

PRÁCTICA : E3 - Asegurar la INTEGRIDAD de los datos en Windows / Linux MF0486_3 : Seguridad en Equipos Informáticos			Fecha	09 / 03 / 2022
			Página 1 de 3	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.I/II.000/1914256	

Nombre y Apellidos:	ALEXIS VENTURA MEDINA	Firma del Alumno:	
DNI:	49946563Q	Firma del Profesor:	

Apto: ☐

No Apto: ☐

Calificación:

Instrucciones Generales

La puntuación máxima será de 10 puntos.
Esta prueba tendrá una duración máxima de 420 minutos
(Temporalizados durante la Unidad de Aprendizaje)

El alumno/a deberá acatar las siguientes normas durante la duración de la práctica :

- Rellene el encabezado con su nombre, apellidos y D.N.I.
- Firme en todas y cada una de las hojas entregadas, incluidas las que estén en blanco.
- Usar exclusivamente bolígrafo azul o negro
- Guardar los ficheros generados en una carpeta con nombre **MF0486_E3**
- El docente le indicará al final como entregar el contenido de dicha carpeta
- Al finalizar el ejercicio y antes de entregarlo **comprueba tus respuestas**, en caso de duda consulta al docente.

Equipo y material

- Bolígrafo azul.
- Folios.
- Ordenadores.
- Conexión a Internet. (Para buscar información a modo de ayuda)
- **SFC** : Sistema operativo Windows (Virtualizado)
- **Rootkit Hunter** : Sistema operativo Linux (virtualizado)
- Pendrive.

PRÁCTICA : E3 - Asegurar la INTEGRIDAD de los datos en Windows / Linux MF0486_3 : Seguridad en Equipos Informáticos			Fecha	09 / 03 / 2022
			Página 2 de 3	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.I/II.000/1914256	

Instrucciones específicas

El objetivo de esta práctica guiada será como se puede asegurar la **integridad** de los datos en sistemas Windows y Linux.

Condiciones de realización:

La actividad se llevará a cabo en el aula y el alumnado contará en todo momento supervisión del docente.

El alumnado contará con una duración de 420 minutos para realizar la práctica.
Se podrá realizar en varias partes con una duración cada una de 60 minutos.

El alumno podrá hacer uso de internet para su realización, y se detallan a continuación algunas webs de ayuda.

Páginas webs :

SFC (System File Check)

https://en.wikipedia.org/wiki/System_File_Checker
<https://neosmart.net/wiki/sfc/>
<https://support.microsoft.com/es-es/kb/929833>

rootkit

<https://es.wikipedia.org/wiki/Rootkit>
<https://es.wikipedia.org/wiki/Rkhunter>
https://rootkit.nl/projects/rootkit_hunter.html

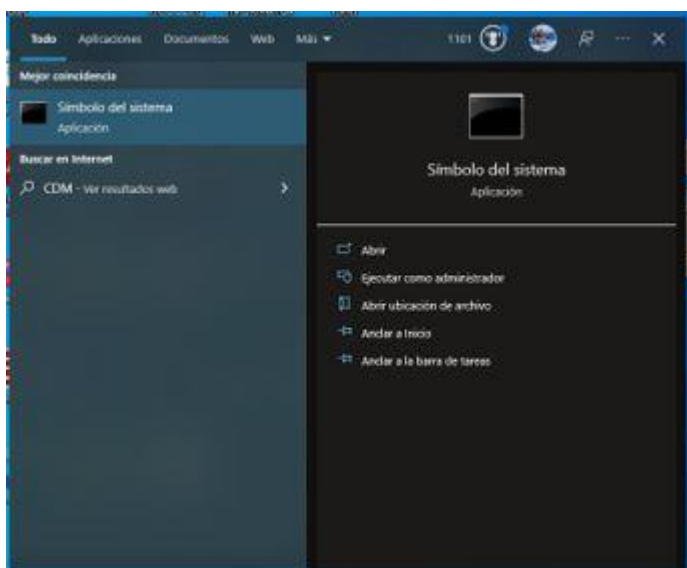
En ella se valorará la utilización de herramientas para la gestión del tiempo y secuenciación del uso de las aplicaciones necesarias. Y se observará especialmente la autonomía del alumnado a la hora de ejecutar y tomar decisiones. Como también la estructuración del ejercicio en donde se solicitará, orden, coherencia y limpieza.

