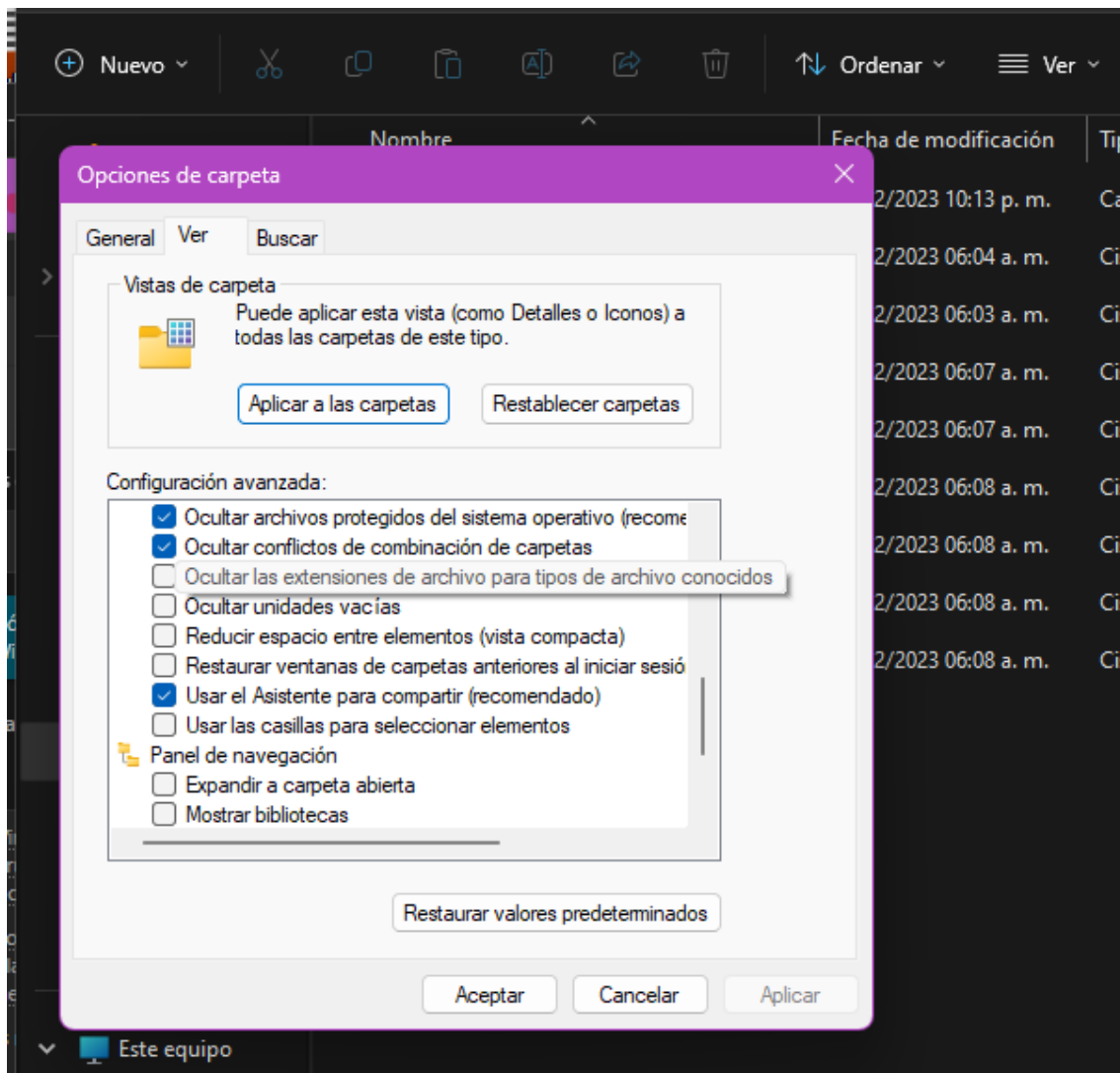
La extensión de un archivo en Windows es un sufijo que aparece separado del nombre del archivo, generalmente por un punto (por ejemplo .exe, .txt, .mp3 o .docx). La extensión de un archivo en Windows es una forma de indicar el tipo de archivo y cómo debe ser manejado por el sistema.

