MODELO DE SEGURIDAD DE LA INFORMACIÓN EN EL USO DE TECNOLOGÍAS DE VOTACIÓN ELECTRÓNICA DE REGISTRO DIRECTO

CARLOS ANTONIO MORALES PINILLA
ELSA CATALINA SAAVEDRA RODRÍGUEZ
SERGIO ANDRÉS GÓMEZ CARVAJAL

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICO-MECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
BUCARAMANGA
2010

MODELO DE SEGURIDAD DE LA INFORMACIÓN EN EL USO DE TECNOLOGÍAS DE VOTACIÓN ELECTRÓNICA DE REGISTRO DIRECTO

CARLOS ANTONIO MORALES PINILLA
ELSA CATALINA SAAVEDRA RODRÍGUEZ

Trabajo de Grado presentado como requisito para optar el título de Ingeniero Electrónico

SERGIO ANDRÉS GÓMEZ CARVAJAL

Trabajo de Grado presentado como requisito para optar el título de Ingeniero Electricista

Director
Ing. SERGIO ENRIQUE MÉNDEZ ACEROS
Codirector
Dr. RICARDO LLAMOSA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICO-MECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
BUCARAMANGA
2010

TABLA DE CONTENIDO

Pág

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

Pág

LISTA DE ANEXOS

Pág

RESUMEN

TÍTULO: MODELO DE SEGURIDAD DE LA INFORMACIÓN EN EL USO DE TECNOLOGÍAS DE VOTACIÓN ELECTRÓNICA DE REGISTRO DIRECTO.[1]

Autores: Carlos Antonio Morales Pinilla, Elsa Catalina Saavedra Rodríguez, Sergio Andrés Gómez Carvajal. [2]

Palabras claves: DRE, análisis de riesgos, SysML, Voto electrónico.

En este artículo se presenta un modelo prototipo de seguridad de la información para sistemas de votación que usan tecnologías de votación electrónica de registro directo, el cual pretende ser un apoyo para el proceso de modernización de los sistemas electorales en la etapa de votación y de esta forma contribuir a la disminución riesgos asociados al proceso electoral. La seguridad de la información en sistemas de voto electrónico no sólo depende del protocolo de votación o software utilizado, concierne a todo el sistema con cada uno de los elementos que lo componen. La seguridad de un sistema electoral no puede ser garantizada a menos que sean examinados, cada elemento y característica de seguridad relacionada, la interconexión con otros elementos y su impacto en todo el sistema. Este artículo presenta un modelo de seguridad de información desarrollado a través del lenguaje de modelado de sistemas SysML, por medio de diagramas de casos de uso y diagramas de jerarquía de herencia para las respectivas clases y actores que conforman el sistema. Este modelo está basado en un análisis parcial de riesgos con base en el estándar de gestión de riesgos AS/NZS 4360:2004, llevado a cabo en el subsistema de votación electoral *in-situ* al implementar tecnologías de votación electrónica de registro directo (DRE), para el sistema electoral colombiano, obteniendo amenazas, consecuencias, puntos críticos y controles de tipo preventivo, mitigativo y de contingencia. Este modelo es creado con el fin de mejorar la seguridad del sistema a través de la seguridad de la información con un enfoque integral del sistema.

[1] Trabajo de grado desarrollado en la modalidad de investigación

[2] Facultad de Ingenierías Fisicomecánicas, Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones. Director: Sergio Enrique Méndez Aceros. Codirector: Ricardo Llamosa.

ABSTRACT

TITLE: MODELO DE SEGURIDAD DE LA INFORMACIÓN EN EL USO DE TECNOLOGÍAS DE VOTACIÓN ELECTRÓNICA DE REGISTRO DIRECTO.[3]

Authors: Carlos Antonio Morales Pinilla, Elsa Catalina Saavedra Rodríguez, Sergio Andrés Gómez Carvajal. [4]

Keywords: DRE, Electronic Voting, Risk Analysis, SysML.

This article presents an information security prototype model for voting systems that use direct recording electronic voting technologies, which pretends to be a support for the modernization process of electoral systems on votation phase, and int his way contribute to lower risks associated with the electoral process. Information security on electronic voting systems depends not only on votation protocol or used software; it concerns to the whole system, which includes each one of its elements **parts.** The security of an electoral system can not be guaranteed unless you examined each element and each related security characteristic, interconnection between elements and its impact on the whole system. This paper presents an information security model, developed through systems modeling language SysML**,** through use case diagrams and inheritance hierarchy diagrams for the respective classes **and stakeholders in the system. This model is** based on a **partial** risk analisys **based on risk management standard AS / NZS 4360:2004, performed** in the electoral votation sub-system "*in-situ*" when direct recording electronic (DRE) votation technology is implemented for the Colombian Electoral system, obtaining threats, consequences, critic spots and **preventive, mitigative and contingency** controls. This model is created with the purpose to improve the system security through information security from a holistic system point of view.

[3] Final undergraduate Project developed in the research modality

[4] Physics-Mechanics Engineering Faculty. School of Electrical, Electronic and Telecomunications Engineering. Director: Sergio Enrique Méndez Aceros. Codirector: Ricardo Llamosa.

donde el fraude

Modelo de seguridad de la información en el uso de tecnologías de votación electrónica de Registro Directo

Carlos Antonio Morales Pinilla
carlos.morales@correo.uis.edu.co
Universidad Industrial de Santander
Centro de Innovación y Desarrollo para la Investigación en Ingeniería del Software – CIDLIS.
Bucaramanga, Colombia.

Elsa Catalina Saavedra Rodríguez
elsa.saavedra@correo.uis.edu.co
Universidad Industrial de Santander
Centro de Innovación y Desarrollo para la Investigación en Ingeniería del Software – CIDLIS.
Bucaramanga, Colombia.

Sergio Andrés Gómez Carvajal
sergio.gomez@correo.uis.edu.co
Universidad Industrial de Santander
Centro de Innovación y Desarrollo para la Investigación en Ingeniería del Software – CIDLIS.
Bucaramanga, Colombia.

Abstract— Information security on electronic voting systems depends not only on votation protocol or used software; it concerns to the whole system, which includes each one of its elements. The security of an electoral system can not be guaranteed unless you examined each element and each related security characteristic, interconnection between elements and its impact on the whole system. This paper presents an information security model, developed through SysML language, based on a risk analisys performed in the electoral votation sub-system "*in-situ*" when direct recording electronic (DRE) votation technology is implemented for the Colombian Electoral system, obtaining threats, consequences, critic spots and controls. This model is created with the purpose to guarantee the system security through information security from a holistic system point of view.

***Keywords*— DRE, Electronic Voting, Risk Analysis, SysML.**

Resumen— La seguridad de la información en sistemas de voto electrónico no sólo depende del protocolo de votación o software utilizado, concierne a todo el sistema con cada uno de sus elementos. La seguridad de un sistema electoral no puede ser garantizada a menos que sean examinados, cada elemento y característica de seguridad relacionada, la interconexión con otros elementos y su impacto en todo el sistema. Este artículo presenta un modelo de seguridad de información desarrollado a través del lenguaje SysML, el cual está basado en un análisis de riesgos llevado a cabo en el subsistema de votación electoral *in-situ* al implementar tecnologías de votación electrónica de registro directo (DRE), para el sistema electoral Colombiano, obteniendo amenazas, consecuencias, puntos críticos y controles del mismo. Este modelo es creado con el fin de garantizar la seguridad del sistema a través de la seguridad de la información con un enfoque integral del sistema.

***Palabras Claves*— DRE, análisis de riesgos, SysML, Voto electrónico.**

I. INTRODUCCIÓN

El voto tradicional ha sido un tema muy controversial desde el siglo XIX, cuando surgen las primeras elecciones de votación popular o democracia directa, electoral ha sido práctica recurrente asociada al clientelismo político como lo ha señalado el historiador David Bushnell[5]. Una larga tradición de fraudes electorales ha estado presente durante el uso de este tipo de votación, en la que la claridad de las elecciones siempre ha estado en cuestión. Irregularidades en el registro electoral, depósito de papeletas, abusos en los escrutinios, control ilegítimo de la organización electoral (*"el que escruta elige"*), compra de votos, son algunas de las modalidades que han hecho parte en los procesos electorales desarrollados a lo largo de estos años, consolidando un verdadero repertorio de coerción al elector. A pesar de la existencia de leyes y normas que castigan penalmente a los responsables de estas conductas e infinidad de medidas que se expiden en cada evento de participación electoral con el propósito de contrarrestar la práctica del fraude, estos sucesos no dejan de hacer parte de cada una de las votaciones desarrolladas. A partir de esto y de diversos argumentos que han sido esgrimidos a favor del voto electrónico[6], muchos países, algunos de ellos con culturas similares a la realidad colombiana, han optado por implementar y adoptar nuevas tecnologías de votación, donde se han utilizado diferentes tipos de sistemas, como el de voto electrónico en papel, votación por Internet y sistemas de registro directo (DRE[7]), siendo este último el que más se ha puesto en marcha en varios países alrededor del mundo. No obstante, para muchos países en los que se han llevado a cabo procesos de votación electrónica, la adopción de la misma ha llegado a ser más un modernismo que una cuestión útil o necesaria. Experiencias realizadas con diversos mecanismos, han despertado dudas acerca de la seguridad de los sistemas y

[5] Máster y Doctor en Historia, Universidad de Harvard. Profesor, Universidad de Florida, Gainesville. Miembro Correspondiente, Academia colombiana de Historia.

[6] Es una forma de voto, en el cual los votantes realizan su selección con la ayuda de un computador. Ver Referencias [4][11][14]

[7] Direct Recording Electronic, Por sus siglas en ingles DRE utilizado para referirse a Votación Electrónica de Registro Directo. Ver Referencia [8][11][14].

la posible manipulación de datos. Es por ello que se ha planteado un modelo, con el propósito de que las personas encargadas de implementar el sistema de votación electrónica sigan un esquema del cual se logre despejar todo tipo de dudas acerca de la confiabilidad, seguridad y transparencia del mismo.

En esta investigación se realizó una comparación del proceso de votación tradicional frente al de voto electrónico, encontrando similitudes y diferencias, además se destacan las potenciales ventajas y desventajas de cada uno, con el fin de encontrar posibles amenazas que pudieran permanecer aún al implementar este nuevo proceso o que solamente llegaran a afectar al sistema de voto electrónico. A partir de la comparación de los dos procesos se logran identificar amenazas al subsistema en estudio, además de aquellas derivadas de la misma tecnología implementada, y con base en esto se procedió a efectuar un análisis de riesgos, el cual ha sido desarrollado siguiendo el estándar de seguridad de la información AS/NZS 4360:2004[8]. Este análisis se ha enfocado en el sistema de votación electrónica de registro directo (DRE), teniendo en cuenta experiencias en los procesos de votación de países socioculturalmente similares a Colombia, las cuales apuntan a que este sistema es el más viable y confiable por su grado de desarrollo tecnológico dejando a un lado sistemas de votación electrónica en papel, y sistemas de votación por internet debido a la presión por parte de grupos armados y otros actores que podrían ejercer coerción al elector.

