


LABORATORIO N ° 5 SEGURIDAD DE SISTEMAS SIS-737S1		
Estudiante: Luis Denilson Mamani Quispe		

## Investigación

4. Con la ayuda del sitio web: <https://products.aspose.app/pdf/es/hash-generator/sha1>

Realizar lo siguiente:

Ud. Es una entidad educativa, que está generando certificados de un curso que brindó, ahora está preparando los mismo para hacer llegar de forma virtual a los participantes. Busque alternativa para que los certificados que genere, puedan ser controlados si es que sufren modificación.

### Solución:

Como entidad educativa, una manera efectiva de controlar si los certificados generados han sido modificados es mediante el uso de un algoritmo hash, como SHA-1, que genera una huella digital única para cada archivo PDF del certificado. Para su control, esta huella digital se puede almacenar en una base de datos interna o registro seguro.

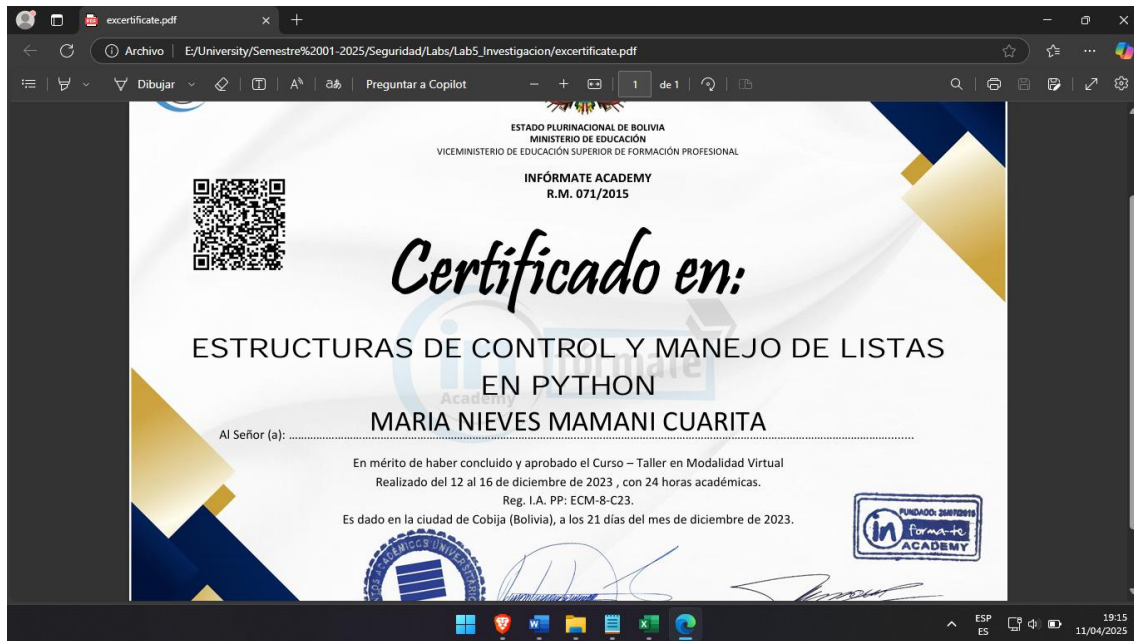
### Demostración práctica de integridad de certificados

