LABORATORIO Nro 5

Univ. Rosa Mariana Torrez Quispe

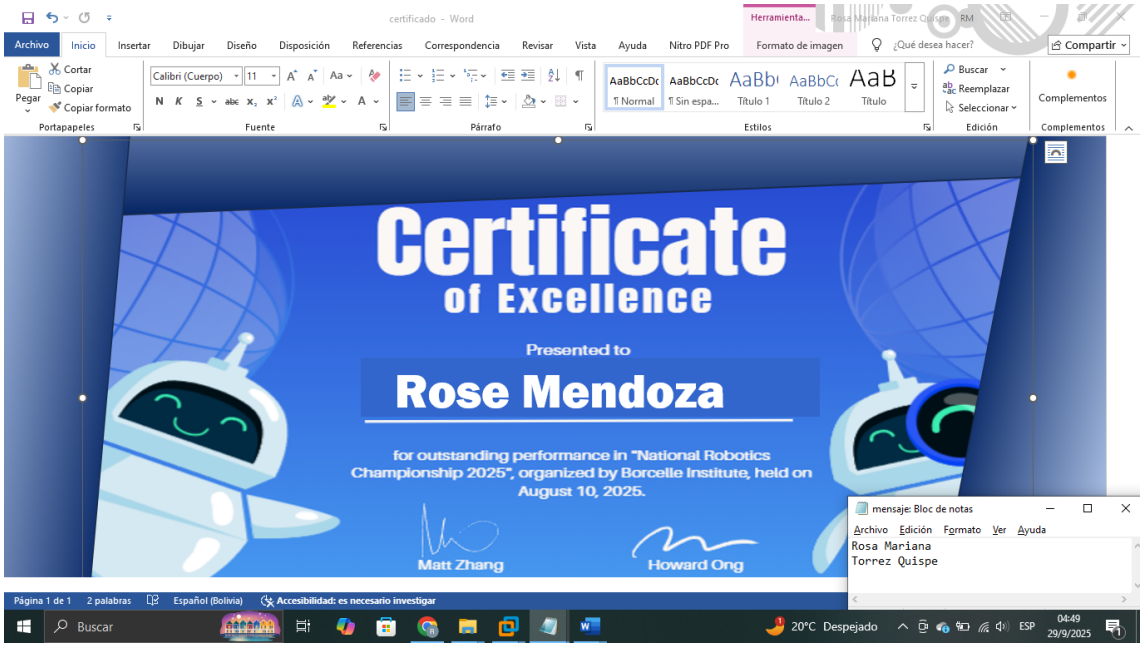
PREGUNTAS DE LA EVALUACIÓN

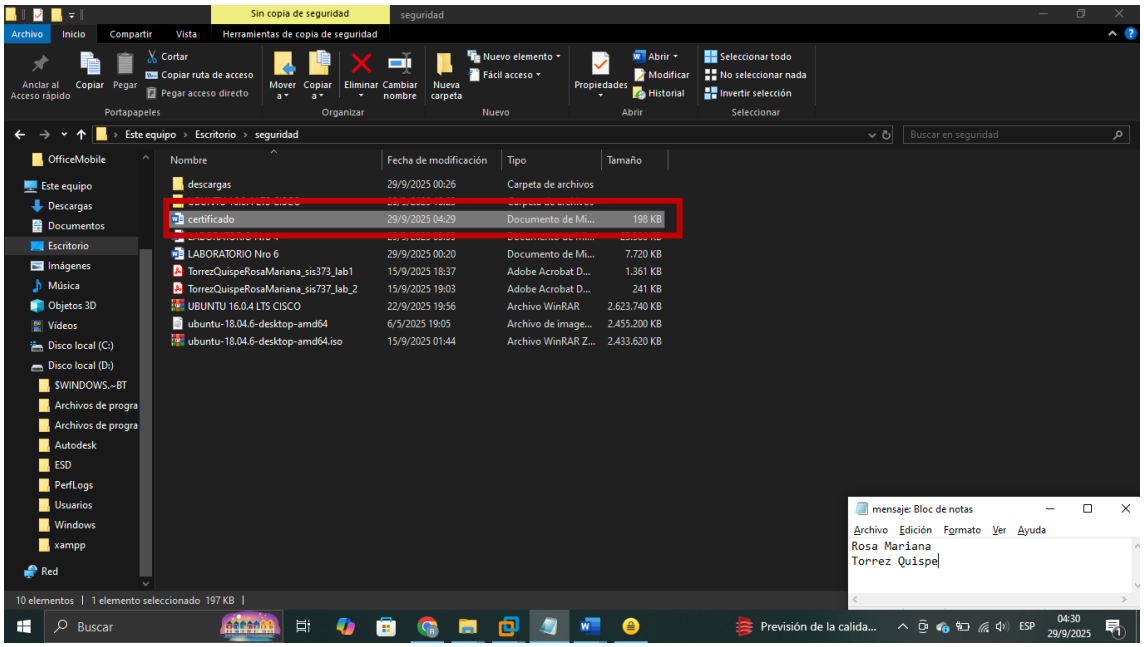
Realice la simulación siguiente:

Ud. Es una entidad educativa, que está generado 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 modificación.

Explique su solución y como realizará el control.

Primeramente, se debe desarrollar el certificado correspondiente en el programa de su preferencia en mi caso es Word, se procede a guardar el certificado para luego ser enviado.

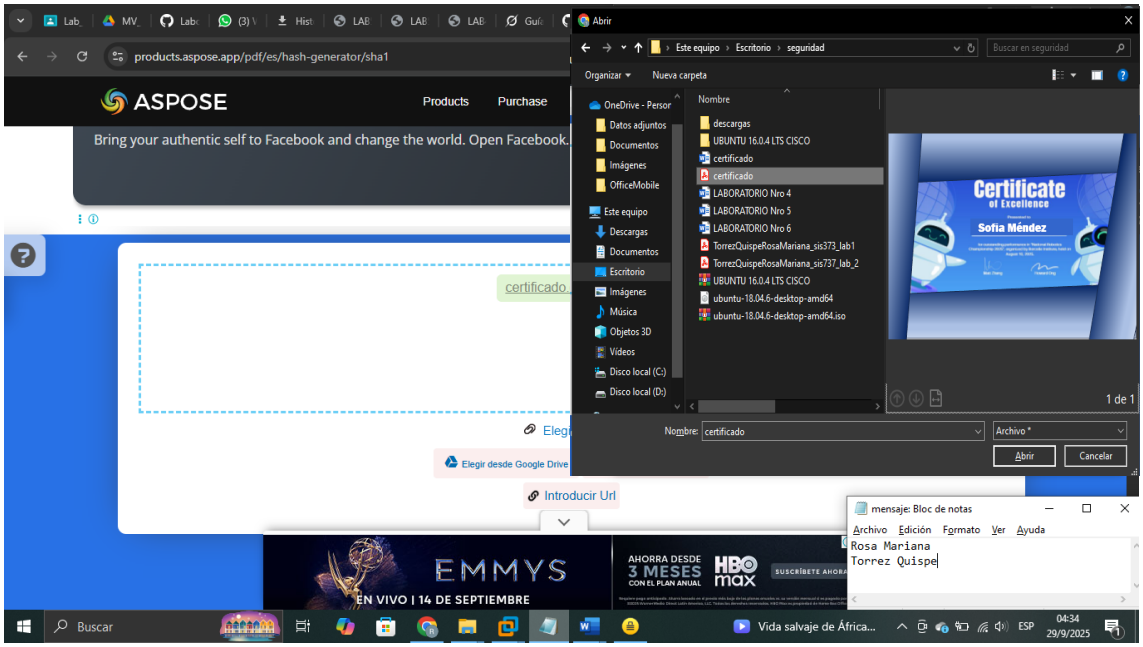




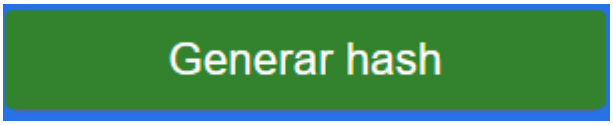
Una vez guardado el documento, subir el archivo a la página que nos brindó:

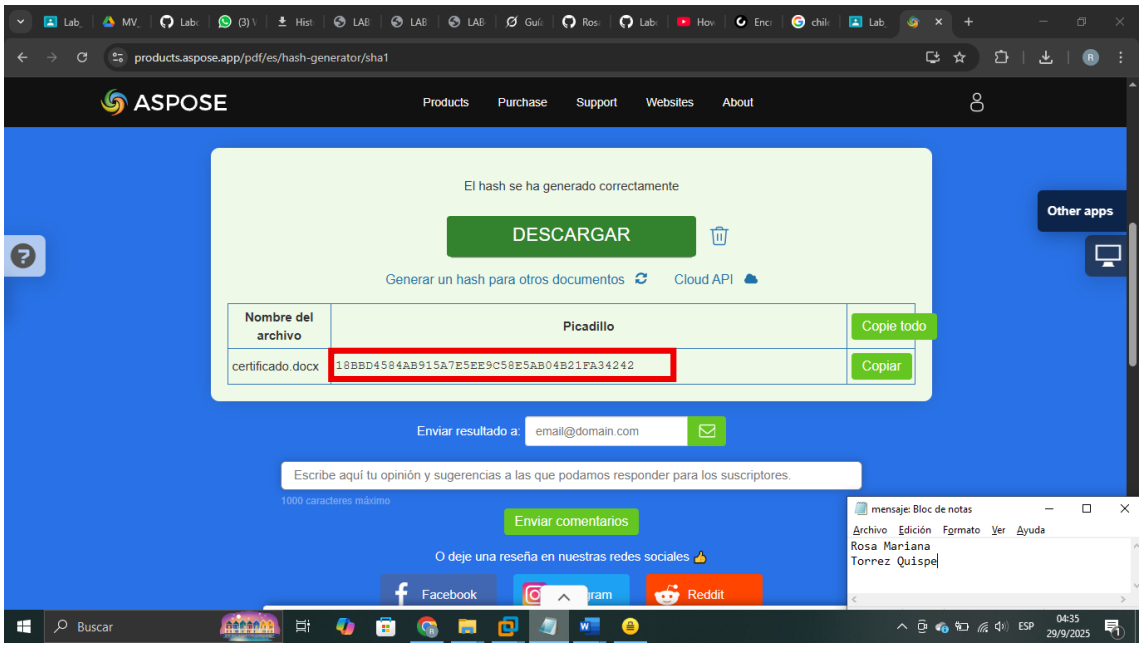
https://products.aspose.app/pdf/es/hash-generator/sha1