Una vez establecido el sistema a utilizar, se lograron establecer amenazas, consecuencias, puntos críticos y controles del subsistema de votación electrónica *in-situ*[9]. Habiéndose revisado la comparación y definido los riesgos a los que se expone el sistema, se procedió a plantear el modelo prototipo de seguridad de la información utilizando el lenguaje de modelado de sistemas SysML[10].

Previamente se han realizado diferentes modelos basados en análisis de riesgos [3], enfocados hacia la máquina de votación, sin embargo hasta el momento no se ha planteado ningún análisis que haga referencia directa al subsistema de votación electrónica *in-situ*, el cual es el objeto de este estudio. Adicionalmente este trabajo derivará en exponer el modelo nunca antes propuesto en este proceso, utilizando el lenguaje SysML.

Del modelo ya descrito en SysML, se puede realizar una extrapolación a un lenguaje de programación de software, a fin de que la persona que realice el aplicativo derivado del modelo propuesto, permita llevar a cabo una simulación del subsistema de votación electrónica desarrollado, en lo que se refiere al análisis de riesgos, con el propósito de encontrar probabilidades de diferentes tipos de situaciones y eventos que puedan ocurrir durante el acto del sufragio.

Este modelo es creado con el objetivo de implementar las mejores prácticas de aseguramiento y protección de la información que consigna la expresión de los derechos de los ciudadanos en un proceso electoral.

[8]AS/NZS 4360:2004. Risk Management Systems Standar. Australia and New Zealand. 2004.

[9]Frase de origen latín significa en el lugar, en el sitio.

[10]Es un lenguaje de modelado de dominio específico para aplicaciones de sistemas de ingeniería.

En este artículo se presenta primero un cuadro comparativo entre los procesos de votación tradicional y votación electrónica. Posteriormente se mostrará el análisis de riesgos empleando el estándar AS/NZS 4360:2004, expuesto en una tabla donde están relacionados los riesgos con sus respectivas consecuencias, principios del voto afectados, amenazas y acciones de control.

Cabe resaltar que este análisis de riesgos esta formulado de forma general para la tecnología DRE sin hacer énfasis en ningún fabricante o máquina, por lo tanto será de utilidad para análisis posteriores con fabricantes específicos. Por último se enseña el modelo prototipo desarrollado.

II. COMPARACIÓN ENTRE VOTO TRADICIONAL Y VOTO ELECTRÓNICO

El éxito del ejercicio democrático visto como sistema de organización política del cual las personas integrantes participan de manera abierta y legal en torno a la toma de decisiones, requiere que a los ciudadanos se les garantice unas condiciones mínimas para ejercer su derecho al sufragio en el proceso electoral; en Colombia la Registraduría Nacional del Estado Civil –RNEC [5]- tiene encomendada dicha función garantizando que las elecciones sean transparentes y el proceso electoral se ejecute de una manera eficiente, así mismo el cumplimiento de los principios básicos del voto, propuestos desde la declaración universal de los derechos humanos [7], los cuales son: libre, secreto, universal, directo, igual y confiable.

En los últimos años Colombia ha obtenido un avance dentro de los procesos electorales debido a la progresiva implantación de tecnologías que han permitido obtener un avance en tiempos de respuesta y entrega de resultados. Sin embargo son muchos los procesos que deben ser optimizados para mejorar la calidad, transparencia y seguridad de la información

Es por esto que el gobierno nacional con la promulgación de la ley 892 del 2004 [6], ha otorgado la responsabilidad a la Registraduría Nacional del Estado Civil –RNEC- y al Consejo Nacional Electoral –CNE-, de implementar e implantar tecnologías de votación electrónica en el país, la cual decreta en su artículo primero "*Establézcase el mecanismo electrónico de votación e inscripción para los ciudadanos colombianos*"[11].

En la Tabla I se expondrá la comparación del proceso de votación tradicional contra el proceso de votación electrónica.

Para la descripción del proceso tradicional electoral se acudió al Código Nacional Electoral [17], de donde se pudo extraer la información más relevante del proceso para lograr una comparación paso a paso de este sistema contra el sistema de voto electrónico. Para el voto electrónico se indagó y se utilizó como base la memoria del plan piloto de voto electrónico en Colombia 2007, el cual fue ejecutado en el marco del convenio interadministrativo suscrito entre la Registraduría Nacional del Estado Civil –RNEC- y la Universidad Industrial

[11]"Por la cual se establecen nuevos mecanismos de votación e inscripción para garantizar el libre ejercicio de este derecho, en desarrollo del artículo 258 de la Constitución Nacional". Ley 892 de 2.004.

de Santander -UIS-. Experiencias electorales en muchos países como Brasil, Venezuela, Argentina y Estados Unidos [11][12][13][15], en donde han implementado urnas electrónicas con sistemas sofisticados permitiendo a los ciudadanos participar tecnológicamente en decisiones políticas y en específico en elecciones, han hecho parte de la documentación requerida para desarrollar una descripción del proceso de votación electrónica.

Tabla 1 COMPARACIÓN VOTO TRADICIONAL Y VOTO ELECTRÓNICO

<table>
<tr><th>Proceso de votación tradicional</th><th>Proceso de votación usando tecnologías de votación electrónica</th></tr>
<tr><td colspan="2">Inscripción de la cédula de ciudadanía

Este proceso es común para los dos procesos de votación. En realidad este es un proceso de la etapa preelectoral y es independiente de la implementación que se realice en la etapa electoral.
Según el artículo 78[12], del código electoral colombiano, la validez de la inscripción del documento de identidad, es un proceso que requiere la presencia del ciudadano, es decir no puede ser hecha por terceros. Además de esto, requiere que la firma y huella del índice derecho, queden plasmadas en el documento destinado para tal fin. En caso de que la persona presente mutilación de su dedo índice, se debe realizar la impresión de otra huella, dejando una constancia en el acta de esta etapa. Una vez realizado esto, el funcionario electoral encargado, debe expedir un comprobante que contenga la información del número del puesto de votación y de la cédula de ciudadanía.
“Las personas con cédulas de ciudadanía expedidas en corregimientos o inspecciones de policía con los cuales se haya integrado o integre un nuevo municipio, podrán votar en el lugar de expedición sin necesidad de previa inscripción. La Registraduría Nacional del Estado Civil adscribirá, por medio de resolución, los cupos numéricos de los corregimientos e inspecciones de policía al nuevo municipio y enviará a dichos lugares las correspondientes listas de sufragantes“.</td></tr>
<tr><td>Preparación previa

En esta etapa se realiza una serie de acciones que resultan indispensables para el éxito del proceso electoral, las cuales corresponde al diseño e impresión de tarjetones y la puesta a punto de todos los elementos del kit electoral.
El diseño del tarjetón es indispensable para garantizar que ningún partido político o candidato obtenga algún tipo de ventaja sobre sus oponentes, esto en el caso de la votación. Con el fin de impedir que se infrinja el primero de los principios orientadores del proceso electoral; principio de la imparcialidad del código electoral Colombiano.</td><td>Preparación previa

Esta etapa se refiere al ajuste de una serie de procesos necesarios para la puesta en marcha del proceso electoral, configurando cada máquina en lo referente a candidatos, total de votantes que estarán habilitados para sufragar en ella, asegurar registros en ceros y generación de claves de seguridad.
El día anterior a las elecciones, se debe levantar el acta de congelamiento. Esta debe contener la información del estado inicial de las máquinas y demás datos relevantes del sistema, que garanticen la seguridad y confiabilidad del mismo.</td></tr>
<tr><td colspan="2">Ingreso de jurados de votación

Los jurados (presidente, vicepresidente, vocal, suplentes y remanentes) deben ingresar al lugar de votación a más tardar a las 7:30 am, portando el documento de identidad y formulario de notificación de nombramiento E-1, para la identificación ante un funcionario de la RNEC.</td></tr>
<tr><td>Instalación de la mesa

El funcionario de la RNEC entregará el kit electoral a los jurados. Éste debe ser revisado por los jurados presentes. Acto seguido los jurados procederán a instalar la mesa de votación, la cual se recibe junto con un cubículo, una urna y seis sillas. Desde este momento estarán presentes los testigos electorales, observadores acreditados y representantes de organismos de control.
Para formalizar el cargo de jurado y el de instalación de la mesa, se diligencia la primera página del formulario acta de instalación y Registro general de votantes E-11.
Los jurados anotarán en el formulario, Urna cerrada y sellada E-9, nombres y apellidos con cédula de ciudadanía y firma de</td><td>Instalación de la mesa

Este proceso se puede analizar teniendo en cuenta diferentes escenarios. Un primer escenario podría ser que el jurado reciba el nuevo kit electoral y se cerciora que la máquina este bajo las condiciones que se estipularon. Un segundo escenario supondría la participación del jurado en la instalación de la máquina como es realizado en Argentina. En este escenario el kit electoral contendrá todos los elementos relacionados a la máquina.</td></tr>
</table>

[12]**ART.78** (INSCRIPCIÓN, VALIDEZ Y REQUISITOS) Del código electoral colombiano. Enunciado dentro de su TÍTULO IV (Censos electorales, inscripción de cédulas y listas de sufragantes).