Para mostrar u ocultar las extensiones usando la cinta de opciones de windows 10:

1. Abre el explorador de archivos.
2. Haz clic en el menú *Vista*.
3. Activa la casilla *Extensiones de nombre de archivo* ubicada en el grupo *Mostrar u Ocultar*.
4. Si deseas ocultar la extensión, simplemente desmarca de nuevo la casilla *Extensiones de nombre de archivo*.

Para mostrar u ocultar las extensiones usando la cinta de opciones de Windows 11:

1. Abre el explorador de archivos.
2. Haz clic en el menú *ver más* y seleccionar *Opciones*
3. En *Opciones de carpeta*, hacer clic en la opción *Ver*
4. En la sección *Configuración Avanzada*
5. Desactiva la casilla *Ocultar las extensiones de archivo para tipos de archivo conocido* .
6. Si deseas ocultar la extensión, simplemente marca de nuevo la casilla *Ocultar las extensiones de archivo para tipos de archivo conocido*.



Dejar que se muestren las extensiones de los archivos

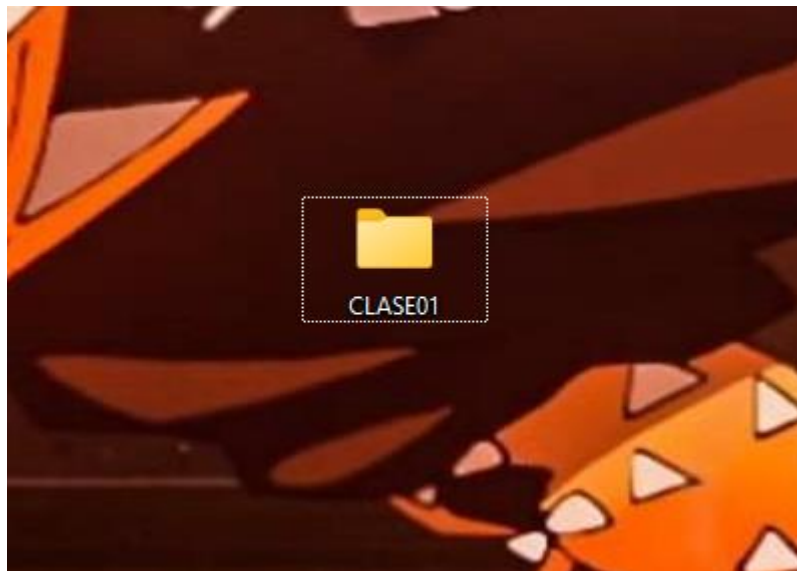
PASO 2. ESCRIBIR PRIMER ARCHIVO BATCH

Un archivo batch en Windows, también conocido como archivo bat, es un archivo de texto simple que contiene una serie de comandos que pueden ser interpretados y ejecutados por el sistema operativo.

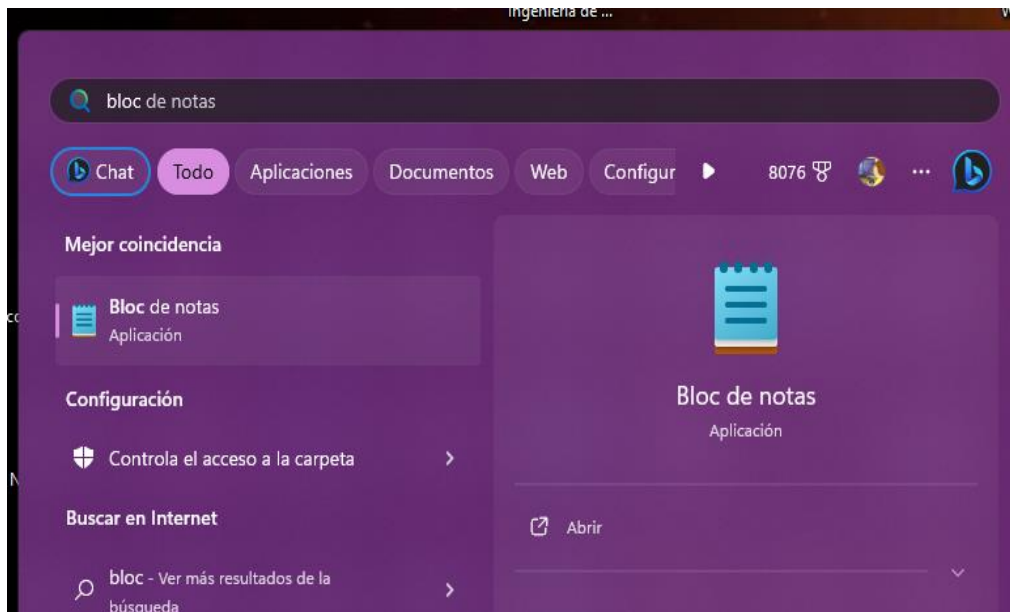
Ejemplos de algunos esos comandos, que aprenderlos no es el objetivo de esta clase, son:

