

## LABORATORIO N°5

**Nombre:** Rafael Antonio Patricio Ayllón

**CI:** 10473854

**RU:** 108771

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

Realice la simulación siguiente:

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

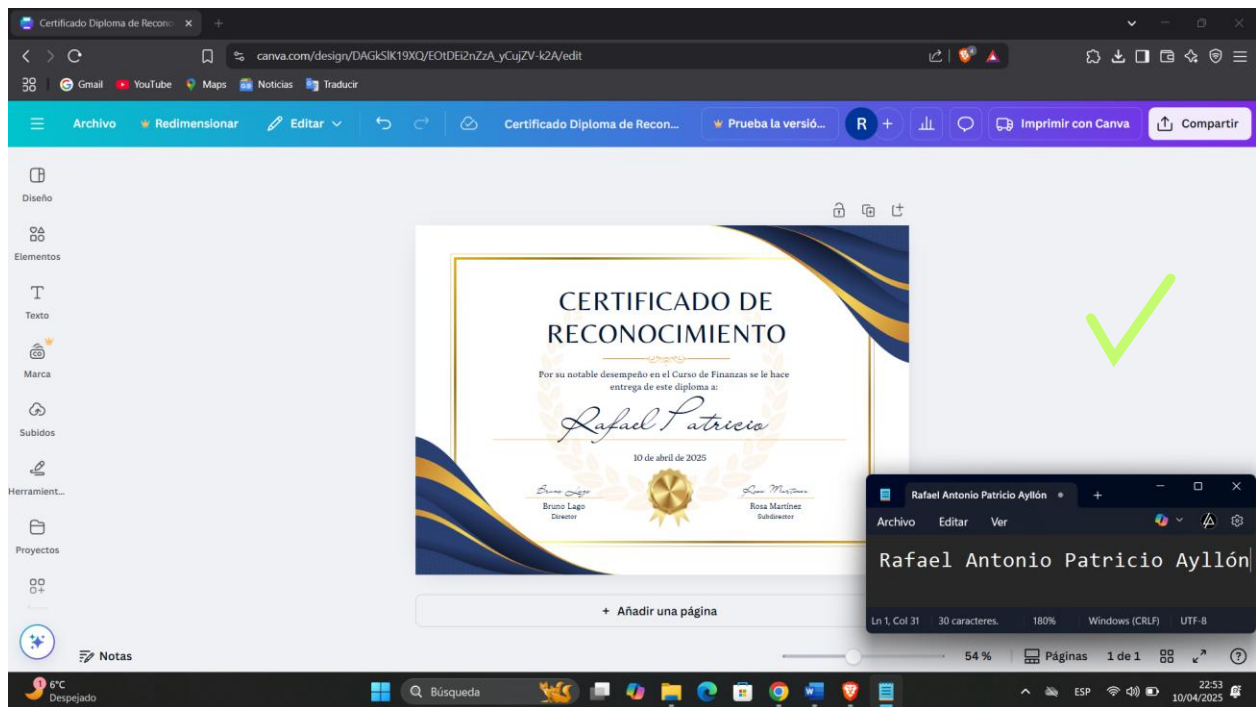
Explique su solución y como realizara el control.