Proceso de votación tradicional	Proceso de votación usando tecnologías de votación electrónica
cada jurado, frente al correspondiente cargo.	
Inicio de votación Antes de comenzar la jornada electoral se debe cumplir con el principio de transparencia[13], se abrirá la urna y se mostrará al público, a fin de que pueda cerciorarse de que está vacía y de que no contiene doble fondo ni artificios adecuados para el fraude. La urna se sellará con el formulario, ***Adhesivo urna cerrada y sellada E-9.***	**Inicio de votación** Antes de iniciar la votación electrónica se debe verificar que las condiciones iniciales del sistema se hayan mantenido sin modificación alguna, para de esta manera levantar el acta de descongelamiento del sistema y así dar paso al inicio de la jornada electoral. Precisado esto el jurado dará la orden a la máquina para el inicio del proceso electoral, de esta manera la máquina generará el acta de inicio.
Ingreso del votante Esta etapa es común a los dos procesos y al igual que la primera etapa es independiente de la implementación que se realice en la etapa electoral. Consiste en el acceso de los votantes al lugar de votación. En este paso del proceso electoral, se debe realizar un control para garantizar las condiciones de seguridad de los votantes y del mismo proceso electoral. Para ello es apropiado realizar una requisa. En este proceso se establece como requisito el porte el documento de identidad, para poder ingresar. El votante se debe acercar al lugar de votación, en el horario establecido, "Las votaciones principiarán a las ocho de la mañana (8:00 a.m.) y se cerrarán a las cuatro de la tarde (4:00 p.m.)" [14] .	
Identificación Una vez el votante se haga presente en el lugar de votación "el presidente del jurado le exigirá al ciudadano la cédula de ciudadanía, la examinará, verificará su identidad y buscará el número de la cédula en el formulario, ***Listado de sufragantes E-10,*** y lo resaltará. En el caso de que la cédula de ciudadanía del votante no aparezca en el formulario E-10, el jurado le indicará al votante el lugar donde se encuentra el funcionario de la RNEC, el cual podrá autorizar al ciudadano para votar, expidiendo el formulario ***Certificado de autorización de votos E-12***. En seguida, otro de los jurados anotará en el formulario, ***Registro general de votantes E-11***, frente al número de cédula de ciudadanía, los datos del elector, apellidos, nombre y género. Se registrará la huella dejando constancia del dedo al que corresponde. Registrado el elector, el jurado de mesa entregará al votante "la tarjeta o tarjetas electorales con el sello del jurado de votación en el dorso de la tarjeta"[15]. Si el ciudadano se equivoca, se le entregarán otras tarjetas nuevamente firmadas. El votante entregará las tarjetas dañadas y el jurado las marcará como inservibles y las depositará en el sobre negro (sobre 1). Después de esto se le permitirá acceder al cubículo de votación.	**Identificación y autenticación** Es esta etapa, el votante se acerca al jurado de mesa, donde debe realizar el proceso de acreditación de su identidad. Para esto debe presentar su documento de identidad (cédula de ciudanía). El jurado de mesa tomará la cédula y verificará si el votante está habilitado para realizar el sufragio. La identidad se podrá verificar por medio de un lector de código de barras, el cual debe escanear el código que se encuentra impreso en el respaldo del documento de identidad. Una vez realizado este proceso, se debe realizar la autenticación de la identidad del votante. Este proceso de validación se realiza mediante el escaneo de la huella utilizando un lector de huella digital. Este mecanismo debe validar la huella del dedo índice derecho, comparándola con la huella que se encuentre en la base de datos de la Registraduría. Este proceso hace parte de la modernización del proceso electoral, sin embargo, la identificación y autenticación puede realizarse de forma manual como se hace en proceso tradicional. Una vez se confirma el éxito de la validación, se puede autorizar al votante para acceder al cubículo y habilitar la máquina, la cual puede ser activada por el jurado de mesa o automáticamente por un software de conectividad entre la máquina de identificación y la de votación, en este caso se debe garantizar que no exista trazabilidad. Si la máquina funciona con "Smart Card", esta le será

[13]**ART.113** (PRINCIPIO DE TRANSPARENCIA) Del código electoral colombiano. Enunciado dentro de su capítulo III (Proceso de las votaciones).
[14]**ART. 111.** (Horario de votaciones) Del código electoral colombiano. Enunciado dentro de su capítulo III (Proceso de las votaciones).
[15]**INC. FINAL. Adicionado. L. 62/88, Art. 3º. ART. 114.** (PROCEDIMIENTO DE VOTACION) Del código electoral colombiano. Enunciado dentro de su capítulo III (Proceso de las votaciones).

Proceso de votación tradicional	Proceso de votación usando tecnologías de votación electrónica
	entregada al votante para que la introduzca en la máquina y de esta manera se habilite para realizar el sufragio.
Ejercicio del voto Una vez se ha autorizado al elector para votar, este se "dirigirá al cubículo y registrará su voto en el espacio que identifique al partido o agrupación política de su preferencia, o en el lugar previsto para votar en blanco."[16] Los jurados de votación y los organismos de control, se deben asegurar, que ninguna persona acompañe al elector en el momento de sufragar. Los mayores de 80 años, los ciudadanos con limitaciones de visión, sin importar su edad, y los ciudadanos con limitaciones físicas, son los únicos electores que pueden ingresar acompañados hasta el cubículo en el proceso de votación, siempre y cuando ellos mismos así lo requieran. El acompañante debe ser una persona de confianza del elector y dicha asistencia está prohibido que la brinden los jurados de votación; los funcionarios de la Organización Electoral; los testigos electorales; las autoridades civiles, militares, policiales, las de control y seguridad.	**Ejercicio del voto** En esta etapa el votante se encuentra frente a la pantalla táctil de la máquina, donde se muestra la información de los candidatos, siendo este el momento donde el votante selecciona entre las distintas opciones la de su preferencia y realiza su voto. Una vez realizado el voto, la máquina automáticamente almacena la información del candidato seleccionado.
Registro Terminado el ejercicio del voto, el elector doblará el tarjetón, regresará ante el jurado de votación y la introducirá en la urna. Acto seguido, el jurado le hace entrega al votante de su certificado electoral y su documento de identidad. El tarjetón a introducir debe estar doblado, de tal forma que se pueda observar la firma del jurado, esto debe ser informado en el momento en que el jurado hace entrega del tarjetón electoral. Si el votante se abstiene de introducir el tarjetón en la urna, el jurado de votación deberá exigir su devolución, tomarlo y marcarlo con la palabra inservible para introducirlo dentro del sobre de *tarjetas no utilizadas e inservibles.*	**Registro** Esta etapa depende directamente del tipo de máquina que se utilice para las votaciones. En el primer escenario la máquina imprime un comprobante de votación, el cual debe tomar el votante para introducirlo en la urna, la cual estará ubicada junto a la mesa de votación. Es importante que el votante se cerciore que la información impresa en el comprobante corresponde a su elección. Un segundo escenario se presenta en el caso que la máquina esté equipada con una urna interna. En este escenario la máquina imprime un comprobante, el cual se muestra al votante para que este se cerciore que la información impresa corresponde a su elección, luego es depositado automáticamente en la urna interna de la máquina sin intervención del votante. En un tercer escenario la máquina no imprime comprobante y el registro se realizaría automáticamente por la máquina. Si la máquina utiliza tarjeta habilitadora, el votante debe retirarla y devolverla al jurado de mesa en el momento del cubículo, o en el momento en que este deposita el comprobante en la urna, esto dependiendo de la máquina utilizada para la votación. Acto seguido, el jurado le hace entrega al votante de su certificado electoral y documento de identidad. Cabe resaltar que en voto electrónico el registro en realidad lo hace automáticamente la máquina y es este el que tiene

[16]**INC. FINAL. Adicionado. L. 62/88, Art. 3º. ART. 114.** (PROCEDIMIENTO DE VOTACION) Del código electoral colombiano. Enunciado dentro de su capítulo III (Proceso de las votaciones).

Proceso de votación tradicional	Proceso de votación usando tecnologías de votación electrónica
	mayor validez, el registro basado en los comprobantes impresos se toma como un respaldo para la información.
Cierre de mesa electoral y pre-conteo El acto eleccionario finalizará a las dieciséis horas y solo votará la persona que haya iniciado el proceso, los que se encuentren en la fila abandonarán el puesto de votación. Una vez se ha finalizado la etapa de votación, se restringe el ingreso de los votantes al lugar de votación. Concluida la votación los jurados destruyen las tarjetas electorales sobrantes sin contarlas, los certificados electorales y dichos residuos se introducirán en el sobre 1. En la última página del formulario ***Acta de instalación y registro general de votantes E-11***, los jurados anotarán el total de ciudadanos que votaron en la mesa asignada descontando las casillas anuladas por haber registrado información erróneamente. Luego se cerrará el formulario ***E-11***, plasmando la firma y cédula de ciudadanía de cada uno de los seis jurados. El jurado debe leer en voz alta el número total de sufragantes que participaron en el proceso electoral[17]. Esto se hará constar en los dos ejemplares del formulario ***Acta de escrutinio de mesa E-14.*** Los jurados procederán a abrir la urna y extraer los votos. Se contarán sin abrirlos o desdoblarlos. Leerán en voz alta los resultados y compararán con el total de votantes registrados en los formularios ***E-11 y E-14***. "Si hubiere un número mayor que el de ciudadanos que sufragaron, se introducirán de nuevo en la urna y después de moverlos para alterar su colocación, se sacarán a la suerte tantos sobres cuantos sean los excedentes y sin abrirlos se quemarán inmediatamente"[18] y se dejará constancia en el formulario ***E-14***. El jurado deberá realizar una clasificación de cada uno de los votos y de esta manera contabilizarlos y dejar constancia del total de los votos en el formulario ***cuenta votos*** y en el ***Acta de escrutinio de jurado de votación E-14***. Esto en coherencia con el artículo 136[19] del código electoral colombiano. Una vez diligenciado este formulario, se debe retirar el desprendible para entregarlo al funcionario de la RNEC. Igualmente, el jurado está autorizado para recibir reclamaciones de los testigos electorales en el momento del	**Cierre de mesa electoral** El acto eleccionario finalizará a las dieciséis horas y solo votará la persona que haya iniciado el proceso, los que se encuentren en la fila abandonarán el puesto de votación. Una vez se ha finalizado la etapa de votación, se restringe el ingreso de los votantes al lugar de votación. Los jurados proceden a realizar el protocolo para cerrar la máquina, donde se inhabilita el registro de nuevos votos y se generará el acta de cierre de la máquina de votación. El acta de cierre de la máquina de votación, posee la hora de impresión, el nombre del presidente, los suplentes que actuaron en la mesa y las siguientes estadísticas: • Totales de votos emitidos • Totales de votos por candidato • Totales de votos en blanco Después de esto, el jurado debe depositar dentro del sobre indicado, las actas de inicio y de cierre de máquina de votación, así como toda otra acta que se haya elaborado durante el transcurso del acto electoral, para así ser entregado al delegado de la RNEC. Una vez entregados los pliegos electorales, los jurados deben entregar al funcionario encargado de la RNEC, los elementos recibidos al inicio de los comicios. Este a su vez hará entrega de los formularios de certificado de entrega de pliegos electorales y constancia de prestación del servicio de jurado de votación, a cada uno de los jurados.

[17]**ART. 134.** (LECTURA DEL NÚMERO TOTAL DE SUFRAGANTES). Titulo VII: Escrutinios, capitulo I: escrutinios de los jurados de votación. Código electoral colombiano, decreto 2241 de 1986.
[18]**ART. 135.** (apertura de la urna). Titulo VII: escrutinios, capitulo I: Escrutinios de los jurados de votación. Código electoral colombiano, decreto 2241 de 1986.
[19]**ART. 136.** (ANOTACIÓN DEL NÚMERO TOTAL DE VOTOS). Titulo VII: Escrutinios, capitulo I: escrutinios de los jurados de votación. Código electoral colombiano, decreto 2241 de 1986.

