ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERIA EN SISTEMAS

DISEÑO Y PROTOTIPO DE UN SISTEMA DE AUDITORIA Y CONTROL ELECTORAL PARA LOS PROCESO DE ESCRUTINIOS Y PUBLICACIONES DE RESULTADOS BASADOS EN DLT

DISEÑO E IMPLEMENTACION DEL PROTOTIPO DEL SISTEMA DE ARCHIVOS DESCENTRALIZADO

Autor: Andrés Armendáriz

Tutor: Dr. Enrique Mafla

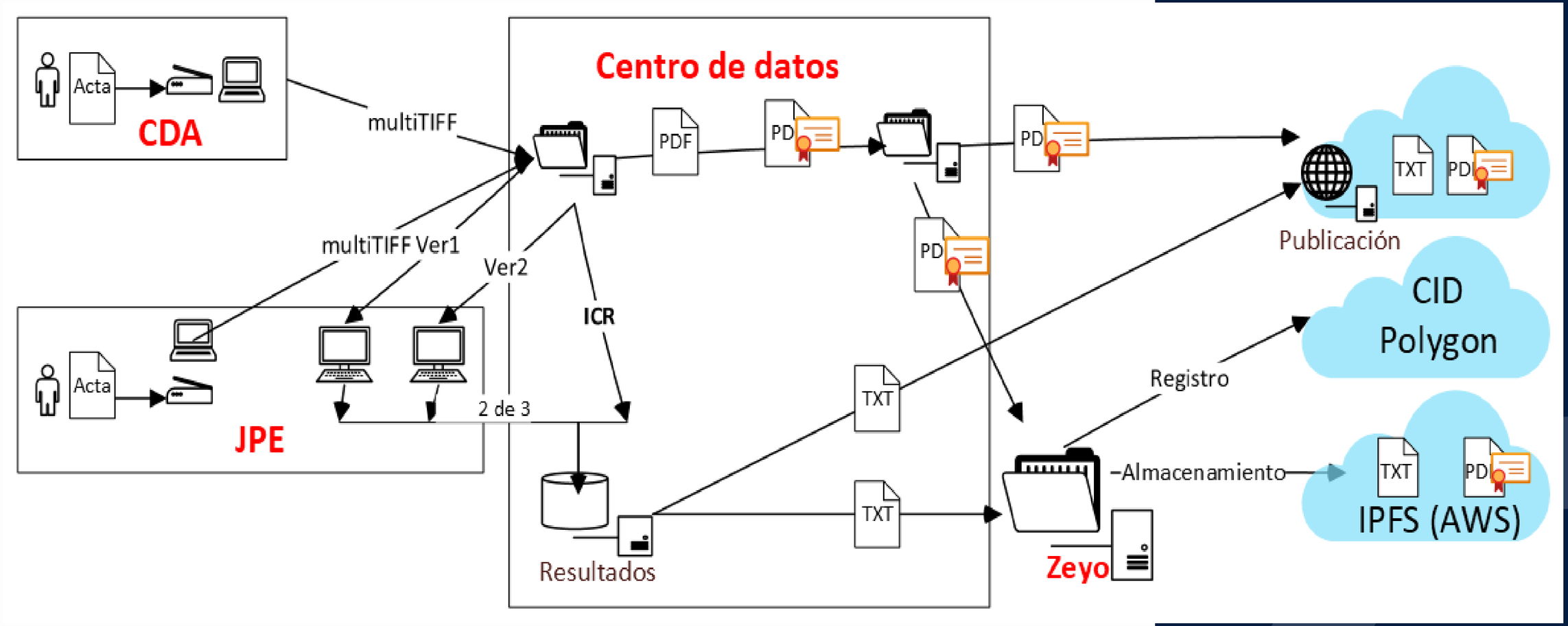
Objetivo General

Demostrar la posibilidad de mejorar la integridad y disponibilidad de los documentos y resultados electorales, mediante el uso de sistemas de archivos descentralizados.

