EVALUACION LABORATORIO 5

NOMNBRE: ALVIN NEIL LOPEZ AGUILAR

CI: 14023800

RU:79642

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

Realice la simulación siguiente:

Ud. Es una entidad e ucativa, q e 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.

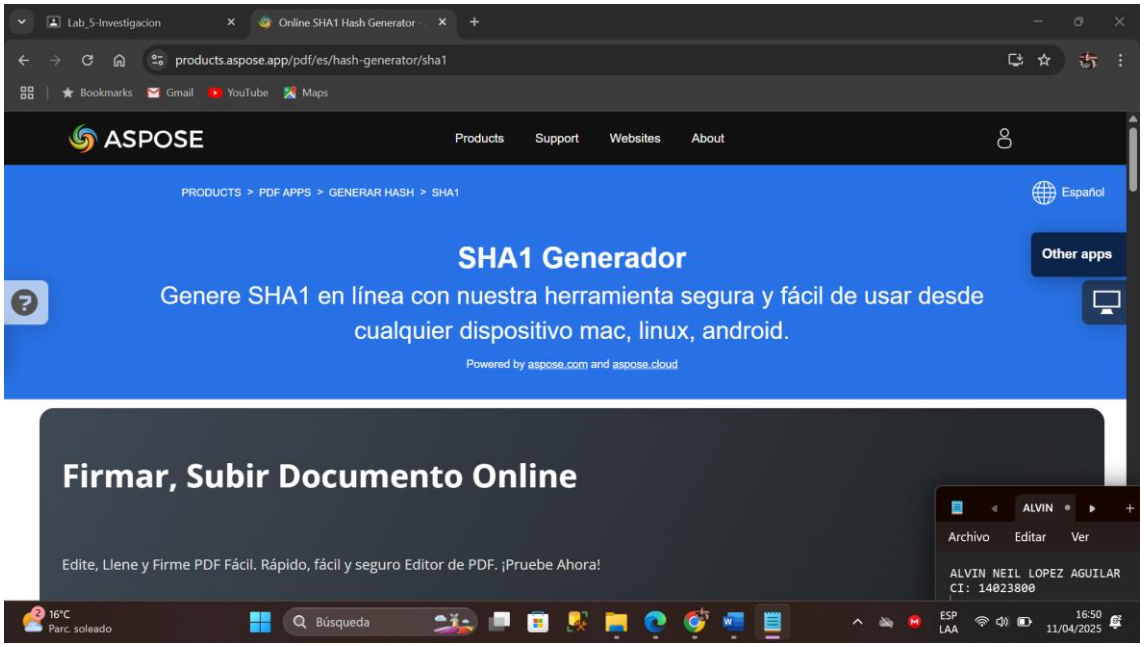
Explique su solución y cómo realizará el control.

Capturas de Pantalla:

Solución propuesta: Uso de funciones hash SHA-1

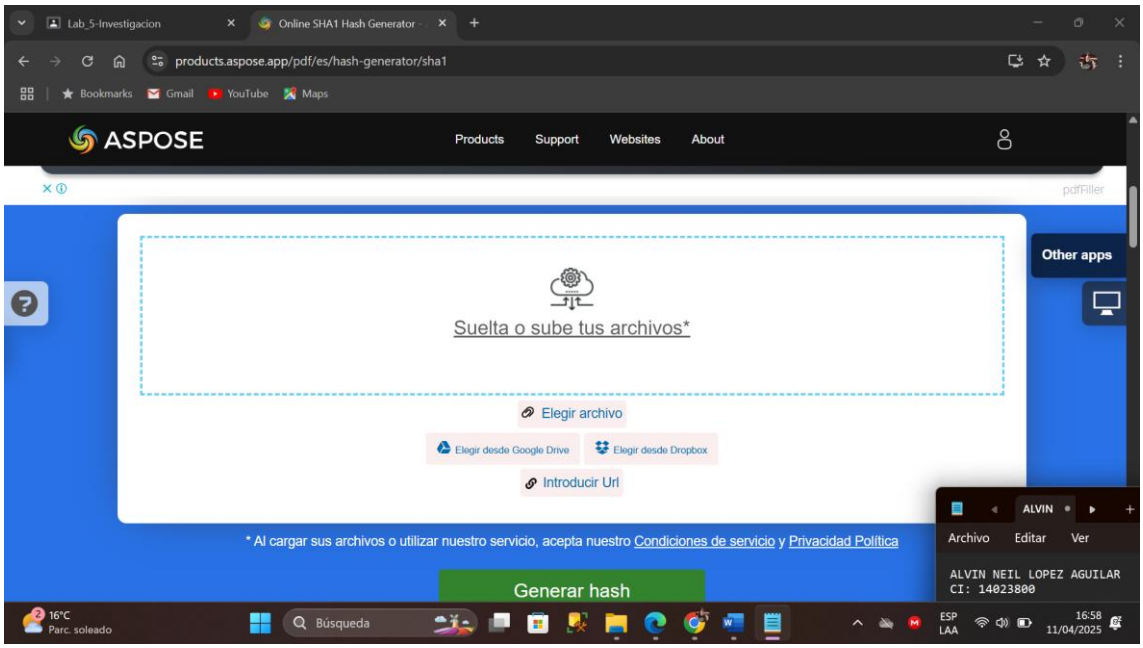
Mi solución se basa en implementar un sistema de verificación usando funciones hash SHA-1:

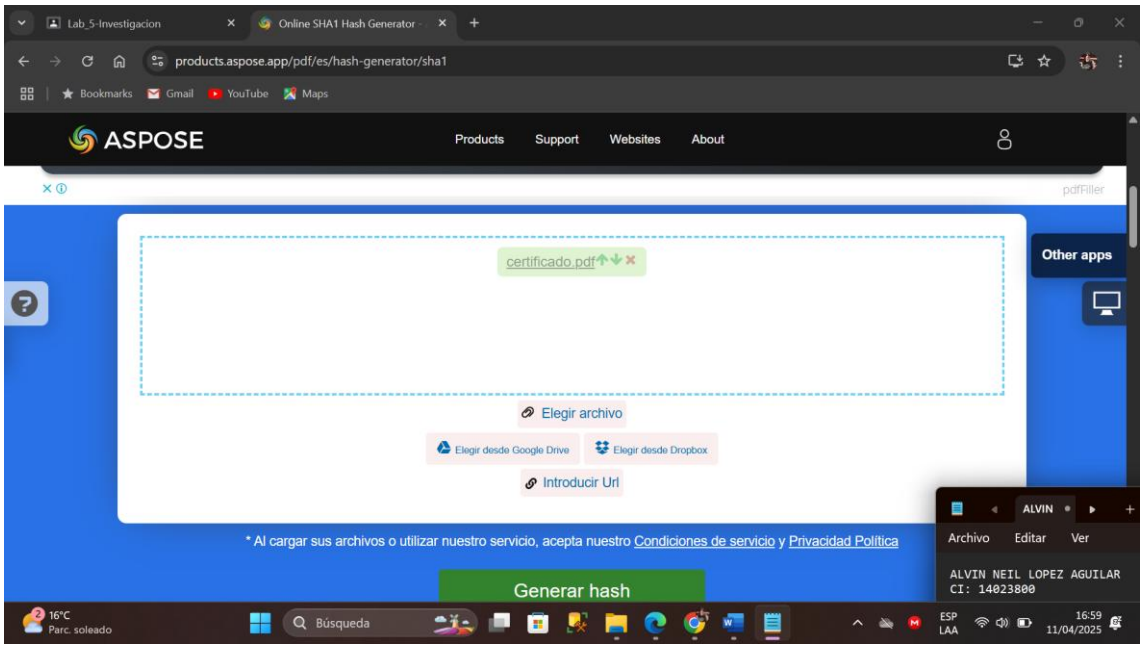
Ingresamos a la página

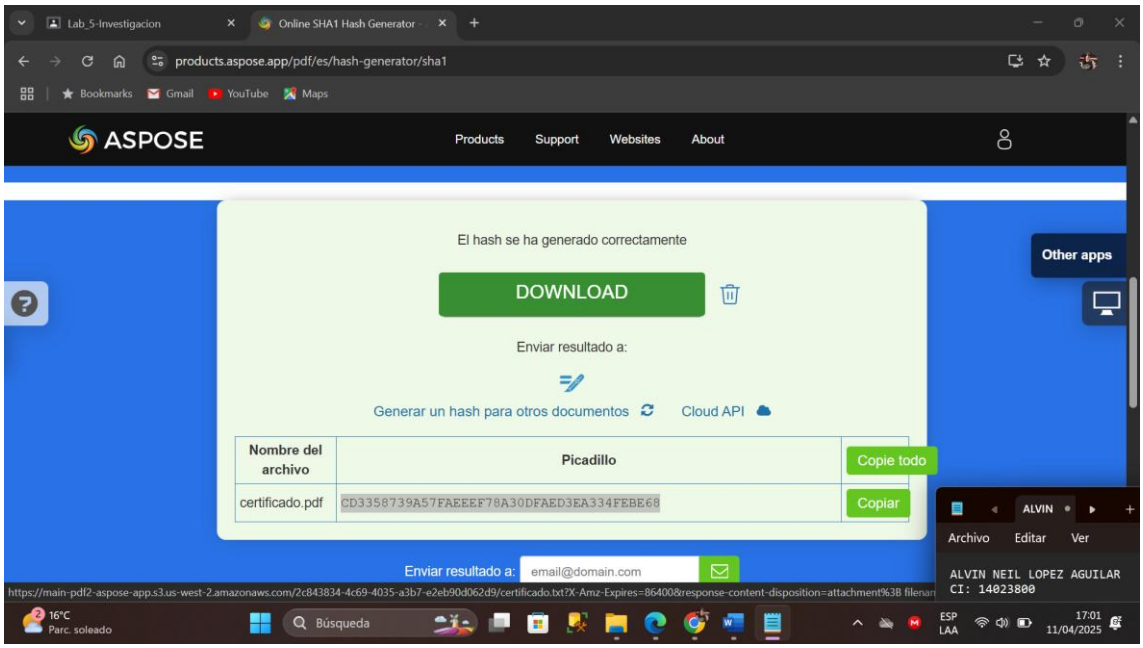


Creamos un certificado para usar de ejemplo

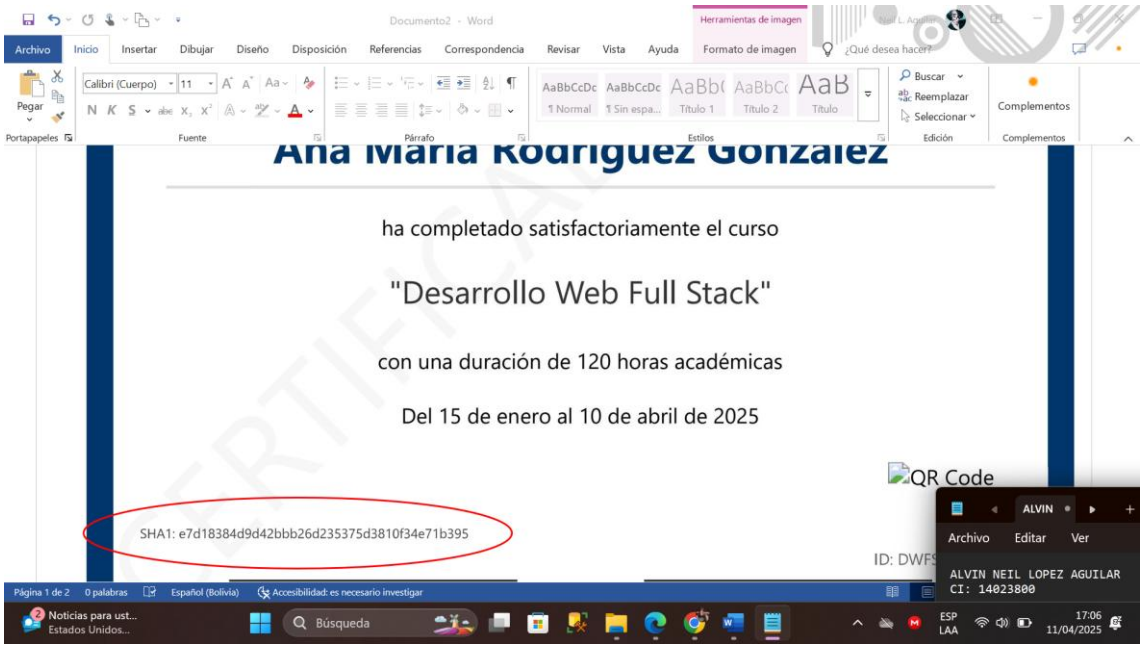
1. **Generación del hash original:**
    - **Para cada certificado generado, calcular su valor hash SHA-1 usando la herramienta de la paina**
    - **Almacenar este valor hash en una base de datos segura junto con la información del estudiante**