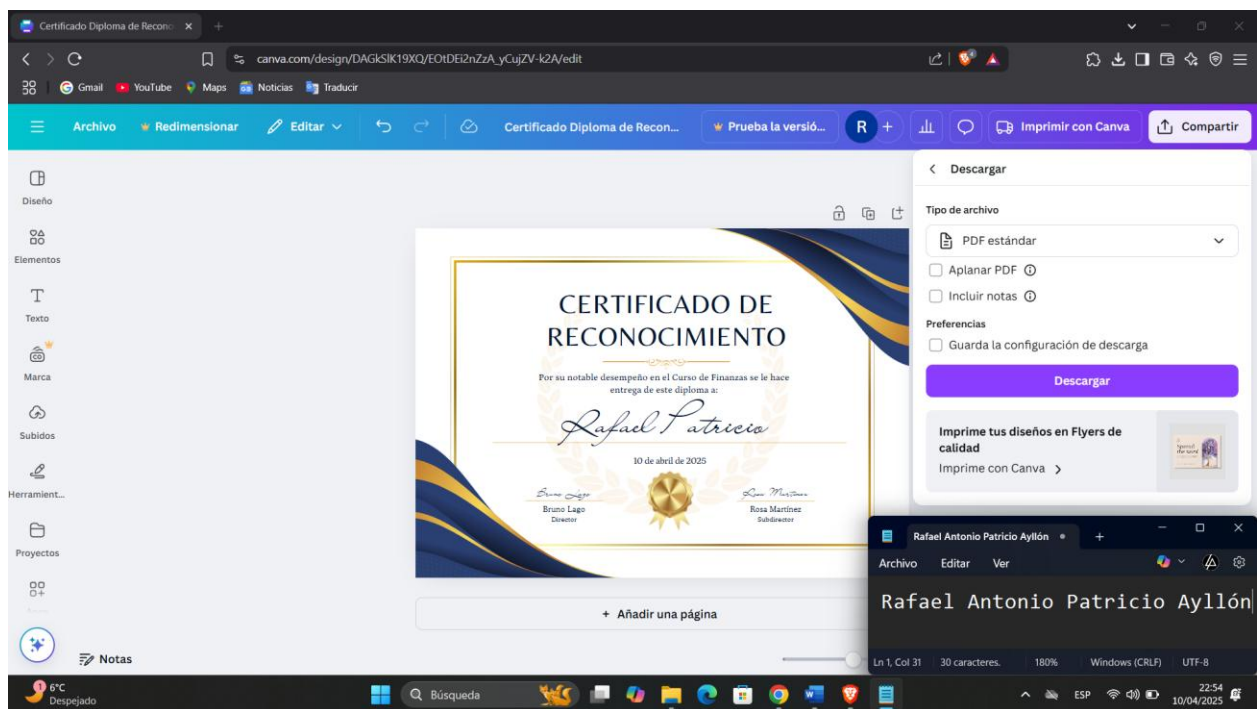
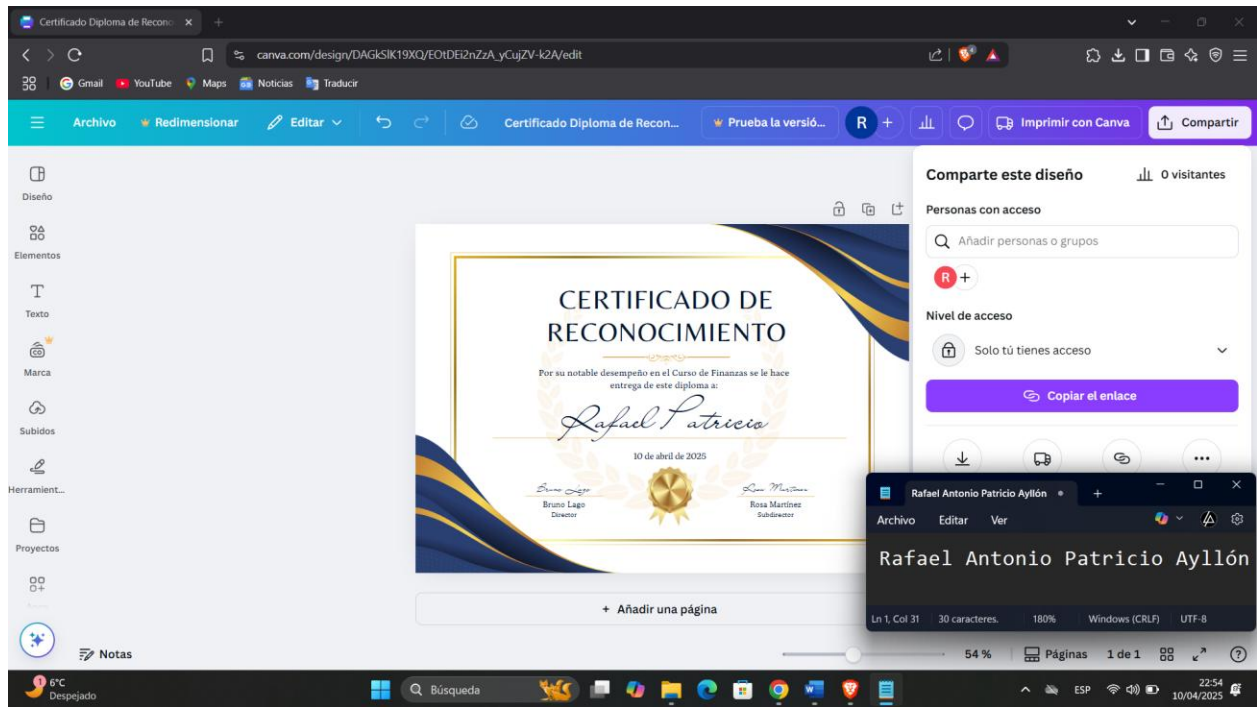
**Solución Propuesta: Uso de Hash SHA-1 para Control de Integridad**