Objetivos Específicos

1. Realizar un diagnóstico del sistema electoral vigente para conocer el estado de situación actual, permitiendo identificar las debilidades del sistema.
2. Diseñar la arquitectura del sistema de archivos descentralizado basado en el protocolo de red *Interplanetary File System*
3. Desarrollar un prototipo de almacenamiento descentralizado para el almacenamiento de actas escrutadas

Análisis de la Situation Actual



Truncamiento de Datos

```
Tamaño del archivo: 786432 bytes
Primeras 3 líneas del archivo:
11|1|0|260|285|1|1|F|35001|002017020|1517|265|5|26|22
11|1|0|260|285|1|1|F|35001|004035|1516|265|5|26|74
11|1|0|260|285|1|1|F|35001|005|207|265|5|26|50
Últimas 3 líneas del archivo:
11|1|0|955|2725|1|3|M|36945|008023|1525|178|2|9|10
11|1|0|955|2725|1|3|M|36945|016|208|178|2|9|0
11|1|0|955|2725|1|3|M|369aaioet@DESKTOP-QAR91PT:~/ioet/IPFS$
```

Candidato	Partido	Nombre del Candidato
005	207	Gonzáles Alcívar Luisa Magdalena
016	208	Armijos Velasco Bolívar Abdon
025	18	Villavicencio Valencia Fernando Alcibíades
033	226	Hervás Mora Marcelo Xavier
004035	1516	Noboa Azin Daniel Roy-Gilchrist
008023	1525	Sonnenholzner Sper Otto Ramon
002017020	1517	Pérez Guartambel Yaku Sacha
006003001	1543	Tópic Feraud Jan Tomislav

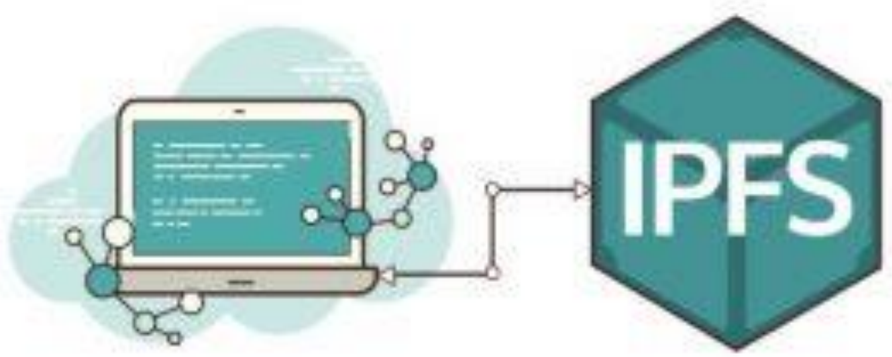
Dignidad
Provincia
Circunscripci
Cantón
Parroquia
Zona
JRV
Sexo
Acta
Candidato
Partido
Sufragantes
Blancos
nulos
Votos

Diseño

¿Qué es IPFS?

¿Como funciona?

¿Cuales son las ventajas?