- CMD
- DIR
- COPY
- DEL }
- ECHO
- EXIT
- FORMAT
- CD
- CLS
- REN
- MKDIR
- TASKKILL

Crear una carpeta en la ubicación de su preferencia, en mi caso la crearé en el escritorio y la llamaré CLASE01.



Abrir un bloc de notas (Notepad)



Y escribir en el bloc de notas el siguiente texto:

```
@echo off  
title Mi primer archivo Batch  
echo Bienvenidos  
pause
```



El comando **echo** lo que hace es mostrar un mensaje al usuario.

El comando **title**, es el título del archivo.

El comando **pause** detiene la ejecución, porque una cualidad de estos archivos batch, es que ejecutan todos sus comandos y se cierran.

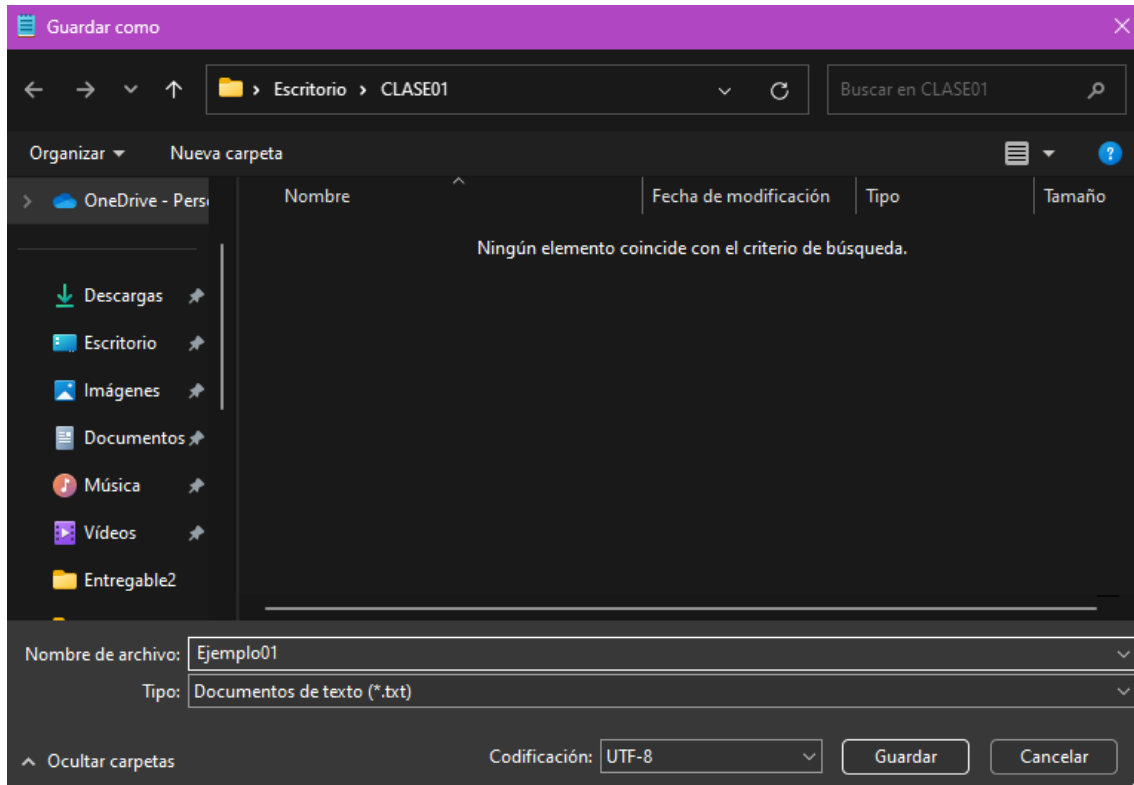
En este caso lo que hace es mostrar un mensaje de Bienvenidos.

