

**LABORATORIO N° 5**  
**SEGURIDAD DE SISTEMAS SIS-737-G1**



**Estudiante:** Marco Antonio Cruz Mamani    **CI:** 10529605    **Fecha de entrega:** 12/04/2025

**Docente:** Ing. J. Alexander Durán M.

**EVALUACIÓN DE CIFRADO ASIMÉTRICO**

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 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.

**1.1. Planteamiento del problema:**

Mi persona es una entidad educativa que ha generado **certificados en formato PDF** para un curso. Estos certificados se enviarán virtualmente a los participantes. Es necesario asegurar que **no sean modificados**, y que cualquier alteración pueda ser detectada.

**1.2. Solución propuesta: Uso del Hash SHA1**

Un hash es una huella digital del archivo. Si el archivo se modifica (aunque sea una letra o byte), su hash cambia completamente. Entonces:

- Antes de enviar un certificado, se genera su hash SHA1.
- Se guarda el hash.
- Cuando un usuario presenta su certificado, se vuelve a generar el hash del archivo recibido y se compara con el original.
- Si los hashes coinciden, el archivo no fue modificado.

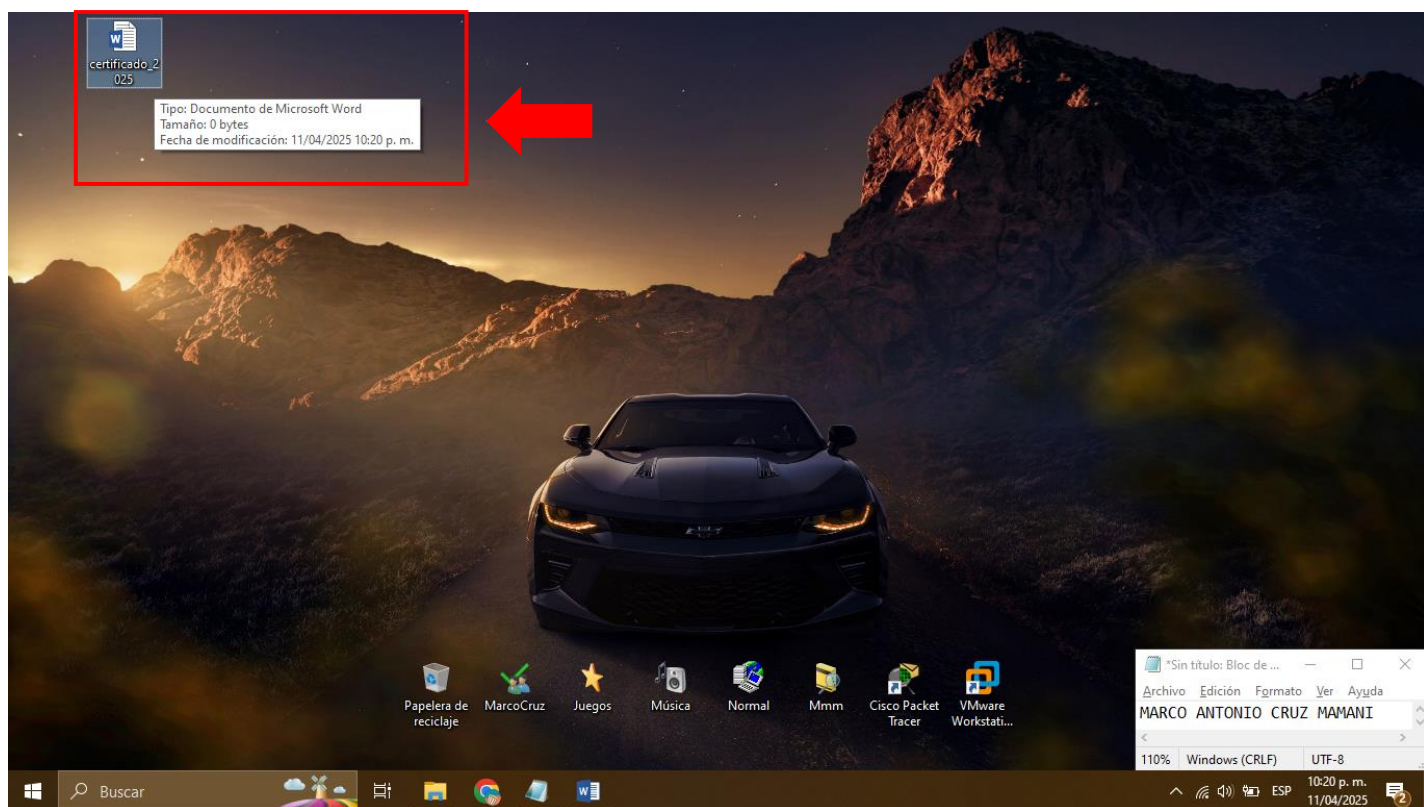
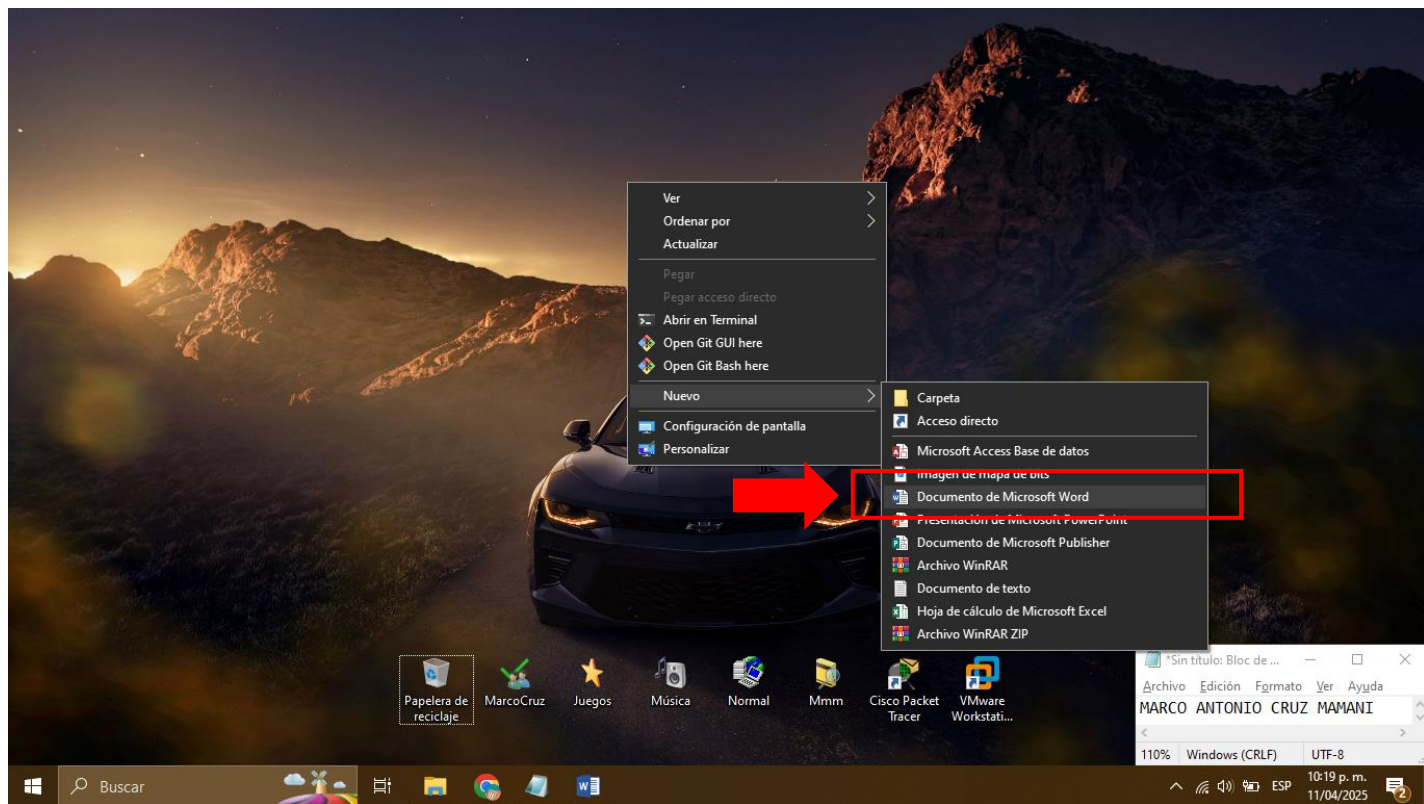
**1.3. Pasos para el control (con capturas):**

Se realizó para dos casos: Certificado NO modificado y Certificado MODIFICADO:

**1.3.1. CERTIFICADO NO MODIFICADO:**

**PARTE 1: Creación del certificado:**

**PASO 1: crear un Word para editar el certificado.**



Microsoft Word interface showing a certificate template. The ribbon includes ARCHIVO, INICIO, INSERTAR, DISEÑO, DISEÑO DE PÁGINA, REFERENCIAS, CORRESPONDENCIA, REVISAR, and VISTA. The document content is as follows:

**CERTIFICADO DE PARTICIPACIÓN**

Se certifica que

**Juan Perez**

Ha participado satisfactoriamente en el curso denominado

"Curso de Criptografía"

Llevado a cabo en modalidad [presencial/virtual], durante el mes de [Mes] del año [Año].