Multibase

Prefix	Name
b	base32

Version

Name
cidv1

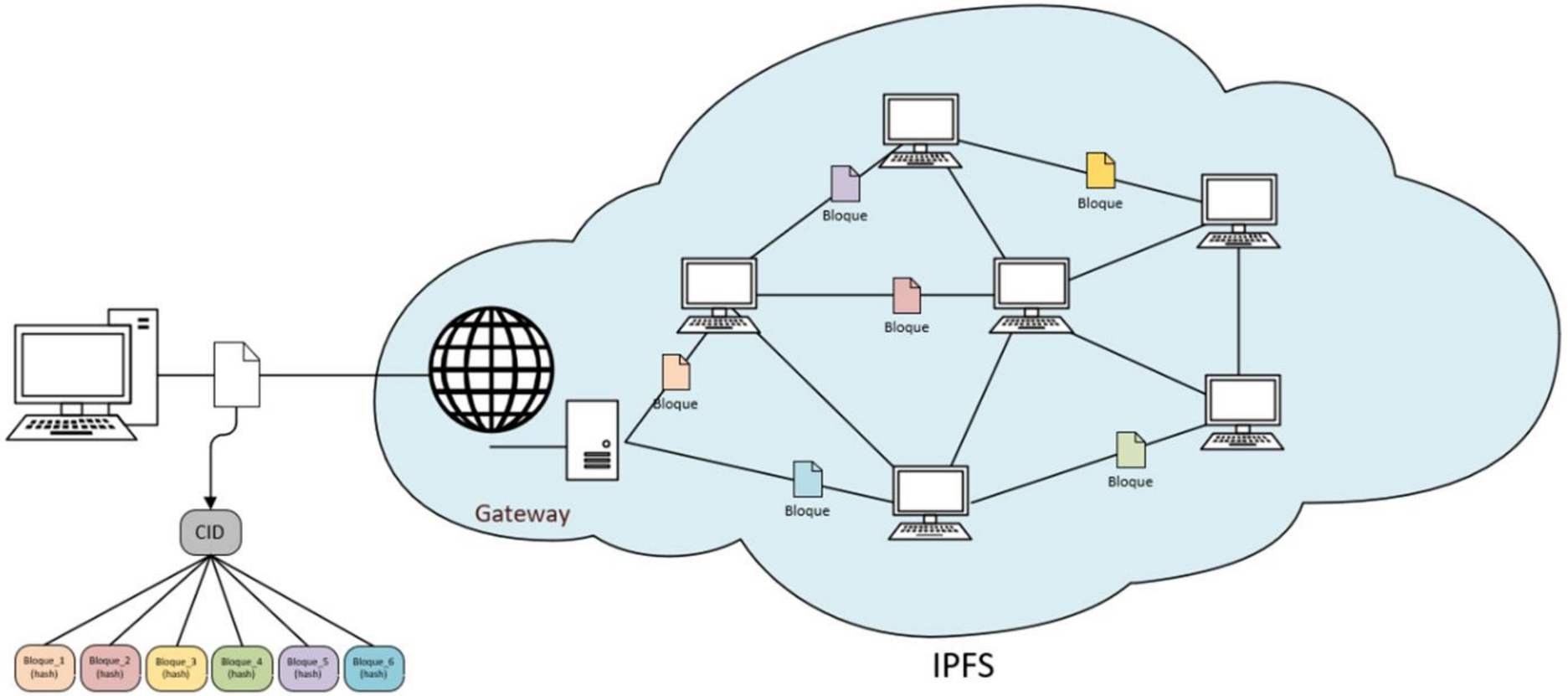
Multicodec

Code	Name	Description
0x71	dag-pb	MerkleDAG protobuf

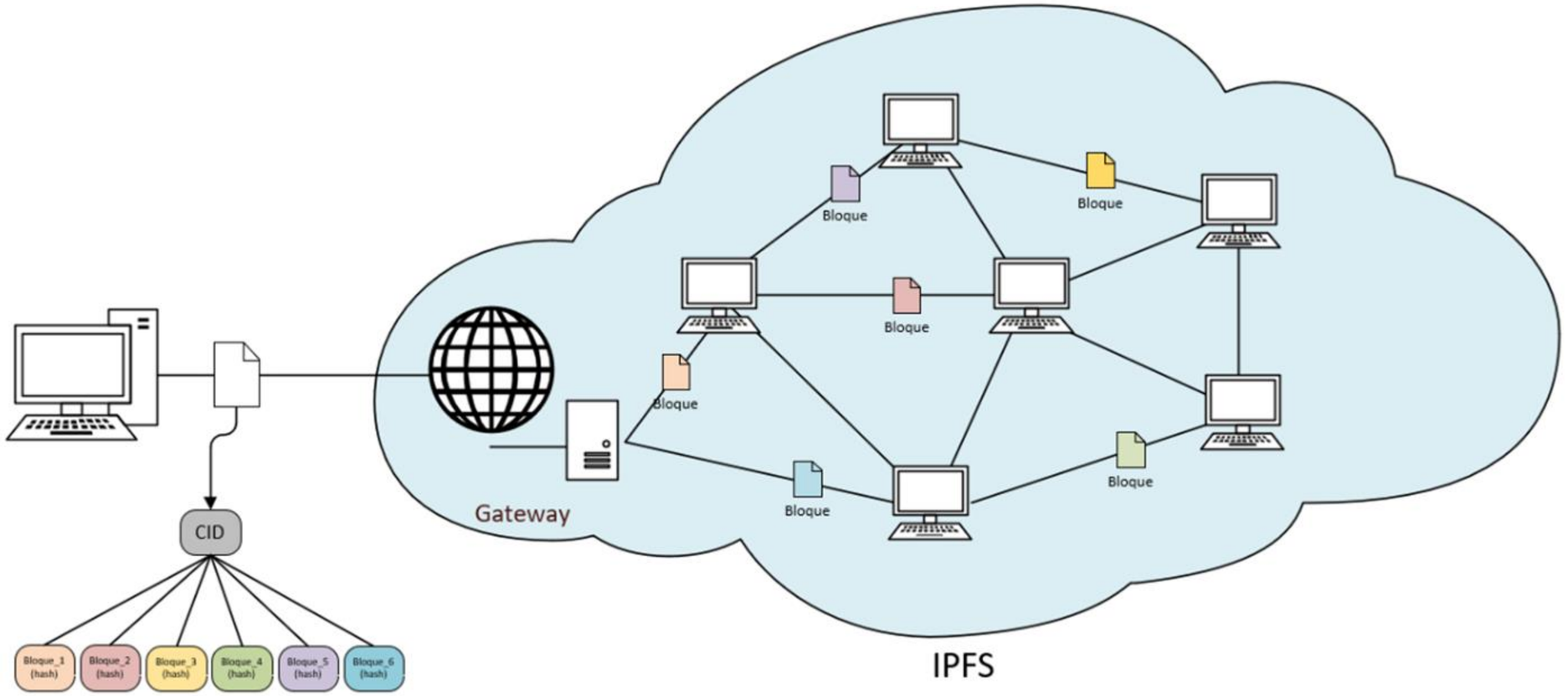
Multihash

Code	Name	Bits	Hash Value
0x12	sha2-256	256	zQmWA...