Generar el hash del certificado

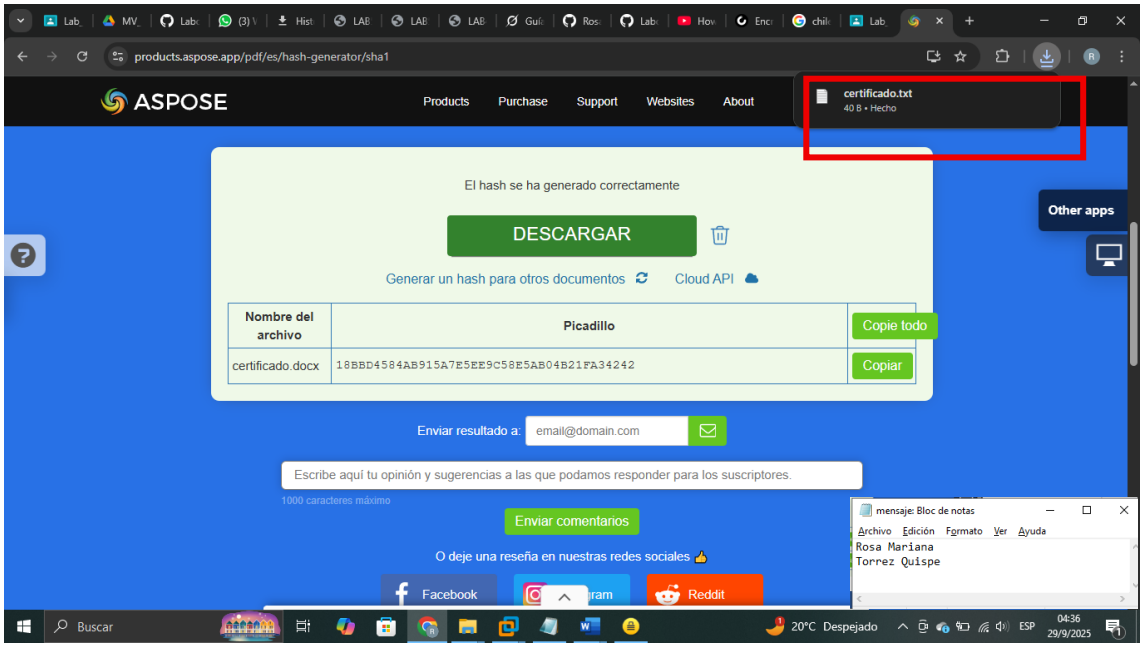


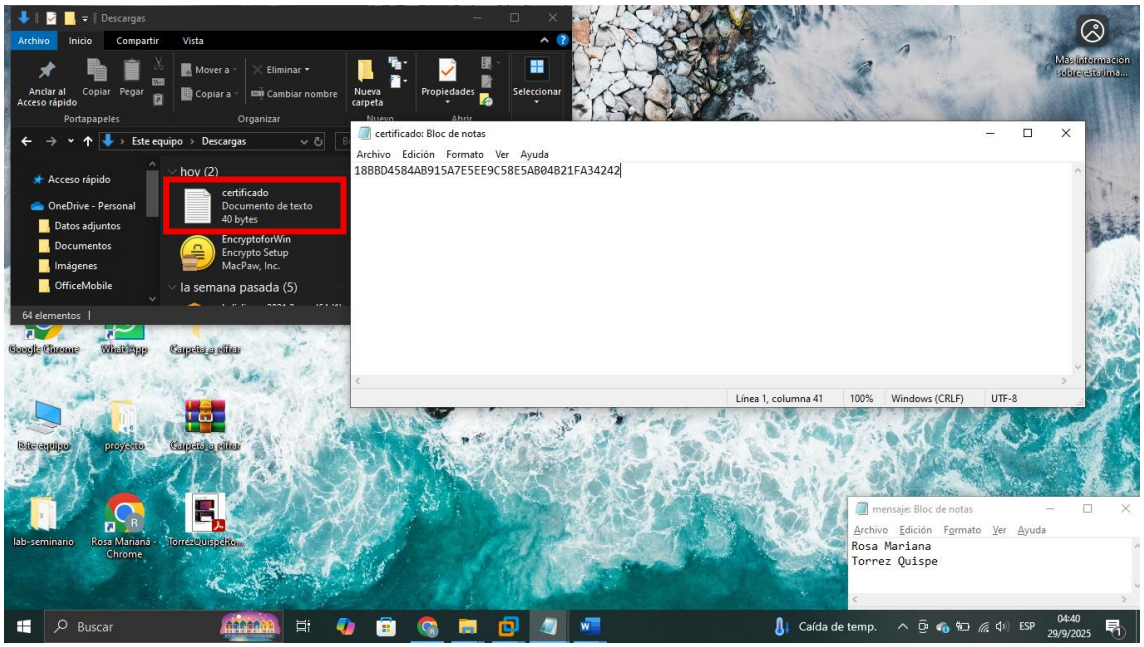
luego presiona “Generar hash”