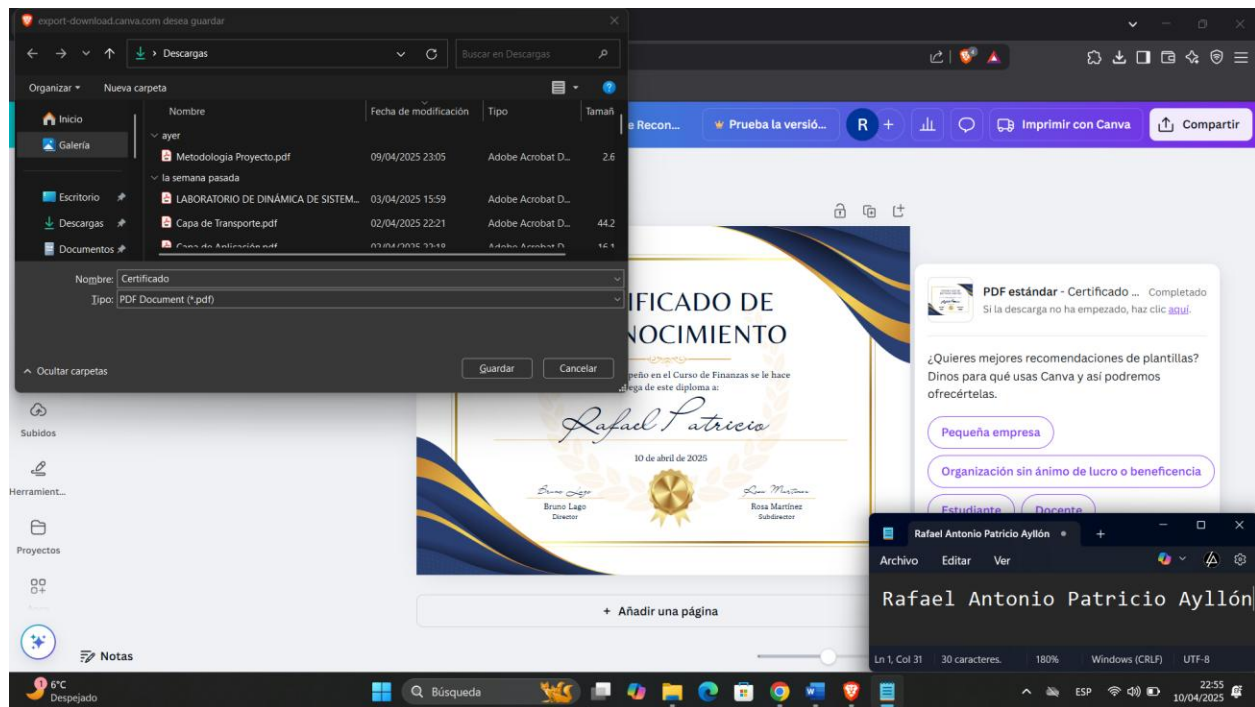
### Generación del Certificado

Se crea el certificado en formato PDF con los datos del participante y del curso.