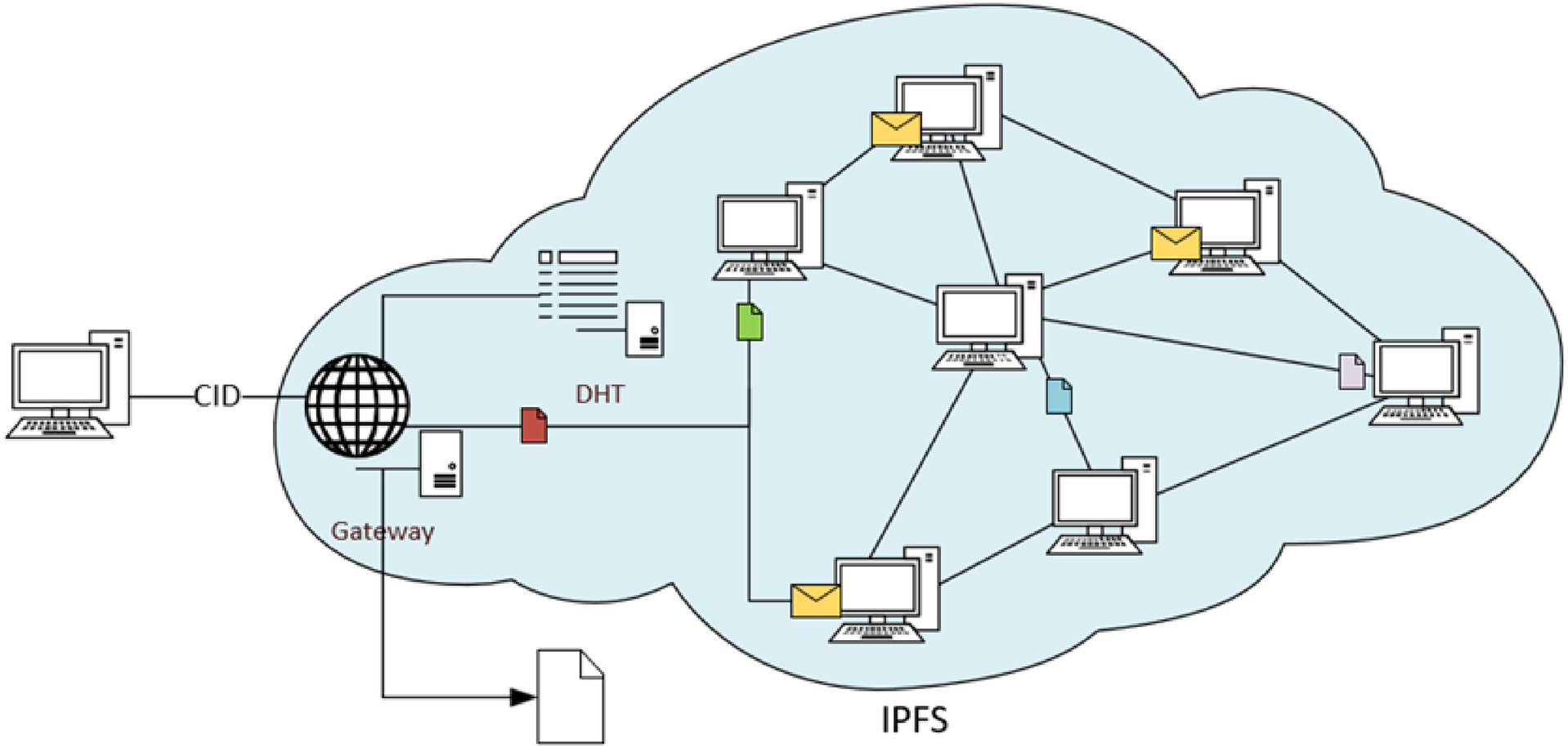
Diseño


Bloque
Bloque
Bloque
Bloque
Bloque
Gateway
IPFS
CID
Bloque_1 (hash)
Bloque_2 (hash)
Bloque_3 (hash)
Bloque_4 (hash)
Bloque_5 (hash)
Bloque_6 (hash)