#### Paso 1: Generación del hash (firma) original:

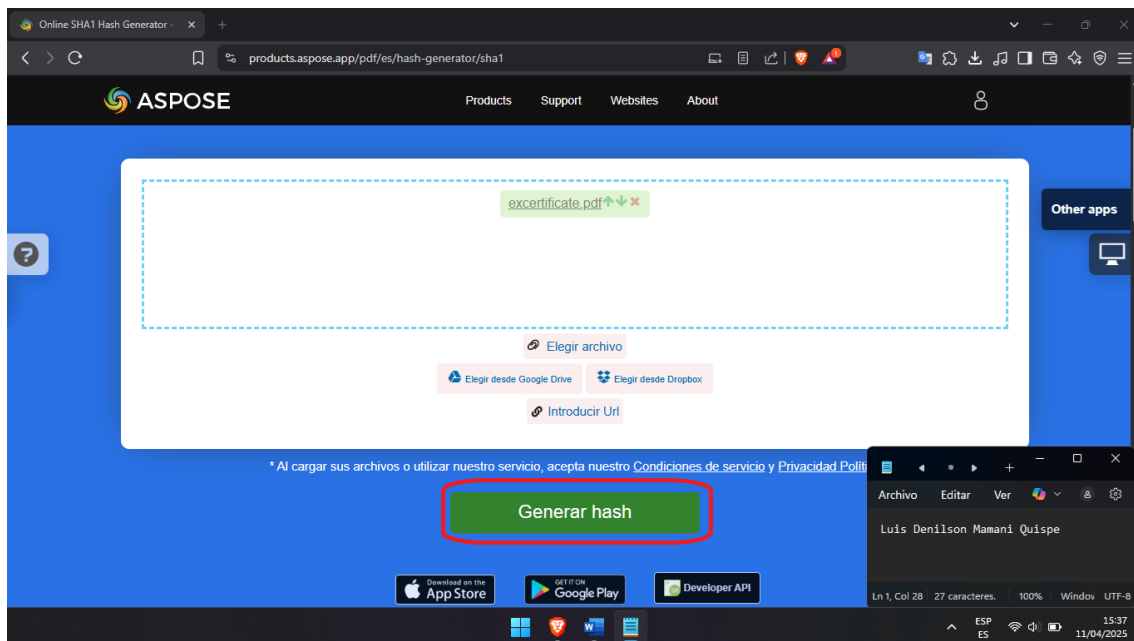
1. Ingresamos a la página proporcionada:

<https://products.aspose.app/pdf/es/hash-generator/sha1>

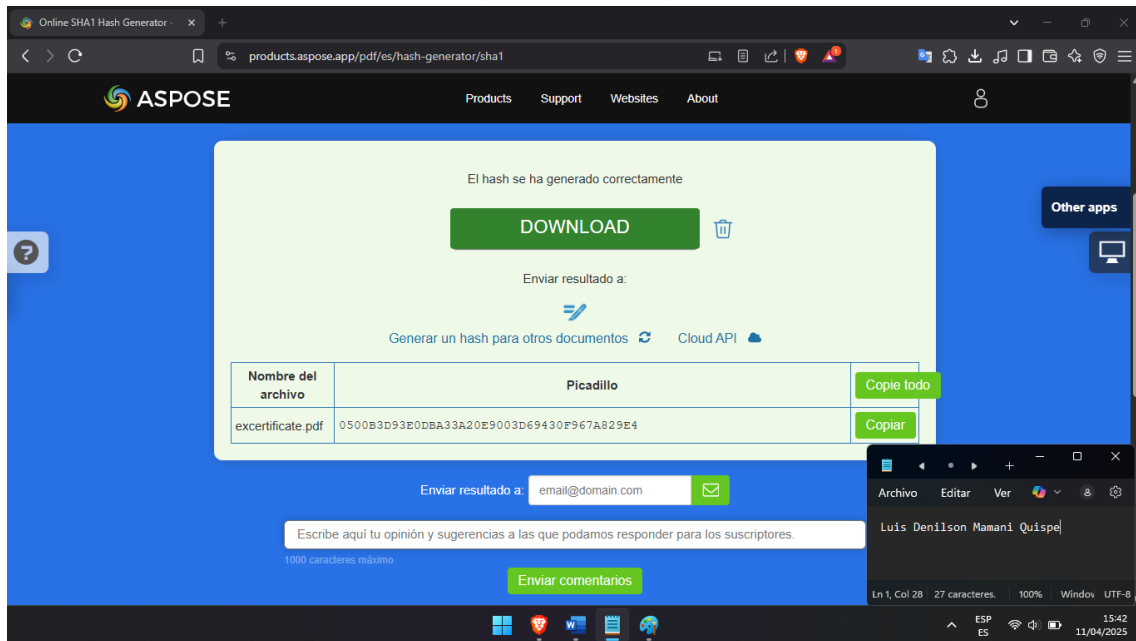
2. Subimos el archivo excertificate.pdf a la plataforma