Se almacena una copia en la base de datos de la entidad educativa.



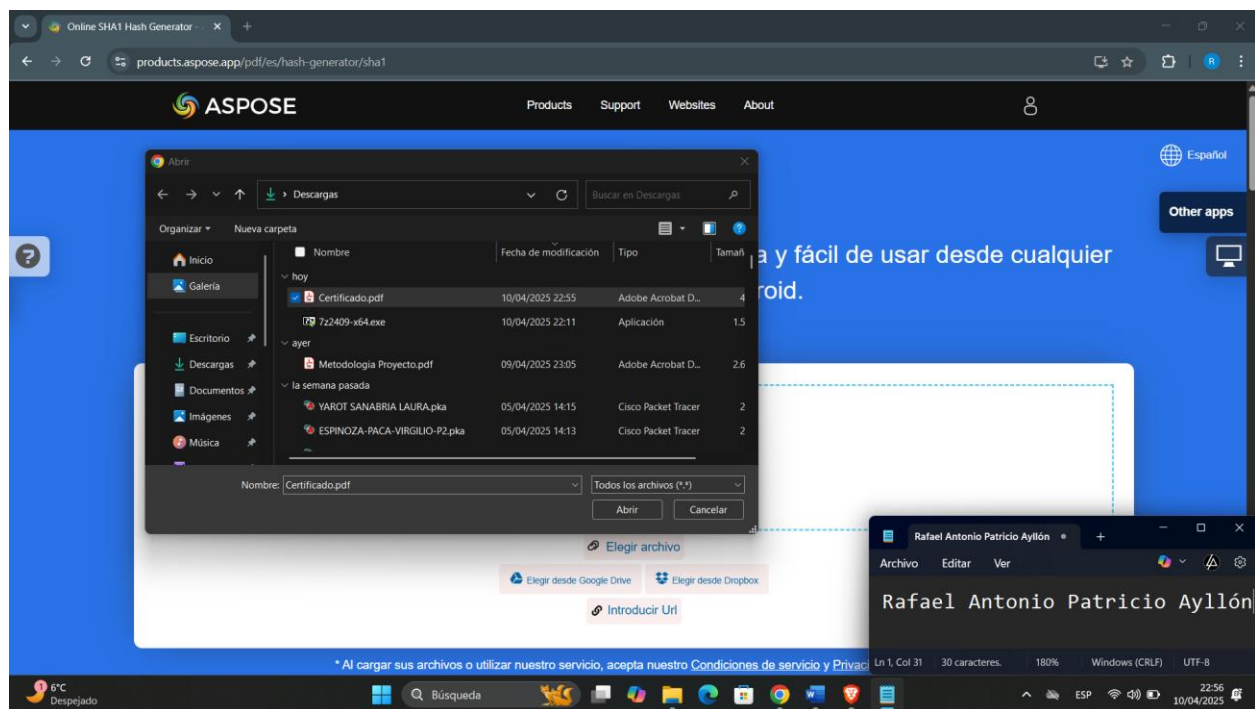
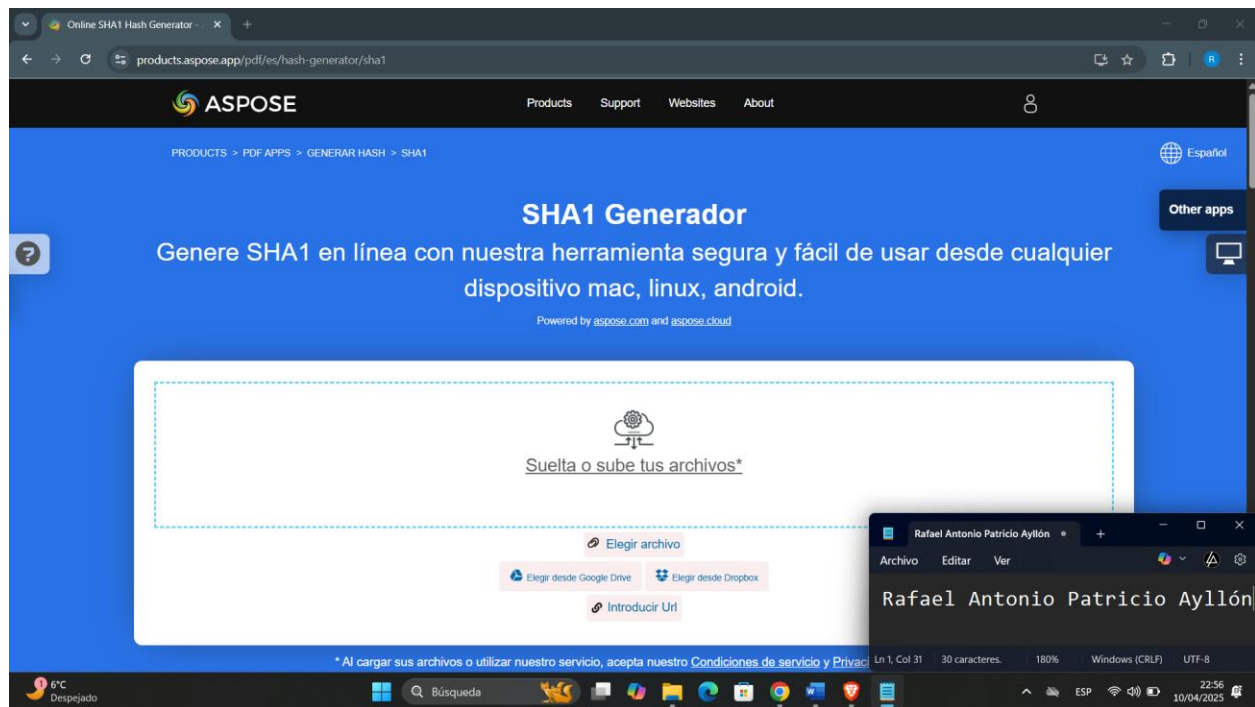