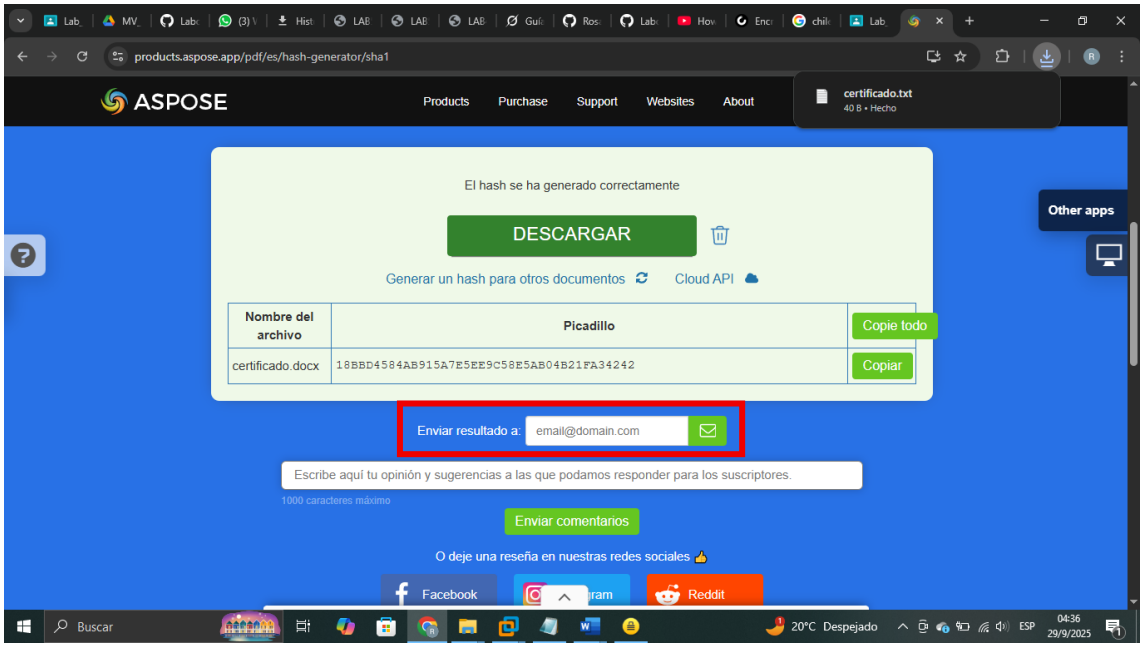


Descargamos el hash generado por la página el cual nos entrega un documento .txt el cual lo almacenaremos.