Lugar y Fecha: Potosi, 11 de abril de 2025

A green checkmark is visible on the right side of the document.

Windows taskbar shows: PÁGINA 1 DE 1, 41 PALABRAS, ESPAÑOL (MÉXICO), Windows logo, Buscar, and system tray with date 11/04/2025.

## PASO 2: guardar el archivo en formato .pdf con el nombre "certificado\_2025"

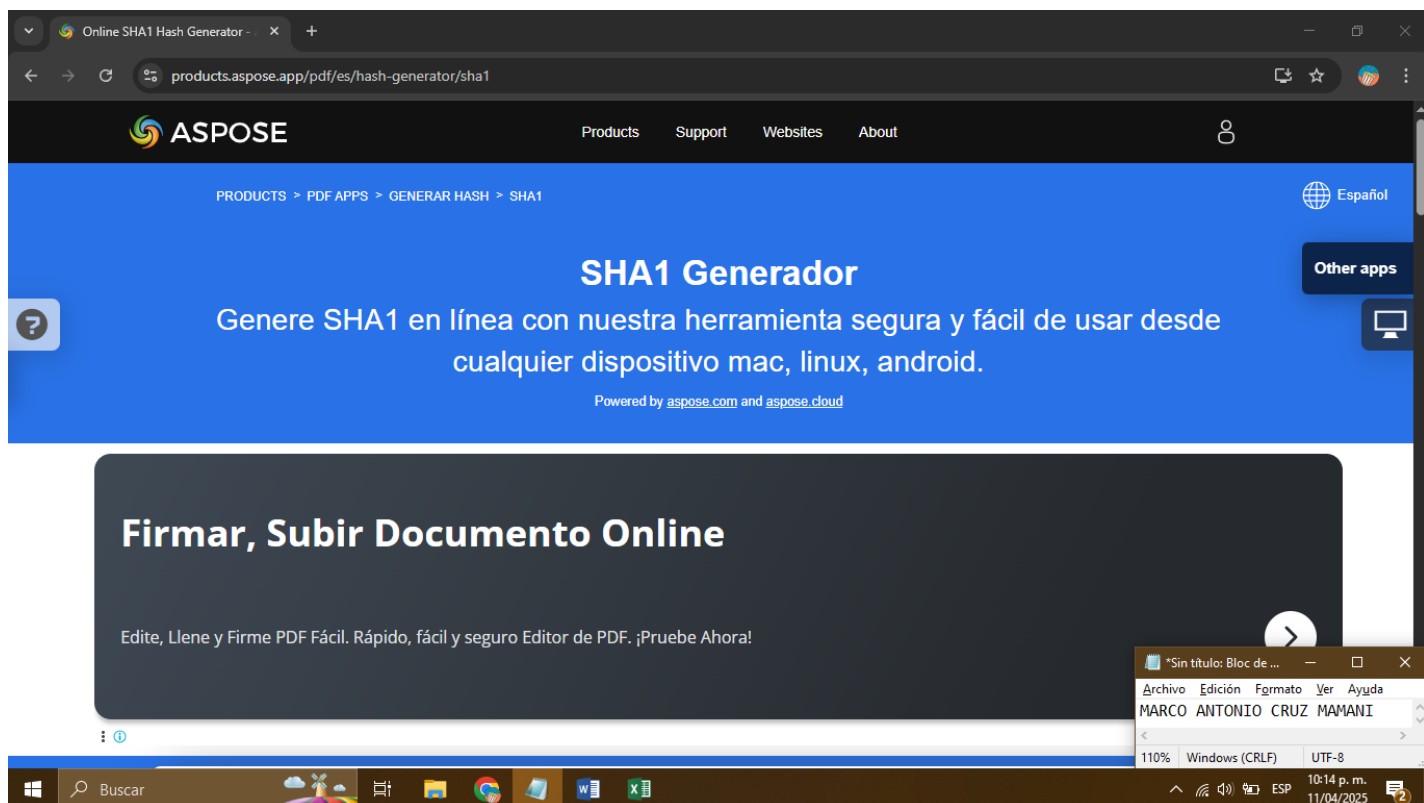
Windows File Explorer window titled "Guardar como" (Save As) showing the Desktop (Escritorio) location. The file name is "certificado\_2025" and the type is "PDF". The "Guardar" (Save) button is highlighted with a red box and a red arrow points to it.

Windows taskbar shows: Windows logo, Buscar, and system tray with date 11/04/2025.



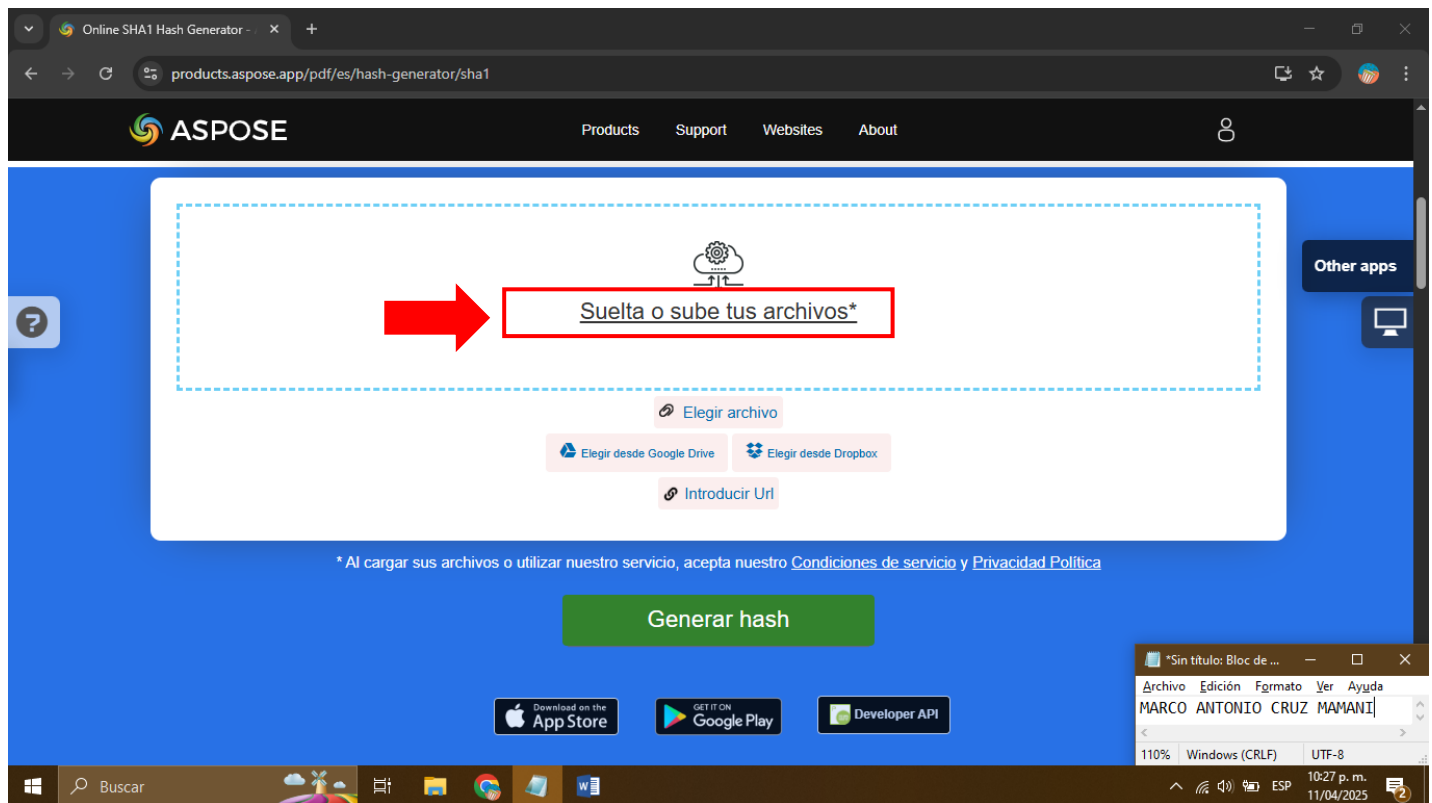
## PARTE 2: Generar el hash del archivo .pdf (certificado\_2025)

