INSTITUTO TECNOLÓGICO DE SALTILLO

PROYECTO

PROTOCOLO URNA IEC

Integrantes:

Armando Flores Valdés
Karina Díaz Rosas
Miguel Ángel Ruíz Valencia
Abel Monsiváis Badillo
Mónica Sofía Vásquez Torres
Marcela Kineret Rivera Santibañez
Fernando Josué Pinedo Orta
Alejandro Alberto Ramírez Vilchis

SALTILLO, COAH. **SEPTIEMBRE DE 2019**

Índice

Introducción

Para los gobiernos y organizaciones resulta necesario el uso de urnas electrónicas para las elecciones de candidatos, agilizando el proceso y otorgando al votante confiabilidad y seguridad con su voto. Las nuevas tecnologías adaptan sistemas que otorgan esas características a las elecciones, disminuyendo la intervención humana en el proceso y otorgando mayor seguridad de la información recabada. Además de facilitar el proceso de conteo de votos y divulgación de resultados, representa una disminución significativa en los costos de materiales utilizados en la elección, evita algunos errores que pudieran ocurrir durante el proceso de conteo de votos y durante el proceso de selección de candidatos para evitarse votos nulos o errores en la elección.

En el siguiente protocolo se presentan las especificaciones y descripción detallada del proyecto a desarrollar, incluyendo especificaciones de hardware, software y funcionamiento general de la urna electrónica propuesta.

Objetivo general

Creación de una urna electrónica que cumpla con las especificaciones requeridas para agilizar y disminuir la intervención humana en el proceso de elecciones y conteo de los votos, además de ser eficiente y de fácil acceso para el ciudadano.

- ***Objetivos específicos***

- Desarrollar una urna que proteja la seguridad del voto.
- Reflejar el conteo de votos de forma eficaz y veraz.
- Permitir al prototipo y protocolo de urna, satisfacer las necesidades de transparencia y rendición de cuentas que demanda la sociedad.
- Implementar un diseño gráfico, accesible y efectivo para el usuario.

Especificaciones del prototipo

Funcionamiento general

La urna electrónica propuesta consiste en un sistema rápido, seguro y barato que permite la selección de candidatos, su conteo y posterior resultado final de la elección. El gabinete contará con pantalla táctil, lector de huella digital, impresora de comprobante, opción de audio para instrucciones durante el proceso de elección y texto escrito en braille en algunas partes de la urna para ciudadanos que presenten discapacidades. Tras proceder a identificarse al ciudadano mediante huella digital y verificar que sus datos sean correctos, se activará una nueva sesión en la que se mostrarán los candidatos para las distintas ramas (gubernatura, diputados, ayuntamiento). Al finalizar de seleccionar al primer candidato se le pedirá al votante que verifiqué si su elección es correcta. En caso de no ser así, podrá regresar y modificar su elección. Al terminar de seleccionar a los candidatos, se le mostrará al votante las opciones seleccionadas para la posterior impresión del comprobante. Al finalizar, con cada ciudadano, se cierra la sesión y se activa con cada lectura de huella digital registrada en el sistema. Las características de la urna electrónica se muestran a continuación:

Características de software

- Sistema Operativo: Parrot Security OS.

  Es una distribución de Linux basada en Debian con un enfoque en la seguridad informática. Está diseñado para pruebas de penetración, evaluación y análisis de vulnerabilidades, análisis forense de computadoras, navegación web anónima, y practicar criptografía . Es desarrollado por el Frozenbox Team.

- Gestión de ahorro de energía: Powertop.

  Es una herramienta para Linux que localiza aquellas aplicaciones que consumen más energía de la necesaria cuando están a la espera y crea soporte al consumo de batería.

- Lenguaje de Programación: Java.

Java es un lenguaje de programación y una plataforma informática. El lenguaje se utiliza en una gran variedad de dispositivos móviles, como teléfonos y pequeños electrodomésticos. Dentro del ámbito de Internet, Java permite desarrollar pequeñas aplicaciones (conocidas con el nombre de applets) que se incrustan en el código HTML de una página, para su directa ejecución desde un navegador.

- Framework: Maven con JavaFX.

  JavaFX: Son los paquetes de gráficos y medios que permiten diseñar, formar, crear, depurar e llevar a cabo aplicaciones.