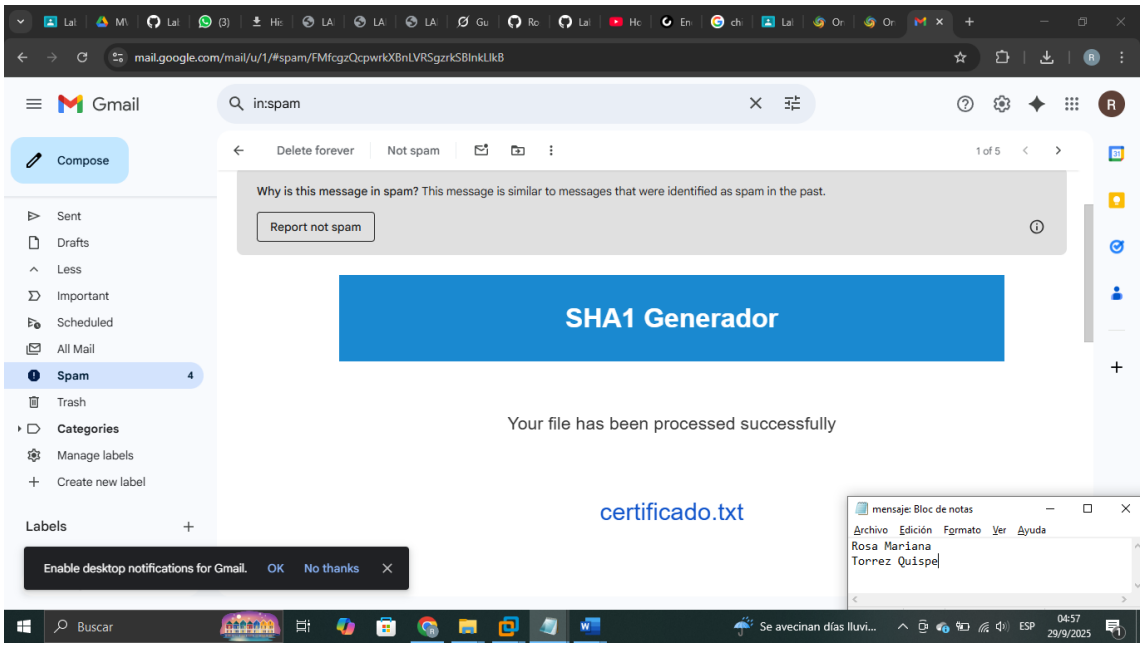




El hash del certificado que se envió al estudiante. Se hizo una simulación de como el estudiante recibiría el certificado y el hash del estudiante:



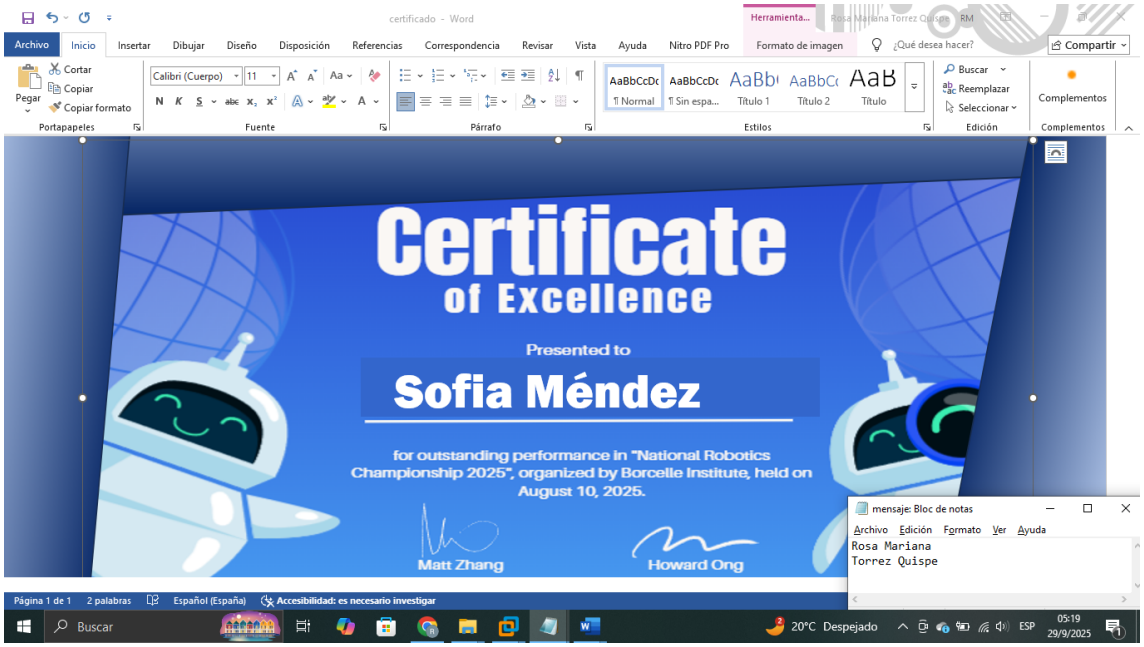
Una vez obtenido el hash introducimos un correo electrónico.



