

**UT1.P13**

**Seguridad Informática**

**Integridad**

**Francisco Javier López Calderón**

## P1.3– Integridad Sistemas

### 1 Integridad en Sistemas Windows

Al ejecutar **SFC**, se crea un archivo de registro que podemos consultar en **C:\Windows\Logs\CBS\CBS.log**

- a En tu máquina virtual ejecuta `sfc /scannow`, en una consola con permisos de administrador. Guarda el archivo log.

```
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 no encontró ninguna infracción
de integridad.
```

Ejecuta `ahorasfc/verifyonly`. Guarda el archivo log.

```
C:\Windows\Logs\CBS>sfc /verifyonly
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 no encontró ninguna infracción
de integridad.
```

- b Ejecuta `chkdsk c: /F`, la opción `/F` es para corregir los errores del disco. La comprobación se realizará la próxima vez que se inicie el sistema. Captura la pantalla durante la ejecución.

```
C:\Windows\Logs\CBS>chkdsk c: /F
El tipo del sistema de archivos es NTFS.
No se puede bloquear la unidad actual.

CHKDSK no se puede ejecutar porque otro proceso ya está usando el
volumen. ¿Desea que se prepare este volumen para que sea comprobado
la próxima vez que se reinicie el sistema? (Y/N)
```

```
Comprobando el sistema de archivos en C:
El tipo del sistema de archivos es NTFS.

Se ha programado una comprobación del disco.
Windows comprobará ahora el disco.

CHKDSK está comprobando archivos (etapa 1 de 3)...
0% completado. (2881 de 76032 registros de archivos procesados)
0% completado. (5426 de 76032 registros de archivos procesados)
```

## 2 Integridad en Sistemas Linux

**Comando *sum*** permite obtener un número a partir de un fichero, equivalente al dígito de control de una cuenta bancaria. Si se modifica el contenido de un fichero, el valor de suma cambia, por muy pequeña que sea la modificación.

- En algún fichero pequeño el comando *sum* puede fallar y generar el mismo par de números, aunque se hayan producido algunos cambios. En estos casos es más fiable el comando **cksum**

**Comando *md5sum***, obtienen un resultado parecido, aunque es algo más complejo. Utiliza una función *hash*, que veremos en un tema posterior. Para utilizarlo, debes instalar el paquete *coreutils*:

```
sudo apt-get install coreutils
```

- c Crea un pequeño archivo de texto con los nombres y apellidos de los integrantes del grupo. Ejecuta en consola el comando ***sum****archivoTexto*. Añade ahora la fecha de nacimiento al final del fichero (puedes hacerlo desde la consola, sin abrir el archivo utilizando las redirecciones >>). Vuelve a ejecutar el comando *sum*, y comprueba cómo cambia el resultado. Haz una captura de pantalla donde se vean los dos resultados.

```
administrador@administrador-VirtualBox:~/Desktop$ rm Archivo.txt
administrador@administrador-VirtualBox:~/Desktop$ > Archivo.txt
administrador@administrador-VirtualBox:~/Desktop$ nano Archivo.txt
administrador@administrador-VirtualBox:~/Desktop$ sum Archivo.txt
31838      1
```

```
administrador@administrador-VirtualBox:~/Desktop$ sum Archivo.txt
29023      1
```

- d Repite el mismo proceso, ahora con *md5sum*. Haz una captura de pantalla donde se vean los dos resultados.

```
administrador@administrador-VirtualBox:~/Desktop$ md5sum Archivo.txt
379163451ad1734d74f7bfd4bbdfa62d  Archivo.txt
```

```
administrador@administrador-VirtualBox:~/Desktop$ md5sum Archivo.txt
a0e46c36ae0234972d8edbe65b8c7575  Archivo.txt
```