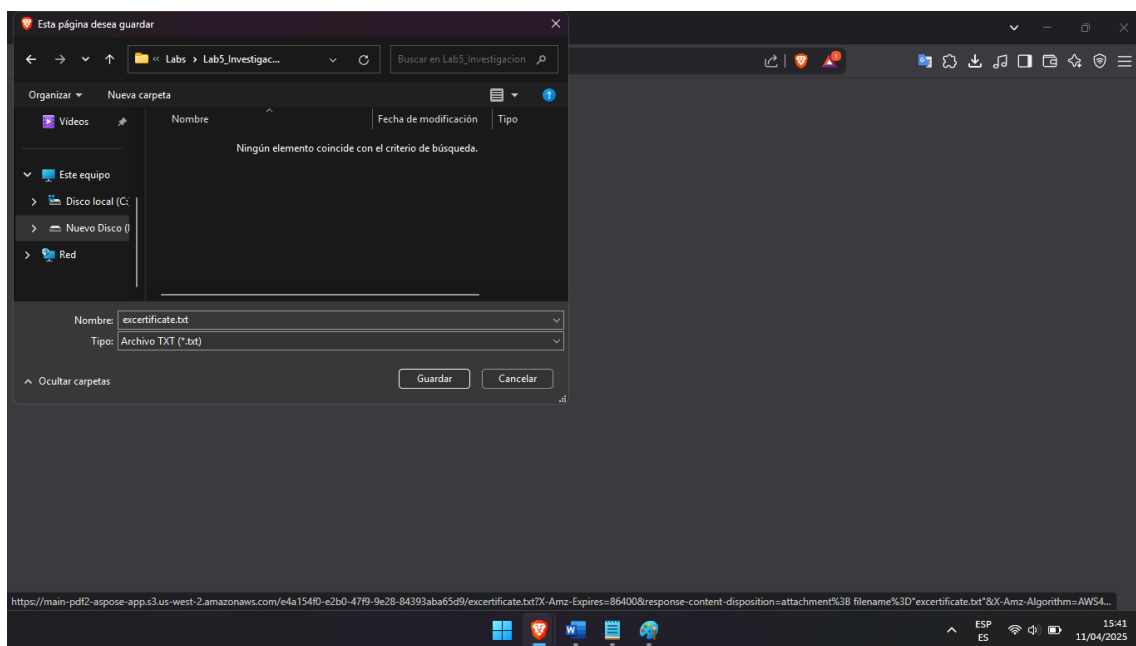
3. Hacemos clic en “Generar hash”



Una vez completado el proceso, el sistema nos proporciona un archivo .txt como resultado.