PASO 3. GUARDAR ARCHIVO COMO BATCH

Una vez que haya colocado esas líneas en el bloc de notas

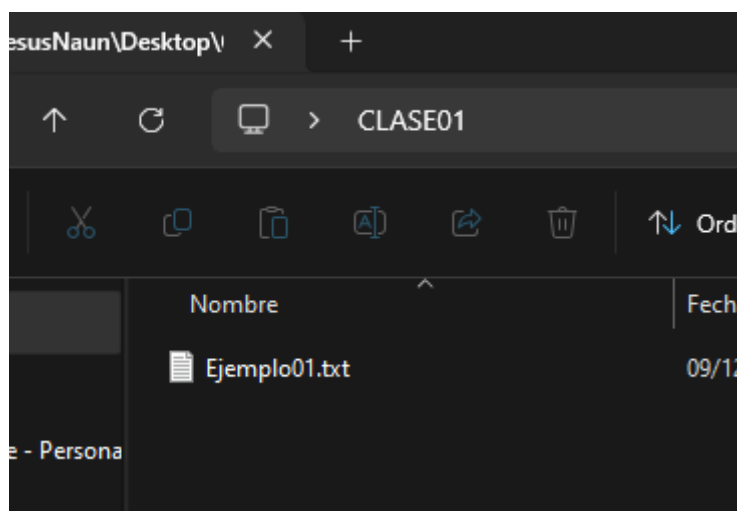
Clic en **Archivo, Guardar como** y seleccione la carpeta CLASE01.

En mi caso le he colocado el nombre “Ejemplo01.txt”



