Evaluación Laboratorio 5

LAB 5 – CIFRADO ASIMÉTRICO

Nombre: Uño Astoraique Maria Fernanda

PREGUNTAS DE EVALUACIÓN

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

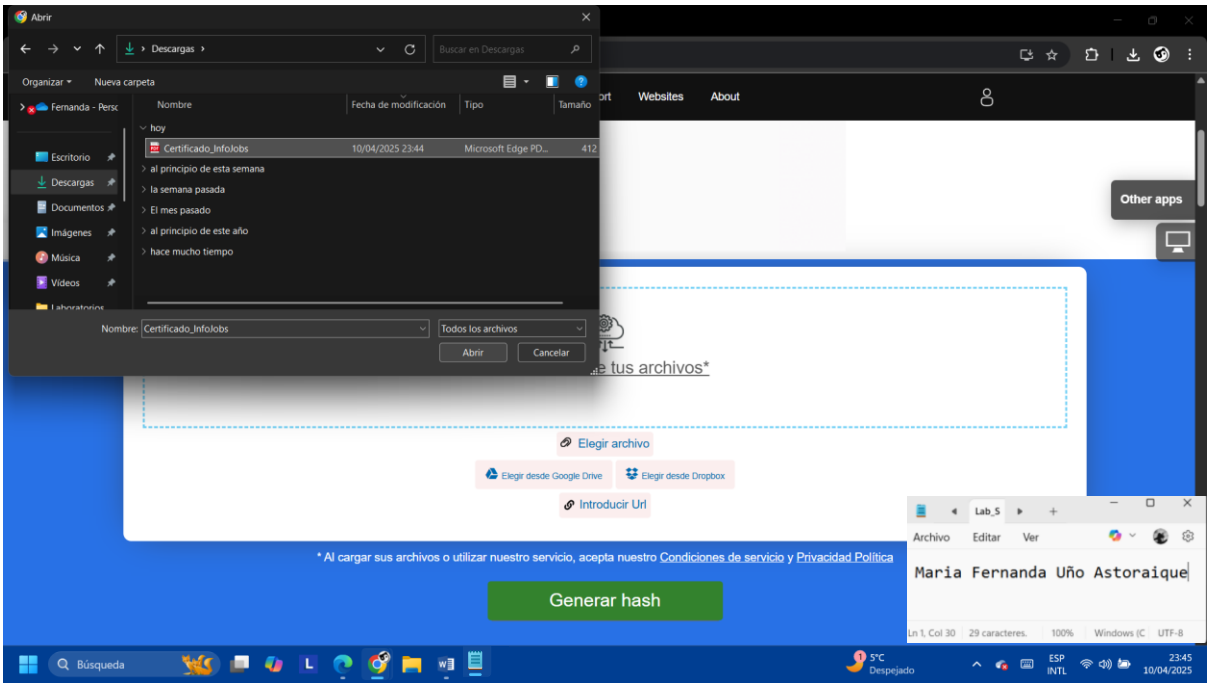
Realice la simulación siguiente:

Ud. Es una entidad educativa, que está generando certificados de un curso que brindó, ahora está 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 modificación.