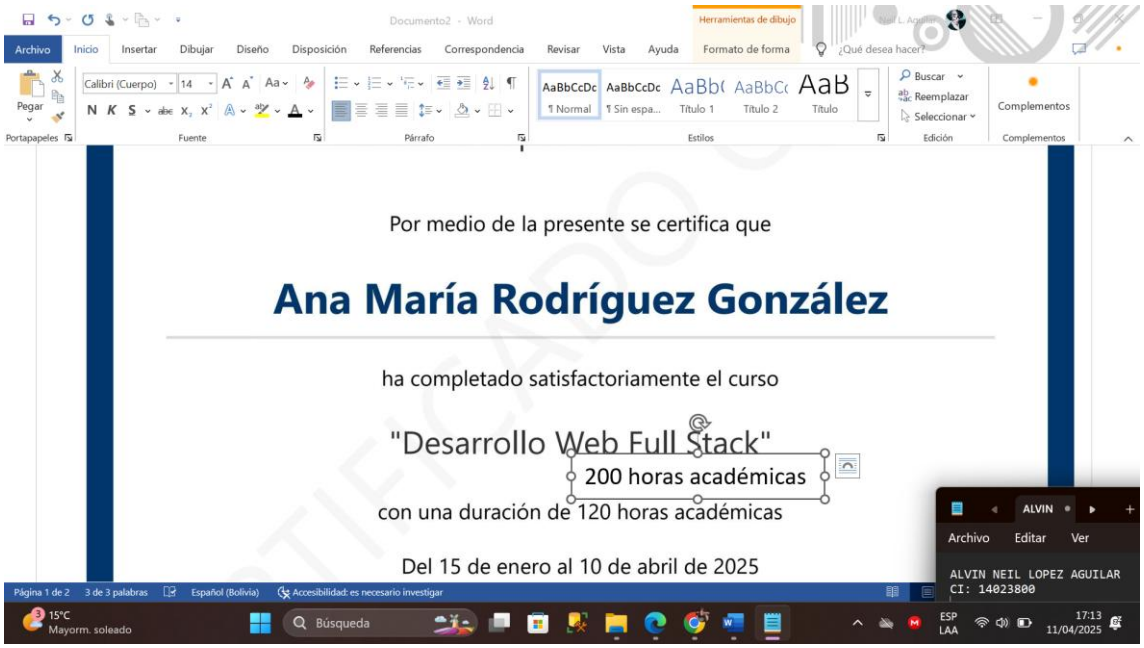
2. **Distribución de certificados:**
    - **Enviar los certificados digitales a los participantes**
    - **Opcionalmente, incluir el valor hash calculado en un registro público o en el mismo certificado como referencia**



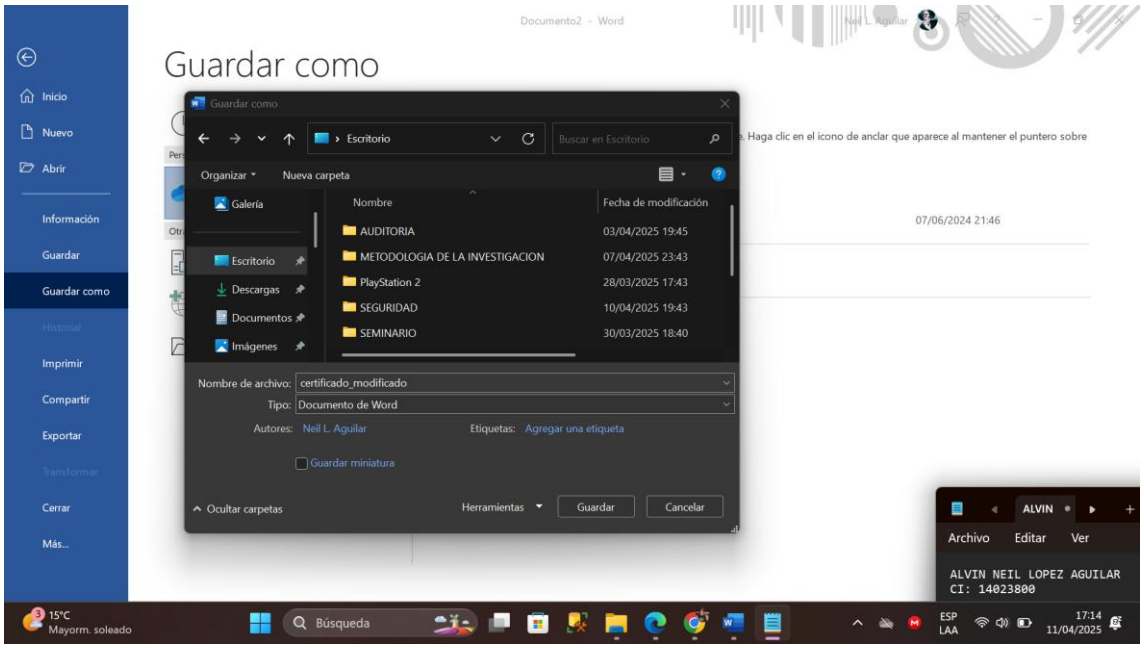
3. **Proceso de verificación:**
    - **Cuando sea necesario verificar la autenticidad de un certificado:**
        - **Recalcular el hash SHA-1 del certificado presentado**
        - **Comparar este nuevo hash con el almacenado originalmente**
        - **Si coinciden, el certificado no ha sido modificado**
        - **Si difieren, el certificado ha sido alterado**

