## Programación de servicios y procesos

Act5.1. Comprobación de integridad

Francisco José García Cutillas | 2FPGS\_DAM

## Índice

-	! _ ! _	4		-
H	ercicio			-
_	CICICIO	_	•	

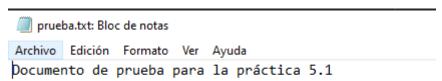
## Ejercicio 1

Comprobación de integridad.

Programa una aplicación que reciba como parámetros de entrada un fichero y su HASH SHA-512 y que certifique la integridad del fichero.

Puedes obtener ficheros y HASH de pruebas en la sección de descargas del IDE Eclipse: https://www.eclipse.org/downloads/

Para la realización de esta práctica nos hemos creado un fichero prueba.txt con el siguiente contenido en la carpeta raíz del proyecto.



Ahora con la ayuda de <a href="https://www.fileformat.info/tool/hash.htm">https://www.fileformat.info/tool/hash.htm</a> que es una calculadora online del hash de un fichero que subamos, obtenemos el siguiente hash SHA-512.

```
SHA-512 e62b9b432c38710a16326edd4712c4f15185fbf2cd86d3a47afb453c6d8f72e43ce385e7692e2ab4fa0e8211ac8e28de32ad31997c2130036756cd5bd8be8796
```

En nuestro programa hemos creado un método que calcula el hash actual de un fichero que se le pasa por parámetro, y otro método que comprueba que el hash recibido por parámetro coincide con el actual del fichero que también recibe por parámetro.

```
package com.mycompany.psp_acts_1;

puport pava.io.file;
import pava.io.file;
import pava.a.o.file;
import pava.a.o.file;
import pava.a.o.file;
import pava.a.o.file;
import pava.a.o.file;
import pava.a.o.o.file;
import
```

```
| catch (IOException ex) (
| System.out.printin("Error: " + ex.getMessage());
| catch (NoSuchAlgorithmException ex) (
| System.out.printin("Error: " + ex.getMessage());
| catch (NoSuchAlgorithmException ex) (
| System.out.printin("Error: " + ex.getMessage());
| catch (NoSuchAlgorithmException ex) (
| System.out.printin("Error: " + ex.getMessage());
| catch (NoSuchAlgorithmException);
| c
```

Si comprobamos la integridad con el hash generado desde la calculadora online y desde el generado por el fichero, vemos que coinciden.

Ahora vamos a probar a modificar el fichero. Esto nos modificará su hash, pero nosotros le seguimos introduciendo el mismo que nos había generado la calculadora online.

prueba.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda

Modifico el documento de prueba para la práctica 5.1

Podemos observar que al modificar el fichero, se modifica su hash, por lo que la integridad ya no sería correcta con el hash anterior.