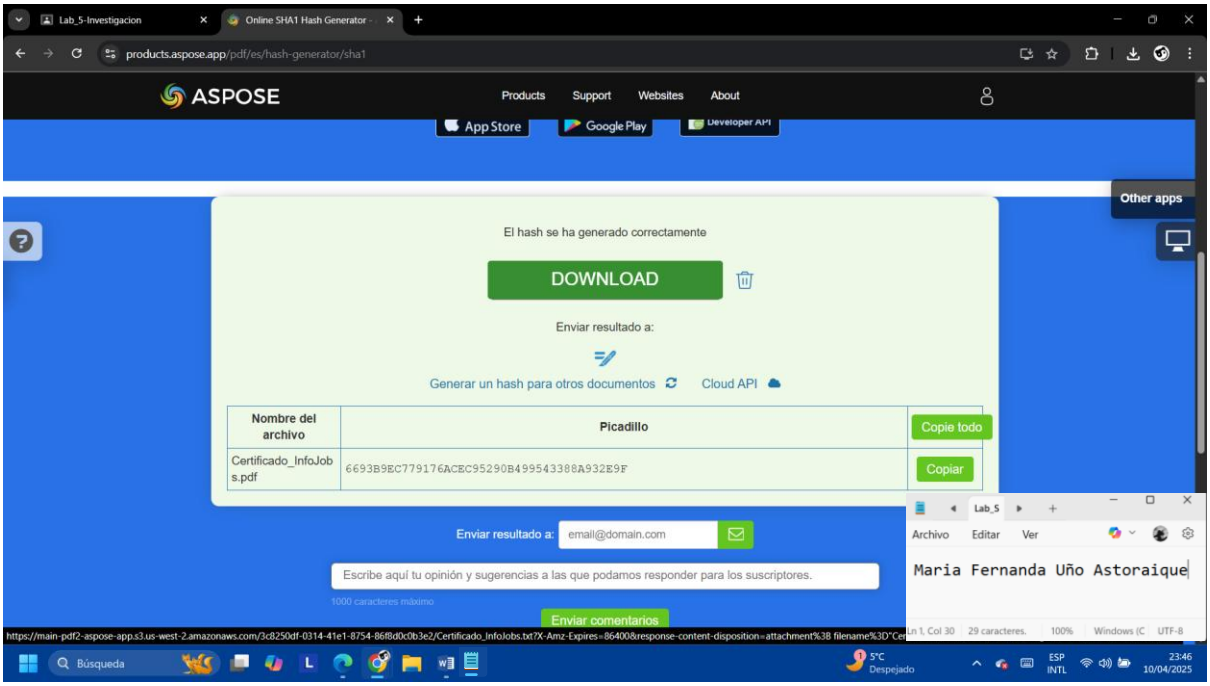
Explique su solución y cómo realizará el control.

Una vez generado los certificados procedemos a lo siguiente:

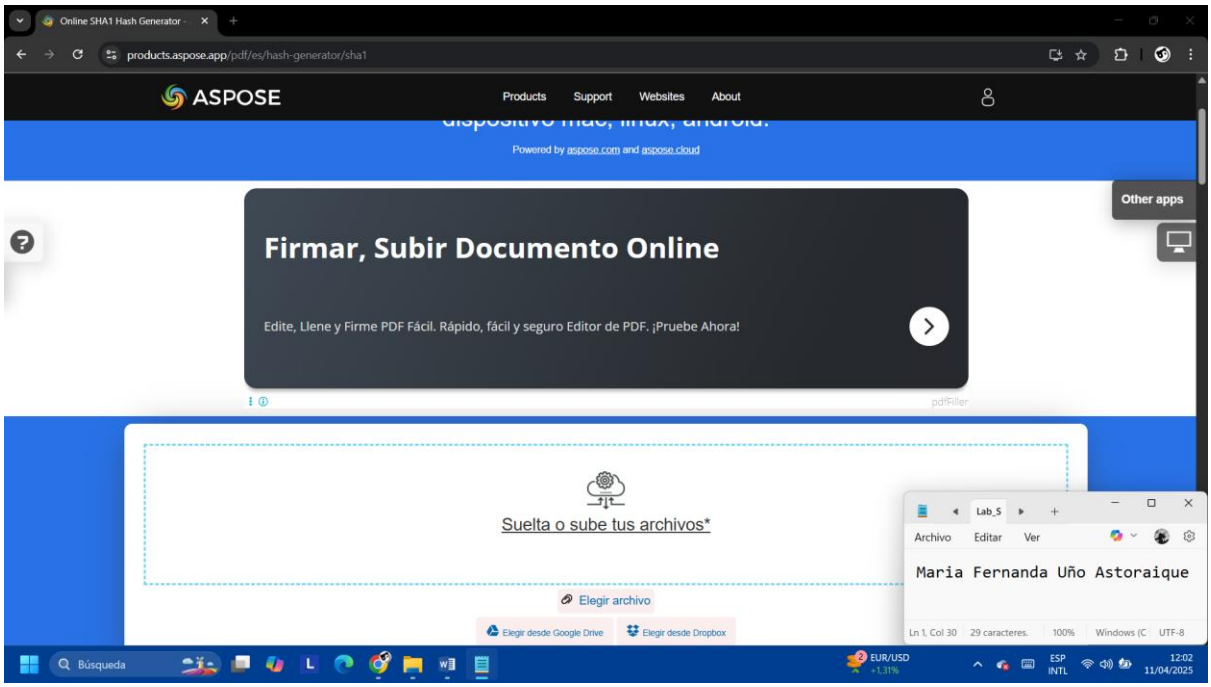
1. Generar el Hash SHA1

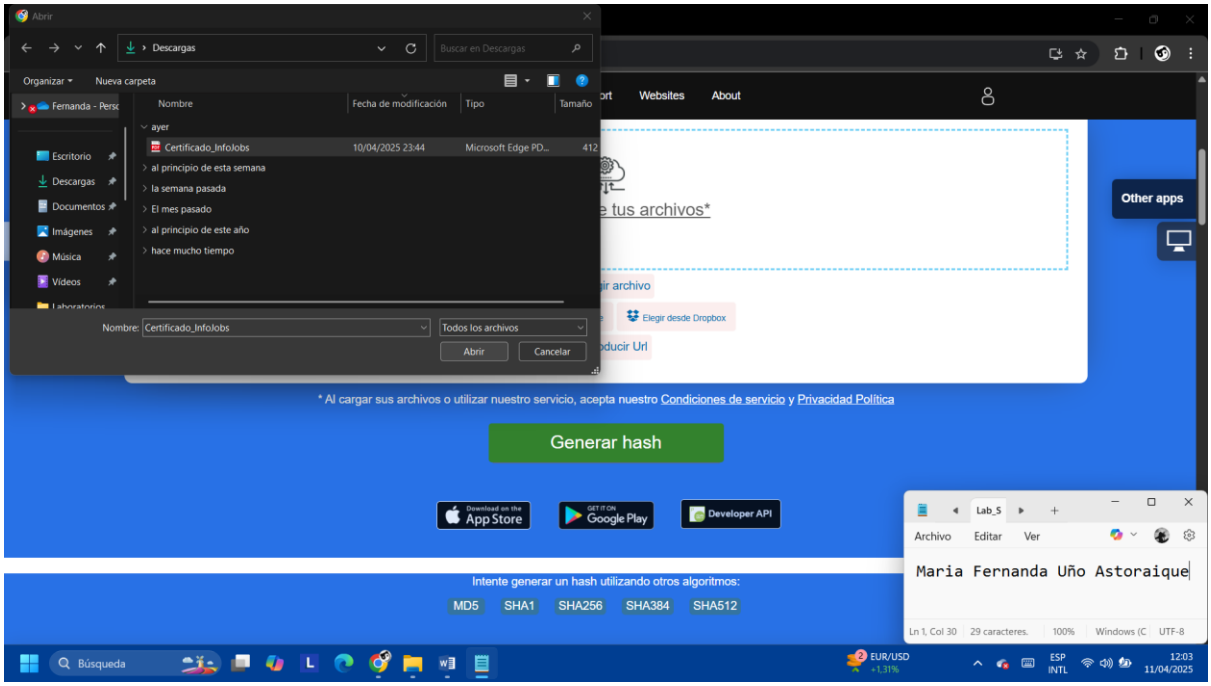


Descargar el archivo proporcionado:

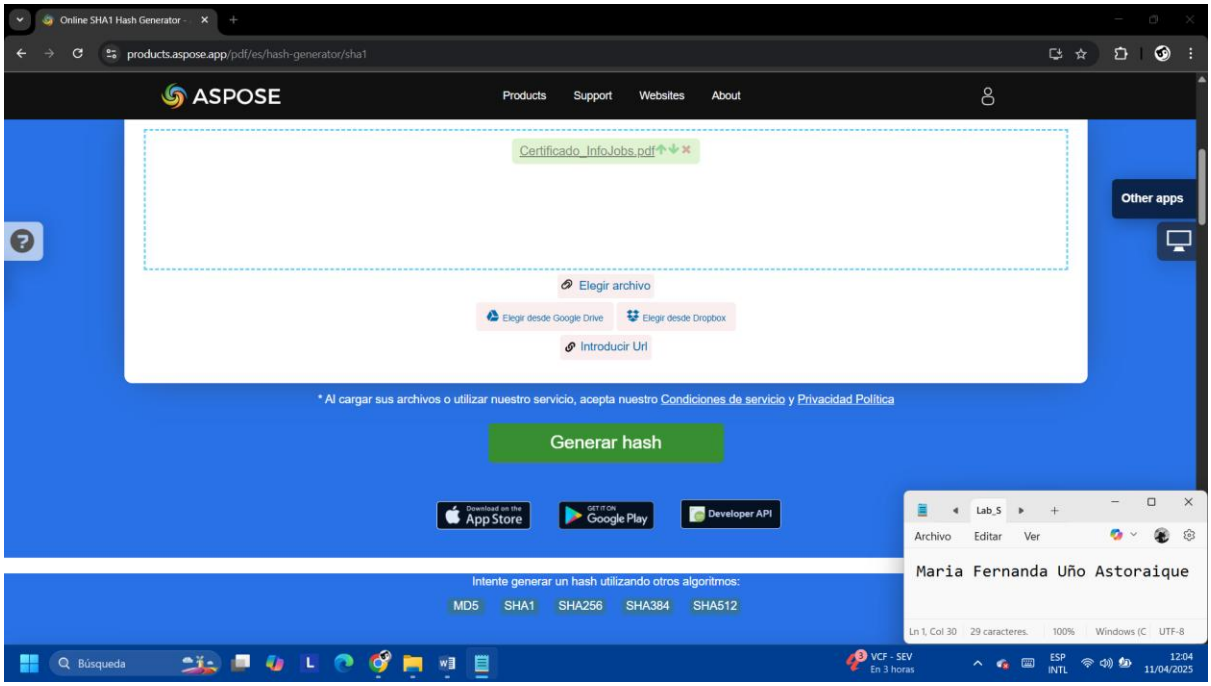


Volvemos a ingresar a la página, y subimos el certificado descargado:

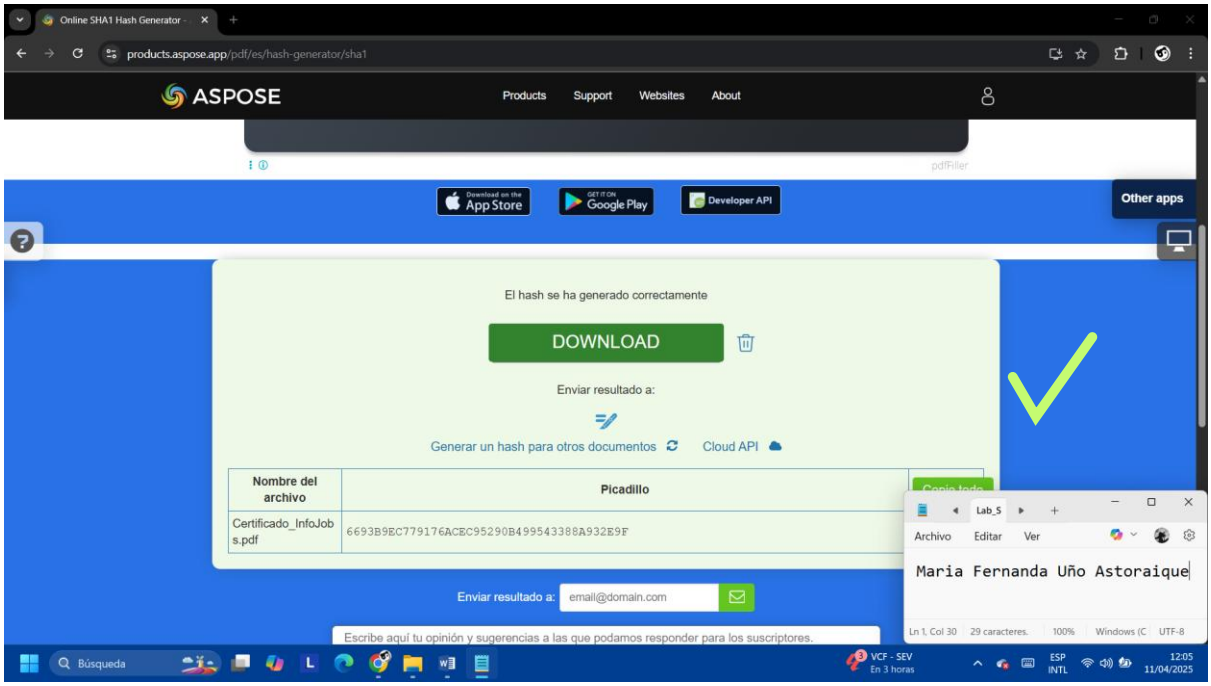




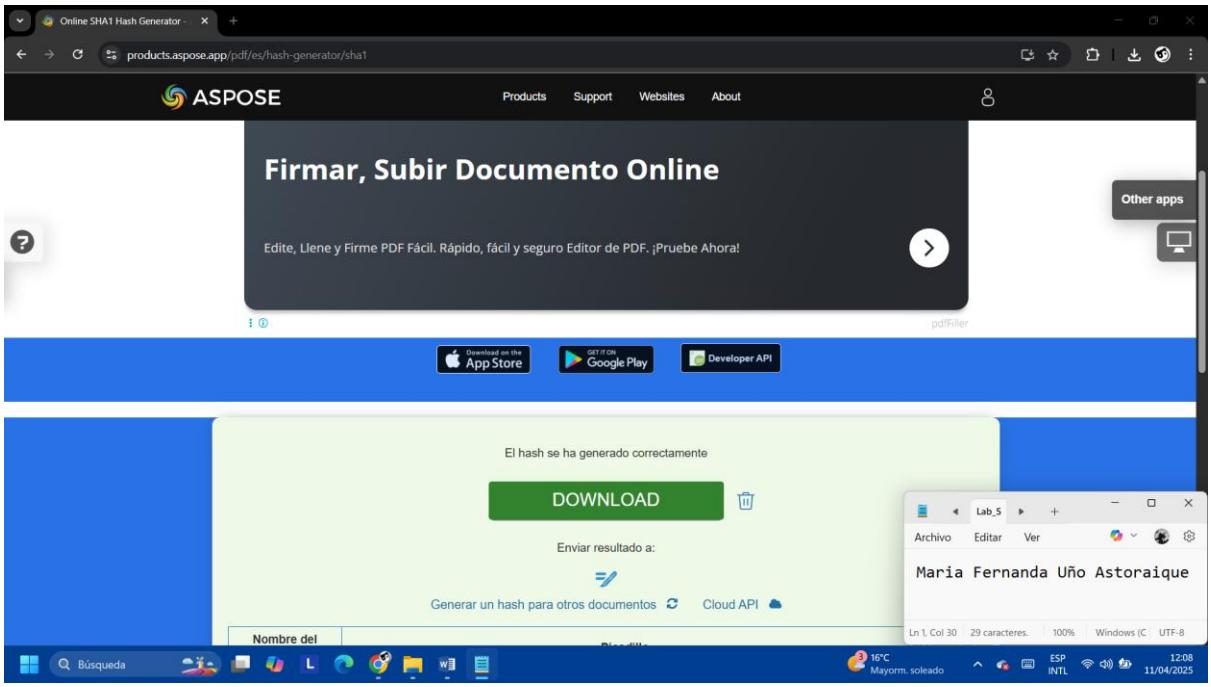
Generamos el nuevo hash:



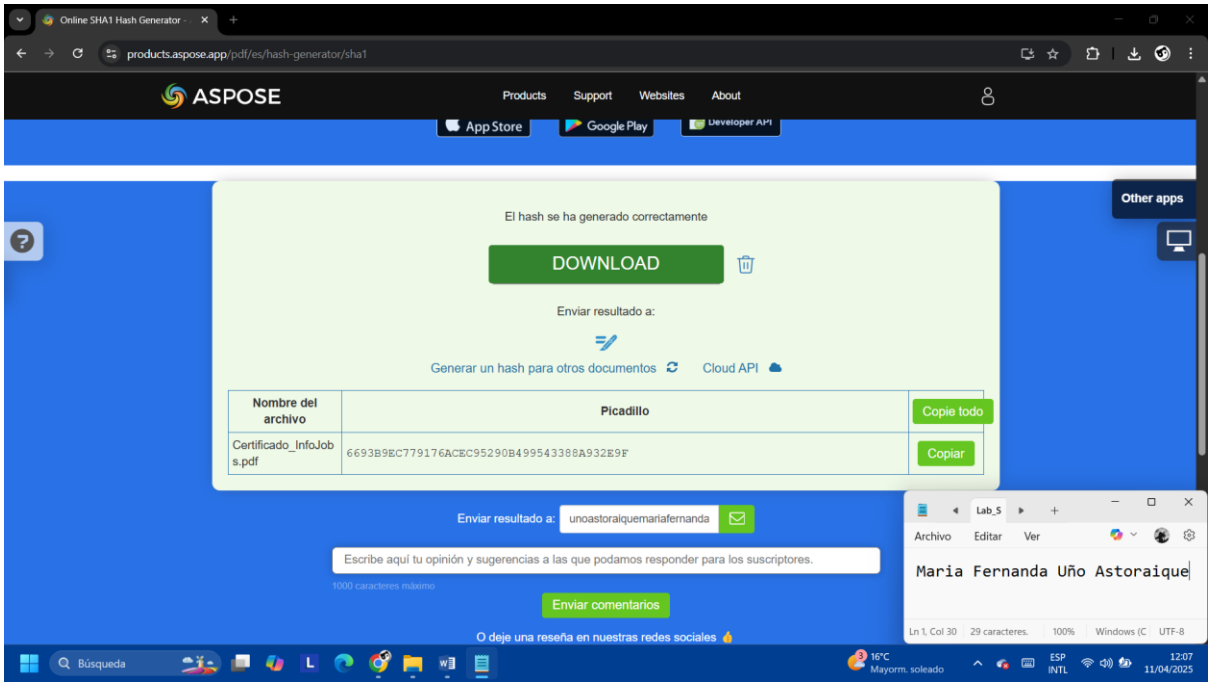
Descargar el archivo:

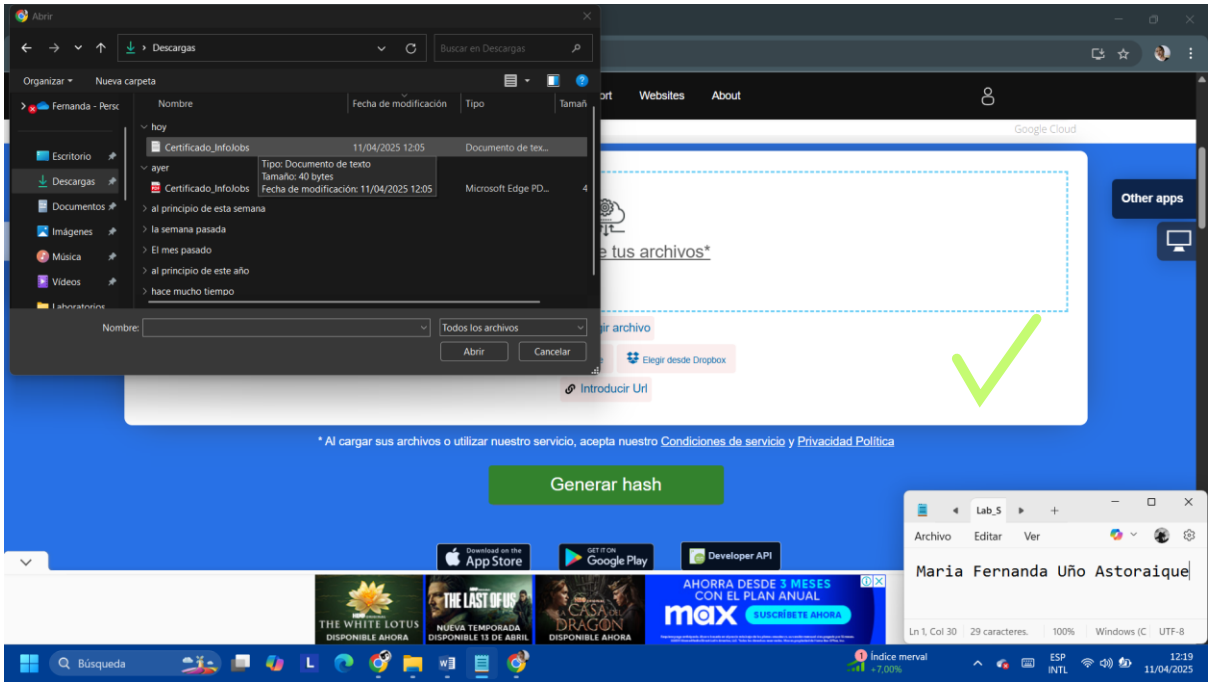


Guardar el hash:

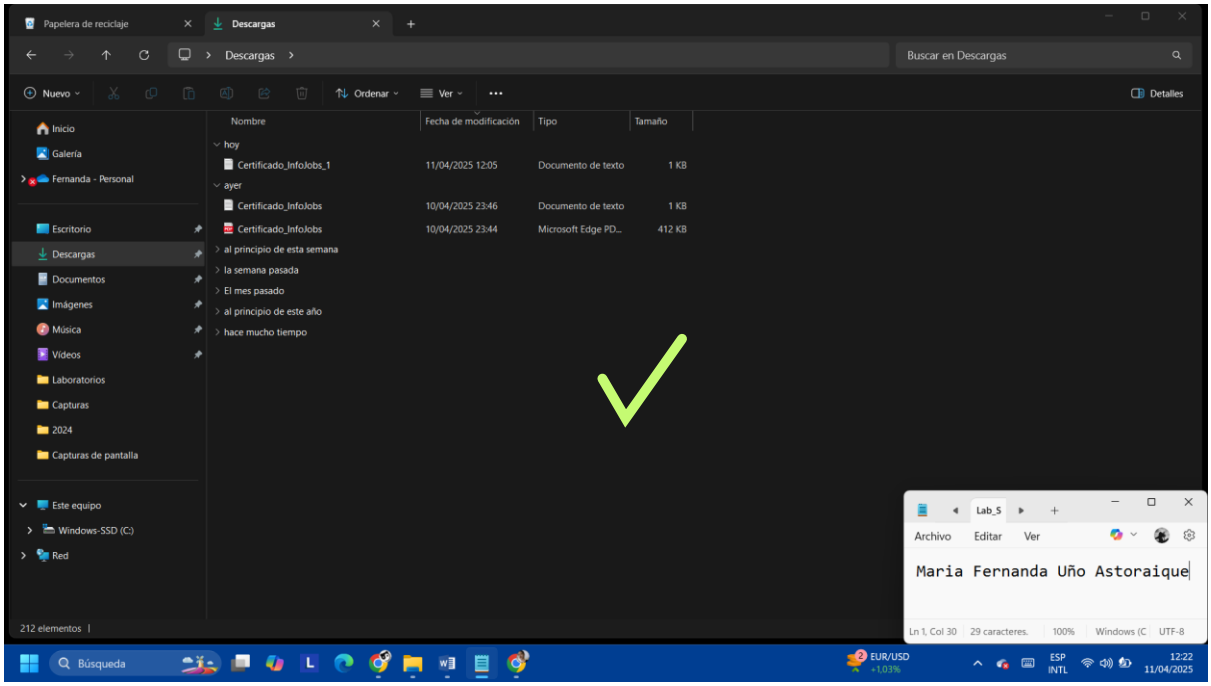


Posteriormente podemos enviar el certificado por correo ():