PASO 1: Entrar a la página proporcionada: <https://products.aspose.app/pdf/es/hash-generator/sha1>

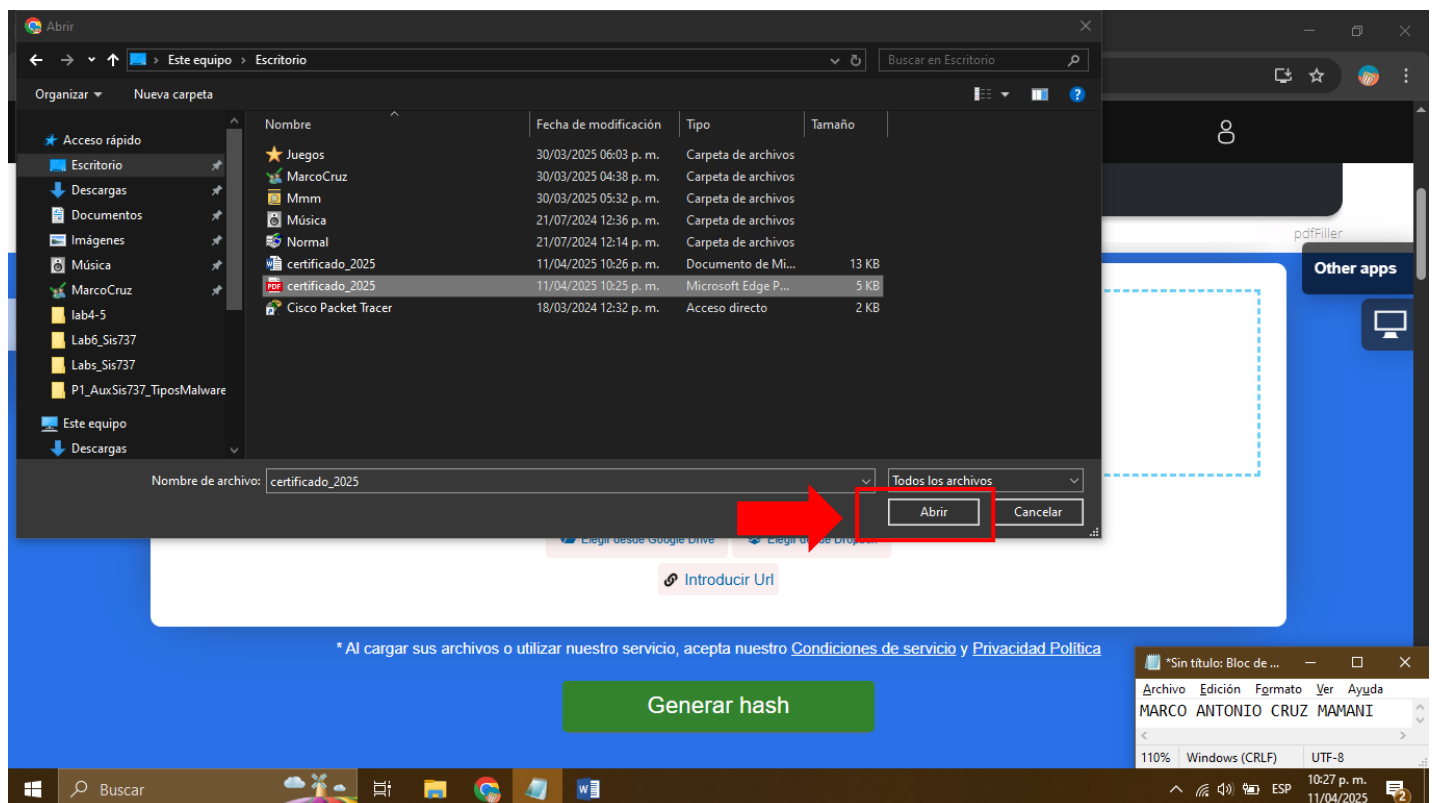


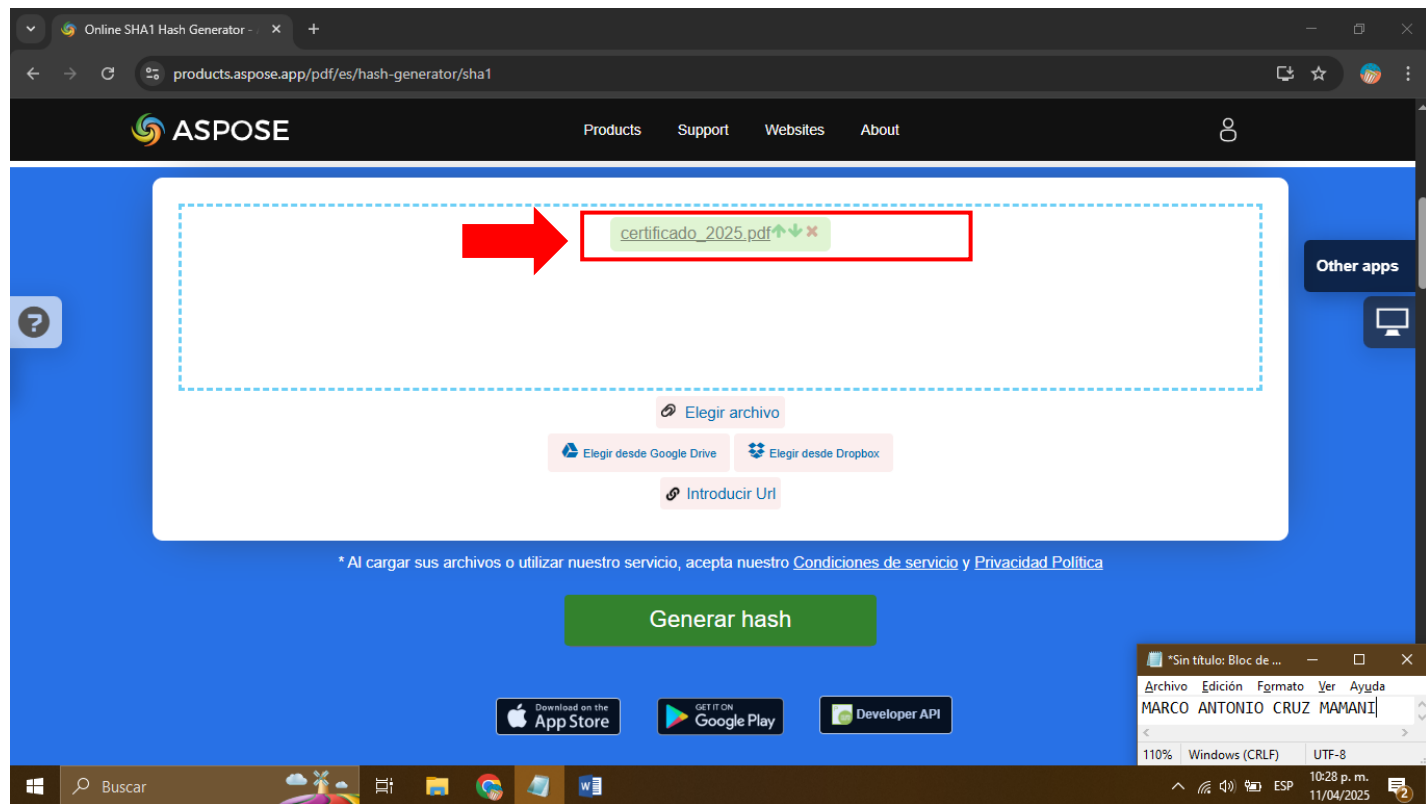


## PASO 2: Subir el archivo PDF del certificado al sitio web:

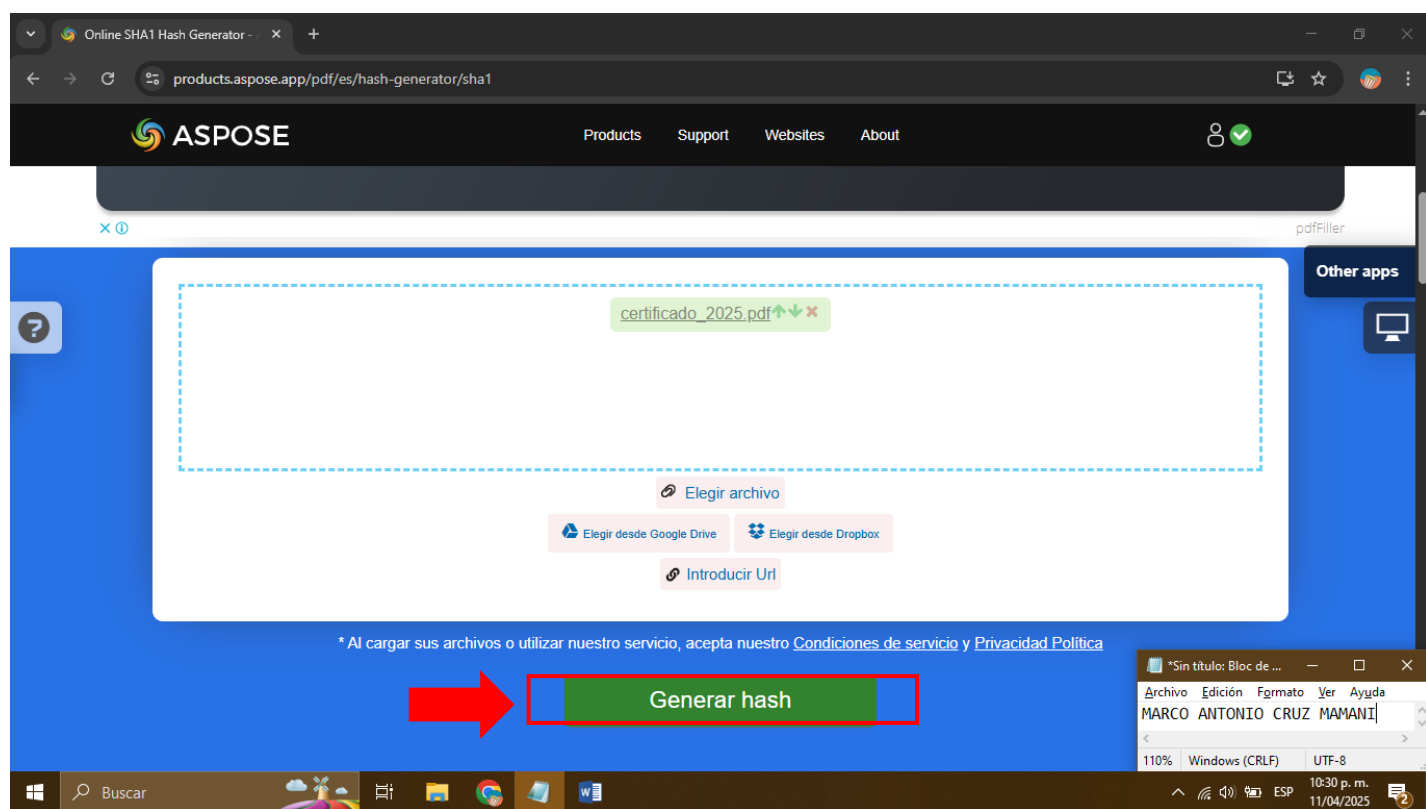


- Seleccionamos el archivo “certificado\_2025” y presionamos “Abrir”





**PASO 3: Genera el hash SHA1, presionamos “Generar hash”:**



Online SHA1 Hash Generator - x +

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

ASPOSE Products Support Websites About

El hash se ha generado correctamente

DOWNLOAD

Enviar resultado a:

Generar un hash para otros documentos Cloud API

Nombre del archivo	Picadillo
certificado_2025.pdf	DB0DF7F1F2A60A1D0160EF6828EA2D1D14E4AE8E

Copie todo Copiar

Enviar resultado a: email@domain.com

Escribe aquí tu opinión y sugerencias a las que podamos responder para los suscriptores. 1000 caracteres máximo

Enviar comentarios

Sin título: Bloc de ...

Archivo Edición Formato Ver Ayuda

MARCO ANTONIO CRUZ MAMANI

110% Windows (CRLF) UTF-8

10:31 p. m. 11/04/2025

**PASO 5: Para validar en el futuro, volver a subir el archivo del usuario al mismo sitio web y genera el hash.**

- Subimos nuevamente el mismo archivo

Online SHA1 Hash Generator - x +

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

ASPOSE Products Support Websites About

Edite, Llene y Firme PDF Fácil. Rápido, fácil y seguro Editor de PDF. ¡Pruebe Ahora!

Other apps

Suelta o sube tus archivos\*

Elegir archivo

Elegir desde Google Drive Elegir desde Dropbox

Introducir Url

\* Al cargar sus archivos o utilizar nuestro servicio, acepta nuestro [Condiciones de servicio](#) y [Privacidad Política](#)

Generar hash

Sin título: Bloc de ...