  Maven: es una herramienta de software para la gestión y construcción de proyectos Java creada por Jason van Zyl, de Sonatype, en 2002. Es similar en funcionalidad a Apache Ant (y en menor medida a PEAR de PHP y CPAN de Perl), pero tiene un modelo de configuración de construcción más simple, basado en un formato XML.

- Base de datos: MySQL o Blockchain

  MySQL: Es un sistema de gestión de bases de datos, que trabaja con bases de datos relacionales.

  Una alternativa de almacenamiento es utilizar la tecnología Blockchain, usada hoy en día para Bitcoin, el sistema de pagos digitales más grande. El uso de una arquitectura Blockchain implica que la responsabilidad de verificar la autenticidad de los votos recaiga no sobre un organismo central, sino sobre una red de nodos en la que todos tienen el mismo poder sobre la información. Este proyecto gira alrededor del concepto de la Web 3.0, un nuevo paradigma de creación de aplicaciones que no dependen de un servidor para funcionar, sino de una red distribuida y abierta al público. Estas aplicaciones descentralizadas —también conocidas como “DApps”— presentan un alto número de ventajas en comparación con las aplicaciones tradicionales, la principal de ella siendo la alta resistencia a penetración.

- Se conectará a un servidor en la nube, mediante VPN y utilizando técnicas para la encriptación de datos.
- Operará en Modo kiosko en el sistema operativo. Éste modo define y permite realizar acciones limitadas, no asigna acceso a otras aplicaciones o contenido de la PC.
- Autenticación: mediante un sensor biométrico de huellas digitales y un lector de código de barras, se harán comprobaciones de votante para evitar la suplantación de identidad. El software no almacenará información que relacione al votante con su elección.
- Asistencias para personas con discapacidades: Se habilitará una forma de acceso a los votantes con discapacidad para que utilicen las salidas de audio mediante audífonos como asistencia para efectuar su voto.

- ***Funcionamiento del protocolo***

1. Inicio de la elección: se habilita la disponibilidad del sistema para dar inicio al proceso de elección.
2. Validación del acceso del votante al sistema: mediante huella digital y código de barras en credencial de elector.
3. Presentación de boleta electrónica: Se muestran los candidatos disponibles para cada una de las ramas (gubernatura, diputaciones y ayuntamientos).
4. Permite marcar uno de los candidatos en la boleta.
5. Registro seguro del voto.
6. Permite modificar la opción seleccionada en caso de ser requerido.
7. Al terminar de registrar los votos, se muestran las opciones seleccionadas y se imprime comprobante.

- ***Cifrado de voto electrónico***

- A cada partido o candidato se le asigna un código diferente por votante mediante el cifrado de la opción. Este código se generará con una operación criptográfica de Hash basada en la opción de voto y cifrándolo con una clave secreta relacionada con un identificador único de la boleta.

- Para verificar el registro correcto del voto se utilizará un segundo código, denominado código de retorno, diferente para cada candidato o partido. Este código se generará usando la misma función de Hash, pero encima del código anterior y usando una clave secreta que solo conoce el servidor de voto.

Características de hardware

La urna contará con los siguientes dispositivos externos:

- Pantalla: Panel IPS, resolución de 1920 x 1080 píxeles, tecnología táctil capacitiva multipunto.
- Batería: LiPO o Li-Ion (capacidad pendiente sujeto a cálculo de consumo energético promedio)
- Impresora térmica.
- Lector de código de barras, tipo ranura.
- Lector de huella digital.

La tarjeta de red inalámbrica se incorporará al interior de la urna, conectada al puerto PCI de la tarjeta madre.

Para las características del computador, se proponen las siguientes opciones:

Basado en Intel:

Opción 1:

- Procesador: Intel i5 9400.
- Chipset: H310 o B360.
- Factor de forma para tarjeta madre: Micro ATX.
- Memoria RAM: 2 módulos de 4GB DDR4 @2400 MHz.
- Almacenamiento interno: SSD 120 GB o HDD 1 TB @7200 RPM.
- Fuente de poder: 400 Watts.