Proceso de votación tradicional	Proceso de votación usando tecnologías de votación electrónica
pre-conteo. Dado este caso el jurado procederá a contar nuevamente los votos en no más de una ocasión. Esta situación debe quedar registrada en los dos formularios ***E-14***. Si la reclamación de los testigos se hace de forma escrita, esta debe ser introducida en el sobre dirigido a los claveros[20] (sobre 5). Después de esto, el jurado debe depositar los sobres con los votos, formularios ***E-10, E-11, E-12*** y ***E-14***, dentro del sobre 5 (dirigido a los claveros). A su vez debe depositar el otro ejemplar del formulario ***E-14*** en el sobre 6 el cual es dirigido a los delegados departamentales del RNEC. Los pliegos electorales deben ser entregados por el presidente de mesa al delegado de la RNEC antes de las 11 pm del día de las elecciones, para posteriormente ser introducidos en el arca triclave. Una vez entregado los pliegos electorales, el funcionario de la RNEC debe hacer entrega de los formularios ***E-17 (certificado de entrega de pliegos electorales) y E-18 (constancia de prestación del servicio de jurado de votación)***, a cada uno de los jurados.	
Consolidación y divulgación Una vez entregados los pliegos electorales de cada mesa, se procede a enviar la información a un centro de consolidación departamental, para luego ser publicados los resultados[21].	**Consolidación y divulgación** En esta etapa, las máquinas envían la información de los resultados del conteo electrónico, ésta es transmitida por redes de alta velocidad a los servidores de consolidación. Se debe auditar la integridad de los datos procesados y certificar la procedencia de la información para evitar agregados y eliminaciones de sufragios. Para esto se debe contar con mecanismos de criptografía y seguridad de la información Una vez la información es consolidada, esta queda dispuesta para ser publicada. La consolidación se realiza sin ningún tipo de intervención humana.
Escrutinio El escrutinio hace parte de la etapa postelectoral. Se divide en tres fases, escrutinio distrital, municipal y zonales[22], escrutinio en corregimientos e inspecciones[23], y escrutinio general (departamental)[24]. En voto electrónico se hace a través de los comprobantes emitidos por la máquina de votación con el fin de validar los resultados obtenidos electrónicamente.	

Fuente: Autores

[20]**ART. 148.** (CLAVEROS). Titulo VII: Escrutinios, capitulo II: Arcas triclaves y claveros. Código electoral colombiano, decreto 2241 de 1986.
[21]**ART.153** (CÓMPUTO DE VOTOS). Titulo VII: Escrutinios, capitulo II: Arcas triclaves y claveros. Código electoral colombiano, decreto 2241 de 1986.
ART. 155 (A QUÍENES SE LES COMUNICA). Titulo VII: Escrutinios, capitulo III: Comunicación de resultados electorales. Código electoral colombiano, decreto 2241 de 1986.
[22]**ART.160** (HORARIO). Titulo VII: escrutinios, capitulo IV: Escrutinios Distritales, Municipales y Zonales. Código electoral colombiano, decreto 2241 de 1986
[23]**ART.161** (ESCRUTINIO EN CORREGIMIENTOS E INSPECCIONES). Titulo VII: Escrutinios, capitulo IV escrutinios Distritales, Municipales y Zonales. Código electoral colombiano, decreto 2241 de 1996
[24]**ART.177** (INICIACIÓN DE ESCRUTINIOS). Titulo VII: escrutinios, capitulo V: Escrutinios generales. Código electoral colombiano, decreto 2241 de 1986

III. ANÁLISIS DE RIESGOS

En esta etapa se elaboró el análisis de riegos de la seguridad de la información del subsistema de votación electrónica *in-situ*, al implementar tecnologías de votación electrónica de registro directo, teniendo en cuenta el estándar AS/NZS: 4360:2004. A partir de este análisis se obtuvieron puntos críticos, que caracterizan la dinámica del proceso, y que llevaron a facilitar el diseño del modelo de seguridad de la información. Con base en el estándar se implementó una metodología para el análisis de riesgos la cual comprende los siguientes pasos básicos:

1. **Identificar, caracterizar y valorar amenazas**
   Este tipo de análisis es ampliamente utilizado como herramienta de gestión en estudios de seguridad para identificar riesgos cualitativos y evaluar riegos cuantitativos.
2. **Valorar la vulnerabilidad de activos críticos para amenazas específicas**
   En esta etapa se debe realizar un análisis para identificar los activos a proteger o evaluar y de esta manera identificar las amenazas específicas a los cuales están expuestos.
3. **Determinar el riesgo**
   La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos y estandarizados previamente.
4. **Identificar formas de disminuir estos riesgos**
   Con base en los resultados obtenidos en los análisis previos, se debe decidir cuál de los métodos de disminución significativa de riesgos se debe aplicar.
5. **Priorizar las medidas de reducción de riesgos basados en estrategias**
   Para el desarrollo de esta etapa se debe analizar el tipo de riesgo al que se está expuesto, y de esta manera elegir la estrategia más apropiada a utilizar en cada situación.

A partir de probabilidades de ocurrencia determinadas y estimadas para cada amenaza, (ver tabla III), las cuales han sido obtenidas a partir de previas investigaciones[3], y documentación acerca de anteriores procesos de votación electrónica, como pruebas piloto y experiencias de elecciones en otros países como Brasil, Venezuela, Argentina y Estados Unidos, se utilizó un método deductivo de análisis de riesgos probabilístico denominado *árbol de fallas*, el cual trata de un método que parte de una previa selección de un "suceso no deseado o evento que se pretende evitar", para averiguar los orígenes de los mismos [19]. A partir de este método se pueden deducir de manera sistemática y lógica ecuaciones que describen la secuencia de cada amenaza.
Los árboles de fallas (ver apéndice A) elaborados a partir de amenazas correspondientes a cada riesgo, están compuestos por compuertas lógicas que establecen una relación entre los eventos básicos. Las compuertas básicas como, AND y OR, fueron empleadas en este proceso ya que cualquier otra compuerta puede ser expresada en términos de estas. La compuerta AND corresponde a una relación en donde la salida ocurre si todos los eventos de entrada ocurren simultáneamente, y la compuerta OR a una relación en donde la salida ocurre si cualquiera de los eventos de entrada ocurre. Para esta última compuerta las expresiones lógicas pueden variar dependiendo si llega a existir una relación entre los eventos que ocurren. Para cada amenaza se empleó un símbolo llamado componente básico, el cual se refiere a un suceso que no requiere posterior desarrollo.

En la tabla IV se muestran las expresiones lógicas y los resultados, que corresponden a una probabilidad general de acontecimiento para cada riesgo. Para el análisis empleado se asume que no se conoce o no se ha elegido al fabricante de la tecnología establecida previamente, *Direct Recording Electronic- DRE*, que se va a utilizar en el proceso. Una vez que la persona o entidad interesada en aplicar este análisis de riesgos, escoja uno de los fabricantes de tecnología DRE, tendrá que referirse a la tabla II, identificando qué amenazas aplican para el fabricante seleccionado y deberá a partir de las expresiones lógicas ubicadas en la tabla IV obtener la probabilidad de acontecimiento para cada riesgo, de la máquina de dicho fabricante.

De acuerdo a la información de riesgos y datos disponibles se llevó a cabo un análisis semicuantitavo, el cual usa palabras descriptivas que representan la magnitud de probabilidad de ocurrencia o impacto para cada riesgo establecido.
Teniendo en cuenta esto, se usaron tablas de medida semicuantitativas de probabilidad e impacto, (ver tabla V y VI), las cuales fueron adaptadas para satisfacer las necesidades de este estudio. La cuantificación de probabilidad para cada riesgo, se basó en las probabilidades de acontecimiento obtenidas a partir del método de árbol de fallas anteriormente mencionado, tabla IV. Además de esto, conforme al estándar utilizado se realizó la cuantificación de impacto para cada riesgo, tomando en cuenta el número de principios de voto incumplidos y partiendo de estimaciones subjetivas[25] basadas en diversos artículos y fuentes bibliográficas que tratan los riesgos que han surgido a lo largo de diversos procesos electorales que implementan la tecnología DRE.

Una vez obtenidas las cuantificaciones para cada riesgo se procedió a utilizar la matriz de riesgos, (ver tabla VII), en la que se relacionan las medidas de probabilidades e impactos conseguidas y de donde se logra un nivel de riesgo, clasificados en niveles bajo (L), medio (M), alto (H) o

[25] "Alternativamente cuando no se dispone de datos anteriores, se pueden realizar estimaciones subjetivas que reflejan el grado de convicción de un individuo o grupo de que podrá ocurrir un evento o resultado particular."

extremo (E). En la tabla VIII se muestran los niveles obtenidos para cada riesgo.

Tabla 2 IDENTIFICACIÓN DE RIESGOS

Riesgo	Consecuencias	Principio de voto incumplido	Acción de control	Amenaza
1. Asistencia irregular al votante por parte de los jurados de votación.	Manipulación de la intención de voto del sufragante.	**Libre** (no coerción, integridad del votante) **Secreto** (privacidad) **Confiabilidad** (integridad, fiabilidad, disponibilidad) **Universalidad**	**Preventivo:** Desarrollar sistemas de votación con ayudas a discapacitados y que sean de manejo intuitivo Entrenamiento de los jurados de votación y personal asociado al proceso electoral. Verificar cualidades de las personas que efectuarán labores de asistencia a los votantes. Definir protocolo de asistencia al votante. **Mitigación:** Aplicación del protocolo que garantice la transparencia, confiabilidad y eficiencia de la asistencia al votante. Restringir el tipo de personas que prestan asistencia a los votantes. Generalmente debe ser un familiar muy cercano (esto es lo que dicta la ley). Verificar cada instancia del proceso de ayuda a un votante, desde el momento que la solicita hasta que ejerce su voto. **Contingencias:** Labores de auditoría. Reemplazo del personal. Acudir a autoridades competentes.	Inadecuada capacitación al votante. C(15) Necesidad de asistencia debido ausencia del votante en las campañas de educación. C(16) Incumplimiento o ausencia del protocolo de asistencia debido al desconocimiento de este por parte del personal encargado. C(17) Escaso personal de auditoría o con inadecuada capacitación. C(7) Falta o poca presencia de testigos electorales. C(18)
2. Intrusión a través del puerto de la tarjeta inteligente	Pérdida y alteración de la información. Daño o bloqueo del lector magnético de la máquina. Cambio del comportamiento de la máquina	**Confiabilidad** (fiabilidad, robustez e integridad) **Igual** (precisión, singularidad)	**Preventivo:** Asegurar que el Software y el controlador de la tarjeta inteligente sean lo suficientemente robustos para evitar cualquier ataque. Capacitar a los entes de control para la vigilancia de este puerto. **Mitigación:**	Hostigamiento al lector de la tarjeta por parte del agresor. C(3) Activación de las capacidades inalámbricas por parte de algún operario o personal externo. C(4) Control inadecuado de las capacidades de Wi-Fi en la

