UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

DISEÑO DE UN PROTOCOLO DE VOTACIONES ELECTRÓNICAS PARA LOS PROCESOS ELECTORALES DE EL SALVADOR

PARA OPTAR AL GRADO DE:

MAESTRO EN SEGURIDAD Y RIESGOS INFORMÁTICOS

PRESENTADO POR:

HÉCTOR OSWALDO MARROQUÍN ARGUETA

OSCAR ROLANDO AGUILAR ROSA

RIGOBERTO ANTONIO REYES ALVARENGA

ASESORA:

DRA. MARÍA DE LOURDES LÓPEZ GARCÍA

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica.

FEBRERO 2016

Diseño de un protocolo de votaciones electrónicas para los procesos electorales de El Salvador

Reyes, Rigoberto; Aguilar, Oscar; Marroquín, Héctor.
rigoberto.reyes@gmail.com, raguilarss@gmail.com, oswaldo.margueta@gmail.com

***Resumen*— Cuando las elecciones se realizan de forma manual, surgen inconvenientes tales como: La duplicidad de los votos, errores u omisiones en el padrón electoral, retrasos en la clasificación de las papeletas cuando se trata de un voto nulo y en el conteo general de los votos. Todo lo anterior produce desconfianza en el proceso electoral en general.**

Por otro lado, el voto electrónico garantiza niveles de seguridad en la transmisión del voto y la rapidez de los resultados, a través de protocolos seguros que satisfacen principalmente el anonimato del votante y la integridad de los votos, por lo que ofrece una alternativa con respecto a las elecciones tradicionales.

En este documento, se propone un protocolo de votación electrónica (e-voto) que automatiza la emisión del sufragio a través de un *token* que ayuda a garantizar el anonimato del votante y evita la duplicidad de los votos. El protocolo usa la criptografía de llave pública, lo que permite que pueda ser implementado en cualquier dispositivo tanto móvil como de escritorio.

***Términos Índice*— cifrado, firma digital, voto electrónico, votaciones electrónicas, urna electrónica.**

I. INTRODUCCIÓN

La democracia es de suma importancia para los países y un aspecto fundamental es la elección de los representantes de los diferentes órganos de gobierno. Las votaciones, idealmente, se deben realizar de manera transparente, confiable y eficiente para la obtención de los resultados.

Muchos países han considerado el uso del voto electrónico como alternativa a los procesos tradicionales. Algunos han realizado pruebas, mientras que otros ya usan las votaciones electrónicas de manera vinculante. Entre los países que han experimentado este tipo de votaciones se encuentran Suiza, Bélgica, Holanda, Inglaterra, Alemania, Escocia, Austria, Francia, España, Italia, India, Canadá, Venezuela, Colombia y Brasil. En [3] se puede encontrar una descripción de la experiencia de cada uno de estos países.

Es importante mencionar que, el voto electrónico se refiere al uso de las tecnologías de información y técnicas criptográficas para la emisión y recuento de los votos. El avance en las técnicas criptográficas ha permitido que éstas sean consideradas como una herramienta valiosa que brinda una alternativa a los procesos de votaciones manuales.

En este artículo, se propone un protocolo de comunicación seguro de votación electrónica, entre las entidades electorales y el votante, según la estructura de las instituciones de El Salvador. Utilizar las votaciones electrónicas, según se plantea en el protocolo, en lugar de la forma tradicional; tiene beneficios tales como: Minimizar el tiempo de procesamiento de los votos, dar resultados confiables y oportunos, además de reducir las posibilidades de fraude y error, entre otros.

El protocolo propuesto considera la separación de funciones de cada una de las entidades involucradas en el proceso electoral salvadoreño, garantizando el secreto electoral y minimizando la posibilidad de fraude, ya que cada una tendrá sólo la información que le compete. Es de resaltar que con la búsqueda de la eficiencia y mejora de los procesos electorales se ha hecho uso de implementaciones tecnológicas. Sin embargo, el uso de estas tecnologías en ocasiones causa que emitir el voto, sea más complejo para la población. Es importante destacar que en el protocolo que se propone, se considera que la población tiene un conocimiento minúsculo en el uso de las tecnologías, es por eso que los votantes no tienen la necesidad de ser dueños de un par de llaves criptográficas o de generar alguna firma digital, de tal manera que el protocolo sea fácil de utilizar en la población, sin generar dudas o rechazos.

Las herramientas criptográficas utilizadas en el protocolo son la función de cifrado y la firma digital RSA [18]. Adicionalmente, el protocolo usa un *token* que garantiza la unicidad del voto, el cual

es un número generado de manera aleatoria por una de las entidades electorales.

La combinación de las funciones RSA y el token dan como resultado un protocolo de votación electrónica seguro, que además está adaptado a las votaciones tradicionales indicadas en las leyes electorales de El Salvador.

El resto del documento se encuentra organizado de acuerdo a lo siguiente. La descripción de la situación actual respecto a las elecciones en el Salvador y el fundamento legal se presentan en las secciones II y III, respectivamente. Los fundamentos criptográficos para entender el protocolo propuesto se muestran en la sección IV, mientras que en la sección V se encuentra la descripción detallada del protocolo propuesto. Las secciones VI, VII y VIII consideran un análisis de seguridad para el protocolo propuesto, las recomendaciones de implementación y una discusión sobre las ventajas y sus limitaciones. Por último, las conclusiones de mencionan en la sección IX.

II. SITUACIÓN ELECTORAL ACTUAL EN EL SALVADOR

Las elecciones electorales en El Salvador realizadas el primero de marzo de 2015, para elegir concejos municipales, diputados para la asamblea legislativa, diputados al parlamento Centroamericano, fueron largas y complejas ya que se introdujeron nuevos elementos en la dinámica electoral, tales como: listas abiertas y el voto cruzado (que promovieron la libertad de opción para el votante), la conformación de los concejos municipales de tipo pluripartidista, la votación directa por rostro de candidatos al parlamento Centroamericano y la integración de planillas con una cuota de género femenino del 30%. Esto implicó un mayor esfuerzo para el Tribunal Supremo Electoral (TSE) para el correcto desarrollo de las elecciones, esto ocasionó problemas en la transmisión y procesamiento de los resultados preliminares y en el escrutinio final creando incertidumbre en la población.

Las elecciones en El Salvador se realizan de forma manual, una junta receptora de votos (JRV) conformada por cinco miembros (Presidente, Secretario, Primer Vocal, Segundo Vocal y Tercer Vocal). Estos se encargan de llevar a cabo las elecciones en el lugar establecido por el Tribunal Supremo Electoral. El sufragio se realiza utilizando una papeleta de votación que el secretario de la junta firmará y sellará una vez verificada la autenticidad del elector, mediante el padrón electoral y su documento único de identidad. Al finalizar la jornada de votación, los miembros de la junta receptora de votos abren la urna en presencia de vigilantes asignados por los partidos políticos participantes, se realiza el conteo de votos y se llena el acta correspondiente; la cual tiene información sobre la cantidad de votos nulos, válidos e impugnados. Se entrega una copia del acta a cada una de las personas que conforman la junta receptora de votos y a los vigilantes de los partidos políticos. La junta receptora de votos Municipal recolecta todas las actas correspondientes al municipio, hace el conteo, escanean las actas y las envían a la junta receptora de votos Departamental para continuar con el proceso. Cuando la junta receptora de votos departamental tiene los resultados de todos los municipios del departamento, los datos son enviados al Tribunal Supremo Electoral; el cual proporcionará datos preliminares conforme se reúne la información. El único proceso en el que se usa la tecnología, es en el traslado de la información y la suma de los conteos individuales de cada una de las juntas receptoras.

En la Fig. 1 se muestran los pasos que siguen los ciudadanos para ejercer su voto [13]. En el protocolo de votaciones electrónicas, este proceso es uno de los elementos que se toma como base en este esquema para realizar la propuesta.

III. BASE LEGAL

En esta sección se presentan los artículos más importantes de las leyes que rigen a las instituciones que intervienen en el proceso electoral de El Salvador, extraídos de la Ley de Creación del Registro Nacional de Personas Naturales [15].

A. Ley Orgánica del Registro Nacional de las Personas Naturales RNPN

Art. 2.) El Registro Nacional administrará los sistemas del Registro Nacional de las Personas Naturales, el Registro del Documento Único de Identidad y los demás que determinen las leyes.

Art. 3.) Son atribuciones del RNPN:

Fig. 1. Pasos para emitir el voto [13]

a) Mantener en forma permanente y actualizada toda la información del estado civil o familiar de las personas y crear los sistemas adecuados para el procesamiento y conservación de la misma;
b) Dar certeza oficial de los hechos y actos relacionados con el estado civil de las personas;
c) Organizar el Registro Nacional con la información proporcionada por los Registros Civiles y del estado Familiar de la República, con base en las copias certificadas de todos los asientos proporcionados por las oficinas respectivas;
d) Proporcionar al Tribunal Supremo Electoral toda la información necesaria para la inscripción de las personas en el Registro Electoral;
e) Informar al Tribunal Supremo Electoral sobre las defunciones de las personas, lo cual deberá hacerse en un plazo no mayor de quince días después de muerta la persona;
f) Facilitar información a solicitud de la Policía Nacional Civil, a la Fiscalía General de la República o de autoridad judicial para la investigación de hechos delictivos;
g) Las demás que la ley le establezca.