Opción 2:

- Procesador: Intel i3 9100.
- Chipset: H310 o B360.
- Factor de forma para tarjeta madre: Micro ATX.
- Memoria RAM: 2 módulos de 4GB DDR4 @2400 MHz.
- Almacenamiento interno: SSD 120 GB o HDD 1 TB @7200 RPM.
- Fuente de poder: 400 Watts.

Basado en AMD:

Opción 3:

- Procesador: AMD Ryzen 3600.
- Chipset: A320 o B350.
- Factor de forma para tarjeta madre: Micro ATX.
- Memoria RAM: 2 módulos de 4GB DDR4 @2400 MHz.
- Tarjeta de video: GT 710 o superior.
- Almacenamiento interno: SSD 120 GB o HDD 1 TB @7200 RPM.
- Fuente de poder: 400 Watts.

Opción 4:

- Procesador: AMD Ryzen 3200G.
- Chipset: A320 o B350.
- Factor de forma para tarjeta madre: Micro ATX.
- Memoria RAM: 2 módulos de 4GB DDR4 @2400 MHz.
- Almacenamiento interno: SSD 120 GB o HDD 1 TB @7200 RPM.
- Fuente de poder: 400 Watts.

Se recomienda la opción 4 para el ensamble del computador, tomando en cuenta la carga de trabajo, eficiencia energética, simplicidad, seguridad informática y capacidad de actualización. La plataforma AM4 de AMD seguirá siendo compatible con los procesadores que se lancen en 2020, mediante actualizaciones de BIOS.

Puede justificarse ésta elección debido a que los procesadores Intel pueden ser más vulnerables que sus competidores, ya que han sido

detectados varios fallos de seguridad en nivel de kernel y arquitectura del procesador, tales como:

- Meltdown
- Spectre
- Spoiler

Éstas vulnerabilidades suponen un alto riesgo para la integridad de los datos que puedan procesarse en la urna, porque existe la posibilidad de que un intruso se infiltre en el sistema, teniendo control directo del ordenador.

Construcción de prototipo

El diseño de la carcasa está pensado para ser:

- Transportable.
- Ligero.
- De fácil instalación.

Para mejorar la accesibilidad para personas con discapacidad, se incluirá un grabado en braille.

El material que, por su durabilidad, coste de producción y mantenimiento, se ajusta mejor para el desarrollo del prototipo, es el HDPE o PEAD. Éste es un polímero que se caracteriza por:

- Excelente resistencia térmica y química.
- Muy buena resistencia al impacto.
- Es sólido, incoloro, translúcido, casi opaco.
- Se puede procesar por los métodos de conformado, empleados para los termoplásticos, como inyección y extrusión.
- Es flexible, aún a bajas temperaturas.
- Es tenaz.
- Es más rígido que el polietileno de baja densidad.
- Presenta facilidad para imprimir, pintar o pegar sobre él.
- Es muy ligero.
- Su densidad se encuentra en el entorno de 0.940 - 0.970 g/cm3.
- No es atacado por los ácidos, se considera una resistencia máxima de 60°C de trabajo para los líquidos, pues a mayor temperatura la vida útil se reduce. Otros termoplásticos ofrecen mejor resistencia a mayores temperaturas.
- Es mucho mejor para el reciclaje mecánico y térmico.

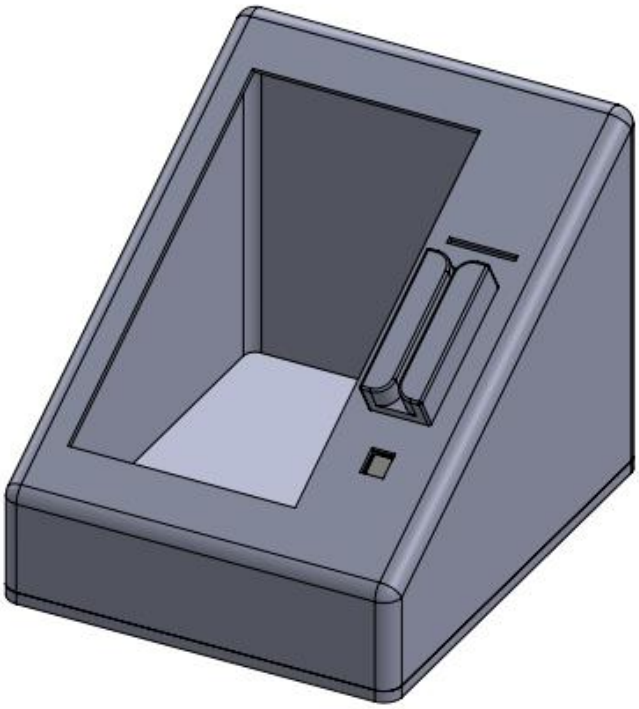

Figura 1. Modelo 3D de carcasa para la urna electrónica.

