AUDITORIA Y SEGURIDAD INFORMATICA

RECUPERACION DE INFORMACION

Realizado por: Luis Carlos Arevalo Ocampo

Docente: Ing. Dr. Carlos Enrique López Rodríguez

TARAPOTO - PERU

Para iniciar el proceso de recuperación de información, utilicé una máquina virtual con el sistema operativo Linux. Además, implementé dos herramientas de Kali Linux: ExifTool y DiffPDF, para analizar los metadatos y comparar las modificaciones de los archivos.

ExifTool

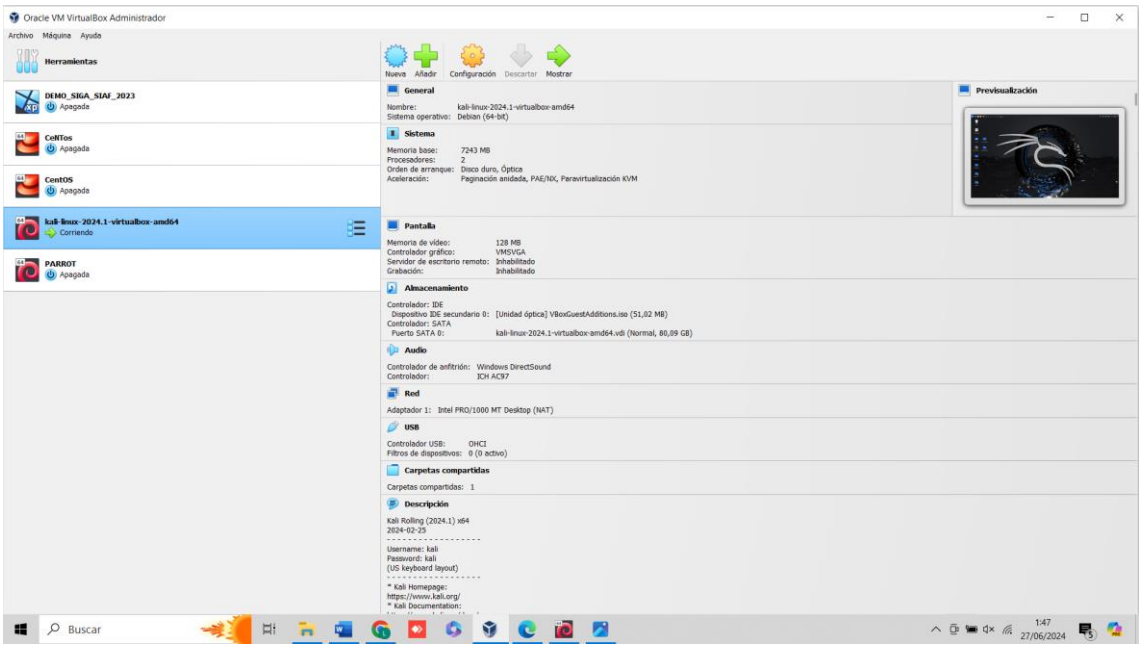
ExifTool es una poderosa herramienta de línea de comandos utilizada para leer, escribir y editar metadatos en archivos de imagen, audio, video y otros formatos. Desarrollada por Phil Harvey, ExifTool es capaz de extraer información detallada como la fecha de creación, ajustes de la cámara, software utilizado y muchos otros datos embebidos en los archivos. Esta herramienta es especialmente útil en el análisis forense digital y la recuperación de datos, ya que permite obtener información valiosa sobre el historial y las características de un archivo.