B. Código Electoral 2015 Tribunal Supremo Electoral

Garantía (Art. 63 C.E.) Son obligaciones del Tribunal como Organismo Colegiado, las siguientes [16] :

a) Velar por el fiel cumplimiento de la Constitución y Leyes que garanticen el derecho de organización y participación política de los ciudadanos y Partidos Políticos.
b) Convocar, organizar, dirigir y vigilar los procesos electorales relacionados con la elección de los

siguientes funcionarios:
   i) Presidente y Vicepresidente de la República,
   ii) Diputados al Parlamento Centroamericano.
   iii) Diputados a la Asamblea Legislativa,
   iv) Miembros de los Concejos Municipales.

c) Practicar el escrutinio preliminar y definitivo de las Elecciones Presidenciales, de Diputados al Parlamento Centroamericano y a la Asamblea Legislativa y de Concejos Municipales.
d) Firmar las credenciales de los funcionarios de elección popular dentro del término de ocho días, contados a partir de la fecha en que se declararon firmes los resultados de la elección, si transcurrido el plazo no se firmaren las credenciales, bastará la declaratoria en firme de los resultados del escrutinio definitivo, para que puedan tomar posesión de sus cargos, previa protesta constitucional.
e) Divulgar por los medios oficiales y privados de comunicación social, los fines, procedimientos y formas de todo proceso electoral.
f) Impartir las instrucciones necesarias para el normal funcionamiento de todos los organismos electorales.
g) Llevar el Registro Electoral debidamente actualizado.
h) Preparar el Presupuesto de Gastos, administrar los fondos que le sean asignados y cualesquiera otros recursos destinados a su normal funcionamiento. Preparar los presupuestos de gastos para los años ordinarios, pre electorales y electorales, a más tardar en el mes de septiembre del año anterior, en cada caso, a fin de cumplir con lo establecido en los artículos 58 y 327 de este Código.
i) Llevar el Registro de Partidos Políticos inscritos, Coaliciones, candidatos para Presidente y Vicepresidente de la República, Diputados al Parlamento Centroamericano y a la Asamblea Legislativa, Concejos Municipales y demás registros que establezca este Código.
j) Denunciar ante los Tribunales comunes, los hechos constitutivos de delito o falta de que tuviera conocimiento dentro de su competencia.
k) Elaborar y publicar la memoria anual de labores, así como una memoria especial de cada evento electoral.
l) Velar por que se cumplan los acuerdos y disposiciones emanadas del Tribunal.
m) Diseñar con la debida anticipación y aplicar coordinadamente con la Policía Nacional Civil el plan general de seguridad electoral.
n) Inscribir a los Partidos Políticos o Coaliciones, previo trámite, requisitos de Ley y supervisar su funcionamiento.
o) Inscribir a los ciudadanos postulados por los Partidos Políticos o Coaliciones, a cargos de elección popular previo el trámite y requisitos de ley.
p) Conocer y resolver sobre las suspensiones, cancelaciones y sanciones a los Partidos Políticos y Coaliciones así como de sus autoridades.
q) Cumplir las Resoluciones y Sentencias Judiciales que le notifiquen con relación a los actos de naturaleza electoral de su competencia y que modifiquen el estado civil de las personas o sus capacidades electorales.
r) Impartir directamente o por medio de los funcionarios a cargo, las instrucciones precisas y necesarias al centro de procesamiento de datos en relación al registro electoral y padrones electorales; y
s) Todas las demás que le asigne el presente Código.

Según [14] la Junta Receptora de votos (JRV) es el Organismo Electoral Temporal, que da la protesta de ley ante la Junta Electoral Municipal (JEM) y que de manera colegiada representa al TSE. Como autoridad electoral es la encargada de facilitar el derecho al voto a la ciudadanía y realizar el escrutinio de mesa. Sus facultades están delimitadas por el artículo 108 del Código Electoral.

El sufragio (Art. 3 C.E.) Es un derecho y un deber de los ciudadanos y ciudadanas, su ejercicio es indelegable e irrenunciable. El voto es libre, directo, igualitario y secreto.

Garantía (Art. 4 C.E.) Nadie podrá impedir, coartar o perturbar el ejercicio del sufragio. Las autoridades competentes están en la obligación de garantizar la libertad y pureza del sufragio y facilitar su ejercicio. Los infractores e infractoras serán sancionados.

Documento para votar (Art. 6 C.E.) Es deber de todo ciudadano y ciudadana obtener el documento único de identidad que lo identifique para ejercer el sufragio conforme a la ley.

C. Funciones específicas de integrantes de la JRV durante la votación

Presidente (Art. 196 C.E.)

- Solicitará el DUI vigente y original al ciudadano, verificando que la fotografía corresponda con el rostro. Si el resto de la JRV o la vigilancia de los partidos políticos o coaliciones contendientes exigen que el votante se identifique ante ella, el presidente o presidenta deberá permitirlo.
- Verificará que el votante, en sus manos u otra parte visible del cuerpo, no tenga marca de tinta indeleble que evidencie que haya votado.
- Buscará al votante en el padrón de búsqueda, confrontando nombre, foto y número de DUI. Estampará sobre el nombre del votante el sello "ELECCIONES 2015 SE PRESENTÓ A VOTAR".
- Anotará en el espacio indicado al final del padrón de búsqueda a las personas que no pudieron votar.

Secretario (Art. 196 C.E.)

- En presencia del votante firmará y sellará las 3 papeletas de votación (Sello "JRV") mostrándolas al resto de la JRV y vigilantes para comprobar que están debidamente firmadas y selladas.
- Retirará y depositará en la bolsa respectiva las esquinas desprendibles de las papeletas.
- Entregará al votante las 3 papeletas y el crayón.

Vocal 1 (Art. 197 C.E.)

- Mientras la persona vota, y recurriendo a su DUI ubicará su nombre en el padrón de firma.
- Verificará que el votante devuelva el crayón, después de haber votado.
- Seguidamente pedirá que el votante firme o ponga su huella dactilar en el padrón de firma, utilizando el espacio delimitado por la regla para firma. Debe verificar que la firma o huella se realice sin rebasar más allá de la casilla correspondiente.
- Asumirá las funciones del VOCAL 2 y VOCAL 3, en ausencia de éstos.

Vocal 2 (Art. 197 C.E.)

- Una vez que el votante ha firmado o colocado la huella dactilar en el padrón de firma, le pedirá que introduzca el dedo pulgar de la mano derecha en el frasco de tinta indeleble. A las personas a las que les faltaren ambas manos, les preguntará en qué parte visible del cuerpo quieren que se les haga dicha marca.
- Devolverá el DUI al votante.
- Llevará el registro de votantes en la Hoja de Control de Asistencia y marcará la casilla correspondiente a su sexo; adicionalmente, si se tratara de una persona ciega, lo marcará en el espacio respectivo.
- Asumirá las funciones del VOCAL 3, en ausencia de este.

Vocal 3

- Velará porque el flujo de personas sea contínuo garantizando que el anaquel doble o los dos anaqueles de mesa estén siendo utilizados simultáneamente.
- Facilitará el trato preferencial para las personas con discapacidades, mujeres en estado de embarazo, personas con bebés en brazos y adultos mayores, ubicándolas al inicio de la fila de votantes.
- Velará porque se mantengan las condiciones apropiadas para que la ciudadanía vote de manera secreta en el anaquel.
- Indicará al votante después de haber marcado y doblado las 3 papeletas, que las introduzca en los depósitos de acuerdo al color y que devuelva el crayón.
- Cuando la persona con discapacidad, así lo requiera lo guiará hacia el anaquel y posteriormente a los depósitos de votos.

D. Artículos de Interés de la Ley de Firma Electrónica

En El Salvador recientemente se ha aprobado la ley de firma electrónica [17].

- **Art. 8.-** Los documentos en soporte electrónico utilizando firma electrónica tendrán el mismo valor que los consignados de

manera tradicional. Quedan exentos aquellos documentos o actos jurídicos que para su perfeccionamiento requieren formalidades y solemnidades especiales.

- **Art. 3.-** Para los efectos de la aplicación de la presente Ley, se utilizarán las siguientes definiciones: **Acreditación:** Es la autorización que otorga la autoridad competente establecida en la presente Ley, a los proveedores de servicios de certificación, para operar y proporcionar certificados electrónicos, y a los proveedores de servicios de almacenamiento de documentos electrónicos, una vez cumplidos los requisitos y condiciones establecidos en la presente Ley.