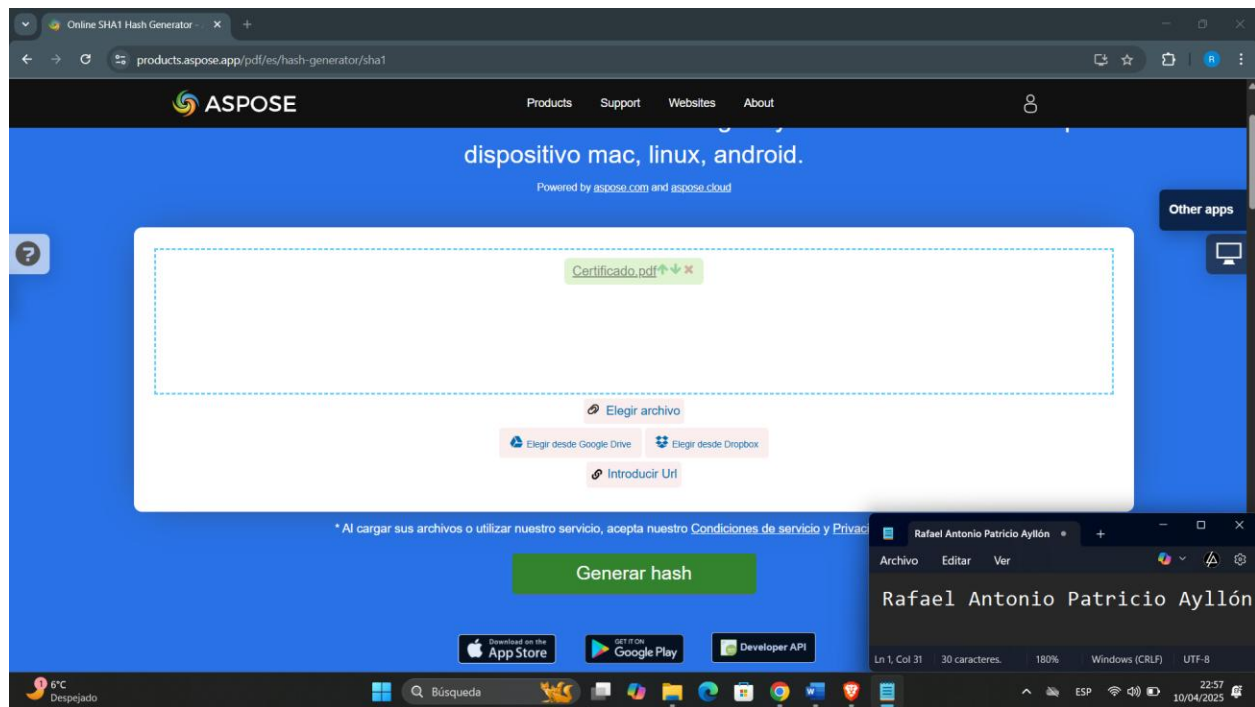


## Cálculo del Hash SHA-1

Se usa la herramienta de Aspose SHA-1 para generar un hash único del archivo PDF.

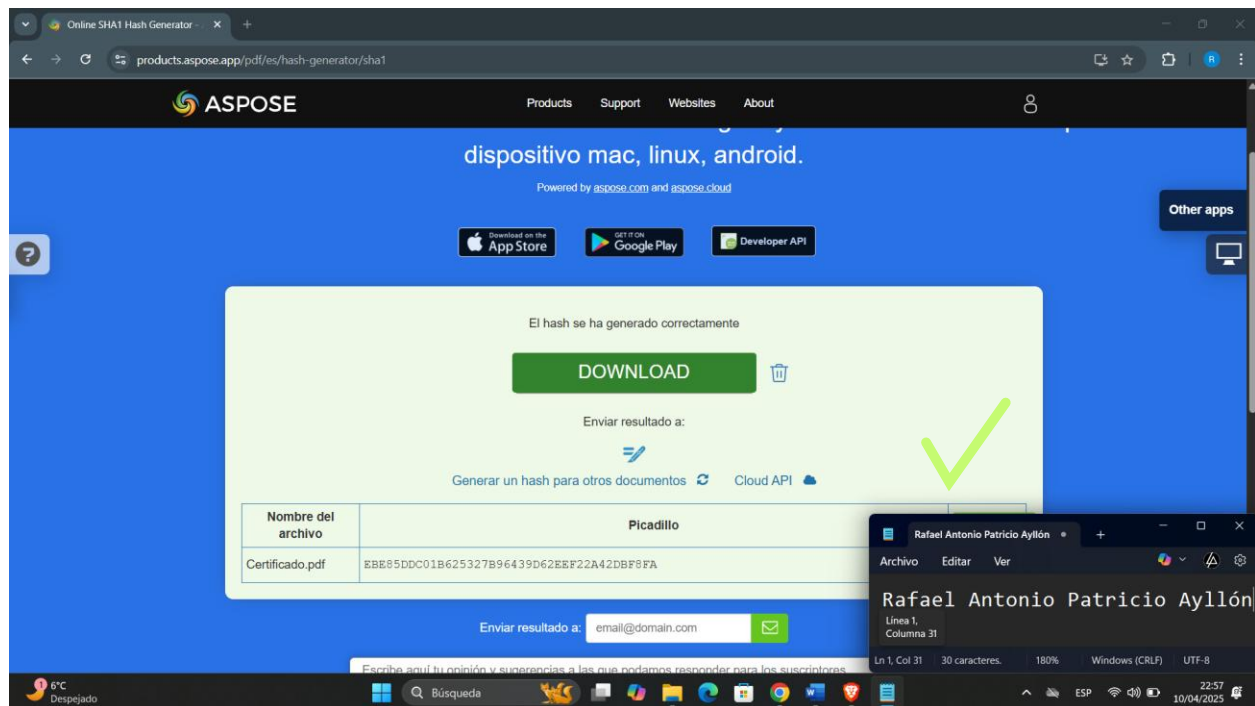
Este hash representa la "huella digital" del certificado.





## Almacenamiento del Hash

Se guarda el hash SHA-1 en una base de datos o servidor seguro junto con el ID del certificado.



EBE85DDC01B625327B96439D62EEF22A42DBF8FA



## Envío del Certificado

Se envía el certificado PDF al participante con una indicación de que puede verificar su autenticidad mediante el hash.