DiffPDF

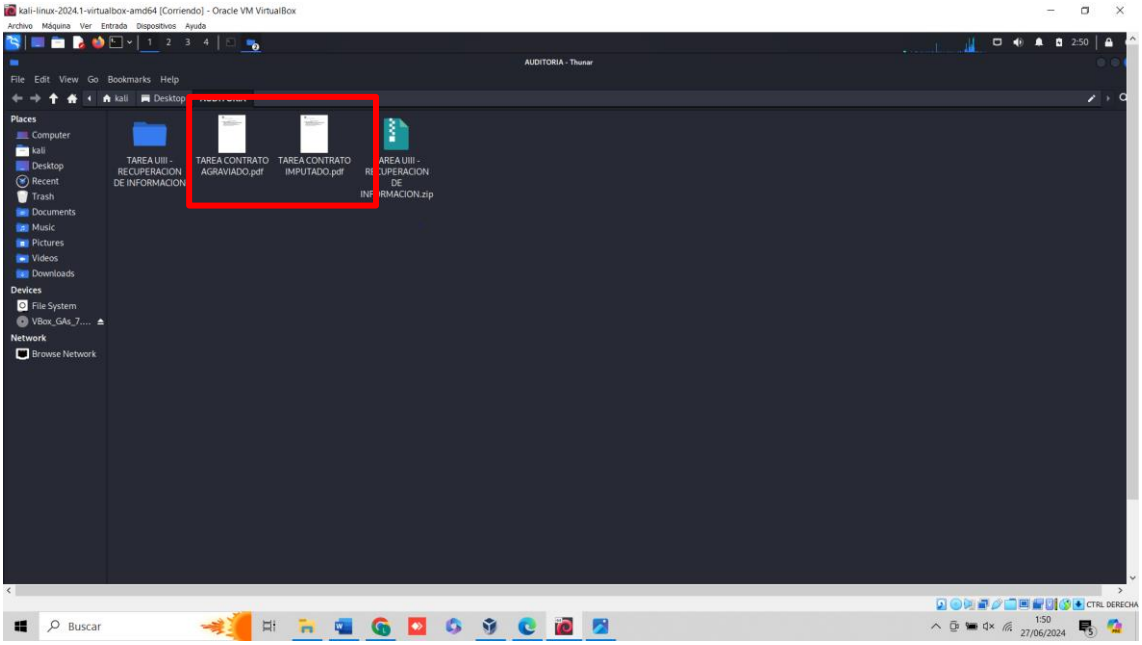
DiffPDF es una herramienta gráfica diseñada para comparar visualmente archivos PDF. Permite identificar las diferencias entre dos documentos en términos de texto, apariencia y estructura. DiffPDF resalta las modificaciones realizadas entre las versiones de un archivo, facilitando la revisión de cambios y actualizaciones. Esta herramienta es esencial para verificar la integridad de documentos y asegurar que no se han realizado alteraciones no autorizadas.

Pasos para la recuperación de la información

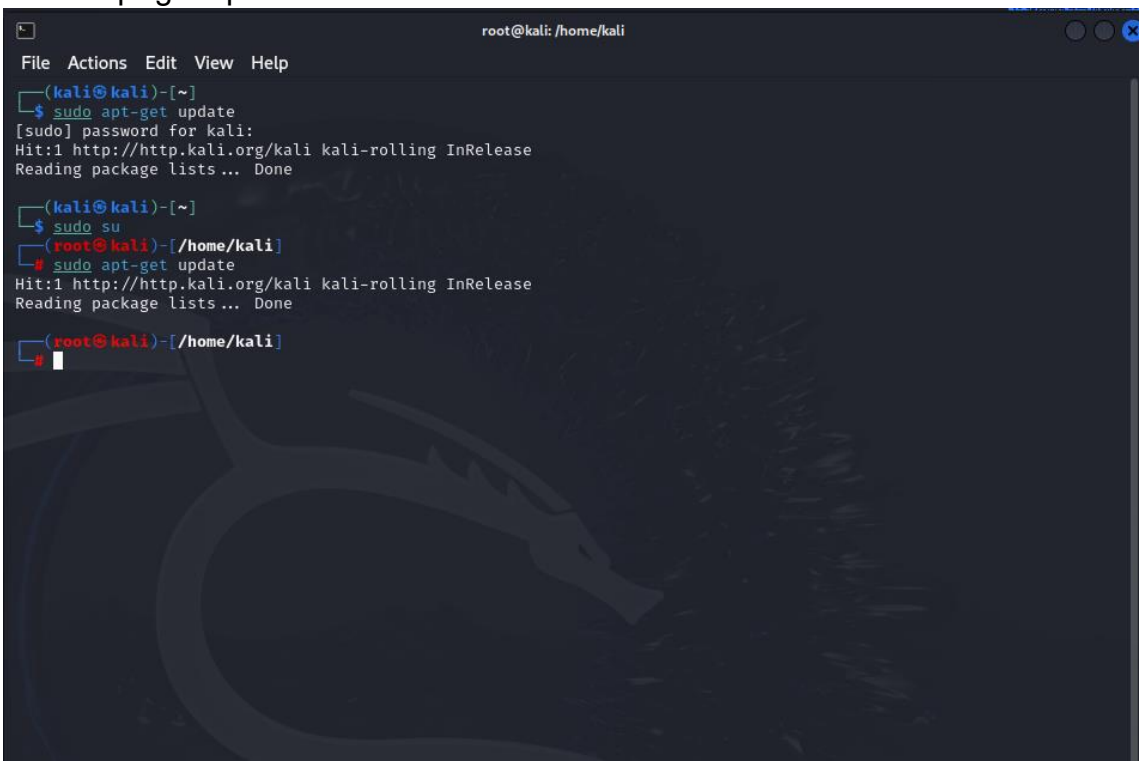
1. Inicia la máquina virtual y abre Kali Linux.