Actualmente tenemos dos archivos que contienen el hash de los certificados:



CONTROL

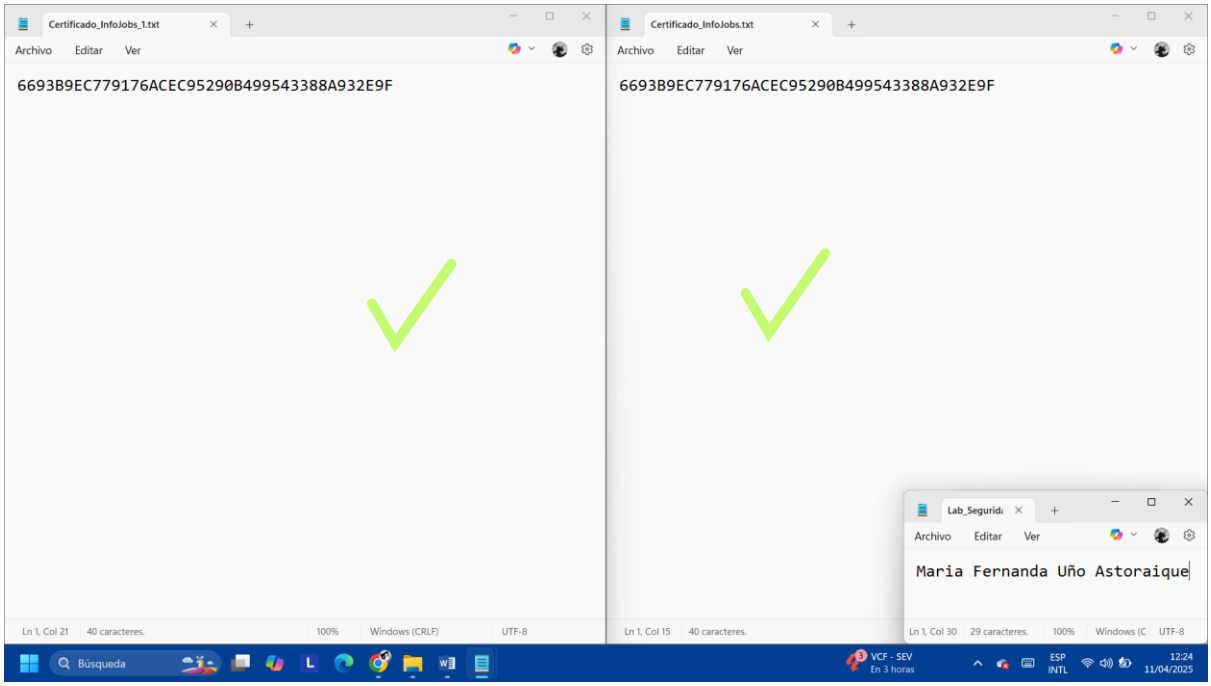
Para el debido control, entregamos el certificado digital al participante junto con el hash SHA1 correspondiente. Esto se puede hacer a través de correo electrónico como se mencionó anteriormente en los pasos.

El participante puede verificar si el certificado ha sido modificado realizando los mismos pasos:

Descargar el certificado y el hash SHA1 que se le proporciono.

Usar la misma herramienta (https://products.aspose.app/pdf/es/hash-generator/sha1) para generar un nuevo hash SHA1 del certificado que recibió.

Comparar el hash SHA1 que generó con el hash SHA1 que le proporcioné originalmente. Si los dos hashes coinciden, esto confirmará que el certificado no ha sido alterado. Si los hashes no coinciden, esto nos indica que el certificado ha sido modificado de alguna manera, y por lo tanto, no es auténtico.



Dada la comparación se puede observar que ambos hash son las mismas:

6693B9EC779176ACEC95290B499543388A932E9F	6693B9EC779176ACEC95290B499543388A932E9F