## Verificación de Autenticidad

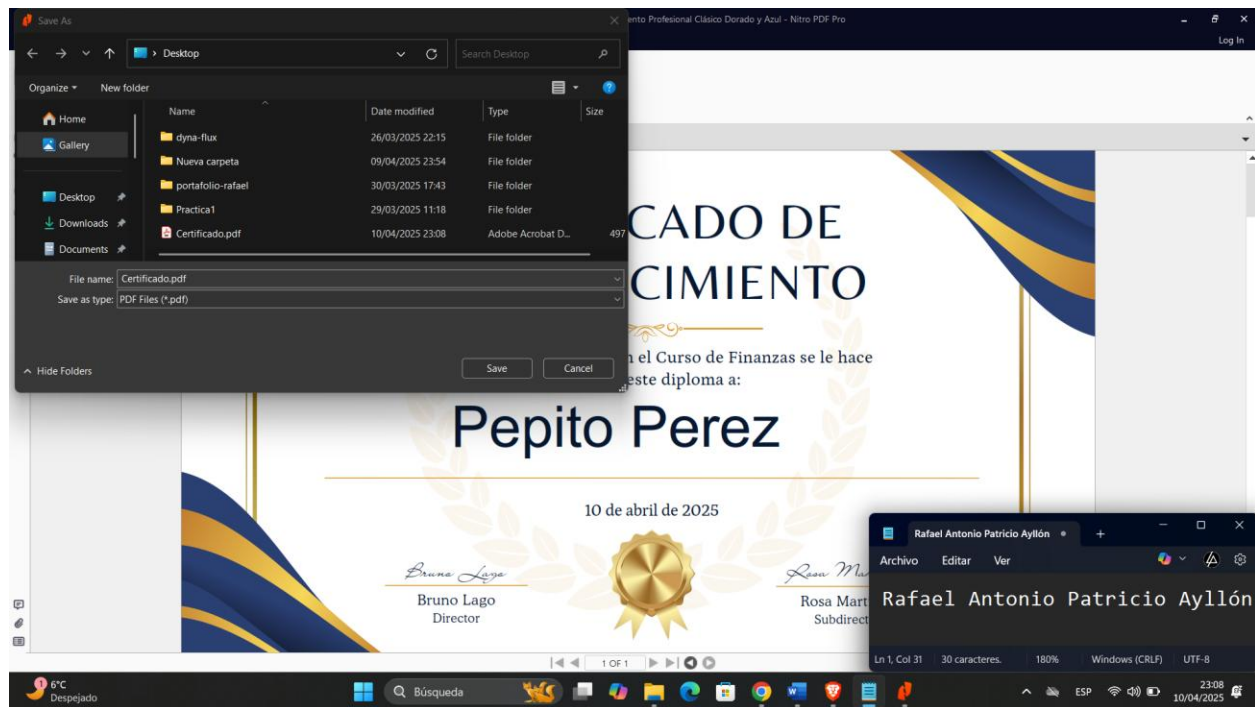
Si alguien quiere validar el certificado, puede subirlo a la misma herramienta Aspose SHA-1 y comparar el hash obtenido con el almacenado en la base de datos.

Si los hashes coinciden, el certificado es válido. Si no coinciden, significa que ha sido modificado.