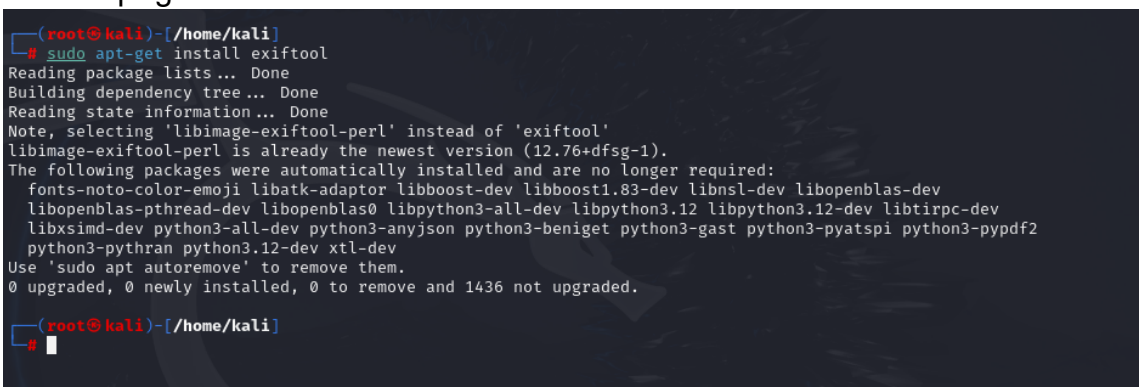
2. Una vez estando en el Kali Linux. Creamos una carpeta donde se almacenará los dos documentos que se revisara, en este caso estarán en una carpeta llamada “AUDITORIA”



3. Antes de instalar cualquier paquete, es una buena práctica asegurar de que EL sistema este actualizado. Abre una terminal y ejecuta el siguiente comando:
- sudo apt-get update

