Escuela Politécnica Nacional

Facultad de Ingeniería 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

Análisis, diseño e implementación del prototipo del sistema de cadena de bloques (infraestructura, contratos inteligentes y aplicación)

Autor: Christian Satama

Tutor: Dr. Enrique Mafla

Agenda

- Objetivos
- Estado actual del sistema del CNE
- Motivación
- Diseño
- Prototipo

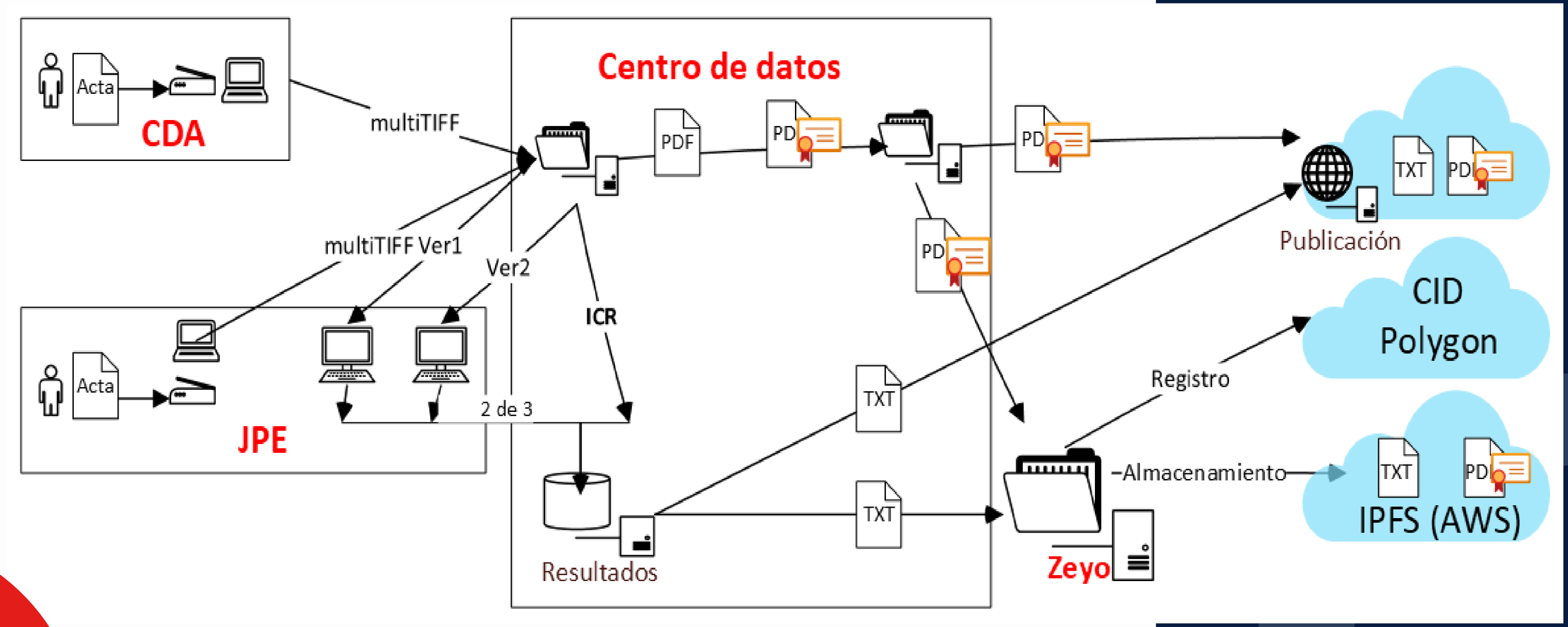
Objetivo General

Diseñar un sistema que garantice la integridad e inmutabilidad de las actas de escrutinio digitalizadas y los resultados electorales.