Lo descargamos



4. Abrimos el archivo .txt, donde encontramos el valor hash generado:

0500B3D93E0DBA33A20E9003D69430F967A829E4

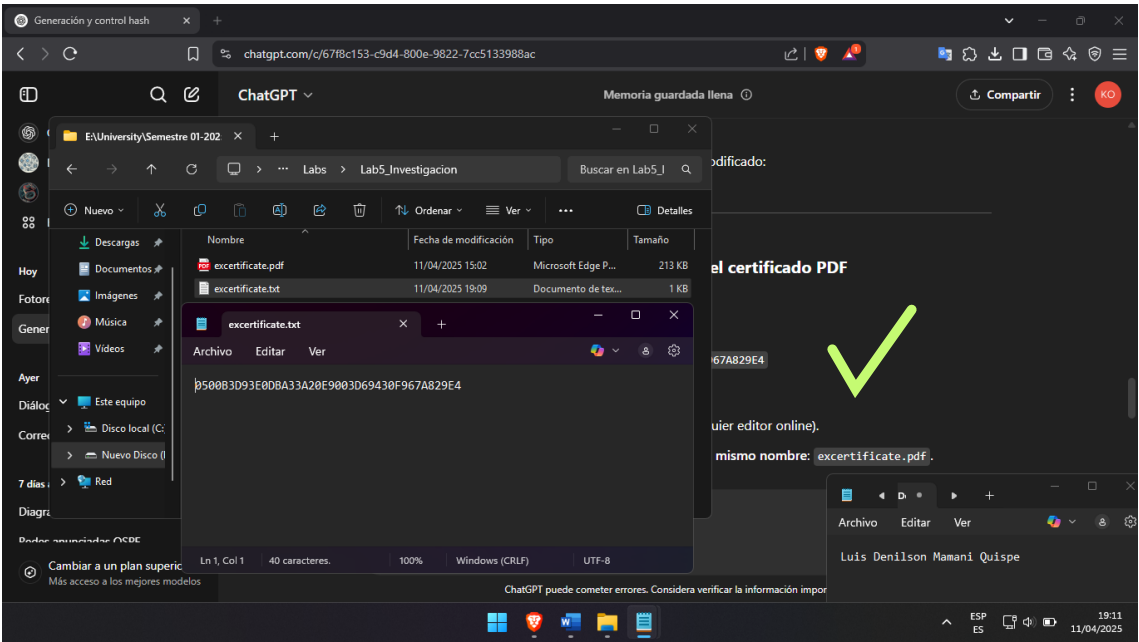


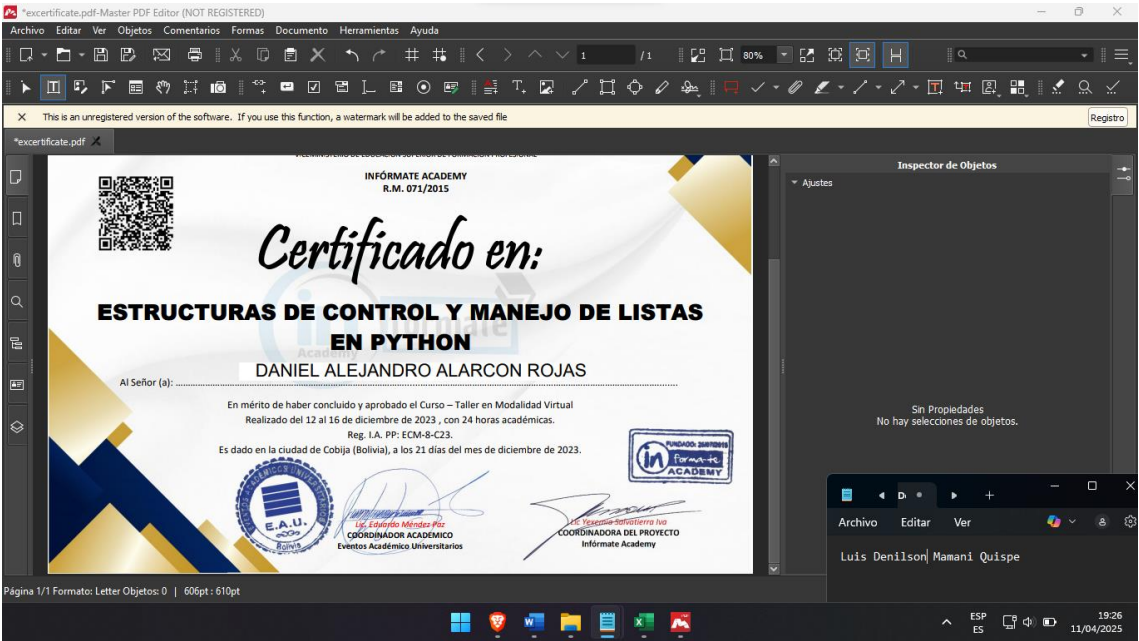
Tabla de resultados originales

N °	Archivo	Contenido (Participante)	Hash SHA-1
1	excertificate.pdf (Original)	Maria Nieves Mamani Cuarita	0500B3D93E0DBA33A20E9003D69430F967A829E4