- **Art. 18.-** Todo prestador de servicios de almacenamiento de documentos electrónicos que brinde servicios a terceros, quedará sujeto a las facultades de supervisión y control de la Unidad de Firma Electrónica de la autoridad competente para los efectos de velar por el cumplimiento de las obligaciones correspondientes que establece esta Ley y su reglamento, y normas y reglamentos técnicos emitidos al efecto.

- **La Autoridad de Control y Vigilancia**
  Art. 35.- Créase la Unidad de Firma Electrónica, como parte del Ministerio de Economía, el que en el texto de esta Ley podrá abreviarse MINEC. El Ministro nombrará al funcionario que estará a cargo de esta Unidad, quien deberá reunir los requisitos que para tal efecto se establezcan en el reglamento de esta ley.

- **Art. 23.-** La firma electrónica certificada debe estar sustentada en un método de creación y verificación confiable y seguro, de manera que aquélla sea inalterable, alertando al destinatario en caso de modificación de la información, después de ser suscrita por el signatario. La firma electrónica certificada tiene los siguientes efectos:
  a) Vincula un mensaje de datos con su titular, de manera exclusiva;
  b) Permite la verificación inequívoca de la autoría e identidad del signatario; y,
  c) Asegura que los datos de la firma estén bajo control exclusivo del signatario.

IV. FUNDAMENTOS CRIPTOGRÁFICOS

En [9] se define la criptografía como la ciencia que estudia la protección u ocultamiento de información a personas no autorizadas. Según [18], criptografía se deriva de la palabra griega **“Krypto”**, la cual contiene un significado de **“oculto”**, y la palabra griega **“Graphein”**, que significa **“escritura”**.

La criptografía se puede clasificar históricamente en dos: clásica y moderna.

La criptografía clásica es aquella que se utilizó desde antes de la época actual hasta la mitad del siglo XX. También puede entenderse como la criptografía no computarizada o mejor dicho no digitalizada. Los métodos utilizados eran variados, algunos muy simples y otros muy complicados de criptoanalizar para su época.

Se puede decir que la criptografía moderna se inició después de tres hechos: el primero fue la publicación de la “Teoría de la Información” por Shannon; el segundo, la aparición del estándar del sistema de cifrado DES (Data Encryption Standard) en 1974 y finalmente con la aparición del estudio realizado por Whitfield Diffie y Martin Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifrado, denominado cifrado de llave pública en 1976.

Tanto la criptografía clásica como la moderna se clasifican de acuerdo a las técnicas o métodos que se utilizan para cifrar los mensajes. Esta clasificación la podemos ver en la Fig. 2.

La criptografía se ha convertido en omnipresente, puede que sin saber en la vida cotidiana se utilicen una gran variedad de aplicaciones criptográficas; como por ejemplo, el acceso a ciertas aplicaciones por contraseña, la realización de compras a través de conexiones seguras (SSL), o aplicar una actualización de software que está firmado digitalmente. Los criptosistemas en la actualidad se pueden dividir en dos grandes ramas, los criptosistemas simétricos y los criptosistemas asimétricos, el protocolo propuesto en este documento utiliza un sistema asimétrico, por lo cual se profundizará un poco sobre el tema.

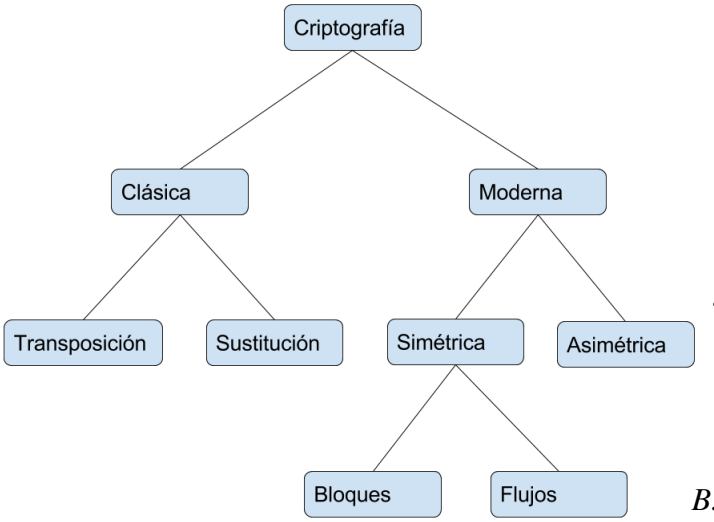

Fig. 2. Clasificación de la criptografía

A. *Función Hash o Picadillo*

Según [6], una función picadillo $H : \{0,1\}^* \rightarrow \{0,1\}^n$ es una función que tiene como parámetro de entrada una cadena de longitud arbitraria $(*)$ y arroja como resultado una cadena de longitud fija (n), el resultado de la aplicación de H sobre x es conocido como digesto.

Las funciones hash para ser seguras deben satisfacer dos propiedades principales [8]:

1) debe ser extremadamente complicado encontrar un mensaje m, tal que
$$H(m) = h$$
es decir, conociendo el valor de la función picadillo (H) determinar el mensaje que lo produjo (m).
2) debe ser difícil encontrar dos mensajes m_1 y m_2, tal que
$$H(m_1) = H(m_2)$$

Como se menciona en [5], existe una gran diversidad de aplicaciones de las funciones hash entre las que se puede mencionar las siguientes:

1) **Contraseñas:** Las funciones hash son ampliamente usadas para almacenar contraseñas, por su característica de irreversibilidad.
2) **Firmas digitales:** Realizar operaciones de firmas digitales sobre mensajes grandes puede consumir mucho tiempo por los algoritmos de firmas digitales. En su lugar, al mensaje se le aplica la función hash y el algoritmo de firma digital se aplica al valor hash obtenido de menor tamaño.
3) **Integridad:** Un mensaje puede ser considerado íntegro si su valor hash ya fue calculado antes de cualquier transmisión. Este valor es comparado con el valor hash del mensaje recibido.
4) **Códigos de autenticación de mensaje:** Hash de un mensaje que se auxilia de una llave secreta "k" para garantizar el origen del mensaje.

B. *Criptosistemas Asimétricos o de Llave Pública*

Según [19] En este sistema criptográfico cada usuario tiene un par de llaves, una pública y otra privada:

- La **llave pública**: será conocida por todos los usuarios.
- La **llave privada**: será custodiada por su propietario y no se dará a conocer a ningún otro.

Esta pareja de claves es complementaria: **lo que cifra una solo lo puede descifrar la otra y viceversa**. Estas claves se obtienen mediante algoritmos y funciones matemáticas complejas de forma que por razones de tiempo de cómputo, es imposible conocer una clave a partir de la otra.

Los sistemas de cifrado de clave pública se basan en **funciones resumen** o **funciones hash de un solo sentido** que aprovechan propiedades particulares, por ejemplo de los números primos. Una función de un solo sentido es aquella cuya computación es fácil, mientras que su inversión resulta extremadamente difícil.

En este caso no es necesario compartir la llave privada, cuando un usuario desea enviar un mensaje a otro usuario, sólo debe cifrar el mensaje que desea enviar utilizando la llave pública del receptor. El receptor podrá descifrar el mensaje con su llave privada (la cual sólo él conoce).

Según [18], el criptosistema RSA es el más importante y extendido en la actualidad, el cual utiliza la exponenciación modular para cifrar y descifrar, y su seguridad está basada en la complejidad del problema de factorización de números enteros grandes.

El criptosistema RSA es sencillo de implementar, algo muy peculiar en este criptosistema es que sus

llaves sirven indistintamente tanto para cifrar como para firmar. Si un atacante quiere descifrar el texto claro a partir del criptograma y su clave pública, tiene que enfrentarse a las dificultades que presenta el problema de factorización de números enteros grandes.

Otro aspecto importante en el criptosistema RSA son los números primos ya que constituyen la pieza básica en la construcción de éste [7]. En la generación de las llaves tanto privada como pública, el cifrado del mensaje y el descifrado del mismo, se utiliza la siguiente notación:

- M representa el espacio de mensajes que pueden ser cifrados, también es conocido como texto claro.
- C representa el espacio de mensajes cifrados o también conocidos como mensajes ofuscados.
- e es parte del par (e, n) el cual es conocido como llave pública.
- d es parte del par (d, n) el cual es conocido como llave privada.
- n es el módulo RSA.

Hay que hacer notar que con este algoritmo los mensajes que se cifran y descifran son números enteros de tamaño menor que n, no letras sueltas como en el caso de los cifrados César o Vigènere. Para obtener el mensaje cifrado C a partir del mensaje en claro M, se realiza la siguiente operación:

$$C = M^e (mod\ n) \tag{1}$$

Para recuperar el mensaje original a partir del cifrado se realiza la siguiente operación:

$$M = C^d (mod\ n) \tag{2}$$

Según [20] los sistemas de criptografía asimétrica se caracterizan por el uso de un tipo de algoritmo con dos llaves, una que no se revela y la otra sí. Dependiendo de la aplicación, el emisor usa su llave privada o la llave pública del receptor, o las dos, para realizar algún tipo de función criptográfica. En términos generales, se puede clasificar el uso de criptosistemas asimétricos en tres categorías:

1) **Cifrado/descifrado:** Para realizarlo el emisor cifra el mensaje con la llave pública del receptor, de esta forma solamente quien posea la llave privada emparejada a la llave pública podrá descifrar el mensaje.
2) **Firma digital:** El emisor firma un mensaje utilizando su llave privada, para verificar la validez de la firma, el receptor utiliza la llave pública del firmante.
3) **Intercambio de llaves:** dos partes cooperan para intercambiar una llave de sesión.