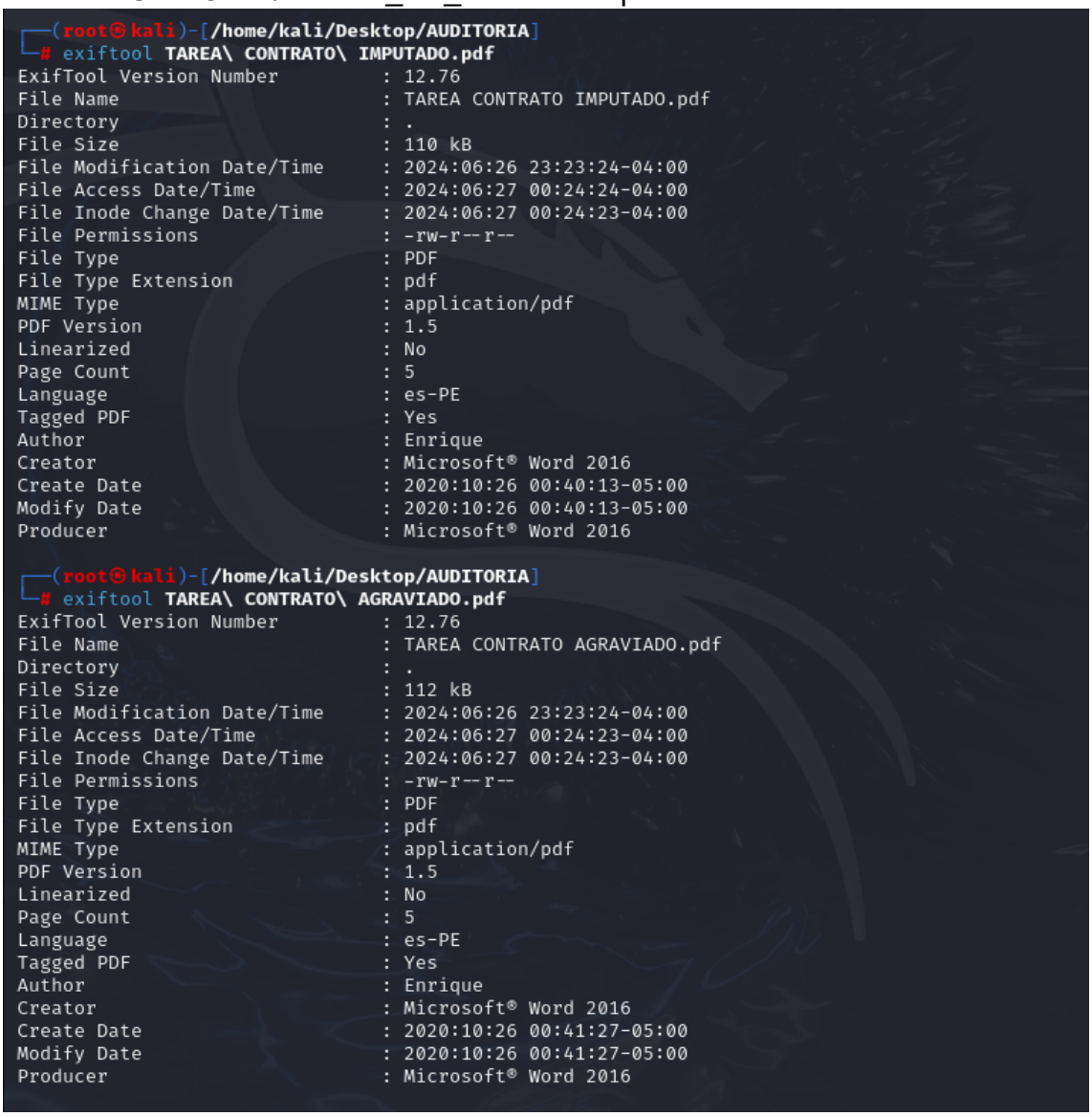


4. Dentro de Kali Linux, abre el terminal y procede a instalar la primera herramienta, "ExifTool". Se ejecuta el siguiente comando en la terminal:
- sudo apt-get install exiftool



5. Para extraer metadatos de los documentos en PDF, primero ingresaremos a la carpeta donde se encuentran los documentos.

6. Ahora, aplica el siguiente comando para extraer los metadatos de los documentos en PDF utilizando ExifTool:
exiftool AUDITORIA/nombre_del_documento.pdf



7. Análisis de los resultados obtenidos

7.1. Fecha de creación (Create Date):

- **TAREA CONTRATO IMPUTADO.pdf**: 2020:10:26 00:40:13-05:00
- **TAREA CONTRATO AGRAVIADO.pdf**: 2020:10:26 00:41:27-05:00

La fecha de creación del documento "TAREA CONTRATO IMPUTADO.pdf" es anterior a la de "TAREA CONTRATO AGRAVIADO.pdf". Esto significa que “TAREA CONTRATO IMPUTADO.pdf" fue creado primero.