Aquí modificamos un poco el certificado y lo subimos para calcular su hash y si sufrió alguna modificación

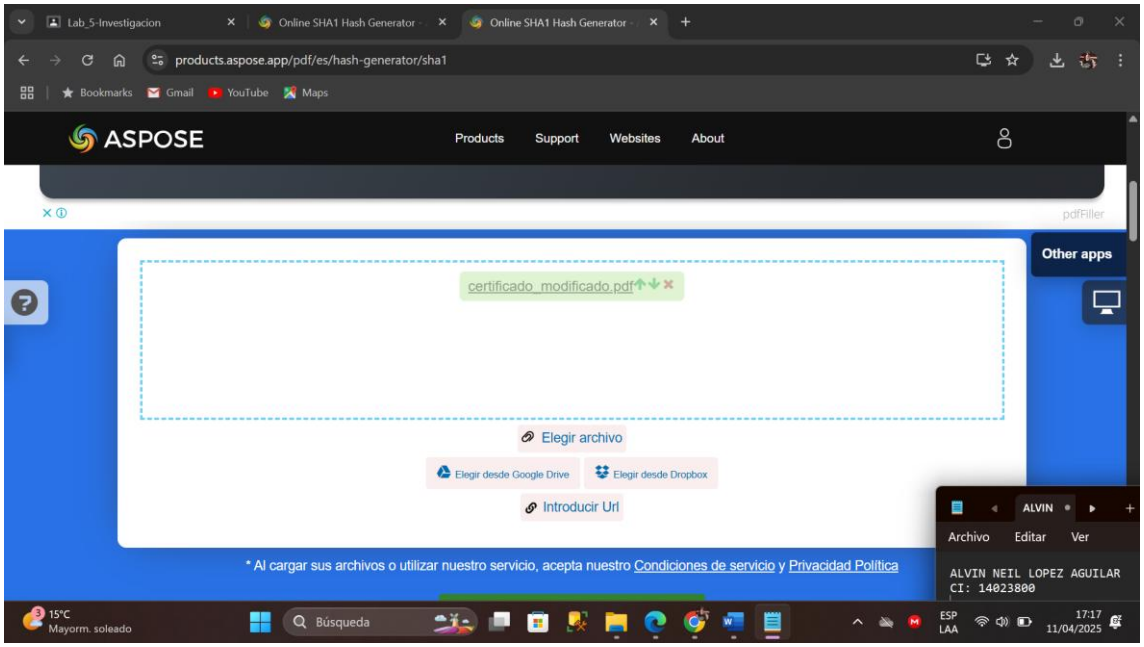
Modificamos de 120 horas a 200 horas académicas