Clic en **Guardar**

Ahora debería tener un archivo con extensión txt dentro de la carpeta CLASE01

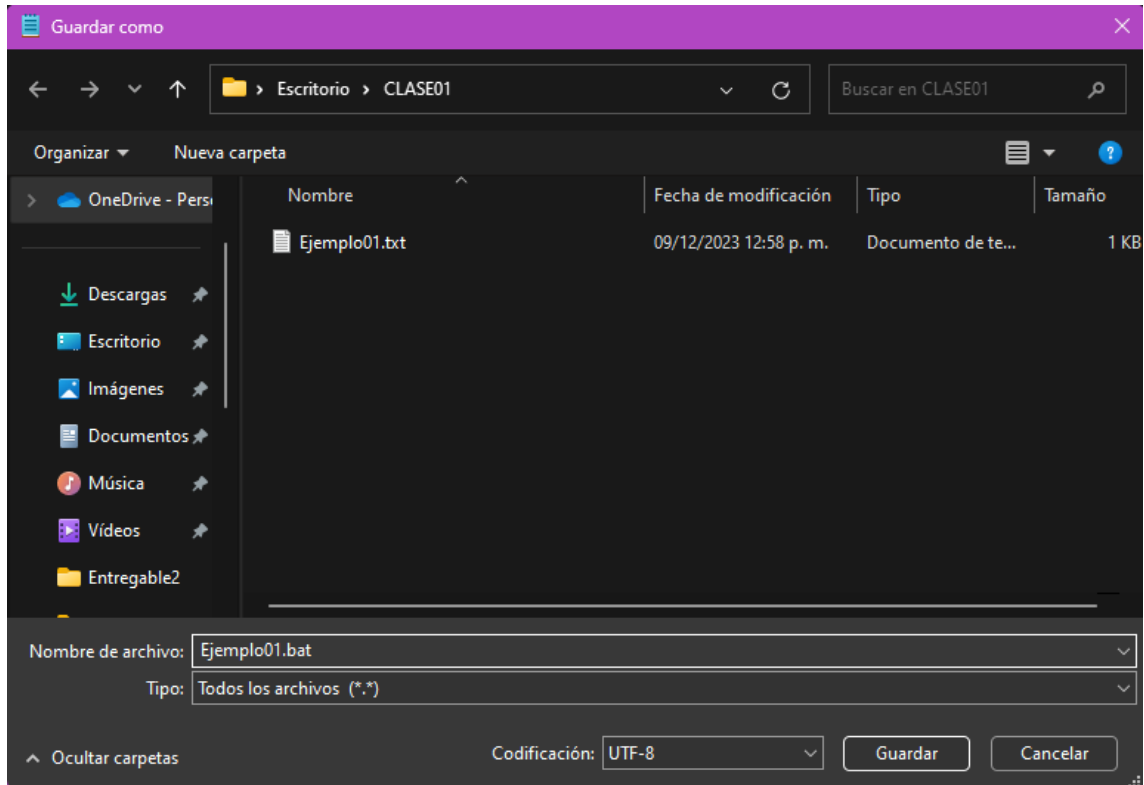


Ahora procederemos a guardar ese mismo archivo, pero con extensión bat

Clic en **Archivo , Guardar como** y seleccione la carpeta CLASE01.

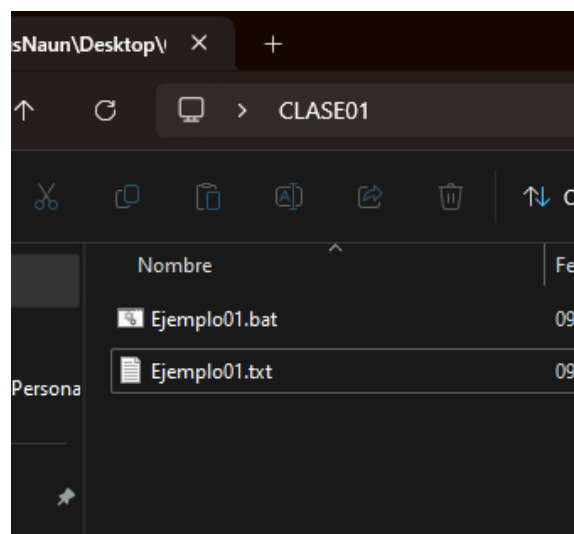
Pero es esta ocasión el nombre del archivo será “Ejemplo01.bat”

Y cosa muy importante, en Tipo debe seleccionar “Todos los archivos (*.*)”