7.2. Tamaño del archivo (File Size):

- **TAREA CONTRATO IMPUTADO.pdf**: 110 kB
- **TAREA CONTRATO AGRAVIADO.pdf**: 112 kB

Aunque el tamaño del archivo de "TAREA CONTRATO IMPUTADO.pdf" es ligeramente menor, esto no es un factor decisivo para determinar cuál es el original.

7.3. Fecha de modificación (Modify Date):

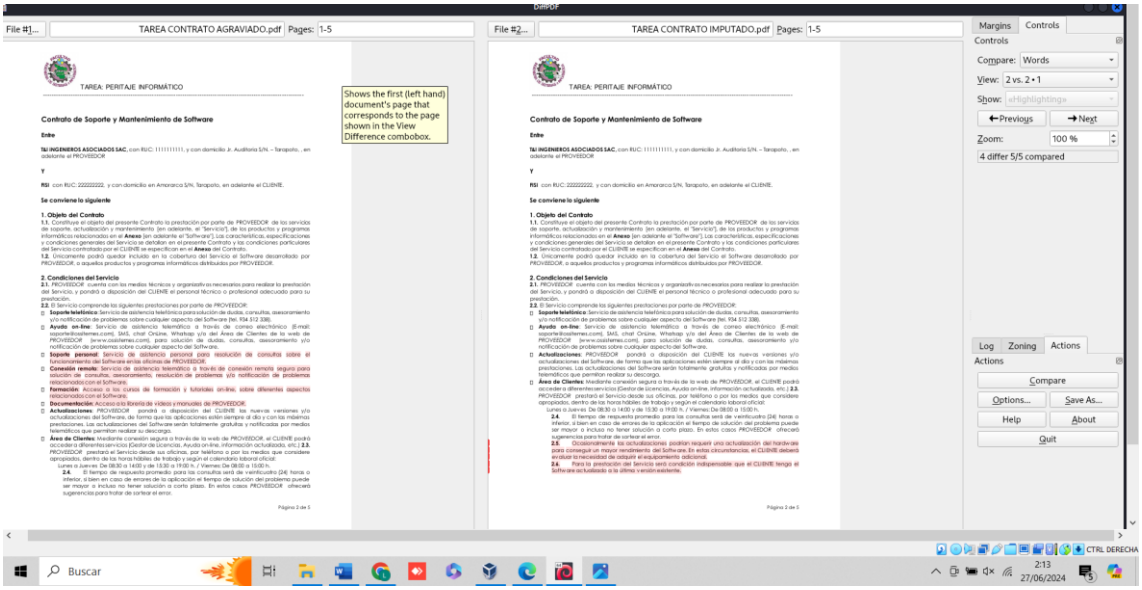
- Ambas fechas de modificación coinciden con sus respectivas fechas de creación, lo cual indica que no ha habido modificaciones posteriores desde su creación.

7.4. Conclusión

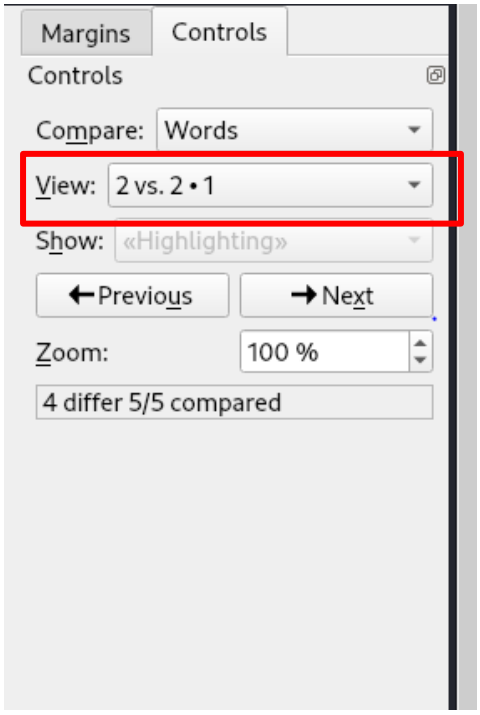
Basándonos en la fecha de creación, el documento "TAREA CONTRATO IMPUTADO.pdf" podemos decir que es el documento original, ya que fue creado primero. La diferencia en el tamaño del archivo es mínima y no influye significativamente en la determinación de la originalidad del documento.