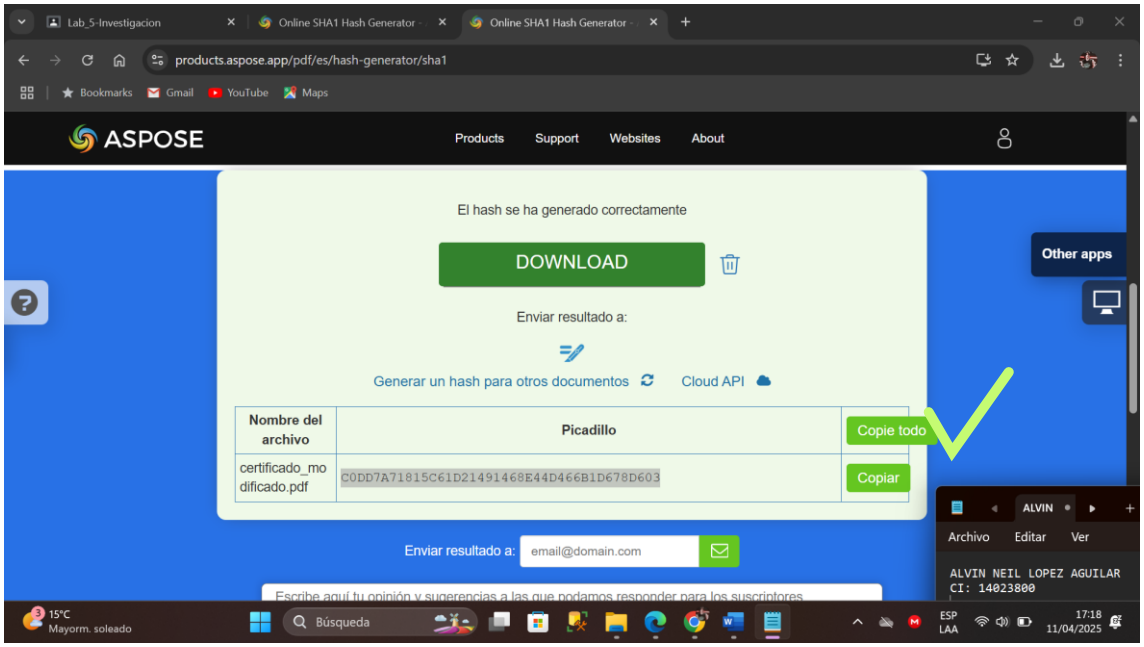


Lo guardamos como certificado_modificado

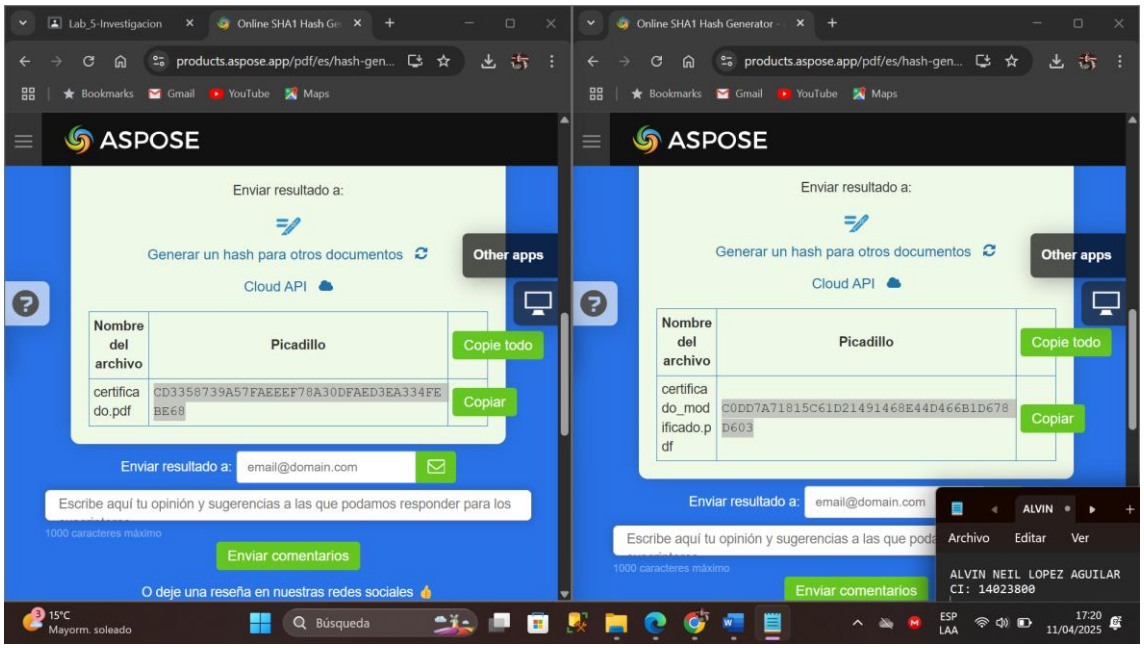


Lo subimos a la pagina y calculamos su valor hash





Comparamos ambos hash y vemos que son diferentes lo cual indica que ah sido modificado el archivo



4. **La solución práctica seria:**
    - **Crear un portal web donde los interesados puedan subir certificados para verificación**
    - **El sistema automáticamente calculará el hash del archivo subido y lo comparará con el registro original**
    - **Se informará inmediatamente si el documento es auténtico o ha sido manipulado**

Esta solución aprovecha la propiedad fundamental de las funciones hash criptográficas: cualquier cambio, por mínimo que sea, en el documento original producirá un valor hash completamente diferente, haciendo imposible modificar el certificado sin que sea detectado.