Para el anclaje de los componentes, se utilizarán guías y sujetadores que no afecten la integridad de la carcasa. Están en proceso de determinación debido a que tendrán que ser modificados conforme a los dispositivos disponibles en el mercado al momento de realizar el prototipo.

El coste de fabricación total, incluyendo las piezas, se dará conforme al promedio de precios del mercado actual, tomando en cuenta las características de hardware. Para la manufactura de la carcasa, es posible reducir el costo utilizando madera como materia prima, debido a que la inyección de plástico incluiría sobrecostes por la fabricación del molde.

A continuación, se da una lista de **precios promedio**, dando un total sugerido:

Artículo	Precio promedio (M.N.)
Pantalla	5730
Batería	6500
Impresora térmica	4500
Lector de código de barras	1500
Lector de huella digital	2600
Tarjeta de red inalámbrica PCI	250
Procesador	2750
Tarjeta madre	1850
Memoria RAM	1964
Almacenamiento interno	660
Fuente de poder	800
Fabricación de carcasa	2500
Total	31604

Precios calculados tomando el precio máximo y mínimo de componentes de referencia. Consultados el 27/09/2019, en https://www.cyberpuerta.mx.

Es preciso señalar que la elección de los componentes puede variar, y si es requerido, se pueden sustituir por otros de la elección que convenga a los representantes del IEC.

Programación y realización de pruebas

Conforme a los parámetros requeridos, se dispondrá a realizar el desarrollo del software, siguiendo una estructura como la siguiente:

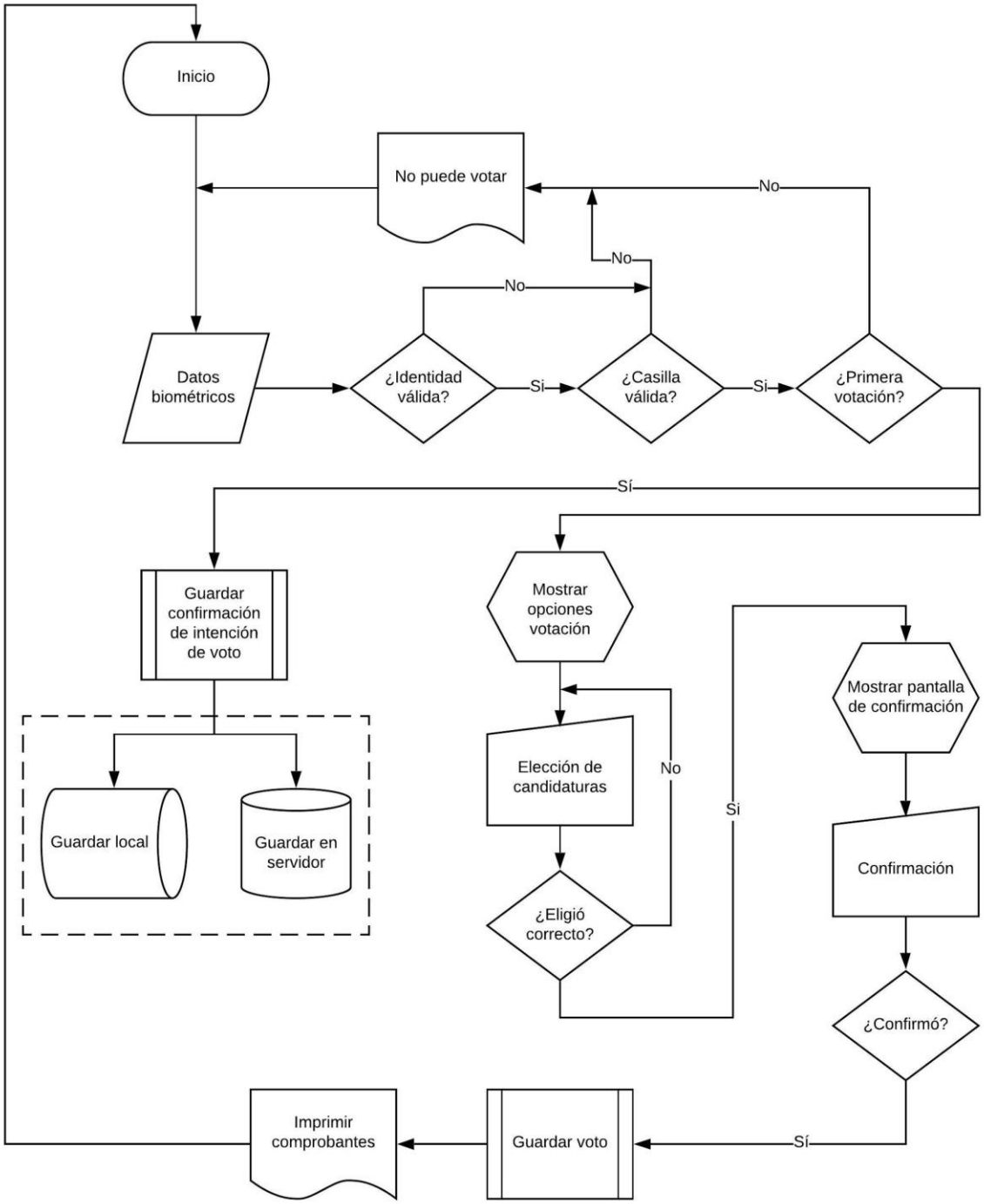

Figura 2. Algoritmo para votar en casilla electrónica.