Una vez terminado la práctica se le notificará al docente y pasará a su evaluación.

PRÁCTICA : E3 - Asegurar la INTEGRIDAD de los datos en Windows / Linux MF0486_3 : Seguridad en Equipos Informáticos		Fecha	09 / 03 / 2022
		Página 3 de 3	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.I/II.000/1914256

Descripción de la práctica

Para realizar esta Práctica debemos colocarnos en modo “Símbolo del Sistema” como Administrador.



Una vez en el modo administrador escribiremos el comando **SFC** (System File Check) Y correrá la instrucción apareciendo la siguiente pantalla

```

Administrador: Símbolo del sistema

las versiones incorrectas por las correctas de Microsoft.

SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<archivo>] [/VERIFYFILE=<archivo>]
[/OFFWINDIR=<directorio de Windows sin conexión> /OFFBOOTDIR=<directorio de arranque sin conexión> /OFFLOGFILE=<ruta
de acceso del archivo de registro>]]

/SCANNOW          Examina la integridad de todos los archivos protegidos del sistema y repara los archivos con
problemas si es posible.
/VERIFYONLY       Examina la integridad de todos los archivos protegidos del sistema, pero no realiza
ninguna reparación.
/SCANFILE         Examina la integridad del archivo al que se hace referencia y lo
repara si se detectan problemas. Debe especificarse la ruta de acceso completa de <archivo>.
/VERIFYFILE       Comprueba la integridad del archivo con la ruta de acceso completa de <archivo>, pero no realiza ninguna
reparación.
/OFFBOOTDIR       Para la reparación sin conexión, indica la ubicación del directorio de arranque sin conexión.
/OFFWINDIR        Para la reparación sin conexión, indica la ubicación del directorio de Windows sin conexión.
/OFFLOGFILE       Para la reparación sin conexión, puedes activar el registro si especificas la ruta del archivo de registro.

Ejemplos:

sfc /SCANNOW
sfc /VERIFYFILE=c:\windows\system32\kernel32.dll
sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows
sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows /OFFLOGFILE=c:\log.txt
sfc /VERIFYONLY

C:\Windows\system32>

```

PRÁCTICA : E3 - Asegurar la INTEGRIDAD de los datos en Windows / Linux MF0486_3 : Seguridad en Equipos Informáticos		Fecha	09 / 03 / 2022
		Página 4 de 3	
Curso	7.1. MF0486_3 Seguridad en equipos informáticos	Plan de Formación	FC-2021.I/II.000/1914256

Y ahora se ejecutan los programas dados como ejemplos. Iniciando por sfc /scannow:

```

Administrador: Símbolo del sistema
Ejemplos:
sfc /SCANNOW
sfc /VERIFYFILE=c:\windows\system32\kernel32.dll
sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows
sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows /OFFLOGFILE=c:\log.txt
sfc /VERIFYONLY

C:\Windows\system32>sfg /acannow
"sfg" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Windows\system32>clear
"clear" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Windows\system32>sfc /scannow

Iniciando examen en el sistema. Este proceso tardará algún tiempo.

Iniciando la fase de comprobación del examen del sistema.
Se completó la comprobación de 100%.

Protección de recursos de Windows encontró archivos dañados y los reparó correctamente.
Para las reparaciones en línea, los detalles se encuentran en el archivo de registro de CBS ubicado en
windir\Logs\CBS\CBS.log. Por ejemplo, C:\Windows\Logs\CBS\CBS.log. Para las reparaciones
sin conexión, los detalles se encuentran en el archivo de registro que proporciona la marca /OFFLOGFILE.

C:\Windows\system32>

```