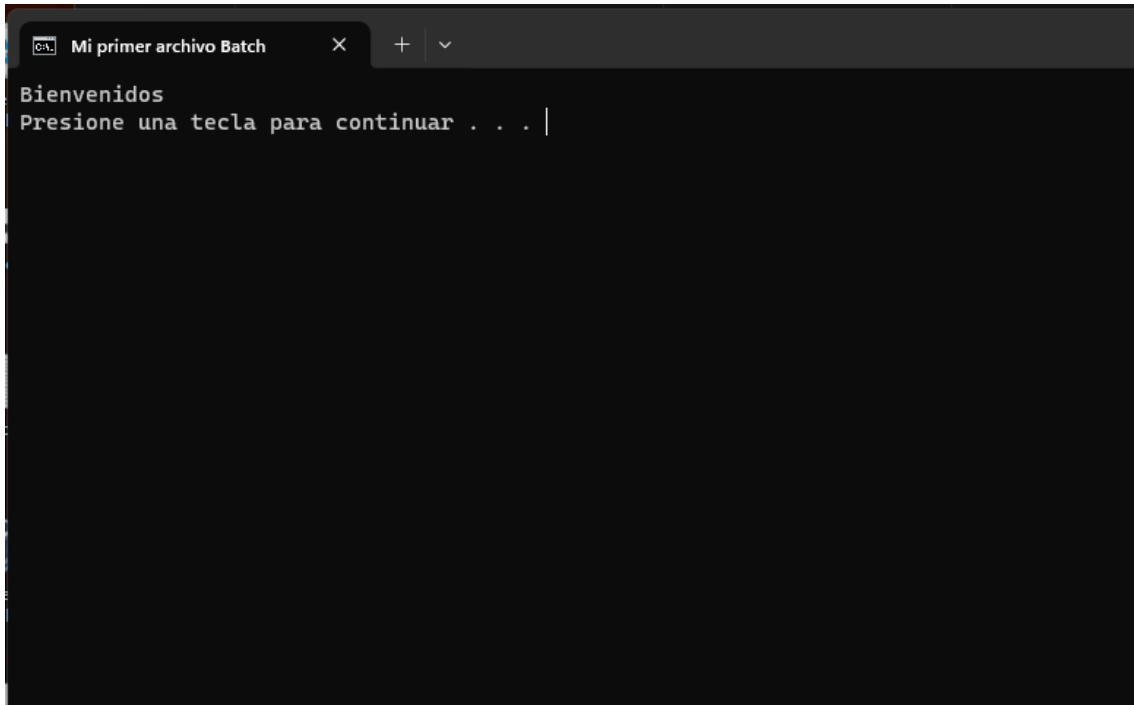
Clic en Guardar

Ahora debería tener un archivo con extensión txt y otro archivo con extensión bat dentro de la carpeta CLASE01.



PASO 4. EJECUTAR ARCHIVO BATCH

Hacer doble clic sobre el archivo con extensión bat y le aparecerá una ventana como esta.



```

Mi primer archivo Batch
Bienvenidos
Presione una tecla para continuar . . . |

```

Puede editar el archivo txt y eliminar el comando “pause”, y guardarlo como txt y como bat según lo explicado en el paso anterior.

```

@echo off
title Mi primer archivo Batch
echo Bienvenidos

```

Al ejecutarlo hará exactamente lo mismo, ejecutará el comando echo para mostrar Bienvenidos y al terminar de ejecutar todo se cerrará automáticamente; pero no será visible para usted pues lo estará ejecutando en segundo plano y pensará que no está ocurriendo nada.

¿Ese tipo de ejecución por debajo no le recuerda algo? Exacto, se asemejan a los malwares cuando atacan sus computadoras, ejecutan comandos en segundo plano sin que usted se dé cuenta. En esta ocasión nuestro archivo batch es totalmente inofensivo pues solo muestra un mensaje.

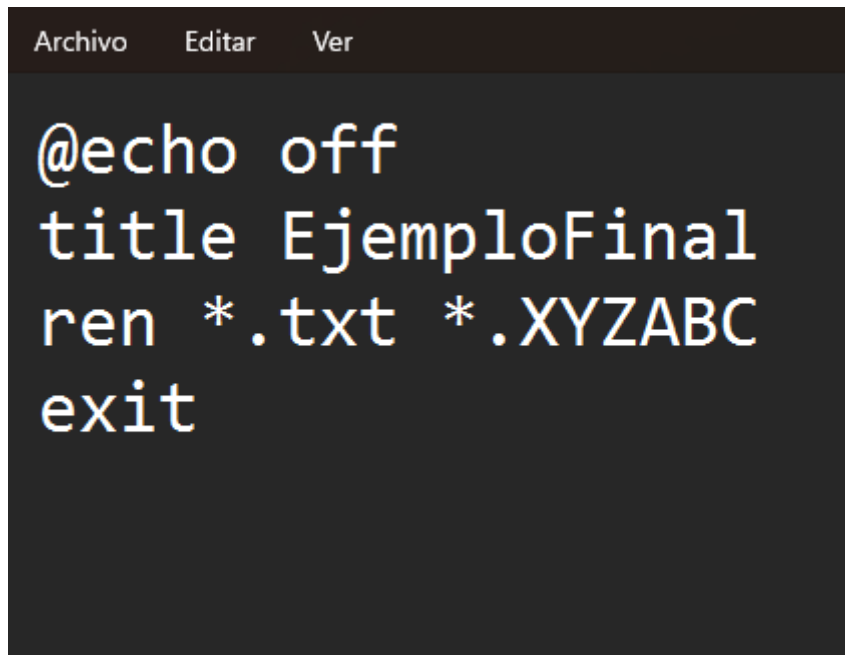
PASO 5. EJEMPLO FINAL

Crearemos otro archivo batch.