Diseño

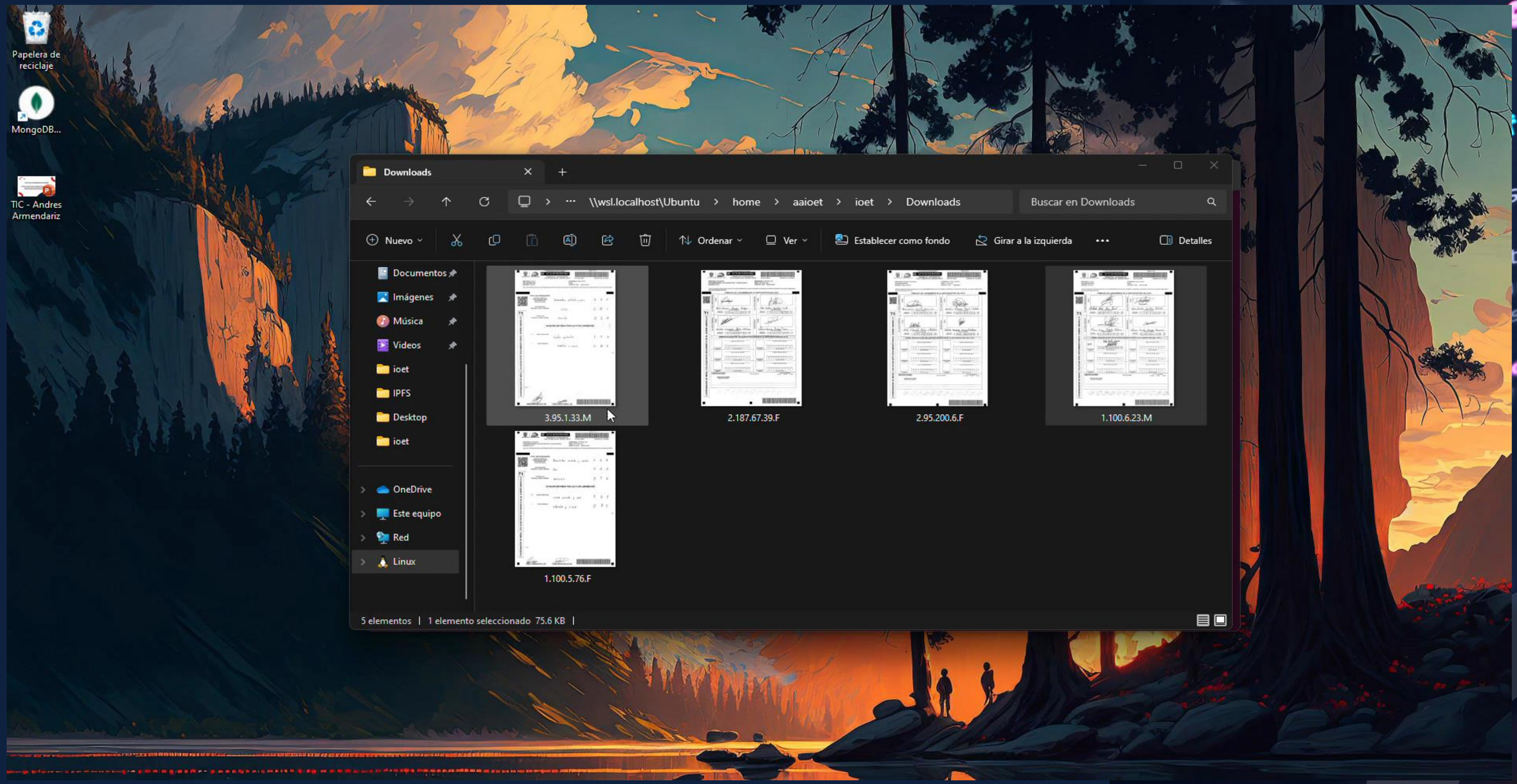

Bloque
Bloque
Bloque
Bloque
Bloque
Gateway
IPFS
CID
Bloque_1 (hash)
Bloque_2 (hash)
Bloque_3 (hash)
Bloque_4 (hash)
Bloque_5 (hash)
Bloque_6 (hash)