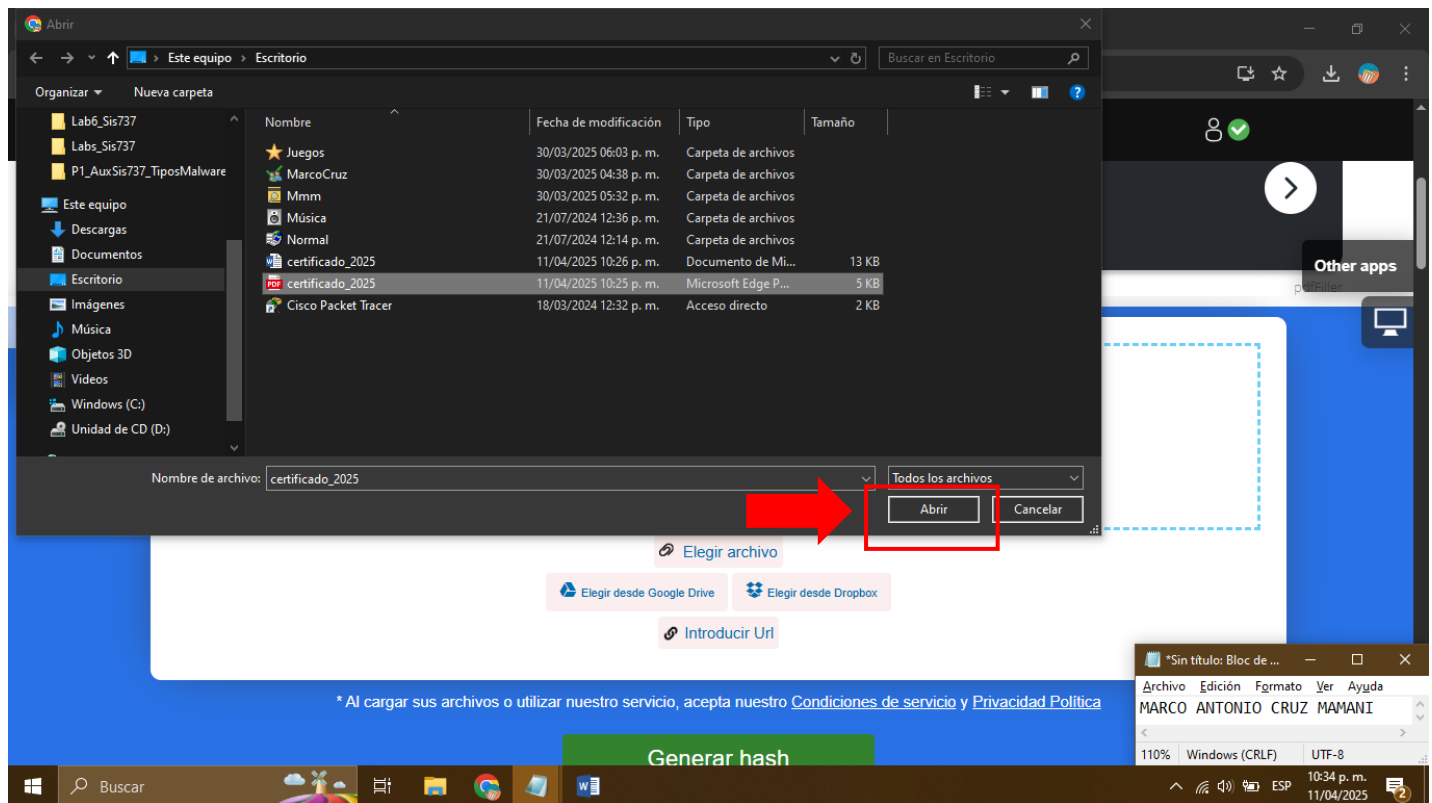
Archivo Edición Formato Ver Ayuda

MARCO ANTONIO CRUZ MAMANI

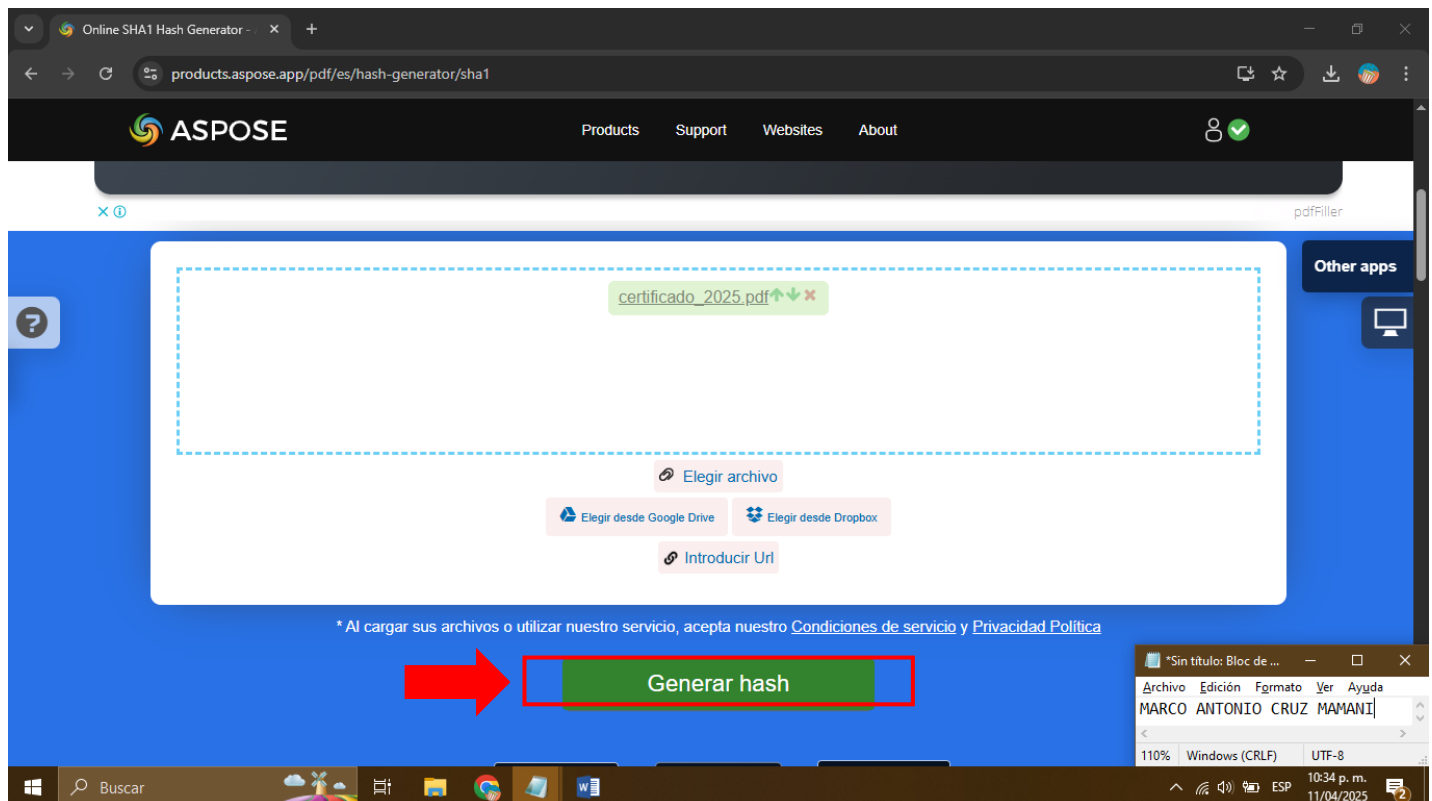
110% Windows (CRLF) UTF-8

10:34 p. m. 11/04/2025

- Seleccionamos el archivo “certificado\_2025.pdf” y presionamos “Abrir”



- Presionamos “Generar hash”, para generar el hash





Online SHA1 Hash Generator - x +

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

ASPOSE Products Support Websites About

pdfFiller

El hash se ha generado correctamente

DOWNLOAD

Enviar resultado a:

Generar un hash para otros documentos Cloud API

Nombre del archivo	Picadillo
certificado_2025.pdf	DB0DF7F1F2A60A1D0160EF6828EA2D1D14E4AE8E

Copie todo Copiar

Enviar resultado a: email@domain.com

Escribe aquí tu opinión y sugerencias a las que podemos responder para los suscriptores.

1000 caracteres máximo

Buscar

Windows (CRLF) UTF-8

10:41 p. m. 11/04/2025

**CONCLUSION:** La coincidencia del hash SHA1 original con el verificado demuestra que el certificado no ha sido alterado desde su emisión, garantizando así su autenticidad e integridad digital.

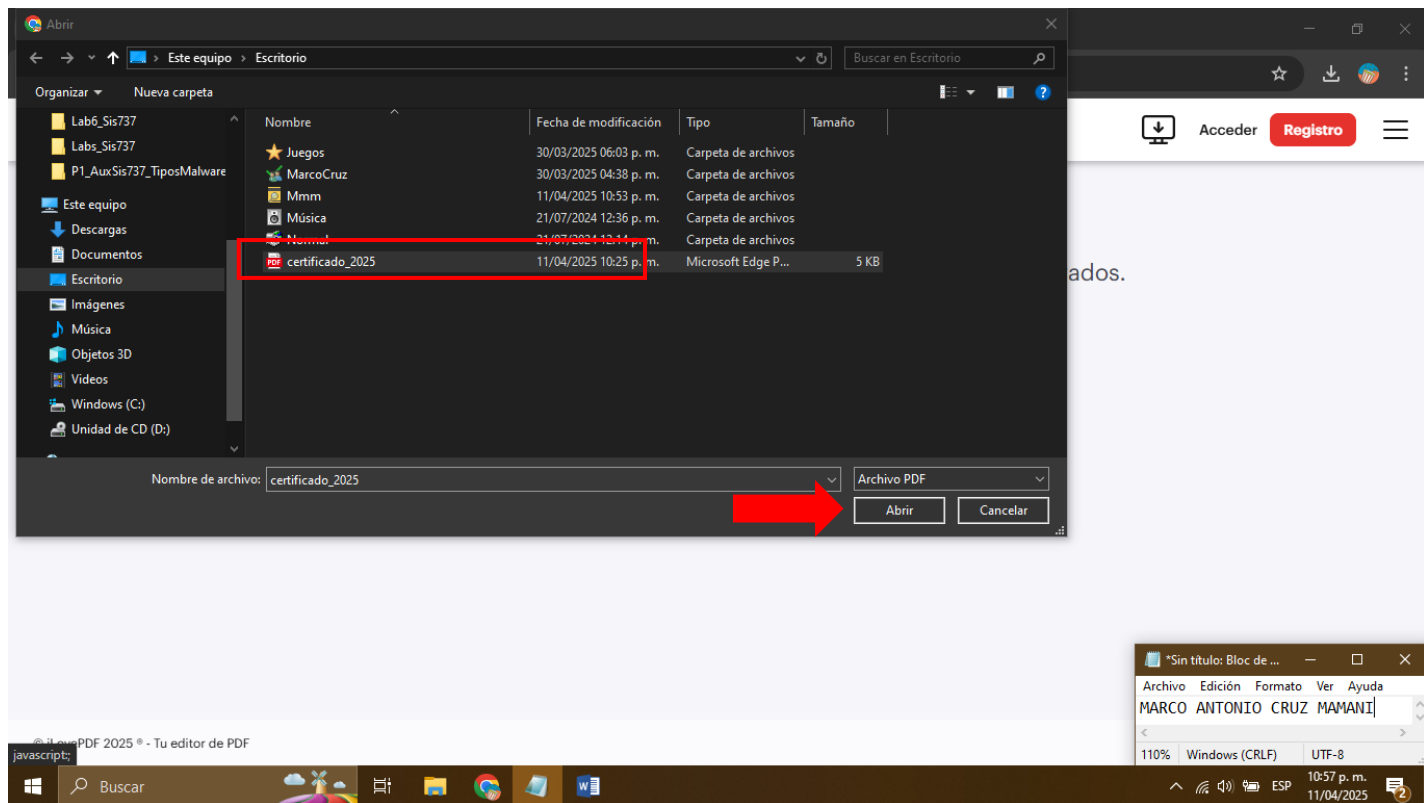
### 1.3.2. CERTIFICADO MODIFICADO

**PARTE 1:** Realizar un cambio en el PDF

**PASO 1:** Para realizar un cambio en el pdf (certificado\_2025.pdf) entramos a la siguiente página web (<https://www.ilovepdf.com/es/editar-pdf>):



