	UNIVERSIDAD AUTÓNOMA TOMAS FRÍAS **CARRERA DE INGENIERÍA DE SISTEMAS**
	ESTUDIANTE: Univ. Beimar Hernán Escudero Apaza
MATERIA: SIS- 737 ING DE SISTEMAS	**FECHA: 11/ 04/25**
DOCENTE: ING. Alexander Duran	**Evaluación LAB 5**

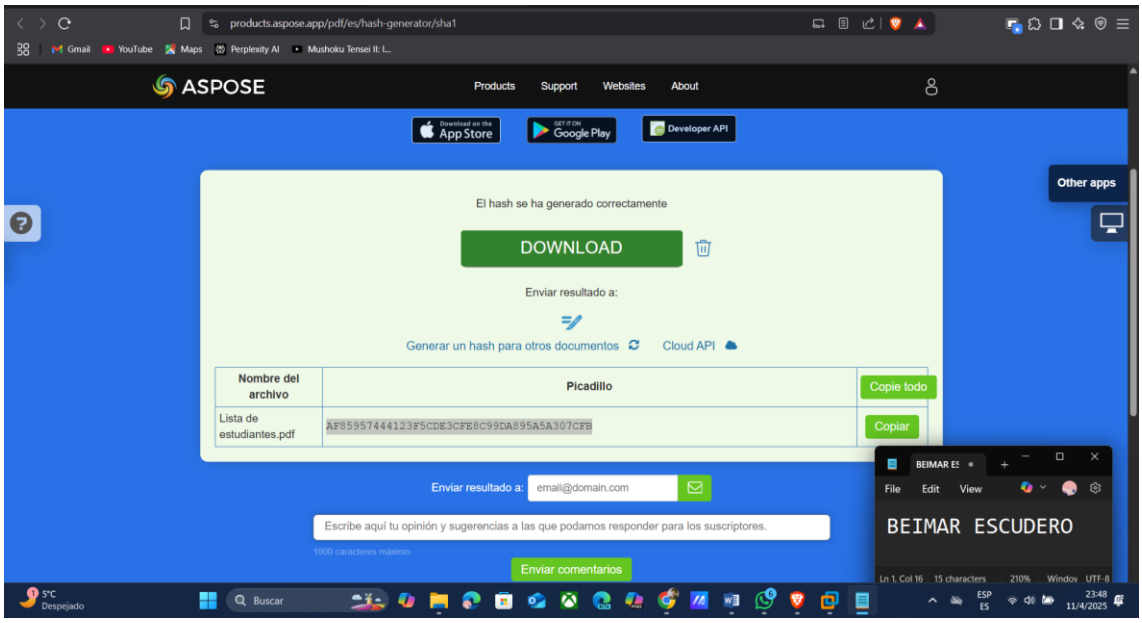
4.- Con ayuda del sitio web:

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

Realice la simulación siguiente:

Ud. Es una entidad er ucativa, que está generando certificados de un curso que brindó, ahora está preparando los mismos para hacer llegar de forma virtual a los participantes. Bus alternativa para que los certificados que genere, puedan ser controlados si esque fufren modificación.

Explique su solución y cómo realizará el control.



AF85957444123F5CDE3CFE8C99DA895A5A307CFB

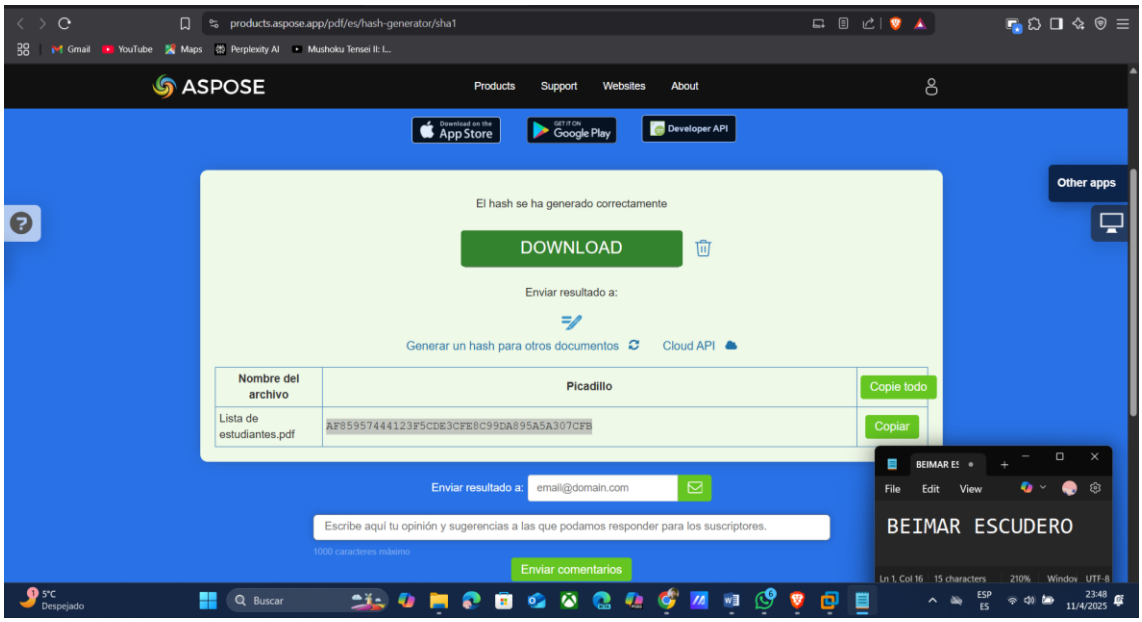
1. Generación del Certificado en Formato PDF

Primero, la entidad educativa crea los certificados para los participantes

2. Generación del Hash del Certificado

Con el certificado en formato PDF, el siguiente paso es generar un valor único que represente el contenido del archivo. Para esto, utilizamos un algoritmo de hash **SHA1**.

Se sube el archivo PDF al **Generador de Hash SHA1** en el sitio web de **Aspose** (https://products.aspose.app/pdf/es/hash-generator/sha1).



3 Firmado Digital del Hash

Para asegurar la integridad y autenticidad del certificado, el hash generado se firma digitalmente usando un **cifrado asimétrico**.

Se genera un par de claves asimétricas (clave privada y clave pública) utilizando herramientas como **OpenSSL**:

```
openssl genpkey -algorithm RSA -out private_key.pem
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

Usando la **clave privada**, se cifra el hash generado anteriormente:

```
openssl dgst -sha1 -sign private_key.pem -out signature.bin hash.txt
```

Esto crea una **firma digital** que se adjunta al archivo PDF del certificado.

4. Verificación del Certificado

Cuando los participantes reciben el certificado, pueden verificar si este ha sido modificado utilizando la **clave pública** de la entidad educativa. La verificación se realiza comparando el hash original con el contenido del certificado y la firma digital.

Los participantes descargan el certificado y la clave pública proporcionada por la entidad educativa.

Usan la **clave pública** y el archivo de la firma digital para verificar la autenticidad del certificado:


```
openssl dgst -sha1 -verify public_key.pem -signature signature.bin hash.txt
```

Si el archivo ha sido modificado, la verificación fallará, lo que indica que el certificado ha sido alterado.