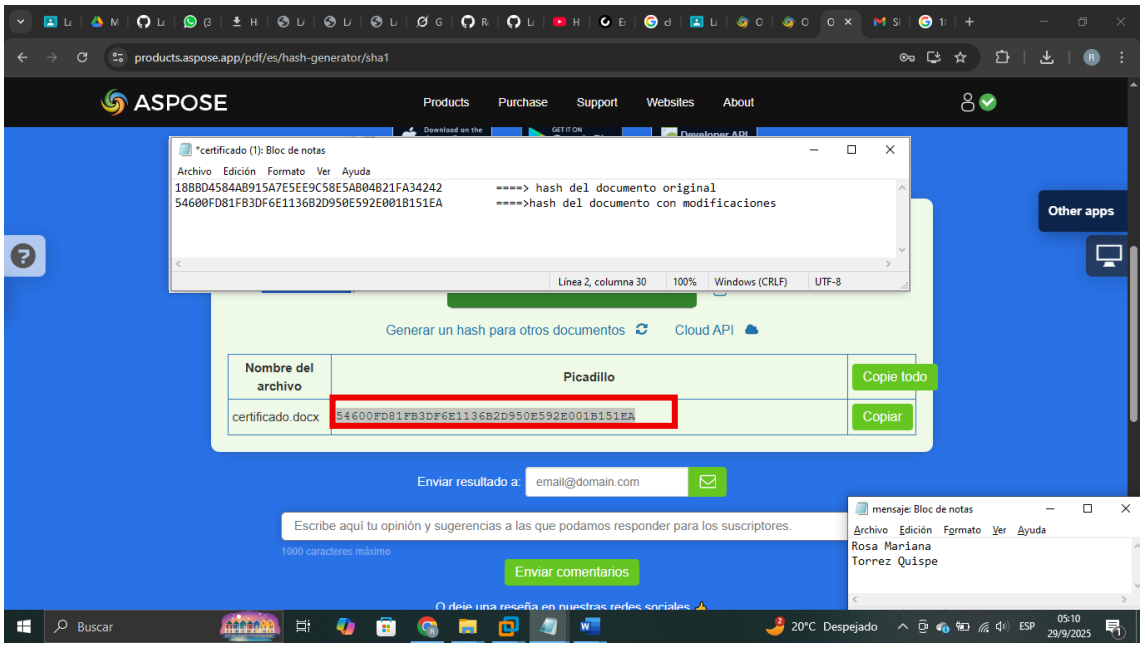
Aquí aparece el hash que se envío al estudiante.

CERTIFICADO MODIFICADO

Realizaremos un cambio al **nombre**, simulando una alteración al certificado intentando falsificarlo.



Comparación de hash modificado y el original



Teniendo la información del hash con cualquier alteración que se haya hecho en el documento automáticamente el valor que tenía el hash cambiará invalido completamente la documentación presentada, se hará una demostración del cambio.

Explicación de como dará la solución y control de los certificados (se toma en cuenta la redacción, la forma de expresión).

Las soluciones y control de los certificados posibles que veo son:

Para mayor seguridad de protección de los certificados en este caso digitales, se tiene que complementar con firmas digitales (aunque eso requiere herramientas adicionales como OpenSSL).

Al momento de terminar de crear los certificados se debe de generar un hash de este, una vez obtenido el hash se debe de almacenar en una base de datos junto con los nombres de los estudiantes y el título del certificado. Este método no previene la modificación, pero permite detectarla los certificados falsos. El control del hash se llevará a cabo mediante la comparación de valores hash (cada vez que un participante desee verificar la autenticidad del certificado, podrá calcular el hash del archivo recibido usando una herramienta como la del sitio proporcionado).