8. Ahora, vamos a comparar los documentos utilizando la herramienta DiffPDF. Para ello, primero instalaremos la herramienta desde el terminal de Linux utilizando el siguiente comando:
   - sudo apt-get install diffpdf

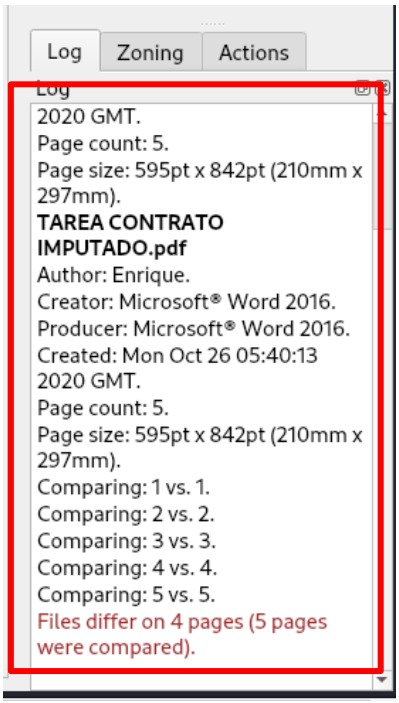
9. Para comparar dos archivos PDF, usa el siguiente comando, reemplazando archivo1.pdf y archivo2.pdf con los nombres de los archivos que deseas comparar. Luego se abrirá una interfaz grafica donde podremos ver las diferencias entre los dos archivos PDF.



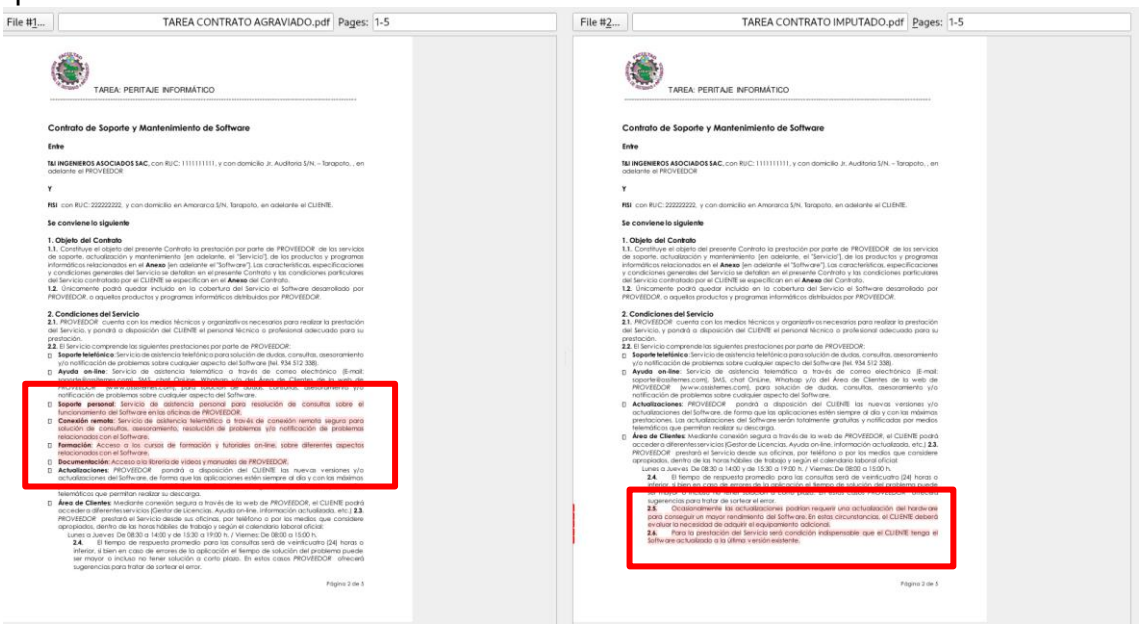
10. En la parte derecha de la interfaz, puedes observar las comparaciones que se están realizando página por página. DiffPDF resalta las diferencias encontradas en el contenido, permitiéndote identificar rápidamente las modificaciones entre los dos documentos.