**PASO 2:** presionar “seleccionar archivo PDF”, luego seleccionar el archivo (certificado\_2025.pdf) y presionar “abrir”:

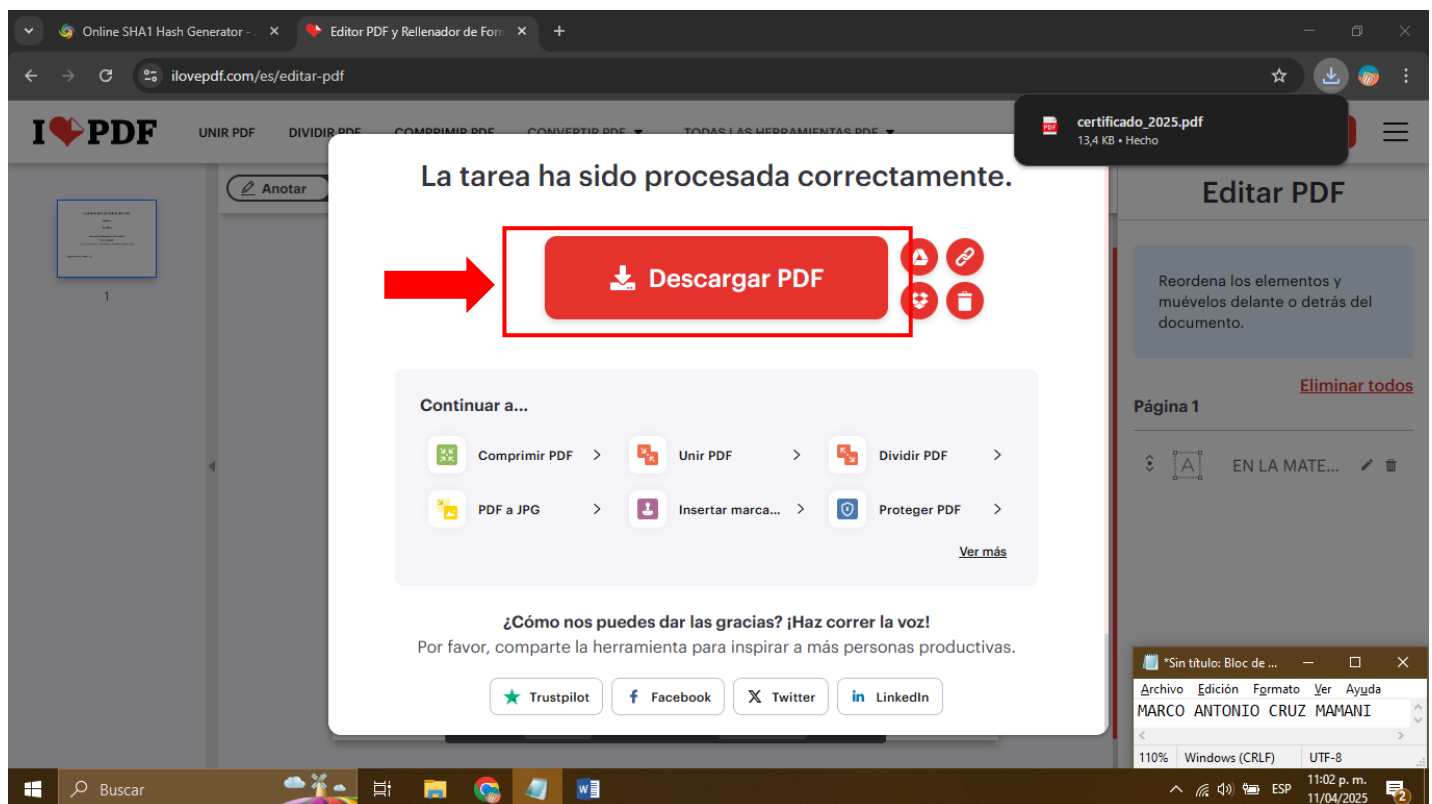
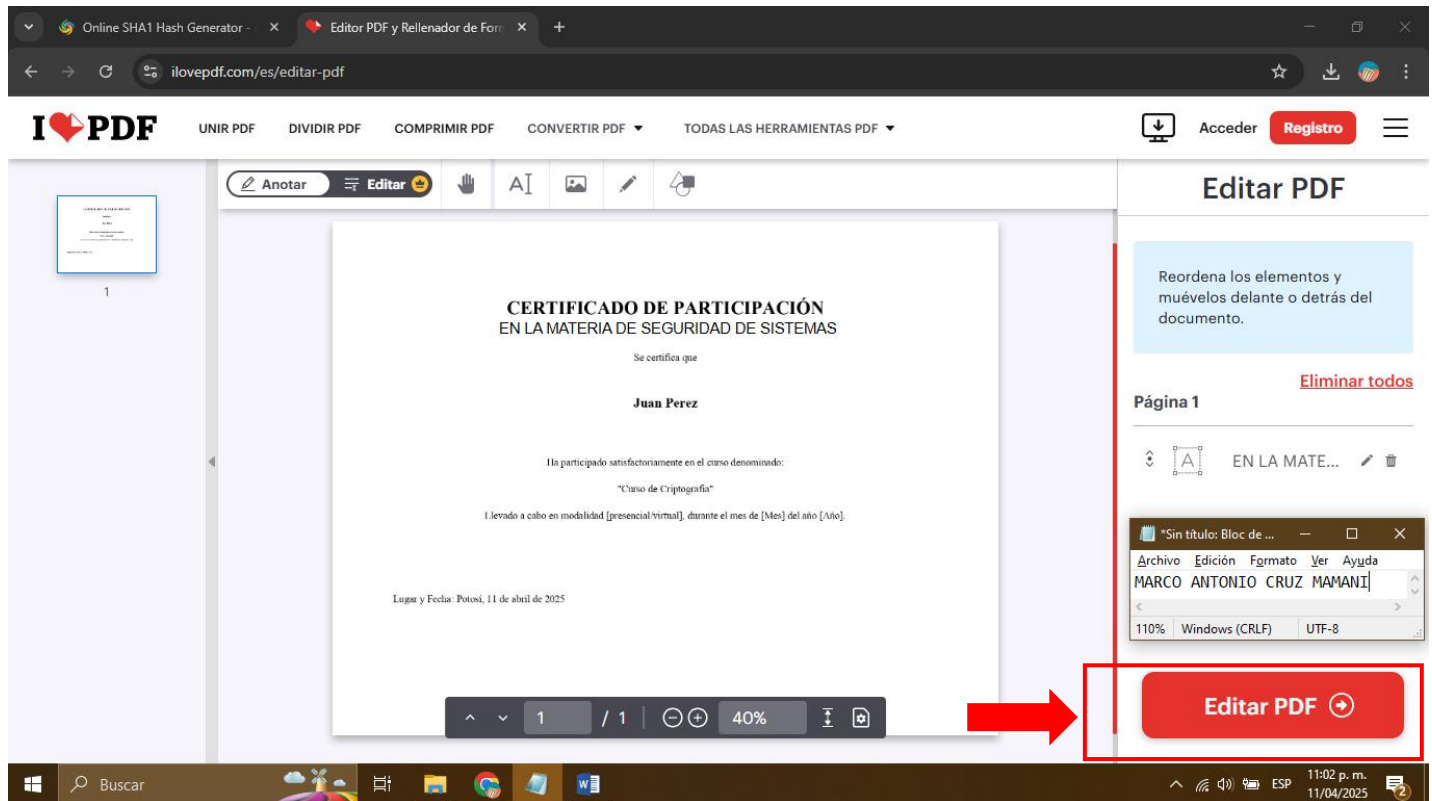