En la Fig. 3 se puede observar el proceso de cifrado/descifrado usando criptografía asimétrica.

Fig. 3. Criptografía asimétrica: cifrado/descifrado

C. *Firma Electrónica*

La firma electrónica consiste en una serie de algoritmos matemáticos basados en técnicas criptográficas de generación y la utilización de un par de llaves: Pública y privada. Éstas son asignadas a cada usuario del sistema y relacionados entre sí asegurando así que el usuario que firme es quien dice ser. La llave privada debe ser conocida únicamente por su propietario ya que ésta es la que utilizará para producir una firma única, la cual será infalsificable en un documento dado, mientras que la llave pública debe ser conocida por el verificador de un documento firmado, con la finalidad de determinar si la firma de ese documento es auténtica o no. La notación en general para un esquema de firma digital es el siguiente:

- M representa el conjunto de todos los mensajes que pueden ser firmados.
- S representa el conjunto de todas las firmas que pueden ser generadas, usualmente con una longitud fija.
- K_s representa el conjunto de llaves privadas.
- K_v representa el conjunto de llaves públicas.

- $k_\varepsilon : M \times K_s \rightarrow S$ representa las reglas de transformacón para que la identidad ε produzca una firma.
- $V_\varepsilon : M \times k_v \rightarrow \{verdadero, falso\}$ representan las reglas de verificación de la transformación para una firma producida por ε. Estas reglas son usadas por las entidades que requieren la verificación de la firma.

Un esquema general sobre cómo se realiza la firma eletrónica se muestra en la Fig. 4.

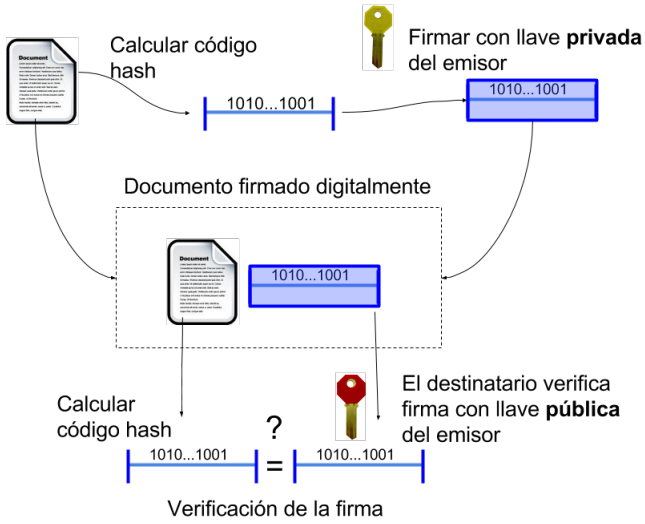

Fig. 4. Firma electrónica

Como se muestra en [21] la firma eletrónica debe cumplir con los siguientes requisitos:

1) Debe ser única; esto es, que sólo la pueda generar el usuario legítimo.
2) Ha de ser no falsificable, ya que el intento de falsificación se encuentra con un problema matemático intratable.
3) Fácil de autenticar, pudiendo cualquier receptor establecer su autoría, aún después de mucho tiempo.
4) Irrevocable, puesto que su autor no puede negar su autoría.
5) Barata y fácil de generar.

D. Voto Electrónico

Según [2] se puede definir al voto electrónico como el acto de sufragio que aplica e incorpora las TICs de manera total o parcial, es decir, en el conjunto de las distintas facetas que componen el proceso electoral o en alguna de ellas. De esta manera, la utilización de componentes de hardware, software y procedimientos que permiten automatizar los procesos de construcción y actualización del registro electoral, la emisión del voto, el escrutinio; así como de una red de comunicaciones para la transmisión y consolidación de los resultados electorales, marca la diferencia entre una votación electrónica y aquellas que se sirven de metodologías tradicionales.

El voto electrónico se ha vuelto atractivo por sus diferentes ventajas, pero también presenta nuevos retos, como se menciona en el siguiente listado de las fortalezas y debilidades del voto electrónico [1]:

Fortalezas

- Mayor rapidez en la votación, conteo y tabulación.
- Mayor precisión en los resultados, ya que la posibilidad de error humano queda excluida.
- Eficiencia en el manejo de sistemas electorales complicados que requieren procedimientos de conteo laboriosos [1].
- Mejora en la presentación cuando las papeletas son complicadas [2].
- Posibilidad de aumento en la participación electoral.
- Prevención del fraude en las mesas de votación y durante la transmisión y tabulación de los resultados, al reducirse la intervención humana.
- Disminución en el número de papeletas anuladas ya que el sistema de votación puede advertirle al votante cuando un voto quedará invalidado.

Debilidades

- Existe la posibilidad de que se viole el secreto del voto, en especial en sistemas que realizan tanto la autenticación como la emisión de los votos.
- Riesgo de manipulación por parte de personal interno con acceso privilegiado al sistema.
- Aumento en los costos por la compra y mantenimiento del sistema de voto electrónico.
- Mayores requerimientos de infraestructura y medioambientales, por ejemplo, asociados al suministro eléctrico, la tecnología de las

[1]Como el voto cruzado implementado en El Salvador, elecciones 2015

[2]Como el voto por rostro cuando existen muchos candidados.

comunicaciones, temperatura, humedad.
- Necesidad de realizar más campañas para educar a los votantes.
- Posibilidad de conflicto con el marco legal vigente.
- Es posible que la ciudadanía desconfíe de las elecciones con voto electrónico como resultado de las debilidades antes mencionadas.

Para cubrir las fortalezas y evitar las debilidades, en el ámbito de seguridad los protoclos de voto electrónico deben cumplir con ciertos requisitos de funcionamiento y seguridad [3]:

- **Autenticación:** que voten sólo los que estén legitimados para el sufragio.
- **Unicidad del voto (democrático):** que sólo se vote una vez y no se pueda modificar el resultado de dicha votación.
- **Anonimato:** que no se pueda relacionar al votante con el voto.
- **Imposibilidad de coacción:** el elector no deberá en ningún caso demostrar o divulgar que voto emitió, impidiendo la compra masiva de votos y la presión (coacción) sobre los votantes.
- **Precisión:** el sistema debe tener la capacidad de registrar los votos correctamente y con seguridad.
- **Verificación (trazabilidad):** cada votante podrá obtener un recibo del sistema de votación que le garantice que su voto será incluido en el escrutinio final.
- **Imparcialidad:** todos los votos deberán permanecer en secreto hasta que finalice el período de sufragio. De esta forma se evitará que los resultados parciales afecten a la decisión de los electores que aún no hayan ejercido su derecho al voto.
- **Auditabilidad:** deberán existir procedimientos para poder verificar que todos y cada uno de los votos se hayan tenido en cuenta en el escrutinio.
- **Confiabilidad:** los sistemas utilizados deben trabajar de modo seguro siempre, sin que se produzcan pérdida de votos incluso en casos extremos.
- **Certificables:** los sistemas deben poder comprobarse por parte de las autoridades electorales, para que puedan confiar en que cumplen con los criterios establecidos.
- **Invulnerable:** de forma que impida la manipulación a todos los niveles.
- **Abierto:** de forma que las autoridades electorales y, si es el caso, el ciudadano en general puedan obtener detalles de su funcionamiento (hardware y software).

V. PROTOCOLO SEGURO DE VOTO ELECTRÓNICO PROPUESTO

Los avances en la tecnología han influido notoriamente en la manera que se llevan a cabo muchas de las actividades cotidianas, sustituyendo las formas tradicionales de realizarlas; logrando a través de la implementación de protocolos criptográficos ofrecer los servicios de seguridad necesarios para generar la confiabilidad y veracidad de las actividades, no repudio, integridad, anonimato, auditoría y además evitan la suplantación de identidad. Tomando en cuenta esto es importante el uso de votaciones electrónicas para mejorar y agilizar el proceso electoral, tomando en cuenta las experiencias de diferentes países, logrando de esta manera fortalecer la democracia.

La propuesta parte de los pasos presentados en la Fig. 1 identificando las funciones realizadas y las instituciones responsables de ellas, además de las funciones atribuidas por la legislación correspondiente la cual se describe en la sección de base legal.

Luego tomando como base varios esquemas de votaciones electrónicas existentes [4] se hace la siguiente propuesta de protocolo para votaciones electrónicas, adecuado a los procesos electorales desarrollados en El Salvador.