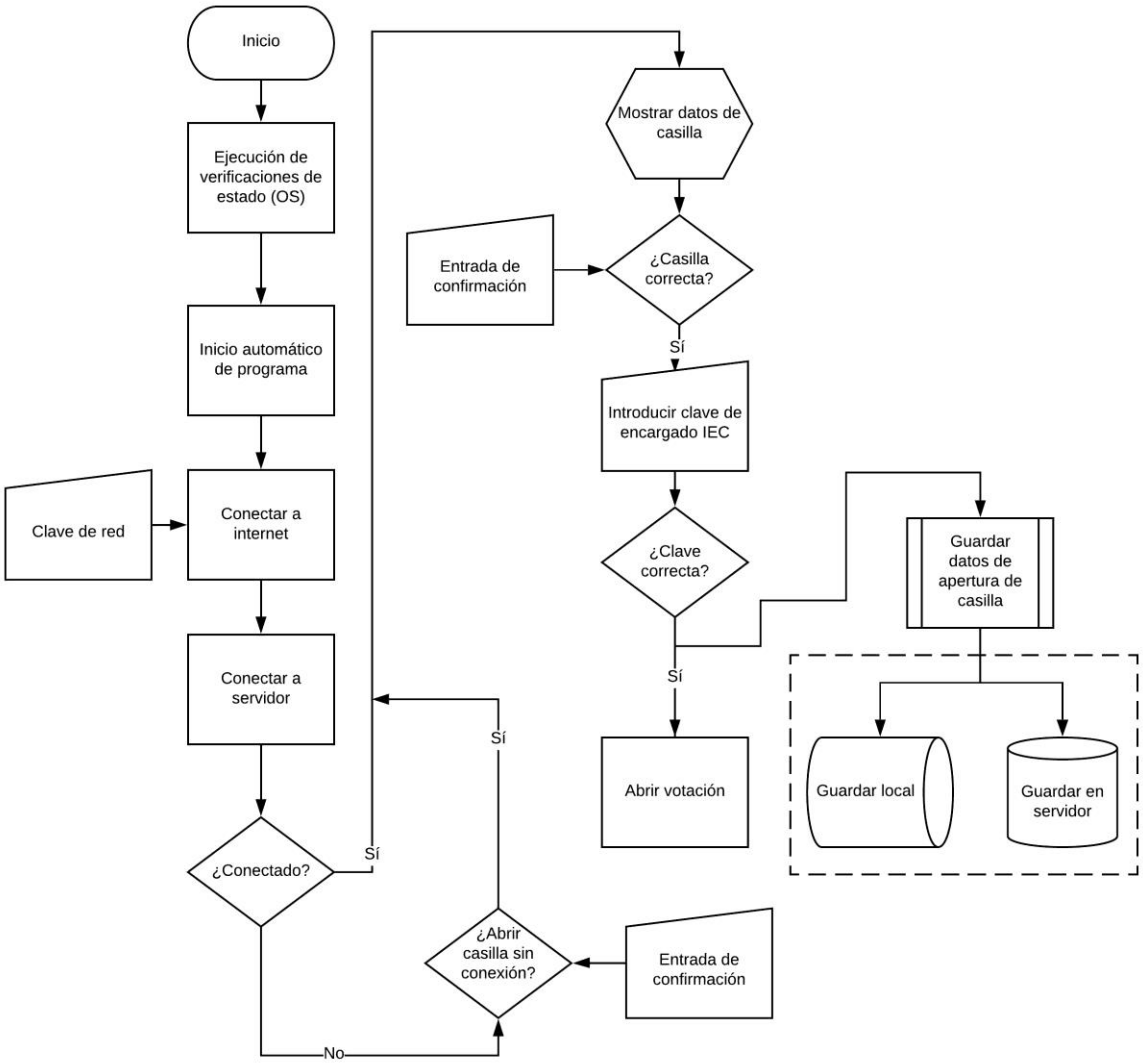

Figura 3. Algoritmo para la apertura de casilla a votación.

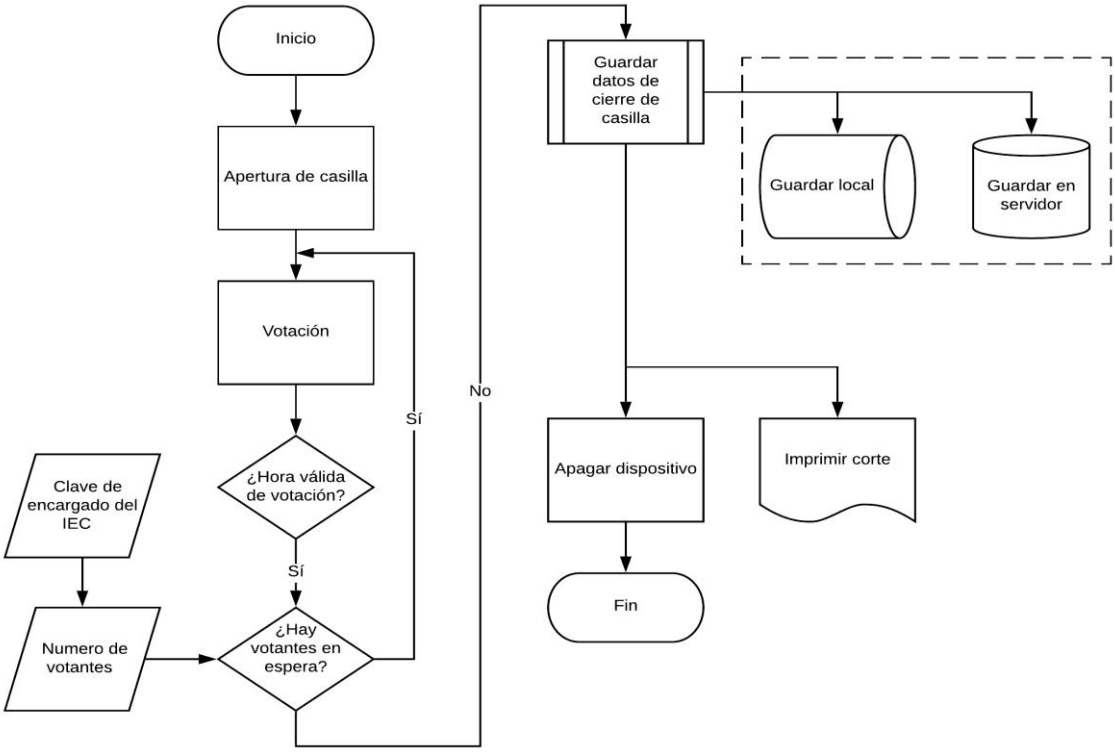

Figura 4. Algoritmo para cerrar la casilla.

La etapa de pruebas se realizará en las instalaciones del Instituto Tecnológico de Saltillo.