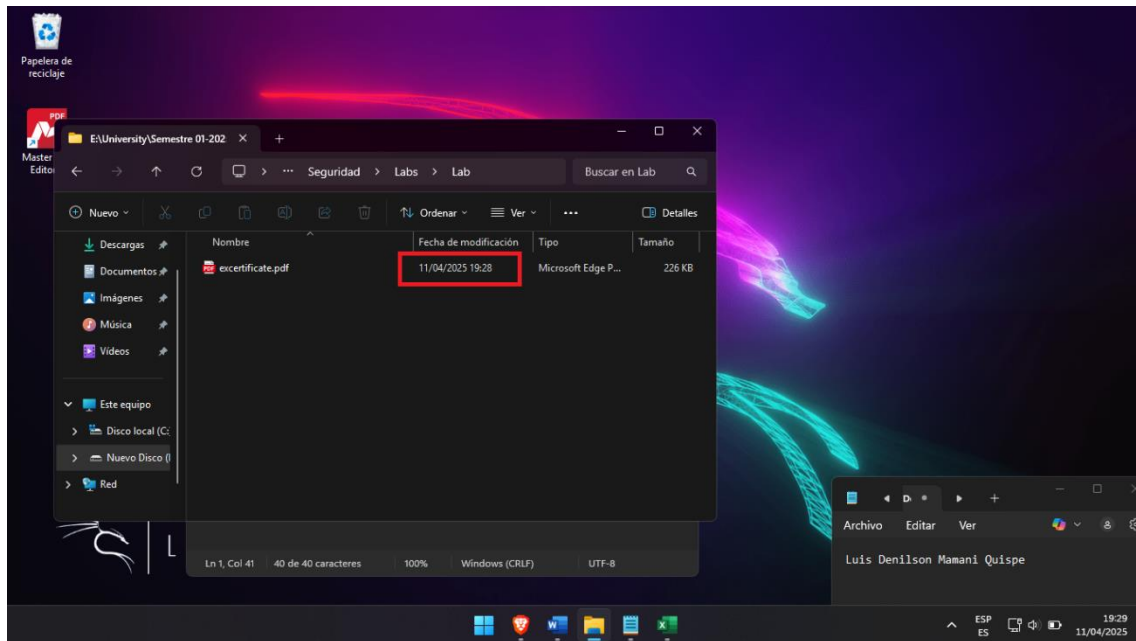
Paso 2: Modificar el archivo

Editamos el contenido del archivo PDF, específicamente el nombre del participante:

- Participante original: **María Nieves Mamani Cuarita**
- Participante modificado: **Daniel Alejandro Alarcón Rojas**



Guardamos.