Abrir bloc de notas (Notepad)

Y escribiremos el siguiente código

```
@echo off  
title EjemploFinal  
ren *.txt *.XYZABC  
exit
```

A screenshot of a Notepad window with a dark background and light text. The window title bar shows 'Archivo', 'Editar', and 'Ver'. The text inside the window is:

```
@echo off  
title EjemploFinal  
ren *.txt *.XYZABC  
exit
```

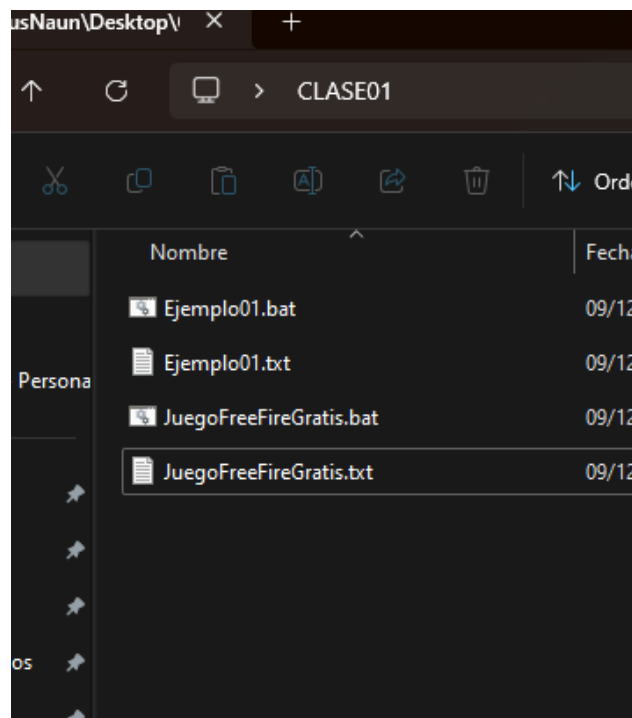
El comando **ren** renombra archivos

El comando **exit** sale al terminar de ejecutar sus comandos

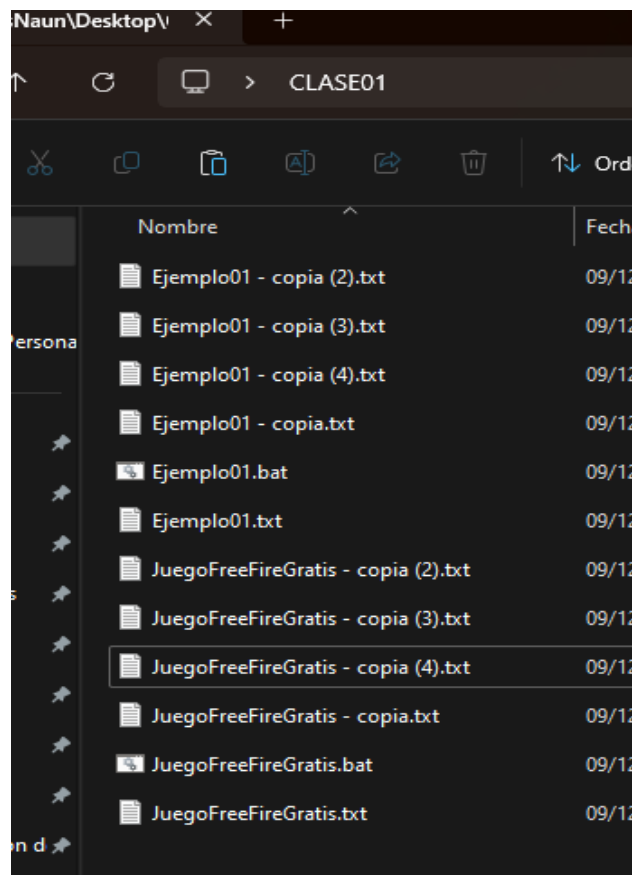
Es obligatorio que este archivo sea guardado dentro de la **CARPETA01** ya que esa carpeta será nuestro ámbito bajo un supuesto ataque por descuido nuestro.