En la Tabla I se muestra un resumen de las funciones legales y las acciones a desempeñar en el protocolo propuesto de cada entidad involucrada en el proceso electoral.

El protocolo propuesto en la Fig. 5 consta de dos macro fases: **Autenticación** y **emisión del voto**. El RNPN es la institución cuya principal responsabilidad consiste en la autenticación del votante determinando si es apto para emitir su sufragio, en esta fase la JRV sirve como interfaz entre el votante y el RNPN. Una vez realizada la autenticación la JRV es la que inicia la siguiente fase de **emisión del voto**, generando la boleta electrónica y activando la urna; la urna es la interfaz con la que interactúa el votante para poder ejercer su derecho al sufragio especificando las opciones de su voto y

TABLA I
ORGANISMOS, RESPONSABILIDADES LEGALES Y SU FUNCIÓN EN EL PROTOCOLO

	Responsabilidades legales	Funciones en el protocolo propuesto
RNPN	• Registro del Documento Único de Identidad • Proporcionar al Tribunal Supremo Electoral toda la información necesaria para la inscripción de las personas en el Registro Electoral	• Encargado de la autenticación de los votantes. • Verificar si el votante ya ha ejercido su sufragio. • Creación de token de sesión.
TSE	• Convocar, organizar, dirigir y vigilar los procesos electorales. • Practicar el escrutinio preliminar y definitivo. • Impartir las instrucciones necesarias para el normal funcionamiento de todos los organismos electorales	• Almacenamiento y custodia de los votos emitidos por los ciudadanos para su respectivo escrutinio. • Gestión de las llaves pública y privada de cada una de las JRV's
JRV	• Representa al TSE. • Como autoridad electoral es la encargada de facilitar el derecho al voto a la ciudadanía y realizar el escrutinio de mesa	• Sirve de intermediario entre el votante y el RNPN en el proceso de autenticación. • Genera la boleta electrónica y activa la urna

es también la encargada del envio del voto al TSE, siendo este último el responsable del resguardo de los votos para su posterior conteo.

En la Fig. 6 se muestra la distribución de los servicios; es de vital importancia que se garantice la independencia entre las instituciones e incluso entre los servidores dentro de la misma institución, las funciones se describen en la Tabla II. El servidor de aplicaciones del RNPN no debe intercambiar más información de la necesaria con el servidor de bases de datos de la misma institución. Así como se debe mantener la independencia en las funciones: el servidor de aplicaciones no debe almacenar datos del ciudadano, y el servidor de bases de datos no debe contener información de los procesos de cifrado.

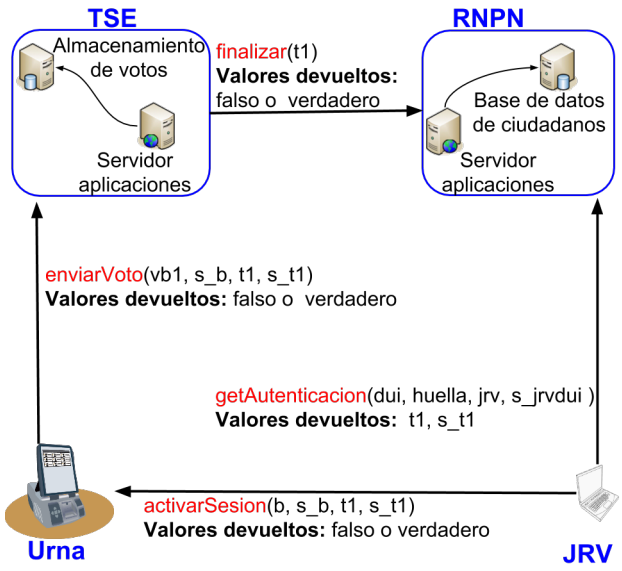

Fig. 6. Distribución de servicios

A. *Autenticación*

El objetivo de esta fase es validar que el elector está apto para emitir el sufragio verificando que se encuentra en el padrón electoral y que no ha emitido su voto. Los pasos son los siguientes:

1) El elector se presenta a la Junta Receptora de Votos, proporciona su Documento Único de Identidad
2) Un miembro de la mesa ingresa el número de documento y pide al votante ingrese su huella digital.
3) Si el votante tiene algún impedimento para ingresar su huella, se valida la identidad mediante la comparación del documento, con los datos del servidor de autenticación, y para aceptar esta validación todos los miembros de la mesa ingresan su huella digital.
4) Se envía al servidor de autenticación: #DUI, huella digital, número de Junta Receptora de Votos.
5) Si los datos son válidos el servidor del RNPN crea un token de sesión, el cual cifra y firma.

La Fig. 7 muestra las operaciones criptográficas realizadas en esta fase.

B. *Emisión del Sufragio*

En esta fase, el elector selecciona las opciones de su sufragio, y se debe garantizar la seguridad de los

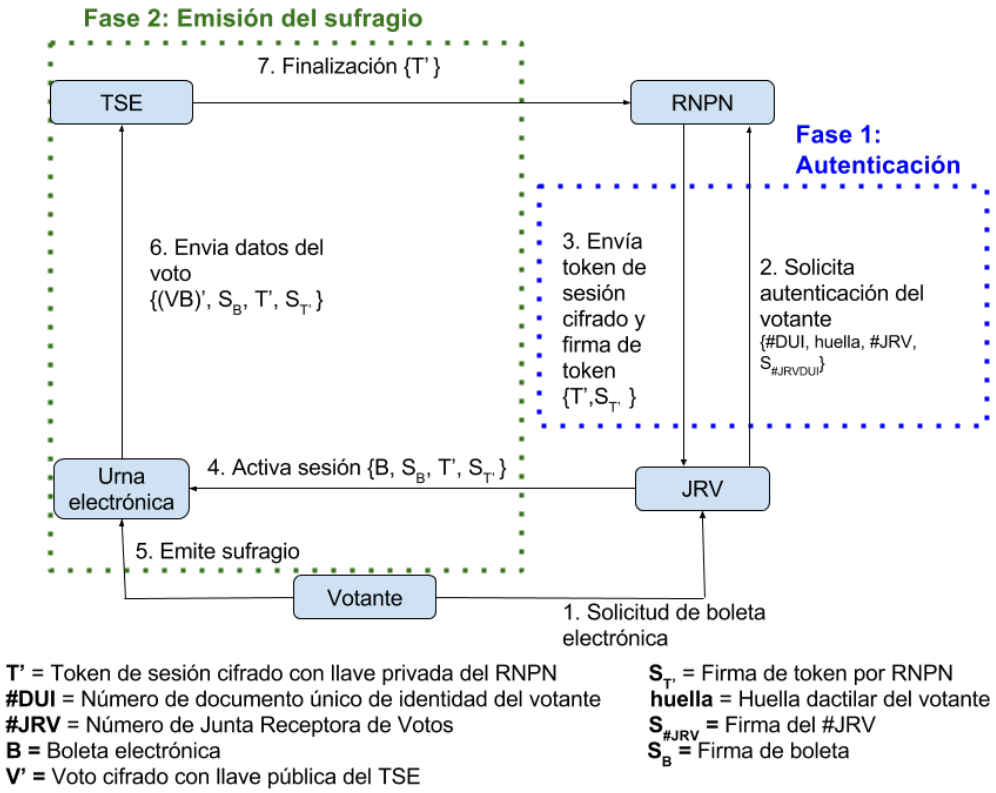

Fig. 5. Esquema de votación propuesto

datos contenidos en esta fase.

1) Con el token de sesión proporcionado por el RNPN, la JRV crea una boleta electrónica en blanco, la firma y se activa la urna electrónica, para lo cual la urna recibe el token de sesión y la boleta en blanco firmada. Esta boleta consta de un número correlativo de boleta, el número de la JRV la fecha y hora de generación.
2) El elector escoge sus opciones de votación. Alternativamente puede cargar un paquete de opciones, para lo cual debe proporcionar el identificador del paquete.
3) Cuando se finaliza la selección de opciones, se cifra la boleta conteniendo el voto emitido, y la urna cifra con la llave pública del TSE.
4) Se envía la boleta firmada y cifrada y el token de sesión al servidor del TSE.
5) El TSE recibe la boleta, la descifra y verifica firma de JRV, verifica que no se haya registrado el voto con ese token, de lo contrario el voto no se toma en cuenta. Si es correcto toma el voto para el conteo y envía el token de sesión al servidor del RNPN.
6) El RNPN recibe el token de sesión, descifra el token y marca que el elector ya emitió el sufragio.

La Fig. 8 muestra las operaciones criptográficas realizadas en la fase de emisión del sufragio

C. *Paquetes de Opciones de Voto*

Una de las dificultades del voto cruzado, implementado en las elecciones 2015 en El Salvador, es el tiempo que puede tardar un votante para elegir todas las opciones, por ejemplo para el caso del departamento de San Salvador el votante puede elegir hasta 20 candidatos para diputados de la Asamblea Legislativa. Se propone un mecanismo para crear de manera previa, paquetes de opciones de voto, el cuál funcionará a través de internet y estará disponible varios días antes del día de las votaciones.