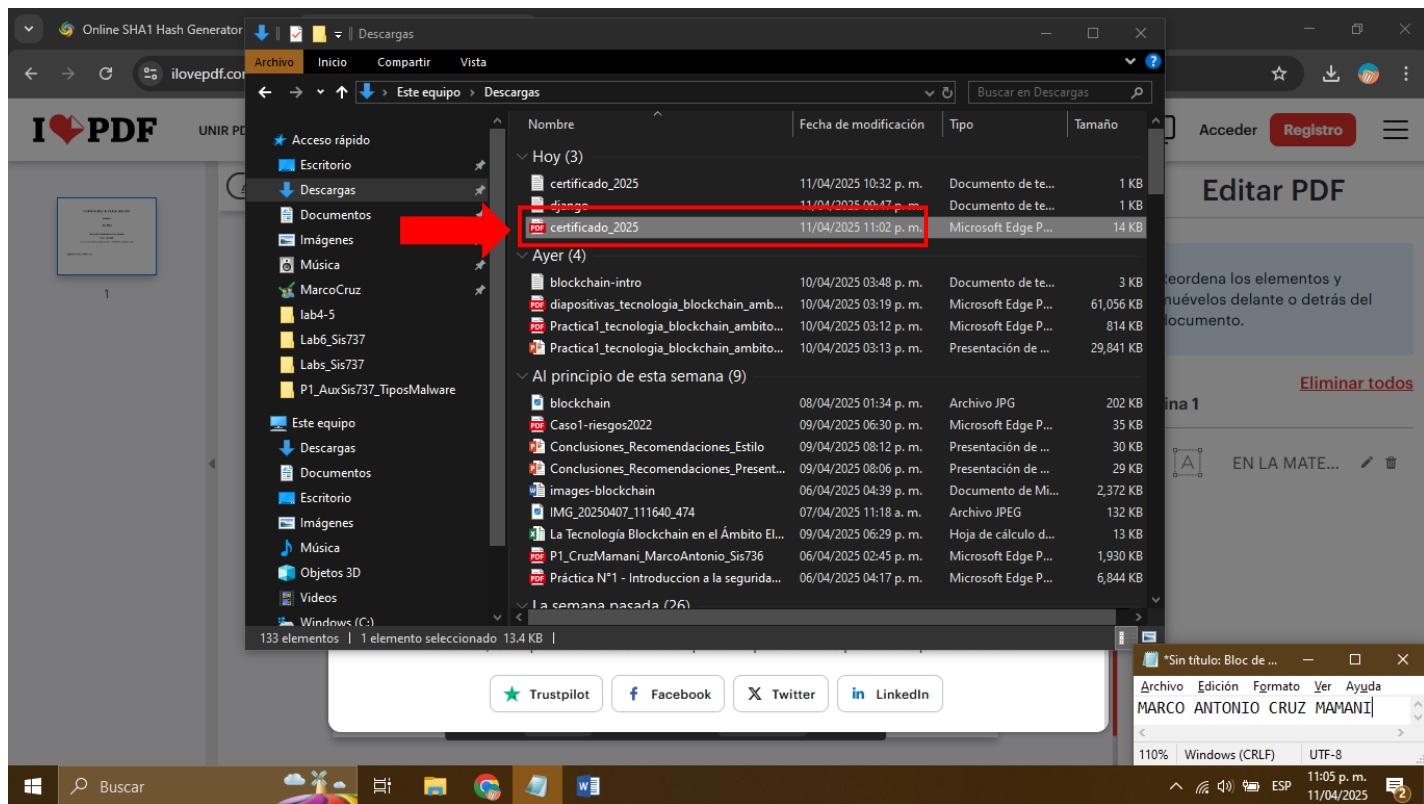
### PASO 3: Añadimos texto al pdf

The screenshot shows the I Love PDF web editor interface. The top navigation bar includes links for 'UNIR PDF', 'DIVIDIR PDF', 'COMPRESOR PDF', 'CONVERTIR PDF', and 'TODAS LAS HERRAMIENTAS PDF'. The main toolbar on the left has icons for 'Anotar', 'Añadir texto', 'Borrar', 'Dibujar', and 'Mover'. A red arrow points to the 'Añadir texto' icon, which is highlighted with a red box. The central workspace displays a PDF document titled 'CERTIFICADO DE PARTICIPACIÓN'. The document content includes: 'Se certifica que', 'Juan Perez', 'Ha participado satisfactoriamente en el curso denominado:', 'Curso de Criptografía', 'Llevado a cabo en modalidad [presencial/virtual], durante el mes de [Mes] del año [Año].', and 'Lugar y Fecha: Potosí, 11 de abril de 2025'. The right sidebar contains a text box with instructions: 'Utiliza la barra de herramientas para modificar o añadir texto, cargar imágenes o anotar de una forma fácil.' The bottom status bar shows the Windows taskbar with the search bar and various application icons.

The screenshot shows the I Love PDF web editor interface after the text 'EN LA MATERIA DE SEGURIDAD DE SISTEMAS' has been added to the certificate. The top navigation bar and main toolbar are the same. The central workspace displays the same PDF document, but with the new text added below the title 'CERTIFICADO DE PARTICIPACIÓN'. A red arrow points to the new text, which is highlighted with a red box. A green checkmark is visible on the right side of the workspace. The right sidebar contains a text box with instructions: 'Reordena los elementos y muévelos delante o detrás del documento.' Below this, there is a section for 'Página 1' with a text box containing 'EN LA MATE...' and a trash icon. The bottom status bar shows the Windows taskbar with the search bar and various application icons.

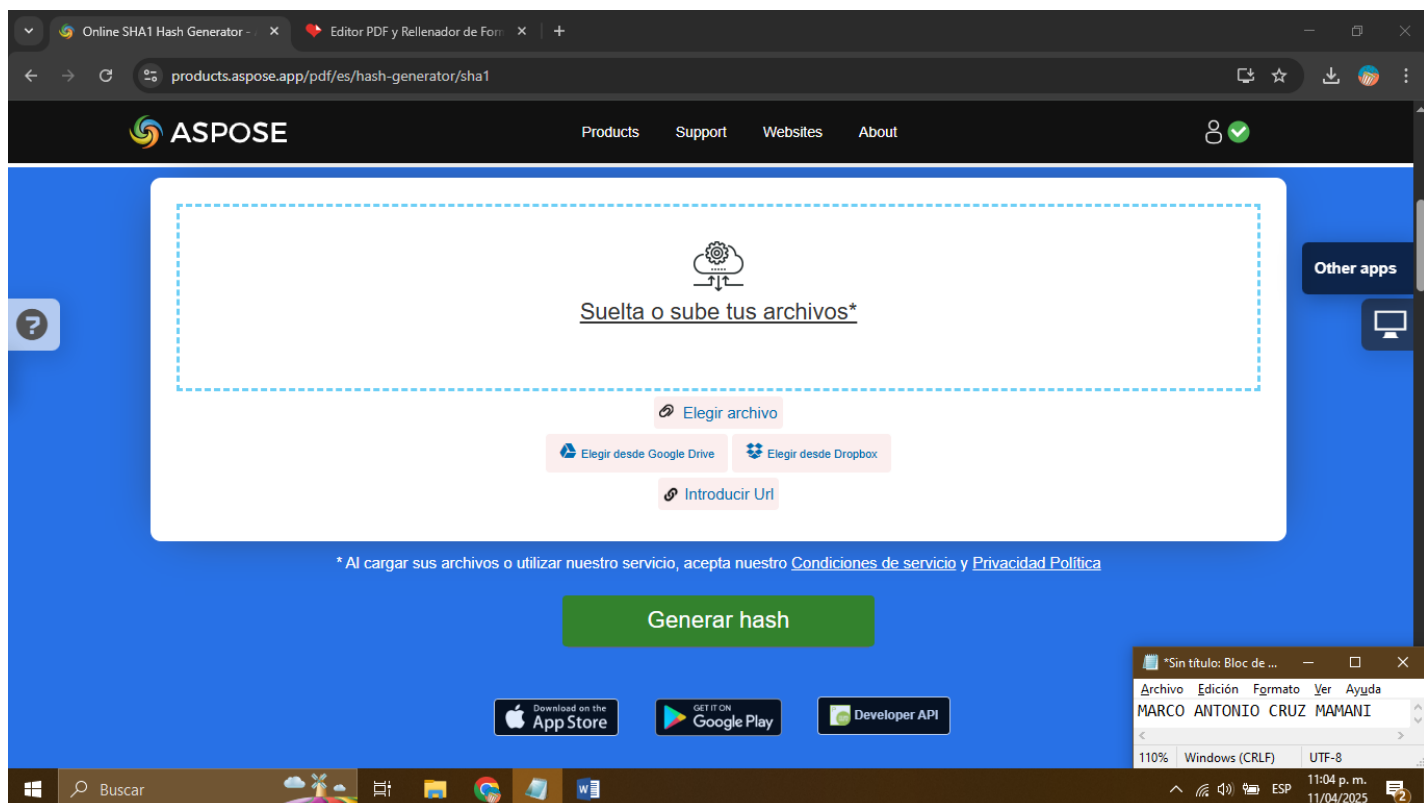
## PASO 4: confirmamos la edición y descargamos el archivo modificado presionando en “”