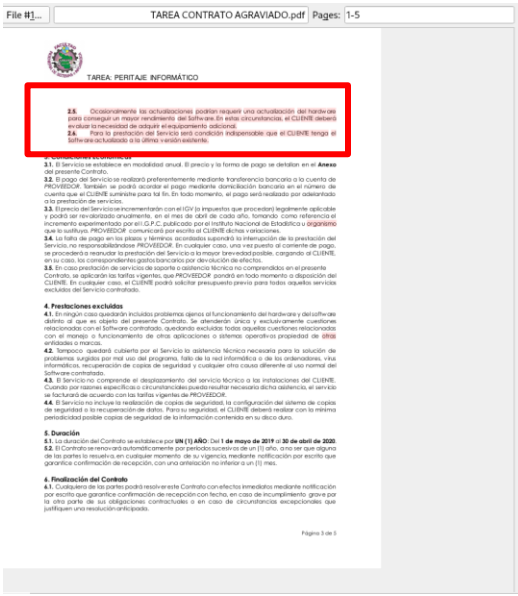


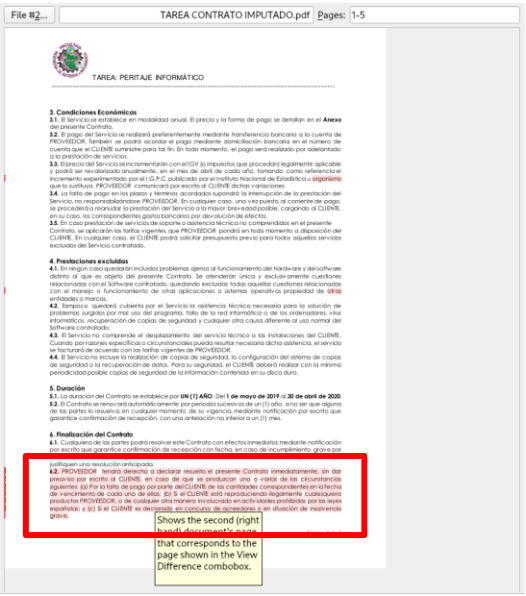
11. Además, esta herramienta también te ayuda a ver y comparar los metadatos. En la parte inferior derecha, puedes ver los metadatos de ambos archivos, como el usuario, la fecha de creación, las páginas del documento, entre otros. Esto te proporciona una visión completa de las diferencias no solo en el contenido, sino también en los atributos del archivo.