El elector se conectará al servidor del TSE y podrá realizar la elección de sus candidatos, para lo cual podrá tomarse el tiempo que crea conveniente, al finalizar se le proporcionará un código, similar al NPE de los recibos de servicios, y el día de las

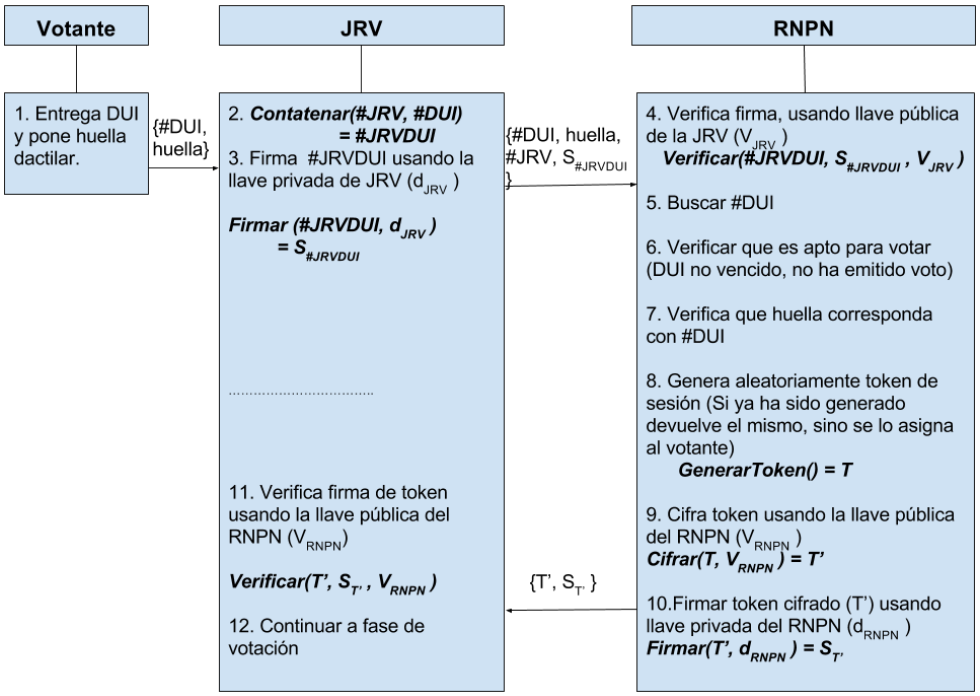

Fig. 7. Proceso de autenticación

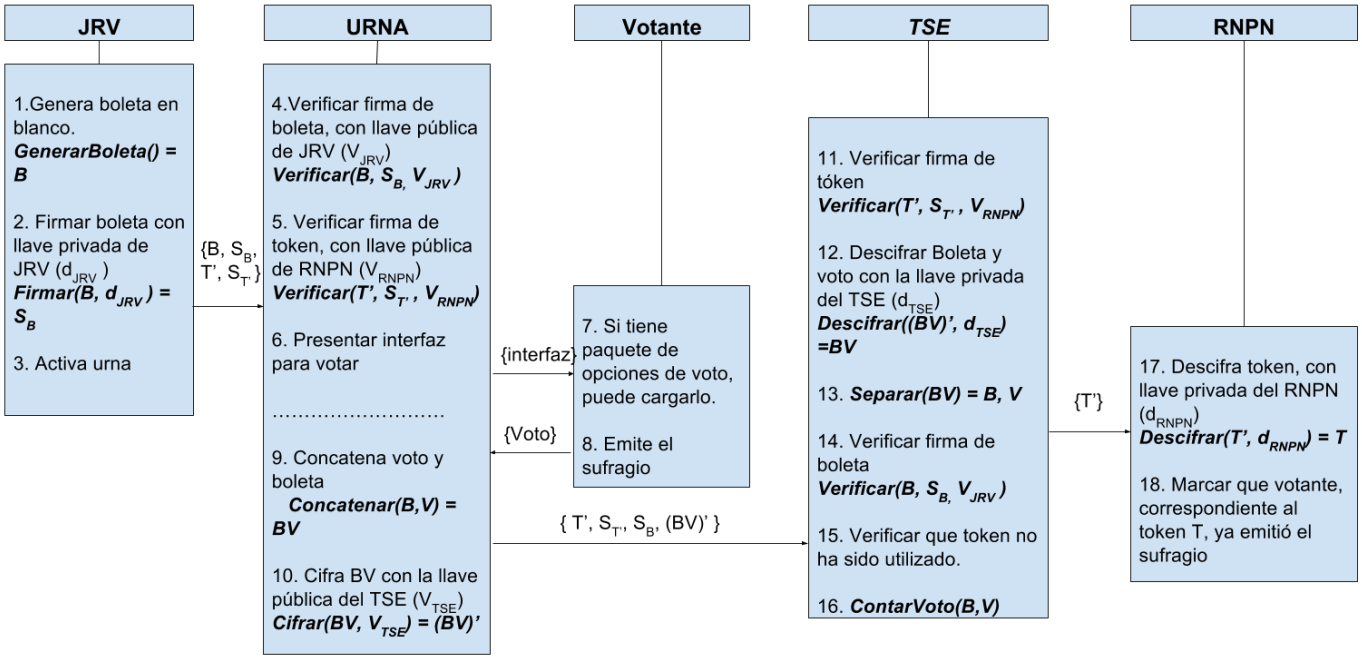

Fig. 8. Emisión del voto

votaciones podrá utilizar dicho código para cargar las opciones elegidas y agilizar el proceso.

Es importante destacar que un ciudadano no se identificará en ningún momento para crear un paquete de opciones de voto, incluso puede crear muchos paquetes pero podrá elegir solamente uno el día de la votación.

VI. ANÁLISIS DE SEGURIDAD

El voto electrónico puede ser tan seguro o incluso más seguro que el voto tradicional en papel siempre y cuando se implanten las medidas de

TABLA II
RESPONSABILIDADES DE LOS SERVICIOS

Servicio	Responsabilidad
JRV	Captura los datos del votante, DUI y huella. Genera la boleta electrónica y activa la sesión de la urna
Servidor de aplicaciones RNPN	Realiza las operaciones criptográficas: verificar firma de JRV, cifrado y firmado de token
Servidor de bases de datos de ciudadanos	Realiza la búsqueda de datos del ciudadano, verificando que sea apto para votar y genera el token de sesion
Urna electrónica	Interfaz con la que interactúa el votante para emitir su voto, se realiza las operaciones de verificación de firmas y cifrado del voto con la llave pública del TSE
Servidor de aplicaciones TSE	Verifica firmas y descifra el voto, envía el voto al servidor de almacenamiento de votos
Servidor de almacenamiento de votos	Almacena el voto para el proceso de conteo

seguridad adecuadas. Las medidas de seguridad convencionales tales como firewalls o comunicación SSL son necesarias pero no suficientes para garantizar los requisitos de seguridad específicos del voto electrónico. Además de estas medidas de seguridad convencionales, es necesario implementar también una capa seguridad especializada para hacer frente a los riesgos específicos planteados por el voto electrónico y garantizar así el cumplimiento de los requisitos imprescindibles en cualquier elección tales como la privacidad del votante, la integridad del voto y la posibilidad de verificación del correcto tratamiento del voto por parte de los votantes.

A continuación se presenta un listado de los posibles ataques que puede sufrir un sistema de voto electrónico y de las soluciones que el protocolo propuesto presenta para evitarlo.

A. Ataques

- **Suplantación de identidad**: También conocido como Robo de Identidad, consiste en hacerse pasar por otra persona para la realización de actividades en nombre de la víctima, en el caso de las votaciones electrónicas es utilizado para que una persona pueda emitir el sufragio en nombre de otras personas.
- **Ataque al anonimato del voto**: Consiste en que alguna entidad está escuchando el tráfico e interceptando paquetes con el fin de poder descifrar la información sobre la identidad de los ciudadanos y conocer el voto que éstos emitieron.
- **Alteración de Voto**: Este ataque consiste en la intercepción de los paquetes para alterar el voto emitido durante el proceso de votación de un ciudadano.
- **Generación de votos falsos**: Consiste en el envío de votos falsos generados desde entidades externas (que no es una JRV) para afectar los resultados a favor o en contra de los candidatos en contienda.
- **Doble voto**: Este ataque consiste en una entidad válida para emitir votos y este lograr votar más de una vez en distintos lugares, por ejemplo cuando un ciudadano está sirviendo en una mesa receptora de votos ya sea como vigilante o miembro de la mesa (JRV) los cuales están obligados a votar en esa misma mesa (JRV), pero estos votan y luego intentan votar en la JRV que les corresponde como ciudadanos (y no como miembros de la JRV o vigilantes).
- **Generación de votos después del periodo**: Este ataque consiste en emitir votos después de la hora de cierre de las elecciones establecidas previamente por el Tribunal Supremo Electoral (TSE).