Diseño

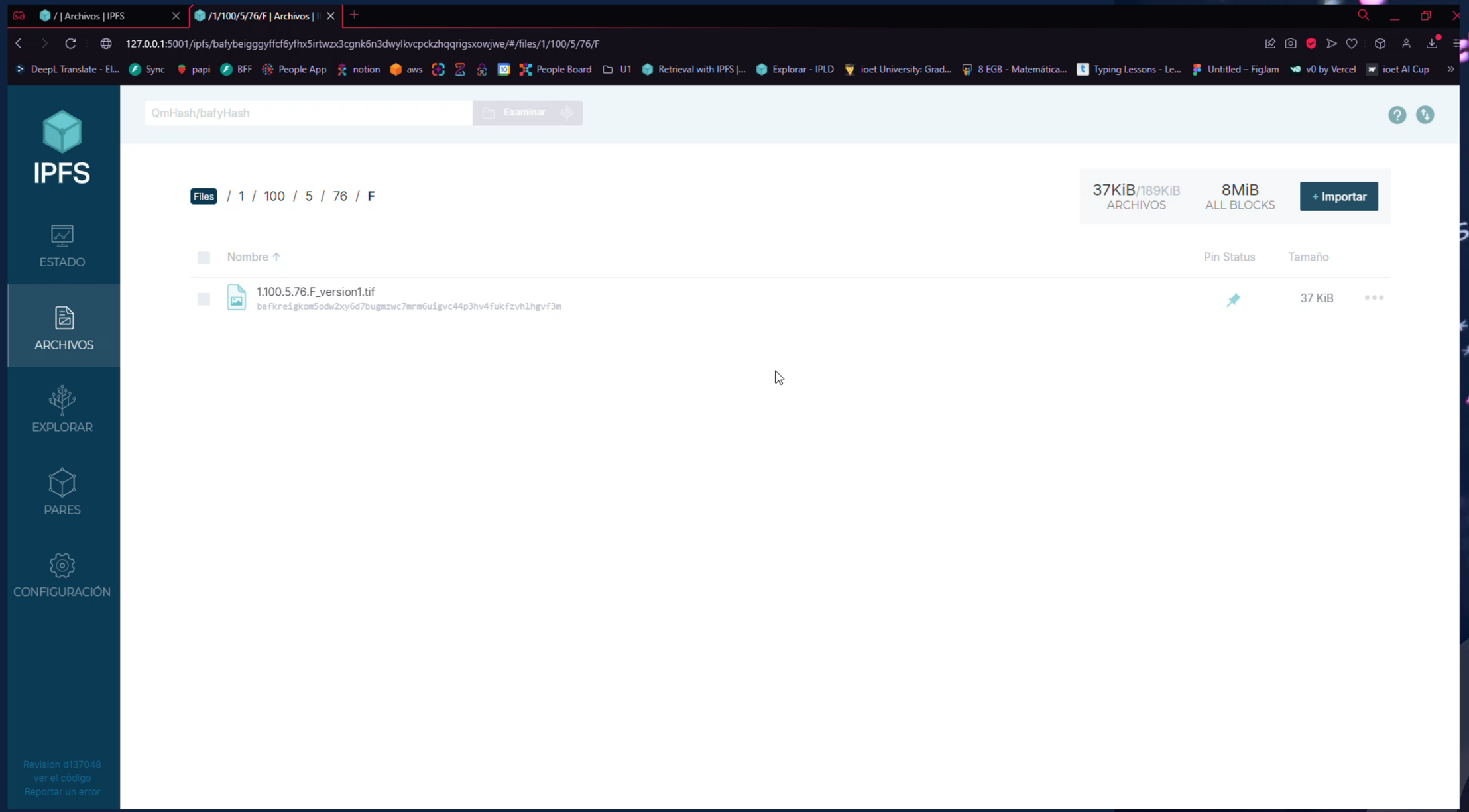


Diseño

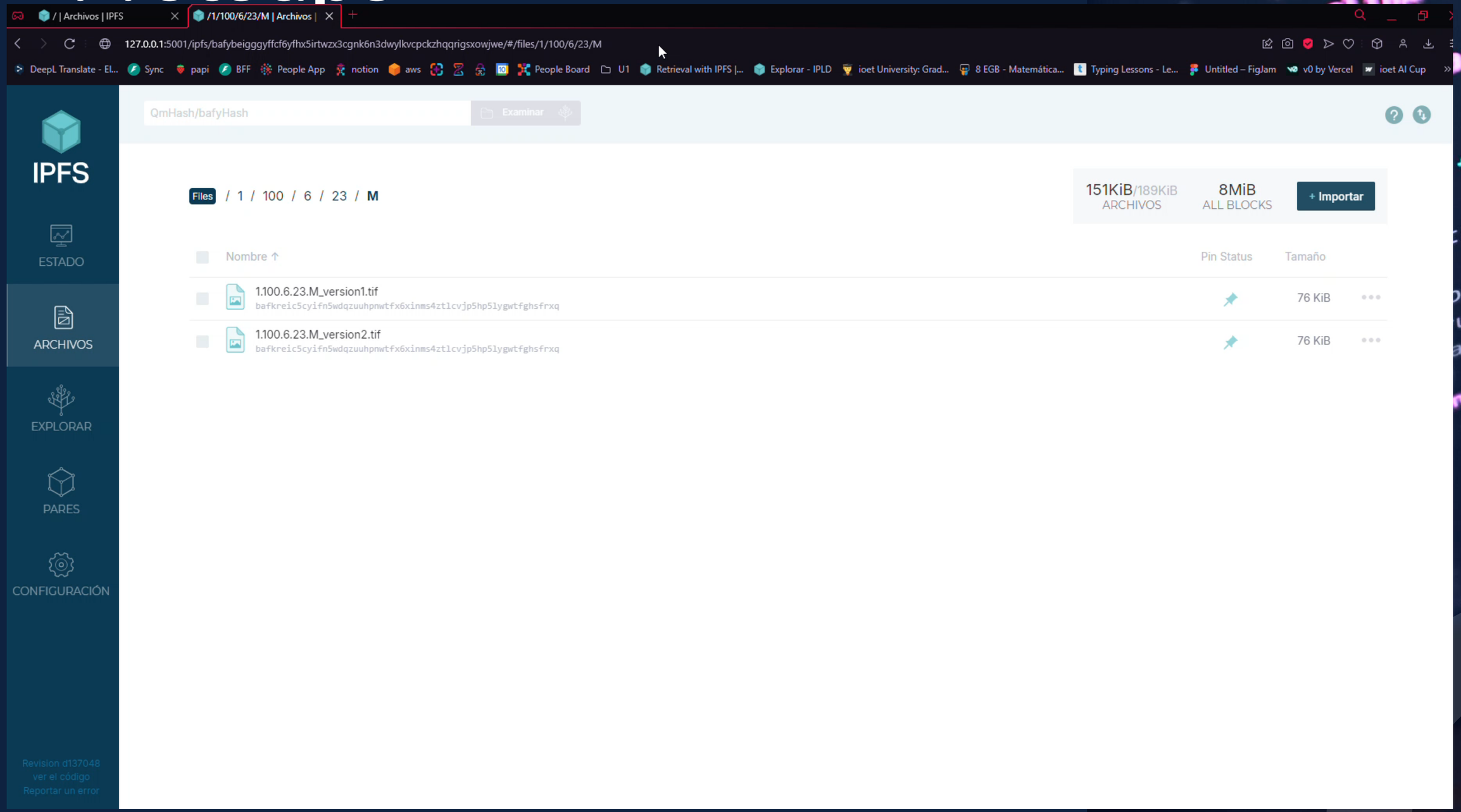
Prototipo


Papelera de reciclaje
MongoDB...
TIC - Andres Armendariz
Downloads
\\wsl.localhost\Ubuntu
home
aaioet
ioet
Downloads
Buscar en Downloads
Nuevo
Ordenar
Ver
Establecer como fondo
Girar a la izquierda
Detalles
Documentos
Imágenes
Música
Videos
ioet
IPFS
Desktop
ioet
OneDrive
Este equipo
Red
Linux
3.95.1.33.M
2.187.67.39.F
2.95.200.6.F
1.100.6.23.M
1.100.5.76.F
5 elementos | 1 elemento seleccionado 75.6 KB

Prototipo


/ | Archivos | IPFS
/1/100/5/76/F | Archivos |
127.0.0.1:5001/ipfs/bafybeigggyffcf6yfhx5irtwzx3cgnk6n3dwylkvcpckzhqqrigsxowjwe/#/files/1/100/5/76/F
DeepL Translate - El...
Sync
papi
BFF
People App
notion
aws
People Board
U1
Retrieval with IPFS |...
Explorar - IPLD
ioet University: Grad...
8 EGB - Matemática...
Typing Lessons - Le...
Untitled – FigJam
v0 by Vercel
ioet AI Cup
IPFS