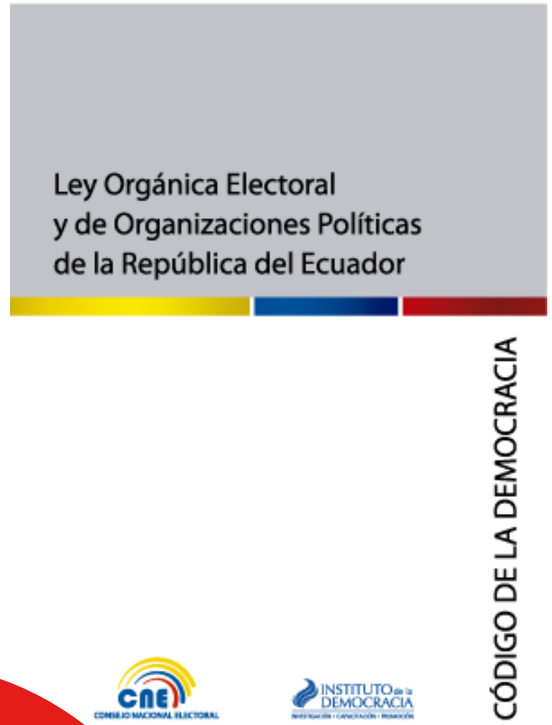
Objetivos Específicos

1. Analizar el sistema de escrutinios y publicación de resultados que utiliza el CNE.
2. Analizar los requerimientos funcionales y legales del proceso de escrutinios y publicación de resultados.
3. Diseñar la infraestructura tecnológica del sistema de cadena de bloques para el registro de las actas de escrutinio y resultados electorales.
4. Diseñar los contratos inteligentes y la aplicación para registrar las transacciones relacionadas al proceso de escrutinios y publicación de resultados.
5. Desarrollar el prototipo del sistema de cadena de bloques.

Estado actual del sistema del CNE

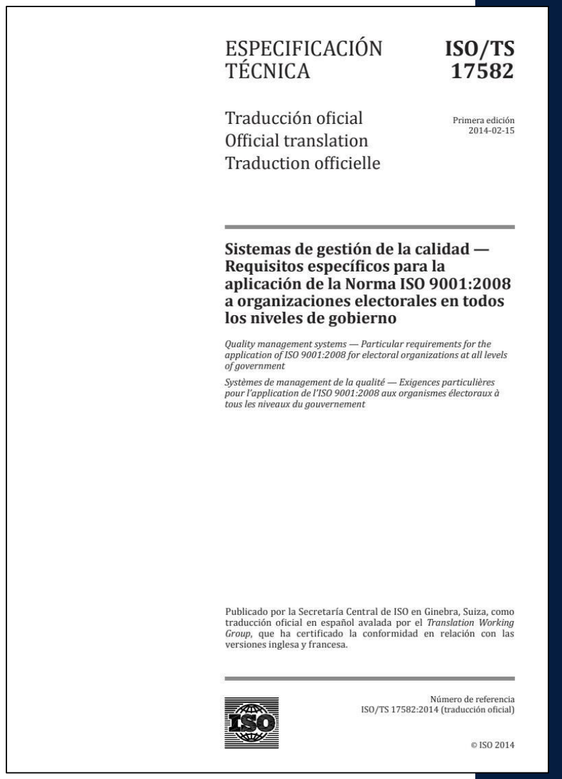


Motivación



Disposiciones transitorias:

- Primera: Sistema de interconexión de datos (SID)
- Segunda: Capacidad de añadir instituciones de control al SID
- Sexta: Auditoria avalada internacionalmente al sistema informático de conteo y publicación de resultados SIER



ESPECIFICACIÓN TÉCNICA **ISO/TS 17582**

Traducción oficial
Official translation
Traduction officielle

Primera edición
2014-02-15

Sistemas de gestión de la calidad — Requisitos específicos para la aplicación de la Norma ISO 9001:2008 a organizaciones electorales en todos los niveles de gobierno

Quality management systems — Particular requirements for the application of ISO 9001:2008 for electoral organizations at all levels of government

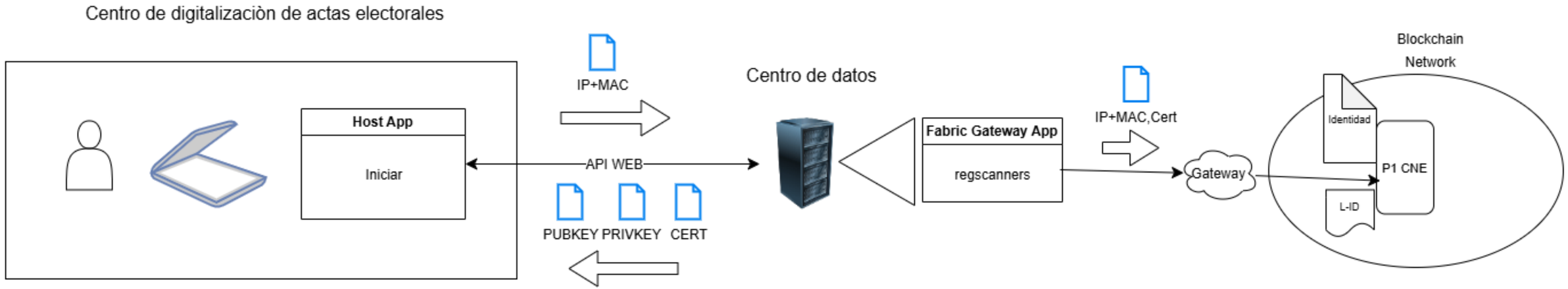
Systèmes de management de la qualité — Exigences particulières pour l'application de l'ISO 9001:2008 aux organismes électoraux à tous les niveaux du gouvernement