Riesgo	Consecuencias	Principio de voto incumplido	Acción de control	Amenaza
	debido a la implantación de un software malicioso a través del lector magnético. Acceso completo a la máquina al activar el puerto Wi-Fi para crear una conexión directa entre la máquina y un computador externo. Intrusión a la red de datos.		Emisión de alarma indicadora que el puerto Wi-Fi ha sido activado. Aplicación inmediata de controles para suspender la intrusión. **Contingencia:** Proceder a verificar el estado de la máquina siguiendo un protocolo de control de cambios. Uso de agentes externos para realizar rastreo y seguimiento de la señal.	auditoría. C(5) Proveedor no informa de las capacidades inalámbricas de la máquina de votación. C(6) Escaso personal de auditoría o con inadecuada capacitación. C(7) Corrupción por parte de supervisores para acceder la máquina a través de su tarjeta maestra o de administrador, aprovechando su capacidad para modificar información. C(8)
3. Daño general de la máquina	Pérdida de información. Retraso en el proceso.	**Confiabilidad** (integridad, fiabilidad, disponibilidad, robustez) **Directo** (derecho al voto)	**Preventivo:** Instalación de UPS y de estabilizadores de energía. Verificar el estado de la máquina. **Mitigación:** Realizar auditorías periódicas durante la jornada electoral del estado de la máquina. **Contingencia:** Cambio de máquina basado en un protocolo que garantice la transparencia y eficiencia del proceso.	Cumplimiento del tiempo de vida útil de los dispositivos internos de la máquina. C(11) Falta de auditoría para la selección de las máquinas y mantenimiento de las mismas. C(13) Escaso personal de auditoría o con inadecuada capacitación. C(7) Operario o personal encargado no conoce el funcionamiento adecuado de la máquina de votación. C(14) Colapso de las redes eléctricas debido a anomalías de funcionamiento. C(2) Descarga de Software malicioso. C(12)
4. Cortes de energía de larga duración.	Pérdida de la información.	**Confiabilidad** (fiabilidad, disponibilidad, robustez e integridad) **Directo** (derecho al voto)	**Preventivo:** Instalación de UPS y de estabilizadores de energía. **Mitigación:** Uso de baterías de respaldo en la máquina. **Contingencia** Habilitar fuente alterna de suministro energía eléctrica	Colapso de las redes eléctricas debido a anomalías de funcionamiento. C(2) Hostigamiento de grupos armados al margen de la ley. C(20) Inadecuada cantidad de personal de seguridad. C(21)

Riesgo	Consecuencias	Principio de voto incumplido	Acción de control	Amenaza
5. La tarjeta inteligente permite que el votante emita el voto más de una vez.	Permite que se realice fraude para favorecer algún candidato.	**Confiabilidad** (fiabilidad e integridad) **Igual** (singularidad)	**Preventivo:** Asegurar que el sistema de activación de la máquina/tarjeta sea para un sólo intento de voto. **Mitigación:** Labor de auditoría periódica durante la jornada electoral verificando que la cantidad de personas autenticadas hasta el momento sea igual al número de votos registrados por la máquina**.** **Contingencia:** Selección aleatoria de los registros de votación sobrantes para ser eliminados en el momento del conteo de la máquina	Falta de auditoría para la selección de las máquinas. C(13) Escaso personal de auditoría o con inadecuada capacitación. C(7) La tarjeta inteligente no se desactiva después de emitir el voto. C(24) Existe complicidad de los jurados de votación para reactivar la tarjeta. C(25)
6. Falla de la batería de respaldo de la máquina de votación.	Pérdida y alteración de la información. Retraso del proceso.	**Confiabilidad** (fiabilidad, disponibilidad, robustez, integridad) **Directo** (derecho al voto)	**Preventivo:** Instalación de UPS y estabilizadores de energía. Asegurar las condiciones de la máquina. **Mitigación:** Instalación de UPS. Baterías de repuesto disponibles.	Falla técnica de la batería. C(1) Colapso de las redes eléctricas debido a irregularidades de funcionamiento. C(2)
7. Inadecuado demarcación del quiosco de votación.	Alteración del orden del proceso electoral.	**Secreto** (privacidad) **Universalidad** **Confiabilidad** (fiabilidad, integridad)	**Preventivo:** Después de demarcados, verificar la señalización de cada uno de los quioscos de votación. **Mitigación:** Acción de personal capacitado para organizar el flujo de votantes.	Inapropiada demarcación del lugar de votación, por negligencia de la entidad encargada. C(19) Escaso personal de auditoría o con inadecuada capacitación. C(7)
8. No existe comprobante de que el voto es registrado	El votante pierde la confiabilidad en el proceso, pues no sabe con certeza si su voto se emitió correctamente.	**Confiabilidad** (fiabilidad, integridad) **Igual** (precisión)	**Preventivo:** Cerciorarse que la máquina se encuentra en condiciones adecuadas para el funcionamiento durante las elecciones y que estén en la capacidad de cumplir con los requerimientos de la mesa a la que corresponde. **Mitigación:** Emisión de alarma indicadora de escasez de tinta o papel.	Máquina no imprime el comprobante, ya sea por daño técnico o agotamiento del papel. C(22) La máquina no posee sistema de impresión de comprobante. C(23)

Riesgo	Consecuencias	Principio de voto incumplido	Acción de control	Amenaza
			Contingencia: Cambio de máquina basado en un protocolo que garantice la transparencia y eficiencia del proceso.	
9. El comprobante es expuesto y permite que otras personas vean por quién se realizó el voto.	Ataque a los principios del voto.	**Secreto** (privacidad) **Confiabilidad** (fiabilidad e integridad) **Libre** (integridad del votante)	**Preventivo:** Ubicar de manera adecuada y bajo los estándares de confidencialidad las máquinas de votación, para que el voto no sea expuesto. Plan de entrenamiento al votante. Utilizar máquinas que no permitan el contacto físico del votante con el comprobante. Que automáticamente introduzcan el voto en la urna, previo la validación del votante. **Mitigación:** Corregir la ubicación de la máquina de votación. **Contingencia:** Asegurar que el comprobante sea introducido en la Urna antes de salir del lugar de votación, para evitar que se haga pública la elección del ciudadano.	No contar con instalaciones apropiadas en el lugar de votación. C(26) No existe la vigilancia y control suficiente para asegurar la privacidad del comprobante. C(27) Escaso personal de auditoría o con inadecuada capacitación. C(7)
10. Máquina no concede el tiempo necesario para realizar el voto.	Manipulación de la intención de voto del sufragante.	**Libre** (no coerción, integridad del votante) **Confiabilidad** (fiabilidad, disponibilidad, integridad, robustez)	**Preventivo:** Establecer márgenes de tiempo suficientes para no limitar la elección del ciudadano. **Mitigación:** Emisión de una alarma que indique al votante que el tiempo para efectuar el voto está por terminar. **Contingencia:** Habilitar tiempo adicional al votante.	Error en la selección del tiempo máximo de voto. C(28) El sufragante no tiene el mínimo conocimiento para interactuar con la máquina, originando que se agote el tiempo de espera. C(29) Escaso personal de auditoría o con inadecuada capacitación. C(7)
11. Fallas en el ajuste y calibración de la pantalla táctil.	Error en la selección del votante. Manipulación de la intención	**Igual** (precisión) **Libre** (no coerción)	**Preventivo:** Utilizar interfaces que permitan seleccionar en cualquier parte del nombre del candidato en lugar de tocar un punto específico	Calibración inadecuada por negligencia del operario o personal encargado. C(9) Escaso personal de auditoría o con inadecuada

Riesgo	Consecuencias	Principio de voto incumplido	Acción de control	Amenaza
	de voto del sufragantes.		para que la opción sea tenida en cuenta. **Mitigación:** Bloqueo del sistema debido a los intentos fallidos. Emisión de alarma de último intento. **Contingencia:** Protocolo de reemplazo de la máquina.	capacitación. C(7) Campañas inadecuadas de capacitación, para los operarios encargados de la calibración. C(10)
12. No existe confirmación del voto.	Errores de selección. Pérdida de la confiabilidad del proceso.	**Igual** (precisión) **Confiabilidad** (fiabilidad, robustez e integridad)	**Preventivo:** Asegurar que las máquinas tengan el sistema de confirmación de voto.	La máquina no posee el método de confirmación de voto. C(30) Falta de auditoría para la selección de las máquinas. C(13) Escaso personal de auditoría o con inadecuada capacitación. C(7)

Fuente: Autores

Tabla 3 LISTADO DE AMENAZAS CON RESPECTIVA PROBABILIDAD DE OCURRENCIA

Amenaza	Causa	Probabilidad de ocurrencia
C(1)	Falla técnica de la batería.	0,15
C(2)	Colapso de las redes eléctricas debido a anomalías de funcionamiento.	0,25
C (3)	Hostigamiento al lector de la tarjeta por parte del agresor.	0,1
C (4)	Activación de las capacidades inalámbricas por parte de algún operario o personal externo.	0,196
C (5)	Control inadecuado del las capacidades de Wi-Fi en la auditoría.	0,181
C (6)	Proveedor no informa de las capacidades inalámbricas de la máquina de votación.	0,196
C (7)	Escaso personal de auditoría o con inadecuada capacitación.	0,151
C (8)	Corrupción por parte de supervisores para acceder la máquina a través de su tarjeta maestra, aprovechando su capacidad para modificar información.	0,48
C (9)	Calibración inadecuada por negligencia del operario o personal encargado.	0,3435
C (10)	Campañas inadecuadas de capacitación, para los operarios encargados de la calibración.	0,196
C (11)	Cumplimiento del tiempo de vida útil de los dispositivos internos de la máquina.	0,2
C (12)	Software malicioso.	0,3
C (13)	Falta de auditoría para la selección de las máquinas y mantenimiento de las mismas.	0,2
C (14)	Operario o personal encargado no conoce el funcionamiento adecuado de la máquina de votación.	0,15
C (15)	Inadecuada capacitación al votante.	0,165
C (16)	Necesidad de asistencia debido ausencia del votante en las campañas de educación.	0,2
C (17)	Incumplimiento o ausencia del protocolo de asistencia debido al desconocimiento de este por parte del personal encargado.	0,343
C (18)	Falta o poca presencia de testigos electorales.	0,236
C (19)	Inapropiada demarcación del lugar de votación, por negligencia de la entidad encargada.	0,221
C (20)	Hostigamiento de grupos armados al margen de la ley.	0,196
C (21)	Inadecuada cantidad de personal de seguridad.	0,221