Se comprobará:

- Que el software y hardware funcionen conforme a especificaciones.
- Ante ataques físicos o virtuales haya protección de los datos.
- La eficiencia energética y térmica.

Si existieran áreas de oportunidad para la mejora del producto, se incorporarán en la medida de lo posible y del presupuesto asignado.

Anexos

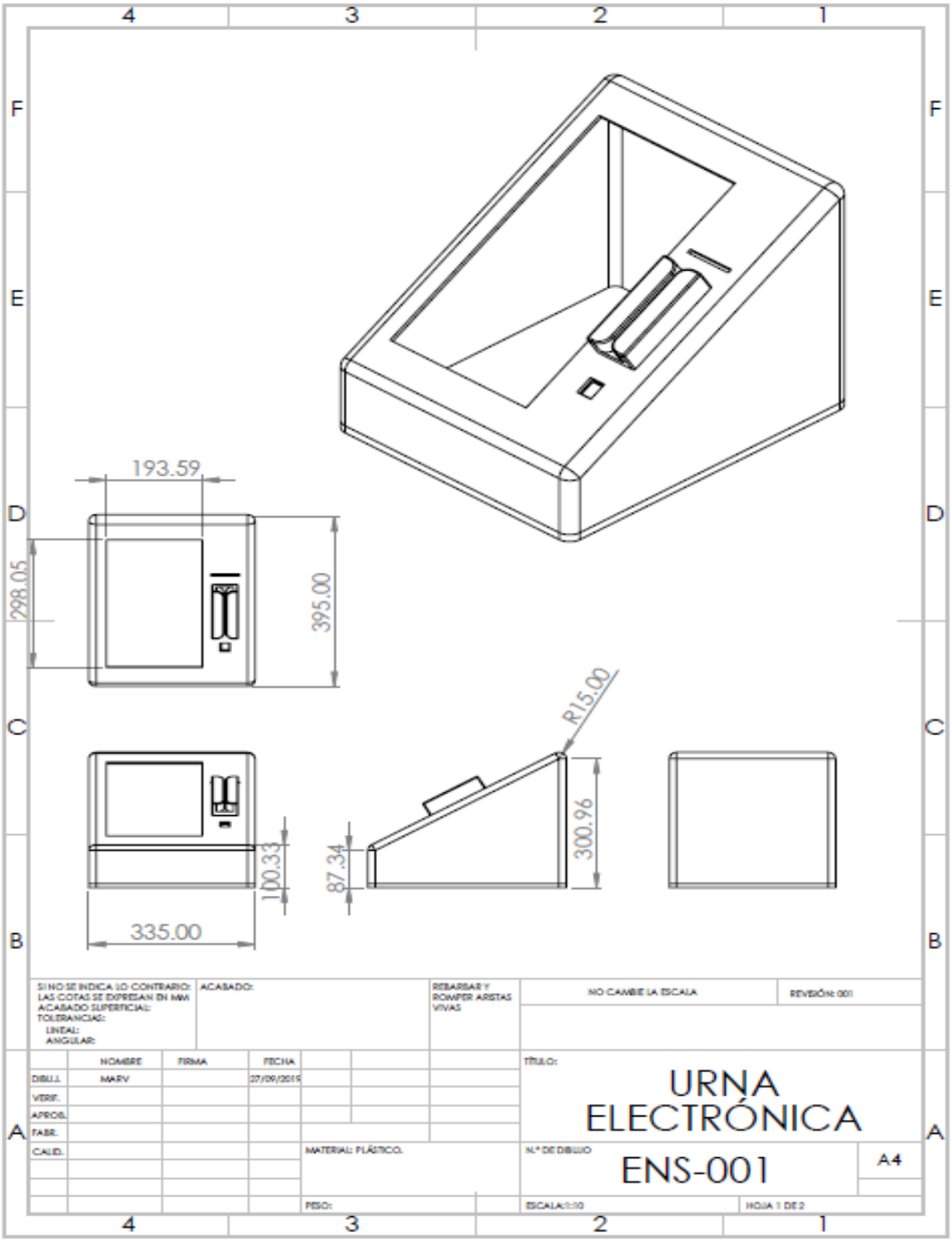

Figura 5. Dibujo técnico de carcasa.