Publicado por la Secretaría Central de ISO en Ginebra, Suiza, como traducción oficial en español avalada por el *Translation Working Group*, que ha certificado la conformidad en relación con las versiones inglesa y francesa.

Número de referencia
ISO/TS 17582:2014 (traducción oficial)

- Registro de escrutinio de votos
- Integridad de los datos electorales
- Disponibilidad de los datos electorales

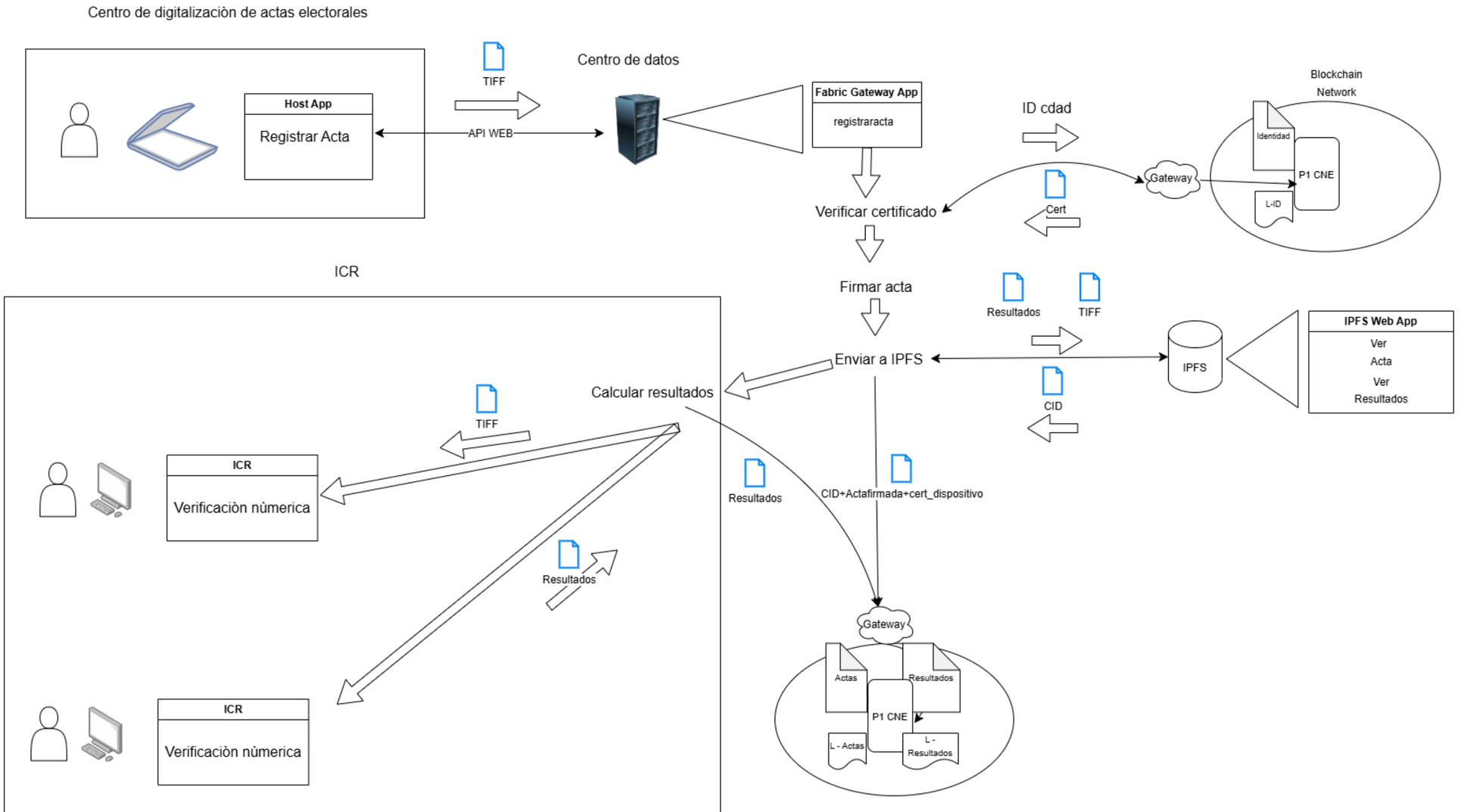
Diseño



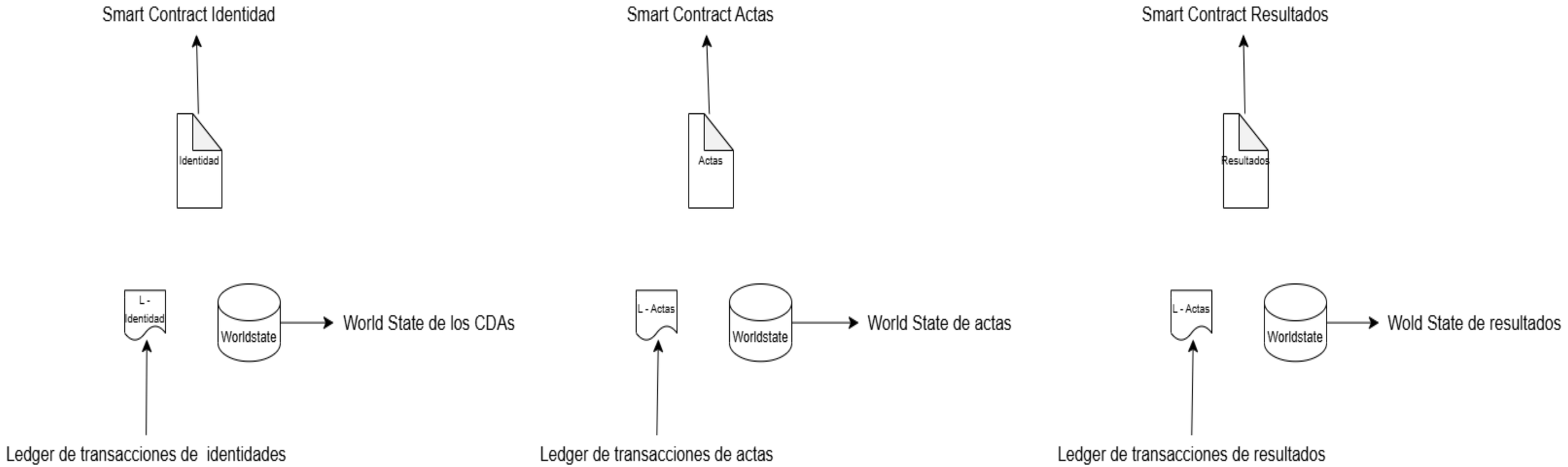
Lista de CDAs y sus dispositivos

Acta notarial

Diseño

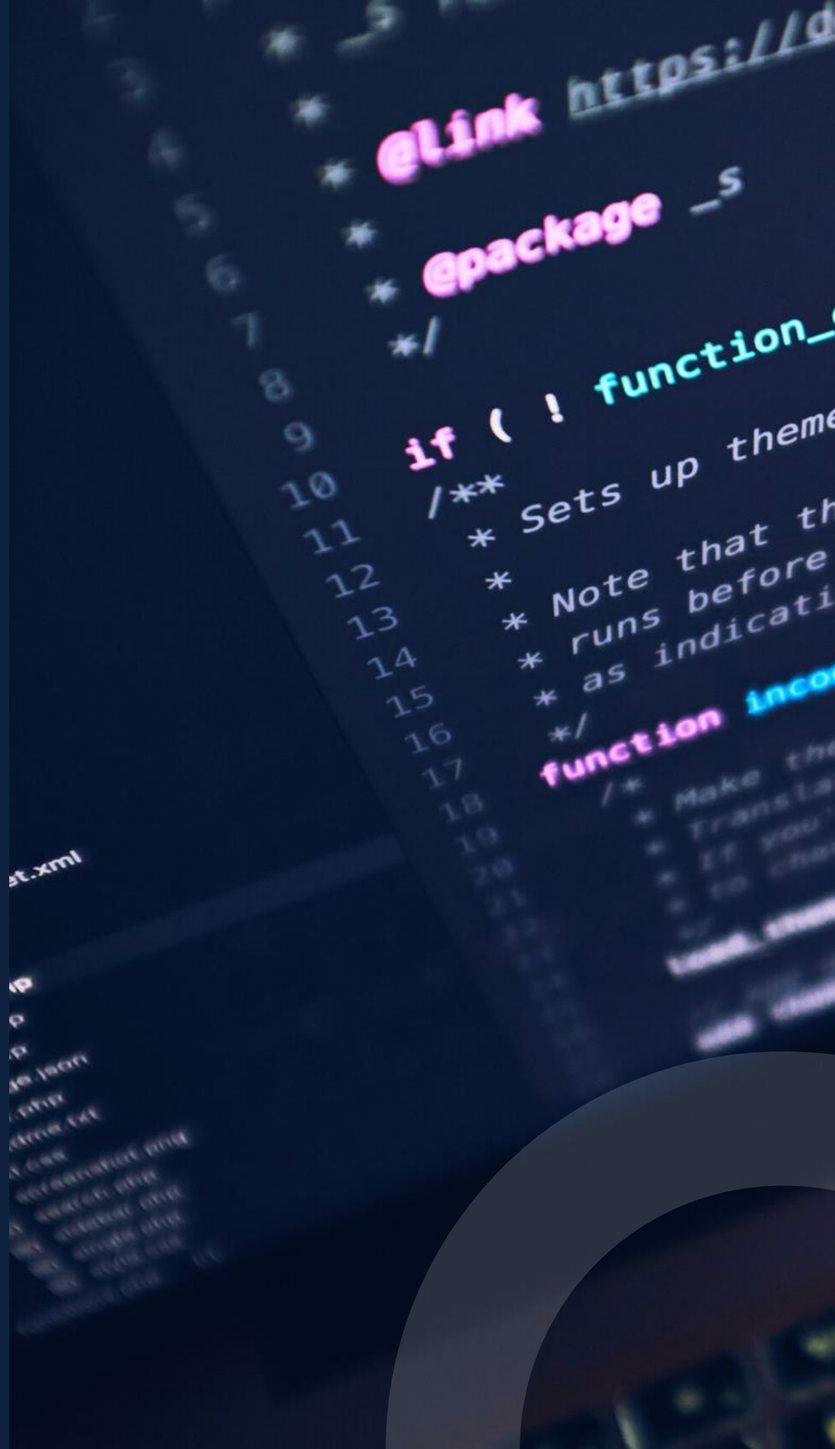

Centro de digitalizaciòn de actas electorales
Host App
Registrar Acta
API WEB
TIFF
Centro de datos
Fabric Gateway App
registraracta
ID cdad
Blockchain Network
Identidad
P1 CNE
L-ID
Gateway
Cert
Verificar certificado
ICR
Firmar acta
Resultados
TIFF