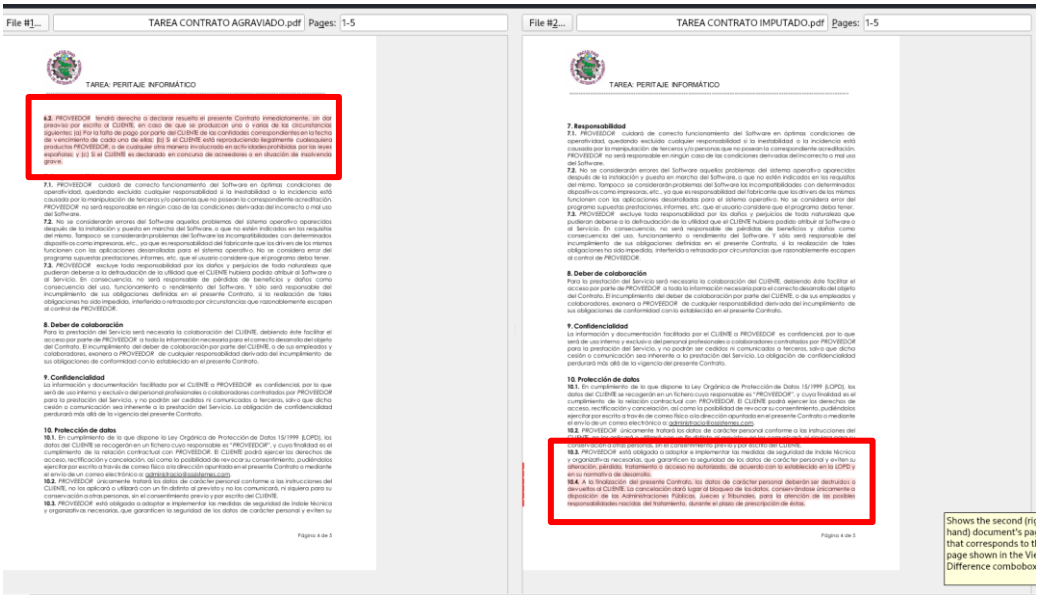


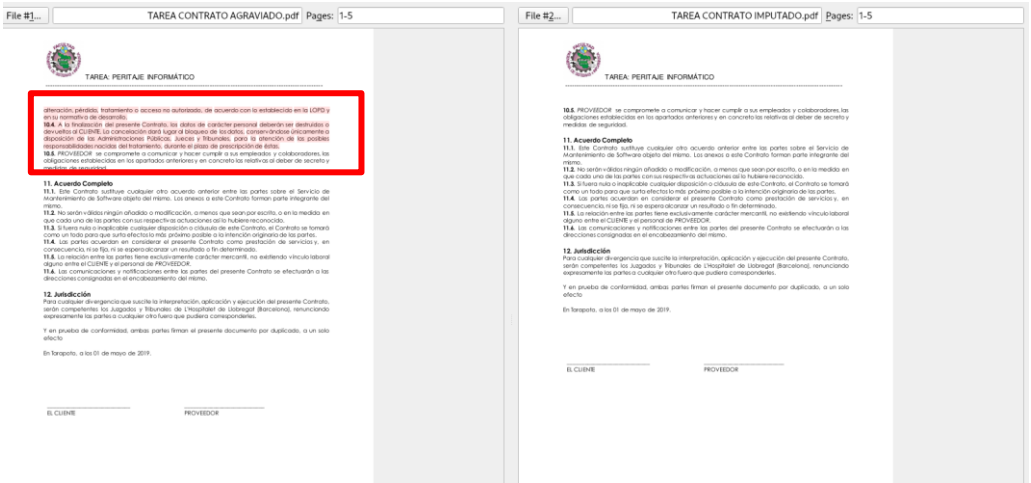
12. Ahora, se mostrarán las modificaciones que se hicieron en cada documento, página por página. DiffPDF te permite navegar por cada página y visualizar claramente las diferencias, ayudándote a identificar qué cambios se realizaron en cada sección del documento.




File #1...
TAREA CONTRATO AGRAVIADO.pdf
Pages: 1-5
TAREA: PERITAJE INFORMÁTICO


File #2...
TAREA CONTRATO IMPUTADO.pdf
Pages: 1-5
TAREA: PERITAJE INFORMÁTICO
Shows the second (right hand) document's page that corresponds to the page shown in the View Difference combobox.


File #1...
TAREA CONTRATO AGRAVIADO.pdf
Pages: 1-5
TAREA: PERITAJE INFORMÁTICO
File #2...
TAREA CONTRATO IMPUTADO.pdf
Pages: 1-5
TAREA: PERITAJE INFORMÁTICO
Shows the second (right hand) document's page that corresponds to the page shown in the View Difference combobox.


File #1...
TAREA CONTRATO AGRAVIADO.pdf
Pages: 1-5
TAREA: PERITAJE INFORMÁTICO
File #2...
TAREA CONTRATO IMPUTADO.pdf
Pages: 1-5
TAREA: PERITAJE INFORMÁTICO