QmHash/bafyHash
Examinar
ESTADO
ARCHIVOS
EXPLORAR
PARES
CONFIGURACIÓN
Files / 1 / 100 / 5 / 76 / F
37KiB/189KiB
ARCHIVOS
8MiB
ALL BLOCKS
+ Importar
Nombre
Pin Status
Tamaño
1.100.5.76.F_version1.tif
bafkreigkom5odw2xy6d7bugmzwc7mrm6uigvc44p3hv4fukfzvhlhgvf3m
37 KiB
Revision d137048
ver el código
Reportar un error

Prototipo


/ | Archivos | IPFS
/1/100/6/23/M | Archivos |
127.0.0.1:5001/ipfs/bafybeigggyffcf6yfhx5irtwzx3cgnk6n3dwylkvcpckzhqqrigsxowjwe/#/files/1/100/6/23/M
DeepL Translate - El...
Sync
papi
BFF
People App
notion
aws
People Board
U1
Retrieval with IPFS |...
Explorar - IPLD
ioet University: Grad...
8 EGB - Matemática...
Typing Lessons - Le...
Untitled – FigJam
v0 by Vercel
ioet AI Cup
IPFS
ESTADO
ARCHIVOS
EXPLORAR
PARES
CONFIGURACIÓN
QmHash/bafyHash
Examinar
Files / 1 / 100 / 6 / 23 / M
151KiB/189KiB
ARCHIVOS
8MiB
ALL BLOCKS
+ Importar
Nombre
Pin Status
Tamaño
1.100.6.23.M_version1.tif
bafkreic5cyifn5wdqzuuhpnwtfx6xinms4ztlcvjp5hp5lygwtfghsfrxq
76 KiB
1.100.6.23.M_version2.tif
bafkreic5cyifn5wdqzuuhpnwtfx6xinms4ztlcvjp5hp5lygwtfghsfrxq
76 KiB
Revision d137048
ver el código
Reportar un error

Conclusiones

- La capacidad de IPFS para generar CIDs inmutables asegura que los documentos no puedan ser manipulados una vez almacenados, lo que incrementa la confianza en la transparencia del proceso electoral
- El diagnóstico del sistema electoral vigente reveló debilidades significativas, incluyendo la falta de transparencia en la publicación de resultados y la ineficiencia en la distribución de resultados.
- El diseño de la arquitectura del sistema de archivos descentralizado se completó con éxito, creando una estructura personalizable a las necesidades funcionales y legales del CNE.
- El prototipo permitió la generación de CIDs únicos para cada documento, asegurando su inmutabilidad y verificación