B. Soluciones

- **Suplantación de identidad**: Para evitar este ataque, el protocolo propuesto utiliza un proceso de validación, el cual consiste en la autentificación de múltiples factores como número de identidad personal y la huella digital del ciudadano, los cuales son almacenados en una base de datos en el momento que la persona se convierte en mayor de edad.
- **Ataque al anonimato del voto**: El anonimato es uno de los requisitos fundamentales del

voto electrónico pero a la vez debe ser posible evitar que un elector emita doble voto. En el protocolo propuesto se hace uso de un token para el proceso del sufragio y control de que la persona ha votado. El token está cifrado con la llave pública del RNPN para que sólo esta institución pueda hacer la relación entre el votante y su token pero en ningún momento el RNPN conoce información del voto emitido; es importante que cuando el protocolo sea implementado se verifique que cada institución realice sólo las acciones que le están permitidas y que almacena sólo la información que le concierne. Dentro del RNPN deben estar separadas las funciones de generación y almacenamiento del token con la firma y cifrado de este. El servidor de aplicaciones del RNPN puede conocer el valor plano del token, pero no a qué persona pertenece; de igual forma el servidor de base de datos de ciudadanos, no podrá generar el token cifrado para asociar el voto emitido por las personas. Además, para evitar que se vote más de una vez, si un elector ya tiene un token generado e intenta votar nuevamente se le devuelve el mismo token para que cuando llegue cifrado al TSE, no se cuente porque ese token ya ha sido utilizado.

- **Alteración de voto**: El voto será enviado cifrado con la llave pública del TSE garantizando con esto que sólo el TSE puede descifrarlo. Otra medida tomada en cuenta consiste en la impresión de un comprobante el cual contiene el voto del ciudadano (sin la información del ciudadano), esto para hacer verificaciones en urnas seleccionadas como muestras para corroborar los datos de los votos enviados contra los existentes en los comprobantes en papel.

- **Generación de votos falsos**: Para evitar este tipo de ataques, el protocolo criptográfico propuesto utilizará la firma electrónica para validar el envío de un voto, además esta información será enviada de manera cifrada. Otra de las características con las que debe contar para evitar votos falsos será que los votos estarán relacionados con un número de token único que se almacenará con el mismo para poder auditar cada voto, ya que este token estará firmado por el RNPN evitando que otra entidad pueda suplantarlo y generar dicho token.

- **Doble voto**: Un elector puede emitir solamente un voto válido, el token asignado asegura que si intentara votar más de una vez y por alguna razón aún no se haya marcado que ha emitido su voto, se devuelve el mismo token que ya tiene generado, de esta forma al llegar varios votos al TSE con el mismo token solamente se tomará el primero.

- **Generación de votos después del periodo**: Para evitar este tipo de ataques el protocolo criptográfico contemplará que la boleta electrónica contenga la fecha y hora de generación.

- **Evitar engaño del votante**:Las máquinas de voto electrónico proveerán una realimentación inmediata al votante que detecta problemas posibles tales como votar por defecto o votar por exceso, que pueden resultar en la anulación del voto. Esta realimentación inmediata puede ser de ayuda para determinar exitosamente el engaño del votante, uno de los principales casos tomados en cuenta es la retroalimentación del voto brindándole un ticket donde el votante pueda aceptar o denegar de tal manera que el votante no será marcado como voto emitido y permitiéndole volver intentar realizar la votación hasta que el este se encuentre conforme con el resultado del mismo.

- **Auditorías**: Un desafío fundamental para cualquier sistema de votación electrónica es asegurar que los votos fueron registrados como fueron emitidos y escrutados. Esto se soluciona mediante un sistema de auditoría independiente, denominado comúnmente **Verificación Independiente**, que también se puede usar para recuentos o auditorías. Estos sistemas pueden incluir la posibilidad de que los votantes verifiquen cómo han sido emitidos sus votos o más adelante, verificar si el recuento de los votos fue correcto. Se pueden usar muchas tecnologías

para asegurar a los votantes que su voto fue emitido correctamente o detectar el fraude o el mal funcionamiento, y proveer los medios para auditar la máquina original. Algunos sistemas incluyen tecnologías tales como la criptografía (visual o matemática), el papel, (conservado por el votante o sólo verificado), verificación auditiva y registros dobles o sistemas testimoniales (distintos del papel), para tal caso en el protocolo se propone la impresión de comprobante en papel que el usuario depositará en urnas y estos servirán para realizar auditorías.

VII. RECOMENDACIONES

La implementación del protocolo está fuera del alcance de esta investigación, a pesar de ello se hacen las siguientes recomendaciones a tomar en cuenta.

- **Del software:** el software utilizado en todas las funciones involucradas en el protocolo de voto electrónico propuesto, debe ser completamente auditable, es decir, todos los partidos políticos, ciudadanos, Tribunal Supremo Electoral pueden verificar su integridad en cada fase, antes de iniciar el proceso electoral y al finalizar el proceso de votaciones, además de ser transparente, seguro y exacto eliminando el margen de error humano.

- **Uso del protocolo https**: se sugiere implementar el protocolo de voto electrónico usando internet sobre un protocolo HTTPS como medio de comunicación segura entre RNPN, TSE, JRV y la urna electrónica. Según [10], el protocolo Secure Socket Layer (SSL) facilita la autenticación y privacidad de la información en internet mediante el uso de la criptografía. Sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar, ya que la autenticación mutua requiere un despliegue de infraestructura de llaves públicas para los clientes. En este caso, se libera al elector de usar las llaves tanto privada como pública, para facilitar la emisión del voto.
  Es importante mencionar que SSL se ejecuta para los protocolos de aplicación como el HTTP (Hypertext Transfer Protocol), proporcionando un intercambio de datos seguros para proteger las páginas World Wide Web (www) en transacciones electrónicas. Debido a lo anterior, el protocolo SSL en HTTP, visto como HTTPS es muy útil para transmitir el voto a través de la red como un primer nivel de seguridad.

- **Uso de software de intercambio orientado a mensajería (MOM)**: para la implementación del protocolo propuesto en este artículo se sugiere como alternativa a los servicios web la utilización un sistema de mensajería, por ser éstos más tolerables a fallos (característica muy deseable en el envío del voto a los servidores del TSE).
  Actualmente, los MOM (Message Oriented Middleware) desempeñan un papel importante en la generación e intercambio de datos financieros [11]. La utilización de un MOM dentro de la implementación del protocolo permitirá una comunicación eficiente entre elementos heterógeos (aplicaciones, sistemas operativos e incluso redes) existentes dentro de las instituciones involucradas en el proceso electoral.
  En [12] se describe el protocolo avanzado de espera de mensajes (del inglés AMQP) como un estándar abierto para la comunicación del protocolo de votación electrónica a través de un MOM.
  Sus principales características son:

  Seguridad: Proporciona una infraestructura para una red con transacciones seguras y de confianza. Soporta la perdurabilidad de los mensajes independientemente de la conexión de los receptores. La entrega de mensajes es resistente a fallos técnicos que pueden ocurrir durante el evento electoral. Por ejemplo: En caso de una interrupción en la conexión entre la urna electrónica y el servidor del TSE, los votos se almacenan en forma de mensajes en la urna y son enviados cuando la conexión sea restablecida.
  Confiable: Capaz de eliminar las brechas y retrasos de diferentes plataformas,

sistemas y componentes críticos de aplicaciones, tanto dentro como fuera de las instituciones involucradas en el proceso electoral. Garantiza la entrega de los mensajes de los votos, implementando una semántica que abarca: al menos una vez, a lo sumo una vez y sólo una vez, conocido como entrega fiable; con lo cual cada voto se envía y se recibe una sóla vez.

- **Seguridad en la comunicación**: asegurar el medio de comunicación en que se enviarán los datos del protocolo de votaciones electrónicas propuesto, es un aspecto fundamental para el correcto funcionamiento de éste, se propone que la comunicación se haga a través de internet asegurando además del uso del protocolo https propuesto anteriormente, el uso de VPN's y túneles IPSec.
  Según [18] IPsec es un estándar que proporciona cifrado y autentificación a los paquetes IP, trabajando en la capa de red. En lugar de tratarse de un único protocolo, IPsec es en realidad un conjunto de protocolos, definidos en diversos RFCs (principalmente en el 2401), encaminados a proporcionar autentificación, confidencialidad e integridad a las comunicaciones IP.
  IPsec debe ser utilizado para proteger las rutas de comunicación entre las instituciones involucradas en las votaciones eletrónicas. Con este conjunto de protocolos que cifra todo el tráfico IP antes de que los paquetes se transfieran desde el nodo de origen hasta el destino (por ejemplo desde la urna electrónica al TSE). IPsec, además, es capaz y responsable de autenticar la identidad de los dos nodos antes se establezca la comunicación real entre ellos, con esto se garantiza que no se agregue ninguna entidad no autorizada en el intercambio de paquetes de datos entre JRV, TSE, RNPN y la urna electrónica.
  Con la utilización de IPSec dentro del protocolo de votaciones electrónicas propuesto, como se muestra en la Fig. 9, se fortalecen los siguientes elementos de seguridad:
  1) Autenticación del origen de los datos: verificar que los datos recibidos han sido enviados por la entidad correspondiente.
  2) Integridad de los datos: verificar que los datos de los votos recibidos no han sido modificados por el camino. Se suele emplear el término autenticación de datos para indicar tanto la integridad de los datos como la autenticación de su origen.
  3) Confidencialidad de los datos: ocultar los datos utilizando un algoritmo de cifrado.
  4) Protección tipo Anti-Replica: evitar que un intruso reenvíe alguno de los mensajes con datos de un voto y no se pueda detectar.