C (22)	Máquina no imprime el comprobante, ya sea por daño técnico o agotamiento del papel.	0,25
C (23)	Máquina no posee sistema de impresión de comprobante.	0,2
C (24)	La tarjeta inteligente no se desactiva después de emitir el voto.	0,2
C (25)	Existe complicidad de los jurados de votación para reactivar la tarjeta.	0,28
C (26)	No contar con instalaciones apropiadas en el lugar de votación	0,1
C (27)	No existe la vigilancia y control suficiente para asegurar la reserva del comprobante.	0,15
C (28)	Error en la selección del tiempo máximo de voto.	0,35
C (29)	El sufragante no tiene el mínimo conocimiento para interactuar con la máquina, originando que se agote el tiempo de espera.	0,45
C (30)	La máquina no posee el método de confirmación de voto.	0,149

Fuente: Autores

Tabla 4 EXPRESIONES LÓGICAS Y PROBABILIDAD DE ACONTECIMIENTO DE RIESGOS

Riesgo	Ecuación	Probabilidad de acontecimiento
R(1)	C(15)+C(16)- C(15)*C(16)+ C(17)*C(7)+C(18)- C(17)*C(7)*C(18)	0,6076
R(2)	C(3)+C(4)+ C(5)*C(6)*C(7)- C(4)*C(5)*C(6)*C(7)+C(8)	0,7803
R(3)	C(11)+C(13)*C(7)+ C(14)- C(14)*C(7)*C(13)+C(2)+C(12)	0,9257
R(4)	C(2)+C(20)+C(21)-C(20)*C(21)	0,6237
R(5)	X1=C(13)+C(7)- C(13)*C(7) ; X1+C(24)+C(25)-X1*(C(24)+C(25))	0,6468
R(6)	C(1)+ C(2)	0,4000
R(7)	C(19)+C(7)-C(19)*C(7)	0,3386
R(8)	C(22)+C(23)	0,4500
R(9)	C(26)+ C(27)+C(7)- (C(26)+ C(27))*C(7)	0,3633
R(10)	C(28)*C(7)+C(29)-C(28)*C(7)*C(29)	0,4791
R(11)	C(9)* C(7)+ C(10)-C(9)* C(7)*C(10)	0,2377
R(12)	C(30)+C(13)*C(7)- C(30)*C(13)*C(7)	0,1747

Fuente: Autores

Tabla 5 MEDIDAS SEMICUANTITATIVA DE PROBABILIDAD

Nivel de ponderación	Probabilidad	Descripción
a	Raro [0;0,2)	Puede ocurrir sólo en circunstancias excepcionales
b	Improbable [0,2;0,4)	Pudo ocurrir en algún momento
c	Posible [0,4;0,6)	Podría ocurrir en algún momento
d	Probable [0,6;0,8)	Probablemente ocurrirá en la mayoría de las circunstancias
e	Casi certeza [0,8;1]	Se espera que ocurra en la mayoría de las circunstancias

Fuente: Autores

Tabla 6 MEDIDAS CUALITATIVAS DE IMPACTO

Nivel de ponderación	Impacto	Descripción
1	Insignificante	Sin perjuicios
2	Menor	Daños e implicaciones leves
3	Moderado	Daños e implicaciones medios
4	Mayor	Daños e implicaciones de gran magnitud
5	Catastrófico-desastroso	Daños e implicaciones irreversibles

Fuente: Autores

Tabla 7 MATRIZ DE ANÁLISIS DE RIESGO CUALITATIVO – NIVEL DE RIESGO

Probabilidad	Impacto				
	Insignificante 1	Menor 2	Moderado 3	Mayor 4	Catastrófico 5
Raro (a)	L	L	M	H	H
Improbable (b)	L	L	M	H	E
Moderado (c)	L	M	H	E	E
Probable (d)	M	H	H	E	E
Casi certeza (e)	H	H	E	E	E

Fuente: Autores

Tabla 8 RESULTADOS DE ANÁLISIS DE RIESGOS

Riesgo	Probabilidad de acontecimiento	Probabilidad cuantificada	Impacto cuantificado	Nivel de Riesgo
1. Asistencia irregular al votante por parte de los jurados de votación.	0,6076	d	4	**E**
2. Intrusión a través del puerto de la tarjeta inteligente	0,7803	d	2	**H**
3. Daño general de la máquina	0,9257	e	2	**H**
4. Cortes de energía de larga duración.	0,6237	d	2	**H**
5. La tarjeta inteligente permite que el votante emita el voto más de una vez.	0,6468	d	2	**H**
6. Falla de la batería de respaldo de la máquina de votación.	0,4000	c	2	**M**
7. Inadecuada demarcación del quiosco de votación.	0,3386	b	3	**M**
8. No existe comprobante de que el voto es registrado	0,4500	c	2	**M**
9. El comprobante es expuesto y permite que otras personas vean por quién se realizó el voto.	0,3633	b	3	**M**
10. Máquina no concede el tiempo necesario para realizar el voto.	0,4791	c	2	**M**
11. Fallas en el ajuste y calibración de la pantalla táctil.	0,2377	b	2	**L**
12. No existe confirmación del voto.	0,1747	a	2	**L**

Fuente: Autores

IV. MODELADO DEL SISTEMA DE VOTACIÓN ELECTRÓNICA *DRE* EN EL LUGAR DE VOTACIÓN

La definición más formal de un sistema expone que, es un "*Conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a determinado objeto*"[26], entendiéndose por objeto un fin o intento a que se dirige o encamina una acción u operación para lograr una meta o alcanzar un objetivo. Este objetivo puede tener distintas naturalezas, como el servicio o la producción. Existen diferentes metodologías para abarcar el análisis de un sistema, pero quizás la más adecuada, es ver el sistema desde su concepción holística, es decir como un todo. Este concepto plantea la idea de que un sistema no debe ser analizado por el desempeño y las propiedades de las partes que lo componen por sí solas, sino que el propio sistema como un todo, determina cómo se comportan sus partes.

Elementos de la modelación del sistema

Un sistema está conformado por entidades, actividades, recursos y controles. Estos elementos determinan el comportamiento del sistema. El sistema que se estudió en este artículo es el sistema de votación electrónica DRE en el lugar de votación *in-situ.*

Entidades: La entidad más importante de este sistema es la información, por esto el diseño del modelo está basado en un análisis de riesgos de la seguridad de la información, entendiéndose por seguridad de la información, el cumplimiento de los 5 principios fundamentales del sufragio.

Actividades: Censar huella digital, almacenamiento de la información, criptografía de la información, envío de información a la central de consolidación, conteo de votos, expedir constancia de voto entre otras.

Recursos: Los recursos de este sistema se pueden clasificar así:

[26]Real academia de la lengua española. RAE

- **Humanos:** Personal de seguridad, testigos electorales, auditores, jurados, personal de la RNEC y el votante mismo.
- **Inanimados:** Lector Biométrico, memoria RAM, procesador, Pantalla táctil, baterías, la máquina en sí.
- **Intangibles:** Electricidad, información.

Los controles de este sistema están enfocados a garantizar la seguridad de la información y surgen del análisis de riesgos.
Para realizar el diseño de este modelo, se utilizó el lenguaje de modelado SysML (Systems Modeling Language), ésta notación surgió en el año 2001, como una adaptación del lenguaje UML para extender el lenguaje en el uso de cualquier tipo de sistema, pues el UML está enfocado básicamente al modelado de sistemas Software.

El fin principal del SysML es dar solución a los problemas de modelado de sistemas, ofreciendo distintas técnicas para el modelado de datos, personas, procesos, software, entre otras, de forma estandarizada. Estas técnicas no son más que una serie de diagramas, entre los que se encuentran: Diagramas de casos de uso, de clases, de montaje, de bloques, de requisitos, paramétricos, de actividad, de interacción, de estados, entre otros.

Estos diagramas son la base para el diseño de códigos software en distintos paradigmas de programación, como la programación orientada a objetos (OOP).
El diseño del modelo se realizó a través de la herramienta *Case*[27] ***Enterprise Architect 7.1***, especial para este tipo de diseños. Se eligió esta herramienta por ser la más popular para el diseño de modelos con SysML, y es recomendada en la página web oficial de SysML [20].
Este modelo se realizó por diagramas de casos de uso y el diagrama de jerarquía de herencia de las clases en forma muy general.

El diseño del modelo del sistema de seguridad de la información se realizó por medio de diagramas de *Casos de Uso*, este tipo de diagramas es un método para extraer requisitos de un sistema y consiste en la interacción de un actor interesado o *Stakeholder*[28], con el sistema, para obtener un objetivo determinado. En el *caso de uso*, se describe y representa una interacción a través del tiempo, entre máquina y el actor (persona, máquina u otro sistema). Normalmente tiene requisitos y limitaciones que describen las características esenciales y las normas bajo las cuales opera.
El modelo describe dos paquetes generales de *casos de uso*, uno describe la interacción entre los actores principales del sistema y el otro describe la interacción entre actores y cada uno de los escenarios del proceso electoral, con la intención no sólo de describir las interacciones, sino de describir el proceso mismo. Esto se puede apreciar en la figura 1.

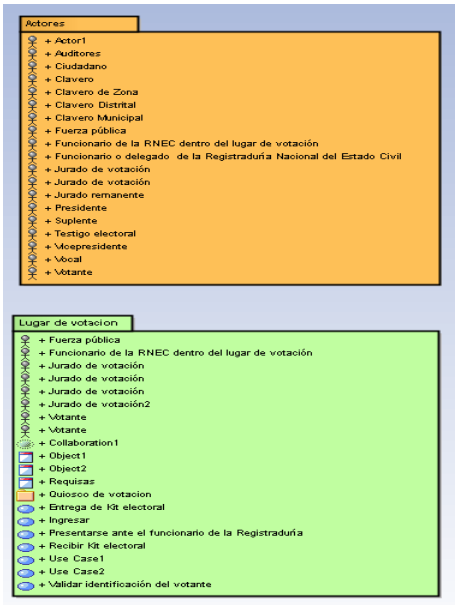


Fig. 1 Paquetes generales de *casos de uso*, del modelo del sistema.