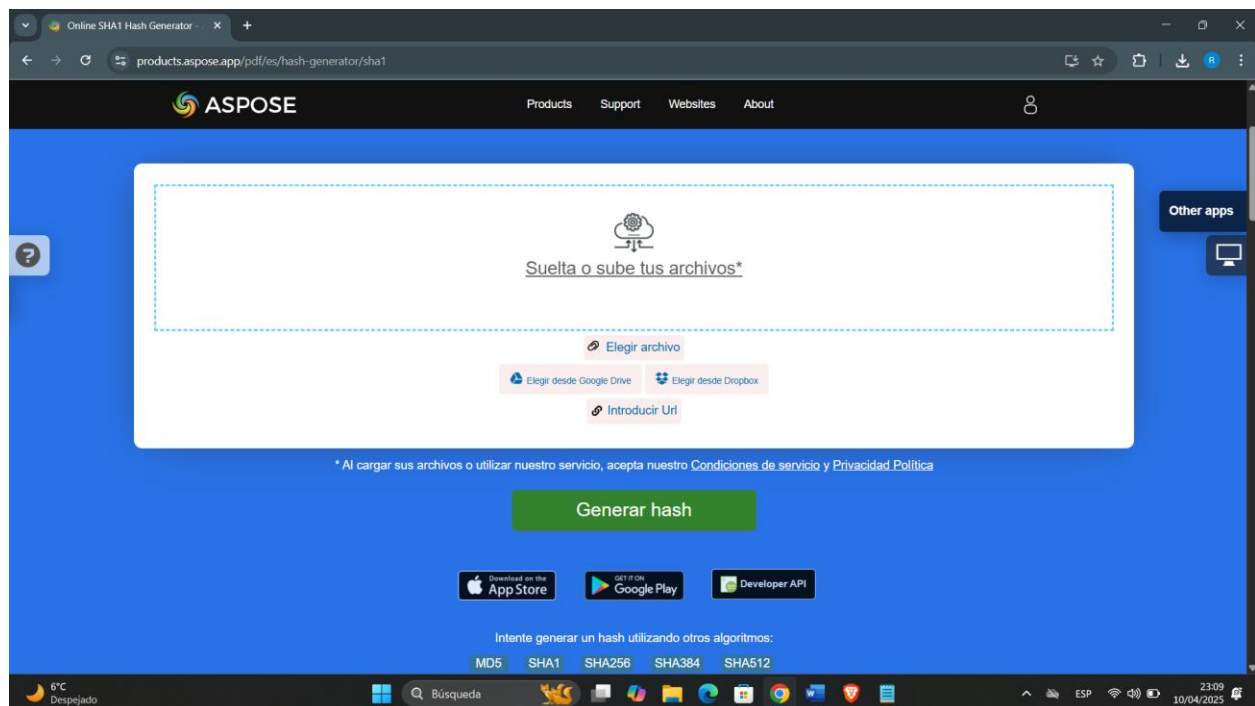
## Intento de Falsificación

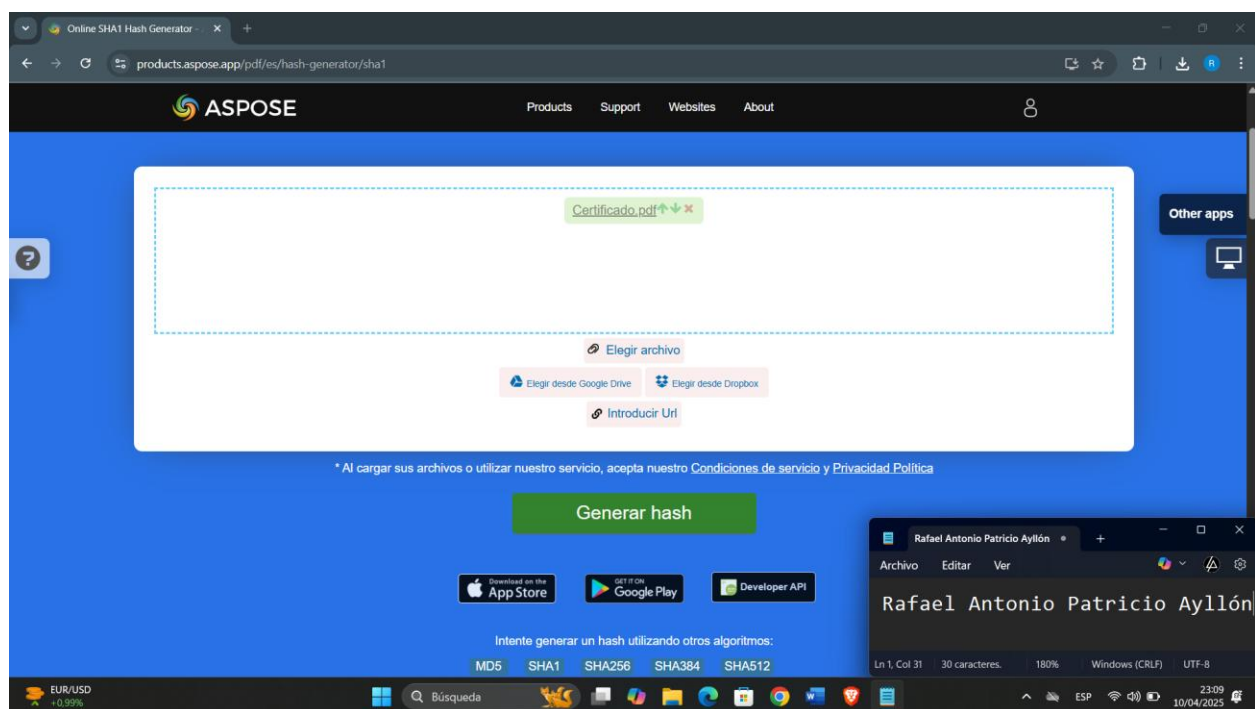
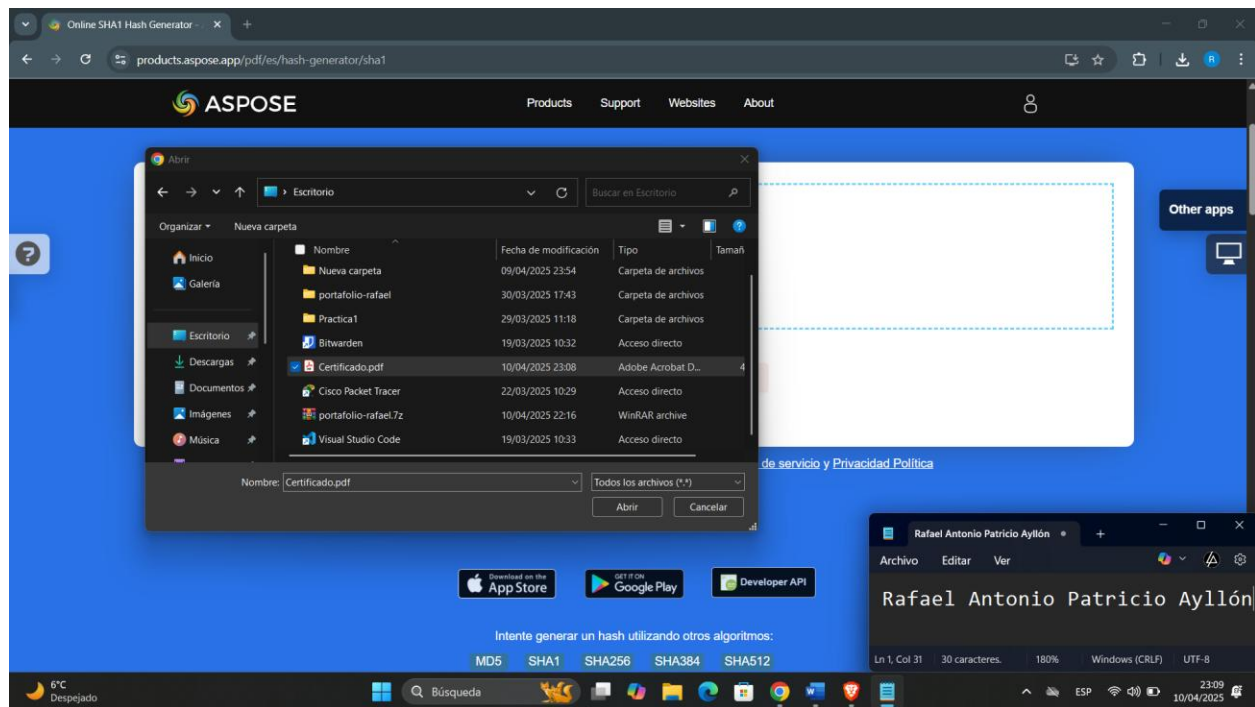
Cambia el nombre del para otra persona y lo guarda como pdf.