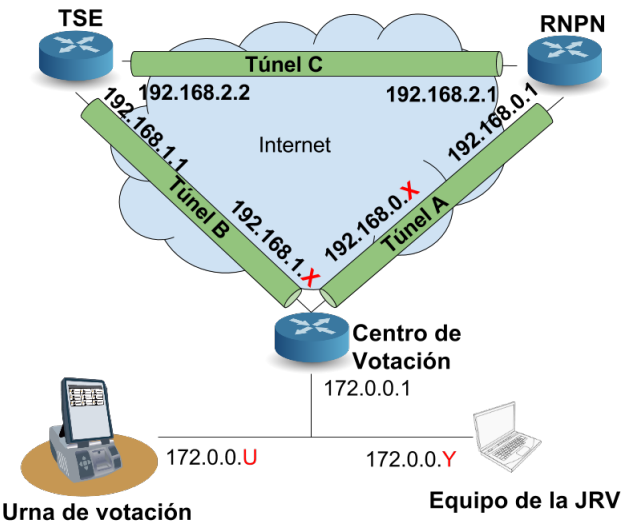

Fig. 9. Propuesta de red de comunicación segura

VIII. DISCUSIÓN

En este artículo se fundamentan las bases criptográficas para la creación de un sistema de votación electrónica, cumpliendo los requisitos de seguridad que actualmente son utilizados. Sin embargo, para que las votaciones electrónicas sean una realidad, se necesita trabajar en las siguientes áreas:

- Diseño del software y hardware específico de la urna electrónica. Se parte de que la urna entrega la selección del votante para luego ser tomado por el protocolo para aplicar las técnicas criptográficas.
- Sistema de conteo de votos. Dentro del diseño del protocolo propuesto se llega hasta la

verificación de la validez del voto recibido para ser enviado al sistema de conteo, las reglas específicas para realizarlo deben ser acordes a la realidad y constantes cambios de cada proceso electoral.

- Uso de software y hardware para la identificación de los votantes mediante la huella dactilar. El Tribunal Supremo Electoral debe adquirir los dispositivos para la lectura de las huellas de los votantes y el RNPN será el responsable de implementar los mecanismos que permitan identificar a cada persona mediante las huellas capturadas. En este protocolo se considera que se cuentan con los dispositivos necesarios para realizar este proceso de identificación.
- Las configuraciones de infraestructuras tales como servidores, dispositivos pasivos y activos de una red.
- Elaboración de planes de contingencia y recuperación de desastres.

IX. CONCLUSIONES

En este artículo se presentó un protocolo de voto electrónico basado en firmas digitales y cifrado RSA, aplicable a los procesos electorales de El Salvador, que contribuya a la transparencia, eficiencia y el fortalecimiento de la democracia.

Se analizó la experiencia de la utilización de distintos protocolos de voto electrónico implementados en diferentes países, para diseñar un protocolo que cumple con todos los fundamentos criptográficos necesarios para garantizar la disponibilidad, confidencialidad e integridad de la información de los procesos electorales.

Con los resultados obtenidos podemos determinar que el protocolo de voto electrónico servirá de guía para el desarrollo de un sistema automatizado que permita: agilizar y facilitar el proceso electoral, eliminar el error humano en el conteo de los votos, mejorar los procesos de publicación de resultados y evitar votos impugnados, entre otros beneficios. Considerando el uso de la firma electrónica como un método factible para la verificación de la autenticidad e integridad de la información enviada entre cada entidad y las funciones de cifrado para proteger la confidencialidad del voto. Logrando con esto, alcanzar las fortalezas del uso del voto electrónico, mitigando las debilidades del mismo.

Finalmente, es de destacar que la principal problemática al diseñar el protocolo propuesto, fue el cumplimiento de todos los requisitos de seguridad y a la vez no crear un proceso complejo para los votantes; es decir, garantizar la validez del voto y que sea fácil la emisión del sufragio. Con la realización del análisis de seguridad del protocolo de voto electrónico propuesto podemos concluir que se tomaron en consideración los diferentes tipos de ataques que pueden ocurrir durante el proceso electoral como: suplantación de identidad, ataque al anonimato del voto, alteración del voto, generación de votos falsos, doble voto, generación de votos después del periodo electoral, y que se han propuesto soluciones para mitigar cada uno de estos ataques.

REFERENCIAS

[1] Wolf, P.(2011) Una Introducción al Voto Electrónico: Consideraciones Esenciales. *Instituto Internacional para la Democracia y la Asistencia Electoral (IDEA)*, 9-10.

[2] Prince, A., Jolías, L., & UBA, F. L.(2012) Voto Electrónico: Experiencias y Tendencias en Argentina, 9.

[3] Panizo Alonso, L.(2007) Aspectos Tecnológicos del Voto Electrónico, 13-29.

[4] López García, M. L. (2011) Diseño de un Protocolo para Votaciones Electrónicas Basado en firmas a ciegas definidas sobre emparejamientos bilineales (Tesis doctoral). Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, Distrito Federal, México, 75-92.

[5] Chacón Zárate, A. (2010). Comparativa de Seguridad de Algoritmos para Resúmenes Criptográficos (Tesis de especialización). Escuela Superior de Ingeniería Mecánica y Eléctrica, Distrito Federal, México, 9-10.

[6] Ochoa Jiménez, J. E. (2013). Función Picadillo Determinista al Grupo G_2 y su Aplicación en Autenticación para Dispositivos Móviles (Tesis de maestría). Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, Distrito Federal, México, 27.

[7] Pérez, L. S. C (2012). Factorización de Enteros (Tesis de maestría). Universidad Autónoma Metropolitana - Iztapalapa, Distrito Federal, México, 8.

[8] Alcaraz, C., Roman, R., y López, J. (2007) Análisis de Primitivas Criptográficas para Redes de Sensores, 3.

[9] Paredes, G. G. (2006). Introducción a la Criptografía. Revista Digital Universitaria, 7-9.

[10] Fonseca, D. S., Pérez, W. R., y Faurés, M. L. M. (2013). Pasarela de Pagos para la Seguridad de Transacciones Bancarias en Línea, 7.

[11] Marsh, G., Sampat, A. P., Potluri, S., y Panda, D. K. (2008). Scaling Advanced Message Queuing Protocol (AMQP) Architecture with Broker Federation and InfiniBand. Ohio State University, Tech. Rep. OSU-CISRC-5/09-TR17.

[12] Pérez, J. R., Muño, M. G., Pérez, H., y Baranda, I. M. D. M. Sistema de Notificaciones para la Plataforma de Desarrollo de Integración Continua de la distribución cubana de GNU/Linux, Nova. Notification System for Development Platforms of Continuous Integration inside the Cuban Distribution.

[13] La Prensa Gráfica. (2014), Proceso para emitir el voto. Recuperado de http://mediacenter.laprensagrafca.com/infografas/i/pasospara-votar
[14] Tribunal Supremo Electoral (2015). Instructivo elecciones. Recuperado de www.tse.gob.sv/documentos/Elecciones%202012/InstructivoJRV.pdf
[15] Ley de Creación del Registro Nacional de Personas Naturales. Diario Oficial Nº 227 tomo Nº 329 de la República de El Salvador, San Salvador, El Salvador, 20 de abril de 2012.
[16] Código Electoral. Diario Oficial Nº 138 tomo Nº 400 de la República de El Salvador, San Salvador, El Salvador, 22 de julio de 2015.
[17] Ley de Firma Electrónica. Diario Oficial Nº 196 tomo Nº 409 de la República de El Salvador, San Salvador, El Salvador, 21 de octubre de 2015.
[18] Lucena López, M. J.(2010) *Criptografía y Seguridad en Computadores*, 182.
[19] Santos, J. C. (2000). Seguridad y alta disponibilidad. RA-MA Editorial. 115.
[20] Stallings, W. (2004). Fundamentos de seguridad en redes: aplicaciones y estándares. Pearson Educación.73-74.
[21] Domingo, J. I. F. (2006). La firma electrónica: Aspectos de la Ley 59/2003, de 19 de diciembre. Editorial Reus. 38.