Enviar a IPFS
IPFS
IPFS Web App
Ver Acta
Ver Resultados
CID
Calcular resultados
TIFF
ICR
Verificaciòn nùmerica
Resultados
CID+Actafirmada+cert_dispositivo
Resultados
Gateway
Actas
Resultados
P1 CNE
L - Actas
L - Resultados
ICR
Verificaciòn nùmerica

Diseño


Smart Contract Identidad
Identidad
L - Identidad
Worldstate
World State de los CDAs
Ledger de transacciones de identidades
Smart Contract Actas
Actas
L - Actas
Worldstate
World State de actas
Ledger de transacciones de actas
Smart Contract Resultados
Resultados
L - Actas
Worldstate
Wold State de resultados
Ledger de transacciones de resultados

Prototipo

ChristianSMorales/HLF_cne (github.com)



Conclusiones

1. El SIER del CNE, al depender de servicios externos, carece de control y trazabilidad; integrar SID y nuevas tecnologías podría mejorar la transparencia electoral.

2. Aunque el CNE sigue la norma ISO/TS 17582:2014, el sistema de escrutinio requiere controles adicionales para asegurar la transparencia y cumplir con normativas legales.

3. El diseño de un sistema basado en Hyperledger Fabric para el SIER mostró viabilidad, mejorando trazabilidad y seguridad contra fraudes en procesos electorales.

4. Se diseñaron tres contratos inteligentes para registrar datos de escrutinio de manera inmutable, esenciales para auditorías y aseguramiento de la integridad de los resultados.

5. El prototipo del sistema blockchain, usando Hyperledger Fabric, se completó exitosamente integrando los tres componentes de infraestructura y seguridad, almacenamiento y redundancia de datos, y aplicación y contratos inteligentes; Lo cual demostró la viabilidad para integrar al SIER Blockchain y sistemas de almacenamiento descentralizado.