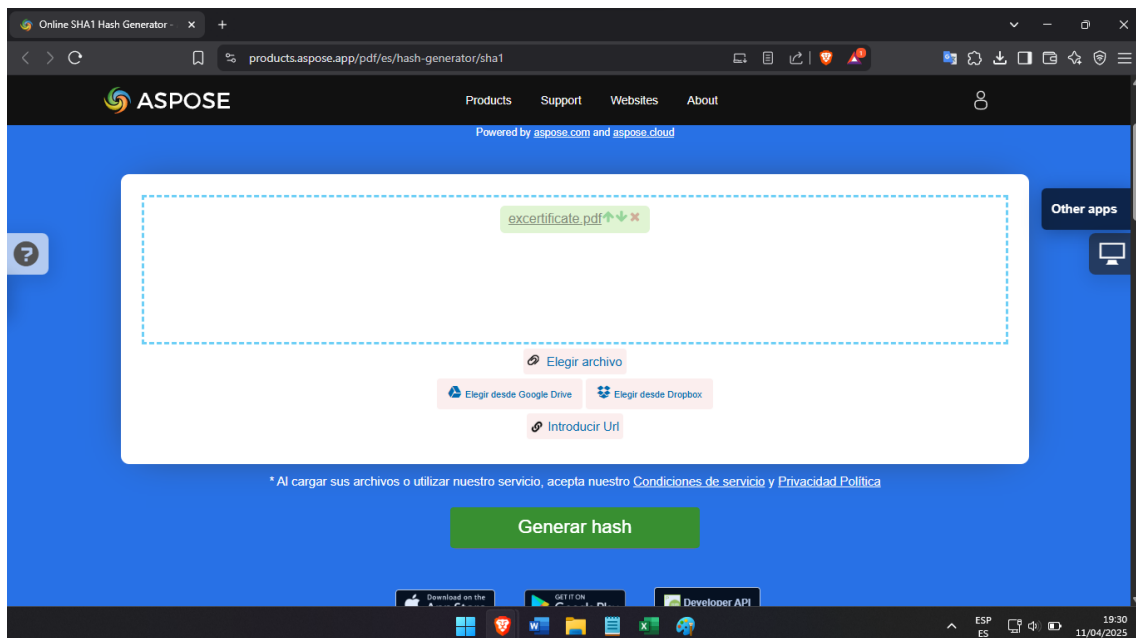


### Paso 3: Calcular el nuevo hash del archivo modificado

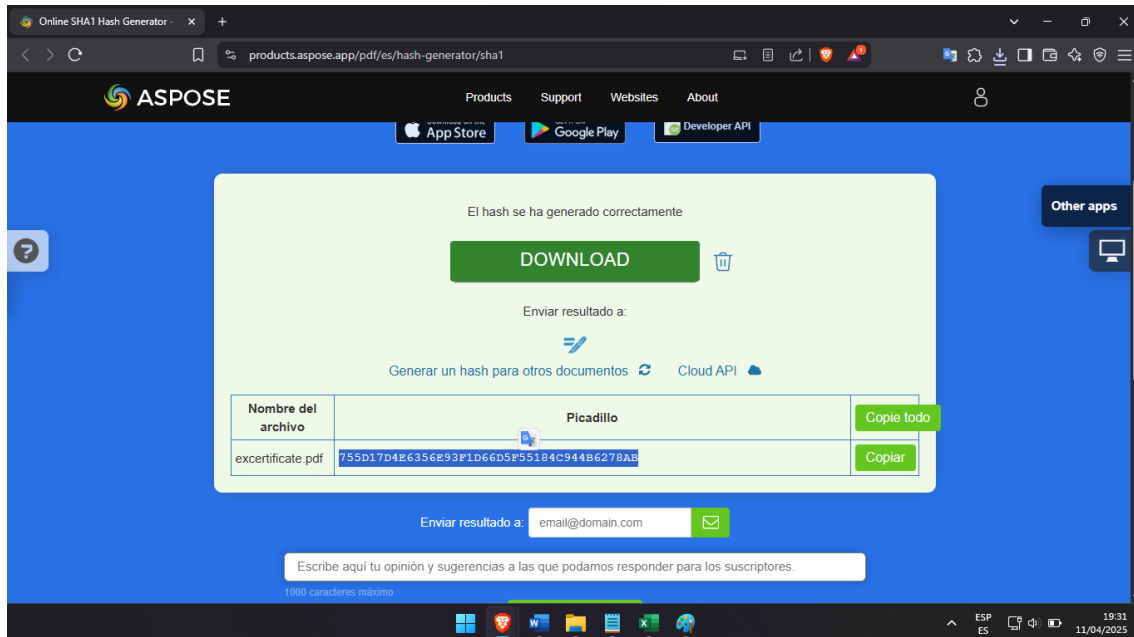
1. Volvemos a la misma página:

<https://products.aspose.app/pdf/es/hash-generator/sha1>

2. Subimos nuevamente el archivo modificado con el mismo nombre: excertificate.pdf



### 3. Generamos el hash



4. Descargamos y procedemos a abrir el archivo .txt, donde observamos que el nuevo hash es diferente:

755D17D4E6356E93F1D66D5F55184C944B6278AB

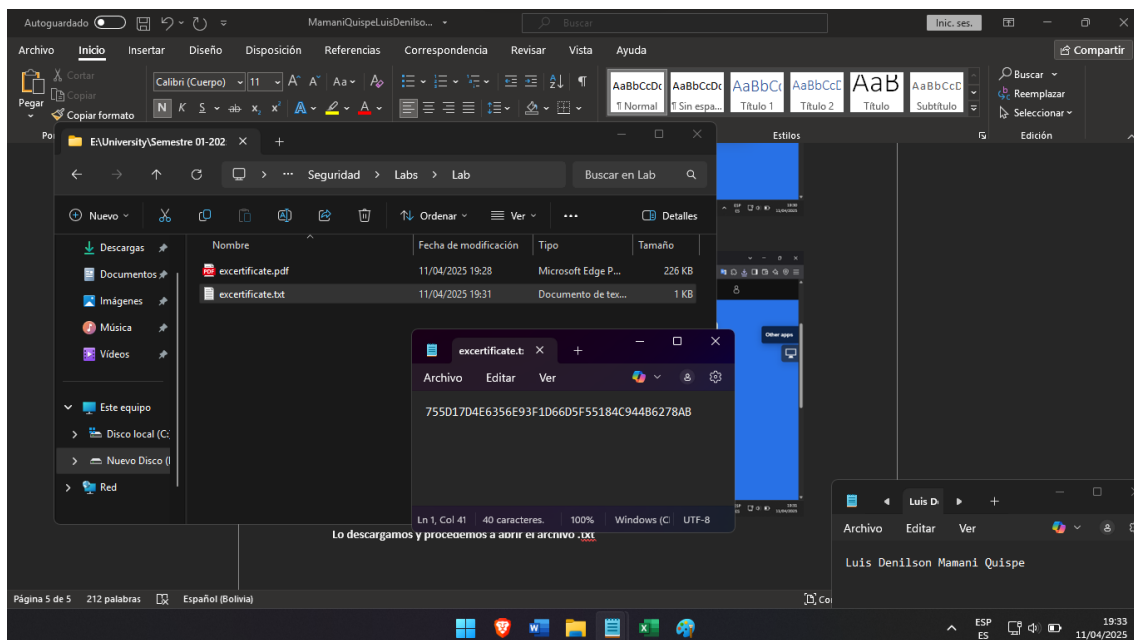


Tabla de resultado:

N <sup>o</sup>	Archivo	Contenido (Participante)	Hash SHA-1
2	excertificate. pdf (Modificado)	Daniel Alejandro Alarcon Rojas	755D17D4E6356E93F1D66D5F55184C944 B6278AB

Tabla de comparación de hashes

N <sup>o</sup>	Archivo	Contenido (Participante)	Hash SHA-1
1	excertificate.pdf (Original)	Maria Nieves Mamani Cuarita	<b>0500B3D93E0DBA33A20E9003D 69430F967A829E4</b>
2	excertificate.pdf (Modificado)	Daniel Alejandro Alarcon Rojas	<b>755D17D4E6356E93F1D66D5F55 184C944B6278AB</b>

### Conclusión

Como se puede observar, aunque el nombre del archivo se ha mantenido igual **excertificate.pdf**, el hash SHA-1 ha cambiado completamente debido a la modificación en el contenido.

Esto demuestra que cualquier alteración, por mínima que sea, en el archivo PDF genera un hash diferente, lo que permite detectar manipulaciones fácilmente. Por tanto, el uso de algoritmos hash es una herramienta efectiva para verificar la integridad de documentos digitales.