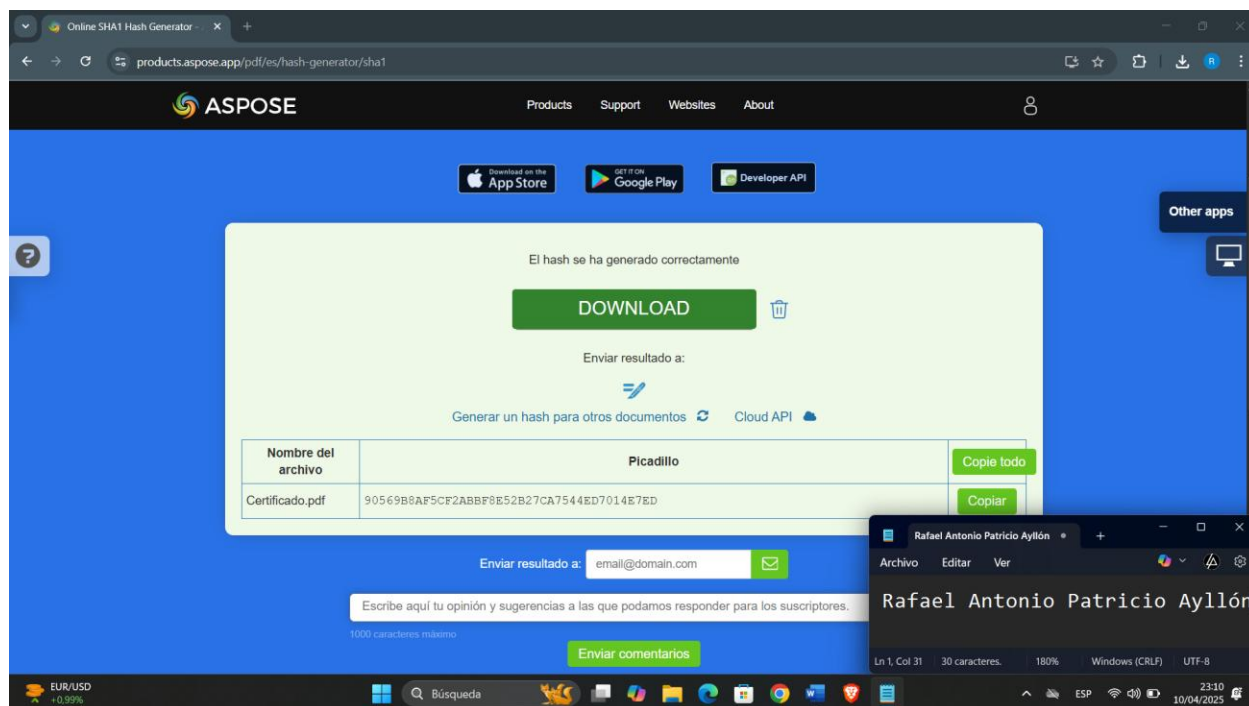
Para la verificación y la integridad del certificado se hace la verificación en Aspose SHA-1





Cuando se genere el hash de este certificado será diferente al primero.





90569B8AF5CF2ABBF8E52B27CA7544ED7014E7ED

## Conclusión

El uso de funciones hash como SHA-1 es una solución efectiva y sencilla para garantizar la autenticidad e integridad de los certificados digitales. Al generar un hash único para cada certificado y almacenarlo en una base de datos segura, se puede verificar si el documento ha sido modificado. Este método es accesible, fácil de implementar y proporciona una manera confiable de validar documentos sin necesidad de software especializado.

Para una mayor seguridad, se puede complementar con firmas digitales, asegurando así la legitimidad de los certificados emitidos. Implementar este mecanismo no solo protege la institución educativa contra fraudes, sino que también brinda confianza a los participantes al garantizar la validez de sus certificaciones.