El diagrama de interacción de actores, figura 2, muestra la generalización de las funciones de cada actor, donde el actor más general es el ciudadano y el más especializado es el jurado remanente, de acuerdo a esto se pueden analizar todas propiedades que puede heredar un actor de otro.

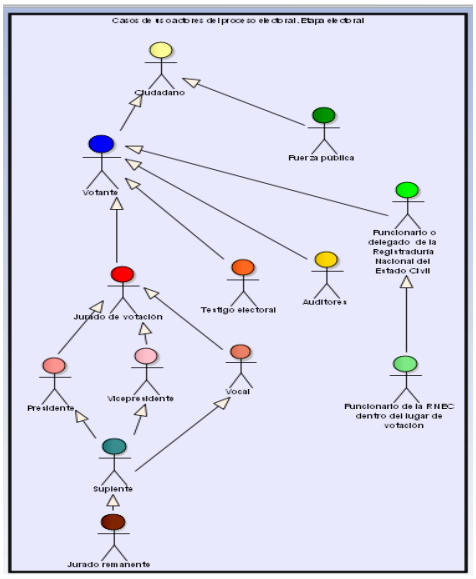


Fig. 2 Diagrama de interacción de actores.

Los *casos de uso* ubicados dentro del paquete *"lugar de votación"*, muestran principalmente la interacción que tiene el votante como actor primario y el jurado de votación como actor secundario en el proceso electoral, en los distintos

[27]Las herramientas CASE son diversas aplicaciones informáticas destinadas a aumentar la productividad en el desarrollo de software reduciendo el coste de las mismas en términos de tiempo y de dinero. Los sistemas CASE a menudo se utilizan como apoyo al método. Ver referencia [9]
[28]Stakeholder: Desde el punto de vista del desarrollo de sistemas, es aquella persona o entidad que está interesada en la realización de un proyecto o tarea. Tomado del libro: A. Cockburn, "Writing Effective Use Case" Published by Addison-Wesley, c. 2001. Ver referencia [9]

escenarios. Dentro de cada escenario existe un nuevo escenario más especializado que hereda las propiedades del escenario al cual pertenece. Esto se puede apreciar fácilmente en el diagrama de jerarquía de herencia de las clases de la figura 3.

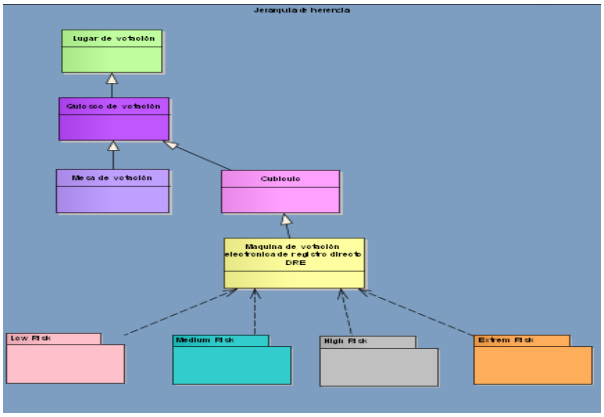


Fig. 3 Jerarquía de herencia de clases

Dentro del paquete "*máquina de votación electrónica de registro directo DRE*" se encuentra el diagrama de *casos de uso* primario, que muestra la interacción del votante con la máquina de votación DRE, además contiene cuatro paquetes, referentes a los riesgos que se determinaron en la investigación; bajos, medios, altos y extremos, como se enunció anteriormente. En cada paquete de riesgo se encuentra cada uno de los riesgos que pertenecen a la categoría correspondiente y para cada uno existe un nuevo paquete control que contiene las mitigaciones, contingencias y controles preventivos vinculados a este.

V. RESULTADOS

Como resultado del análisis del paralelo entre los dos procesos de votación, se obtuvo que el principal cambio que se debe realizar en el proceso electoral con tecnologías de votación electrónica es todo lo que concierne con la modernización y tecnificación del proceso de identificación y autenticación del votante, para lo cual se recomienda utilizar lectores de códigos de barra y lector biométrico que permitan validar la huella dactilar con una base de datos establecida por la RNEC. Este proceso debe garantizar efectividad para los tres tipos de cédulas existentes en Colombia. Por esto el sistema debe incluir un método de digitación de número de cédula para acceder a la base de datos y poder validar la información con la huella dactilar, esto para el caso de cédulas de primera generación.

A partir de experiencias y desafíos de procesos con votación electrónica, se pudo hacer un análisis ubicando debilidades y fortalezas de los procedimientos de votación, a fin de obtener posibles amenazas y efectos de los mismos. Se obtuvieron doce riesgos de relevancia en el momento de votación *in-situ*, los cuales se clasificaron de acuerdo a su impacto y probabilidad, en cuatro niveles, bajo, medio, alto y extremo. Se obtuvo un riesgo de clasificación extrema, cuatro con clasificación alta, cinco con clasificación media y dos con clasificación baja. Es importante resaltar que estos niveles pueden variar en el momento en que se seleccione el tipo de máquina y fabricante que se va a utilizar en el proceso electoral.

Se realizó el análisis de riesgos parcial de seguridad de la información, entendiendo impactos y efectos de ataques, logrando controles que pudieran llevarse a cabo durante la ejecución del procedimiento de votación electrónica. Para cada uno de los riesgos se encontraron tres tipos de controles, de tipo preventivo, mitigación y contingencia, los cuales permitirán al usuario disminuir las consecuencias y probabilidades del mismo riesgo. Por medio del análisis se identificaron con más precisión, las condiciones para garantizar un proceso de votación electrónica segura y confiable.

En el modelo se describió el proceso de votación electrónica analizado, de donde se puede ver una aproximación real y el cual contiene la información acerca de procedimientos, activos utilizados, características, actores y correspondiente papel que desempeñan al participar en el proceso electoral.

La construcción del modelo enfoca el análisis de riesgos del subsistema de votación electrónica por medio de la descripción de posibles amenazas, consecuencias y acciones de control.

VI. CONCLUSIONES Y OBSERVACIONES

De acuerdo al cuadro comparativo de los dos procesos de votación, se determinaron una serie de cambios que deben efectuarse en el proceso de votación electrónica con respecto al proceso de votación tradicional, resaltándose el uso de tecnología en la identificación del votante, utilizando lector biométrico, lector de código de barras para las cédulas de segunda y tercera generación y un sistema de ingreso numérico por medio de digitación para las cédulas de primera generación, que permitan realizar una validación de la identidad del votante por medio de la comparación con la base de datos de la Registraduría. Sin embargo cabe resaltar que para implementar estos cambios es necesario mitigar los vicios que tiene el proceso electoral desde su etapa preelectoral, que permitan devolver a los ciudadanos la credibilidad y confianza en el proceso electoral.

Se generó un modelo de seguridad de la información basado en un análisis de riesgos efectuado teniendo en cuenta el estándar AS/NZS 4360:2004. Se determinaron los puntos más críticos y se implementaron los controles respectivos.
Se definieron una serie de protocolos para ser tenidos en cuenta en caso de que los riesgos se materialicen, diferenciados en tres tipos, preventivos para disminuir la probabilidad que el suceso ocurra, mitigación para disminuir el impacto cuando dicho riesgo se materialice, y de

contingencia para tomar acciones correctivas frente a la materialización de dicho riesgo.

Se elaboró un modelo que comprende los riegos, las situaciones que lo generan y las acciones posteriores a las materialización en un lenguaje gráfico y fácilmente entendible como es el caso de SysML, el cual puede ser tomado para el desarrollo de una herramienta software que permitirá simular los eventos de riesgos que se podrían presentar cuando se implementa un subsistema de votación DRE.

Se logró identificar que muchos de los riesgos encontrados provienen principalmente de agentes externos a la máquina de votación, sin embargo no puede descartarse la posibilidad de materialización de riesgos derivados de la tecnología dado que podrían incurrir en un evento catastrófico para la continuidad y confiabilidad del sistema, de ahí la importancia de que se institucionalice y se implemente un modelo de seguridad de información para estos procesos electorales dada la importancia de estos frente al futuro y desarrollo de los sistemas políticas y económicos de los países que lo implementan.

La implementación de un lenguaje de modelado estandarizado internacionalmente facilita el entendimiento de este para poder desplegarlo hacia el desarrollo de componentes de tipo hardware y/o software dependiendo de la implementación que se haga a través de este, en este orden de ideas se garantiza con este trabajo la continuidad de este estudio dado que los resultados de la investigación realizada pueden ser extrapolables al desarrollo de nuevos trabajos concernientes no sólo con el desarrollo de nuevas herramientas y aplicaciones sino también con el mejoramiento de sistemas vitales para el ejercicio ciudadano como el caso del proceso electoral.

Si bien las experiencias internacionales son de gran ayuda no se puede basar un sistema electoral en otro, por esto el modelo se elaboro ceñido en la constitución política de Colombia y código electoral colombiano. Además de esto es importante cuando se determine la tecnología a utilizar, tener en cuenta la idiosincrasia del pueblo Colombiano en cuanto a tradiciones y aspectos socio-culturales, para de esta manera disminuir las posibilidades de tener un impacto que pueda traer consecuencias negativas. Por este motivo es importante también, que el proceso de cambio no se realice durante la etapa preelectoral sino con un tiempo bastante lógico y coherente que asegure las condiciones de confiabilidad y credibilidad en el sistema. En este momento en el que el país está en las puertas de terminar un proceso electoral, como lo son las elecciones presidenciales del próximo 30 de mayo del 2010, es el momento para empezar a hacer la gestión y la labor de administración electoral, la cual debe ser labor fundamental del próximo gobierno.

Durante el proceso electoral cualquier desviación de los procedimientos dictados por la ley, podría ocasionar violación de derechos fundamentales de los ciudadanos, o provocar amenaza a la integridad de los datos electorales y de resultados electorales. Por lo tanto estos procesos deben ser estudiados y analizados detenidamente con el fin de determinar mecanismos que garanticen la detección de dichos riesgos. Es por esto que a partir del análisis se logra evaluar la seguridad de los procedimientos y efectos de las desviaciones de comportamientos, con el objeto de destacar vulnerabilidades de la seguridad.

A pesar de todos los riegos de seguridad que podrían ocurrir en la máquina de votación electrónica DRE, no significa que se deban desechar esta tecnología, son muy buenos los beneficios que se pueden obtener como por ejemplo la rapidez en la consolidación y entrega de resultados, mayor alcance a la población con algún tipo de discapacidad. Pero si significa que debemos reconocer sus limitaciones y diseñar sistemas más precisos.

Una elección sin ningún tipo de problemas detectados, no es una prueba de que el sistema que se empleó es exitoso y seguro, es como si en una noche nadie irrumpe en su casa no significa que las cerraduras funcionan y su casa es segura, probablemente nadie intentó entrar o quizá alguien lo intento y lo logró, pero nadie lo notó.