Sigamos los pasos descritos anteriormente para guardar los archivos, en mi caso he colocado el nombre "JuegoFreeFireGratis" tanto en txt como en bat

De modo tal que tendrá una imagen como esta:



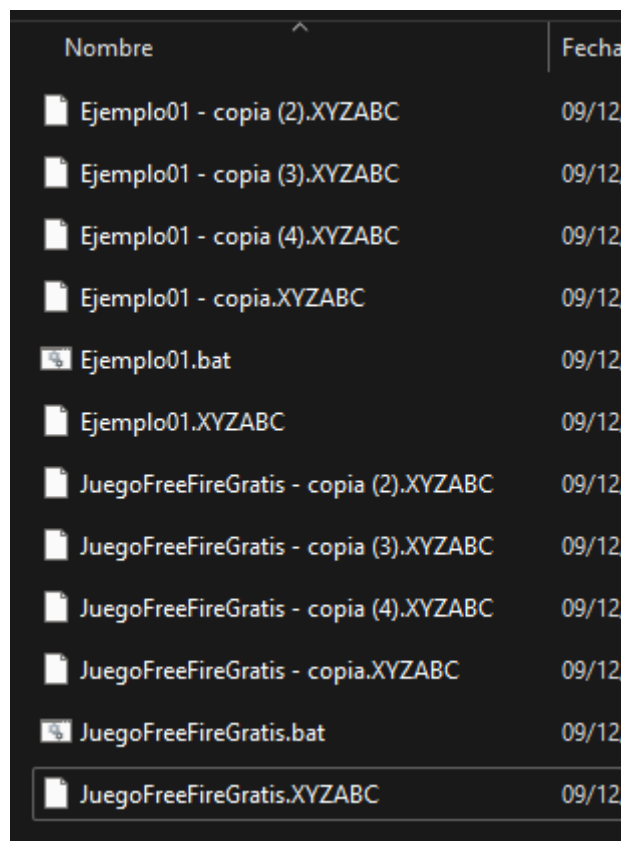
Para que pueda observar el daño que podría causar, haga copias de sus archivos txt y péguelas en esa misma carpeta.



Lo único que hace ese archivo batch es modificar los archivos con extensión txt (visible o no visible) dentro del ámbito donde se vaya a ejecutar; es por ello que todo debe estar dentro de la carpeta CLASE01.

Llegó el momento, imagine la situación que quizás haya bajado de internet el último juego del momento, la canción de moda, la película en estreno o una aplicación que necesitaba; pero ese instalador de dudosa procedencia contiene un archivo batch que se ejecutará cuando instale o abra el archivo descargado.

Dele doble clic al archivo “JuegoFreeFireGratis.bat” y observe lo que sucede



Nombre	Fecha
Ejemplo01 - copia (2).XYZABC	09/12/
Ejemplo01 - copia (3).XYZABC	09/12/
Ejemplo01 - copia (4).XYZABC	09/12/
Ejemplo01 - copia.XYZABC	09/12/
Ejemplo01.bat	09/12/
Ejemplo01.XYZABC	09/12/
JuegoFreeFireGratis - copia (2).XYZABC	09/12/
JuegoFreeFireGratis - copia (3).XYZABC	09/12/
JuegoFreeFireGratis - copia (4).XYZABC	09/12/
JuegoFreeFireGratis - copia.XYZABC	09/12/
JuegoFreeFireGratis.bat	09/12/
JuegoFreeFireGratis.XYZABC	09/12/

Les cambió la extensión a todos sus archivos con extensión txt dentro de esa carpeta convirtiéndolos en inutilizables.

Podría haber modificado un poco el código y haber cambiado no solo a los txt sino a todos los archivos, podría no solo cambiar la extensión sino también los nombres, podría no sólo cambiar la extensión sino también modificar el contenido, podría haber apuntado no solo a la carpeta CLASE01 sino a la carpeta donde están sus documentos o el mismo sistema operativo WINDOWS, , se podrían hacer muchas cosas peligrosas que nosotros permitimos por ejecutar un archivo que no conocemos y podríamos perder toda nuestra información que hoy por hoy es el activo más valioso que hay.

CONCLUSIONES FINALES

Los malwares no son tan sencillos como este ejemplo, y no tienen por qué ser .bat; hay de muchos tipos y de ataques distintos; podrían mimetizarse en otro tipo de archivos y conseguir su propósito de hacernos daños, robarnos nuestra información, tomar control de nuestra computadora, encriptar nuestros datos, y un largo etcétera.

Espero que con este caso práctico ahora hayan comprendido un poco más de lo peligroso que puede resultar abrir o ejecutar archivos desconocidos y evitar hacerlo.

Gracias por su atención.

Ing. Jesús Naún Agurto Rojas