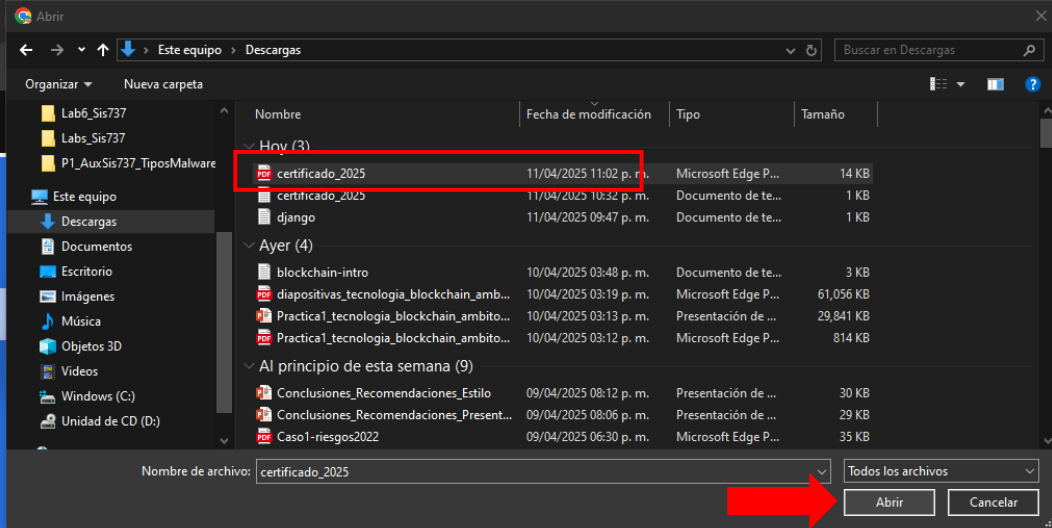
## PARTE 2: Generar un Nuevo hash del archivo modificado.

PASO 1: Entrar a la página proporcionada: <https://products.aspose.app/pdf/es/hash-generator/sha1>





## PASO 2: Subir el archivo PDF del certificado al sitio web:



Nombre de archivo: certificado\_2025

Todos los archivos

Abrir Cancelar

\* Al cargar sus archivos o utilizar nuestro servicio, acepta nuestro [Condiciones de servicio](#) y [Privacidad Política](#)

Generar hash

Download on the App Store GET IT ON Google Play Developer API

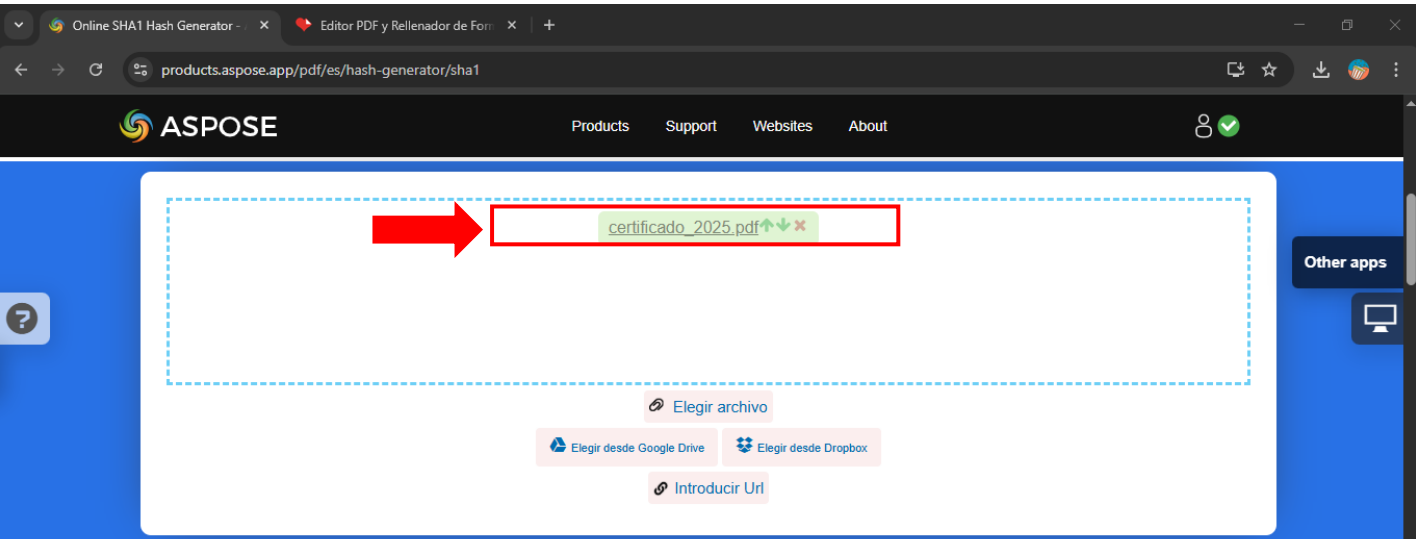
Archivos de texto: \*Sin título: Bloc de ...

Archivo Edición Formato Ver Ayuda

MARCO ANTONIO CRUZ MAMANI

110% Windows (CRLF) UTF-8

11:06 p. m. 11/04/2025



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

ASPOSE Products Support Websites About

certificado\_2025.pdf

Elegir archivo

Elegir desde Google Drive Elegir desde Dropbox

Introducir Url

\* Al cargar sus archivos o utilizar nuestro servicio, acepta nuestro [Condiciones de servicio](#) y [Privacidad Política](#)

Generar hash

Download on the App Store GET IT ON Google Play Developer API

Archivos de texto: \*Sin título: Bloc de ...

Archivo Edición Formato Ver Ayuda

MARCO ANTONIO CRUZ MAMANI

110% Windows (CRLF) UTF-8

11:06 p. m. 11/04/2025

### PASO 3: Genera el hash SHA1, presionamos "Generar hash":

Online SHA1 Hash Generator - x Editor PDF y Rellenador de Form x +

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

ASPOSE Products Support Websites About

certificado\_2025.pdf

Elegir archivo

Elegir desde Google Drive Elegir desde Dropbox

Introducir Url

\* Al cargar sus archivos o utilizar nuestro servicio, acepta nuestro [Condiciones de servicio](#) y [Privacidad Política](#)

Generar hash

Download on the App Store GET IT ON Google Play Developer API

Buscar

11:06 p. m. 11/04/2025

Online SHA1 Hash Generator - x Editor PDF y Rellenador de Form x +

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

ASPOSE Products Support Websites About

El hash se ha generado correctamente

DOWNLOAD

Enviar resultado a:

Generar un hash para otros documentos Cloud API

Nombre del archivo	Picadillo
certificado_2025.pdf	45C4D15A16F8940A56D871D689D5943537B543AD

Copie todo Copiar

Enviar resultado a: email@domain.com

Escribe aquí tu opinión y sugerencias a las que podamos responder para los suscriptores. 1000 caracteres máximo

Enviar comentarios

11:07 p. m. 11/04/2025

## PARTE 3: COMPARACION DE HASHs

### PRIMER HASH GENERADO

The screenshot shows the Aspose Online SHA1 Hash Generator interface. A red arrow points to the table containing the first hash. The table has two columns: 'Nombre del archivo' and 'Picadillo'. The row shows 'certificado\_2025.pdf' and its corresponding SHA1 hash. A green checkmark is visible on the right side of the interface.

Nombre del archivo	Picadillo
certificado_2025.pdf	DB0DF7F1F2A60A1D0160EF6828EA2D1D14E4AE8E

### ULTIMO HASH GENERADO (con archivo modificado)

The screenshot shows the Aspose Online SHA1 Hash Generator interface after the file has been modified. A red arrow points to the table containing the new hash. The table has two columns: 'Nombre del archivo' and 'Picadillo'. The row shows 'certificado\_2025.pdf' and its new SHA1 hash.

Nombre del archivo	Picadillo
certificado_2025.pdf	45C4D15A16F8940A56D871D689D5943537B543AD

**CONCLUSION:** *La diferencia entre el hash original y el nuevo indica que el archivo fue modificado, lo cual invalida el certificado y evidencia que su contenido ya no es confiable.*