VII. RECOMENDACIONES

Se entiende que el voto electrónico no fomenta ni facilita el derecho de expresión en las personas que se encuentran en una situación donde carecen de acceso a bienes materiales y educación. Por lo tanto, para que una urna electrónica asegure el acceso a los derechos de todo ciudadano de un país, resulta necesario implementar campañas educativas a fin de capacitar al ciudadano en unos aspectos mínimos como lo son la emisión del voto a través de la máquina de votación y el significado y la importancia de participar activamente en un proceso electoral y en especial concientizarlo sobre el poder que ejerce como integrante de un sistema democrático al ejercer su derecho. Estas campañas deben ser realizadas con mucha anticipación a la implantación del nuevo sistema de voto.

La seguridad es el primer requisito fundamental para lograr la confiabilidad en cualquier sistema, por lo tanto se debe tener mucho cuidado y conocimiento al momento de elegir el fabricante de las máquinas de votación DRE, ya que si se va a invertir dinero en un nuevo sistema de votación, tiene sentido invertirlo en tecnología que minimice el problema y no que lo incremente.

Es de alta recomendación que la máquina elegida tenga confirmación de voto física donde el votante solo pueda ver la confirmación y no pueda conservarla, de esta forma se puede realizar una auditoría o recuento en el eventual caso de alguna sospecha de fraude.

Si bien el proceso de reforma y modernización electoral es una buena alternativa para poder sanar los problemas de confiabilidad y credibilidad de los comicios colombianos, se debe tener en cuenta, como lo dice Carlos Mario Valenzuela

en su comentario sobre el trabajo de asistencia preparatoria de la Organización de las Naciones Unidas para diseñar un proyecto integral de modernización del sistema electoral colombiano, que el voto electrónico debe ser visto como un punto de llegada y no un punto de partida, por esto es necesario primero reformar los procesos que traen problemas de fondo, como el mismo censo electoral y la inscripción de las cédulas en la etapa preelectoral.

Aunque la ley 892 del 7 de Julio de 2004, en el parágrafo 2º del artículo 1º, sanciona y promulga que las urnas serán reemplazadas por registros en base de datos, los resultados del presente estudio permiten recomendar la utilización de una urna para almacenar un comprobante en papel que permita validar y soportar la información obtenida de la base de datos de la máquina de votación electrónica.

VIII. RECONOCIMIENTOS

Los autores expresan su agradecimiento a la Universidad Industrial de Santander y a la Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones por los conocimientos proporcionados a través de los años académicos.

Al Centro de Investigación y Desarrollo de la Ingeniería del Software – CIDLIS, en cabeza de su líder científico el Dr. Ricardo Llamosa, por su colaboración técnica, suministro de herramientas necesarias para realizar este estudio y por facilitarnos un espacio adecuado para la investigación.
Al ingeniero y director del proyecto Sergio Enrique Méndez Aceros, por su disponibilidad permanente, así como la continua colaboración técnica y científica brindada.

A Hugo Ernesto Martínez, estudiante PhD en Gestión y Desarrollo Tecnologico, por su colaboración y apoyo en temas técnicos, además quien encaminó a llevar a cabo este trabajo de investigación.

IX. BIOGRAFÍAS

Carlos Antonio Morales, nacido en la ciudad de Bogotá, Colombia, en el año de 1985. Recibió el título de Bachiller Académico en el 2001 del colegio Seminario Conciliar San Pio X (Bucaramanga, Colombia). Actualmente se encuentra cursando décimo nivel de Ingeniería Electrónica en la Universidad Industrial de Santander (UIS, Bucaramanga, Colombia) y adelanta estudios en administración empresarial en el centro industrial del diseño y la manufactura (CIDM, Bucaramanga, Colombia) perteneciente al servicio nacional de aprendizaje (SENA, Bucaramanga, Colombia).
Elsa Catalina Saavedra, nacida en la ciudad de Tuluá, Colombia, en el año de 1985. Recibió el título de Bachiller Académico en el 2001 del Colegio La Presentación (Bucaramanga, Colombia). Realizó un intercambio cultural durante el año 2006 a la ciudad de Portland, Maine, USA, con el objeto de perfeccionar el idioma inglés como segunda lengua. Actualmente se encuentra cursando décimo nivel de Ingeniería Electrónica en la Universidad Industrial de Santander (UIS, Bucaramanga, Colombia).
Sergio Andrés Gómez, nacido en la ciudad de Bucaramanga, Colombia, en el año de 1983. Recibió el título de Bachiller Académico en el 2001 del Colegio Agustiniano Bucaramanga (CAB, Bucaramanga, Colombia). Realizó un intercambio cultural durante el año 2006 a la ciudad de Portland, Maine, USA, con el objeto de perfeccionar el idioma inglés como segunda lengua. Actualmente se encuentra cursando décimo nivel de Ingeniería Eléctrica en la Universidad Industrial de Santander (UIS, Bucaramanga, Colombia).

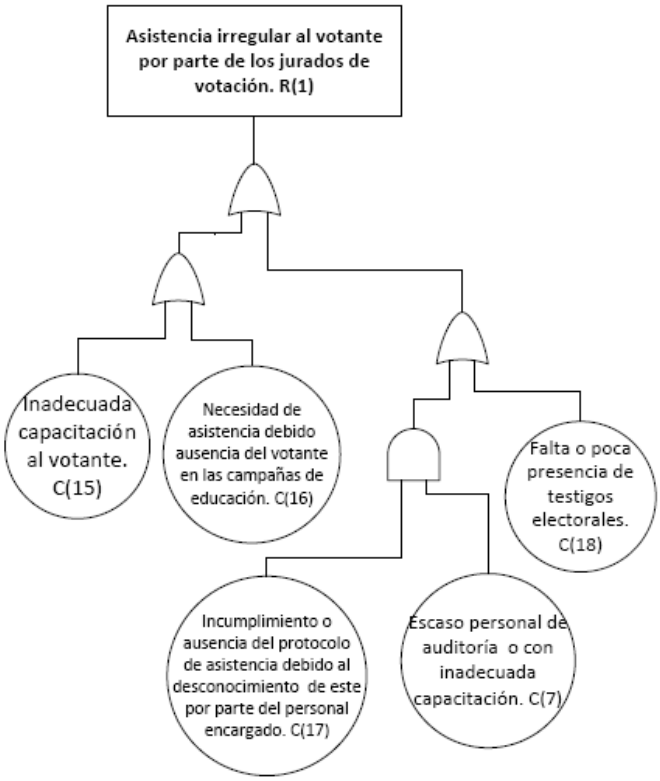
X. REFERENCIAS

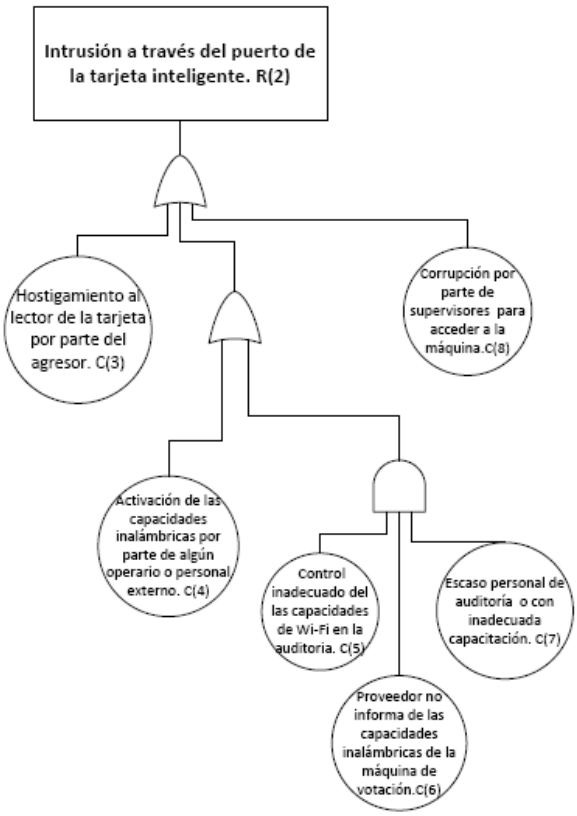
[1] Acevedo L. Andrea, Martínez A. Hugo, Pachón F. Carlos, Herrera L. Herly, Llamosa V. Ricardo. “Voto Electrónico en Colombia: Memorias de Prueba piloto de votación electrónica, realizada el 27 de Octubre de 2007”. Centro de innovación y Desarrollo para la investigación en ingeniería del Software, CIDLIS de la Universidad Industrial de Santander-UIS. Diciembre de 2007. Registraduría Nacional del Estado Civil.
[2] AS/NZS 4360:2004. Risk Management Systems Standar. Australia and New Zealand. 2004.
[3] Acevedo, A; Modelo de Análisis de confiabilidad basado en gestión de riesgos, aplicado al proceso de votación electrónica en Colombia. Tesis Magister, Universidad Industrial de Santander, Colombia, 2009
[4] http://www.britannica.com/EBchecked/topic/1472946/electronic-voting, visitado por última vez 20 Mayo de 2010
[5] Página Oficial de la Registraduría Nacional del Estado Civil, Republica de Colombia, disponible en: http://www.registraduria.gov.co/index.htm, visitado por última vez 20 Mayo de 2010
[6] Ley 892 de 2.004, República de Colombia
[7] Declaración Universal de los Derechos Humanos, Disponible en http://www.un.org/es/documents/udhr/index.shtml, visitado por última vez 20 Mayo de 2010
[8] Definición DRE disponible en:
[9] http://www.fec.gov/pages/dre.htm, visitado por última vez 20 Mayo de 2010
[10] A. Cockburn, “Writing Effective Use Case” Published by Addison-Wesley, c. 2001
[11] S. Friedenthal, A. Moore, R. Steiner, “OMG Systems Modeling Language Tutorial”, published by INCOSE, 2009.
[12] Tuesta Soldevilla, Fernando (2004). “El voto electrónico”. *Revista Elecciones*. Año 3, no. 3. Oficina Nacional de Procesos Electorales. pp. 55-81.
[13] Panizo Alonso, Luis. “Aspectos tecnológicos del voto electrónico”.--Lima: ONPE, 2007
[14] Confederación parlamentaria de las Américas. Primera vuelta de las elecciones presidenciales y legislativas de Brasil. Informe de la misión de observación electoral.
[15] Beatriz Busaniche; Federico Heinz; Alfredo Rezinovsky [et alt.]. “Voto electrónico: los riesgos de una ilusión”. 1ra ed. Córdoba: Fundación Vía Libre, 2008.

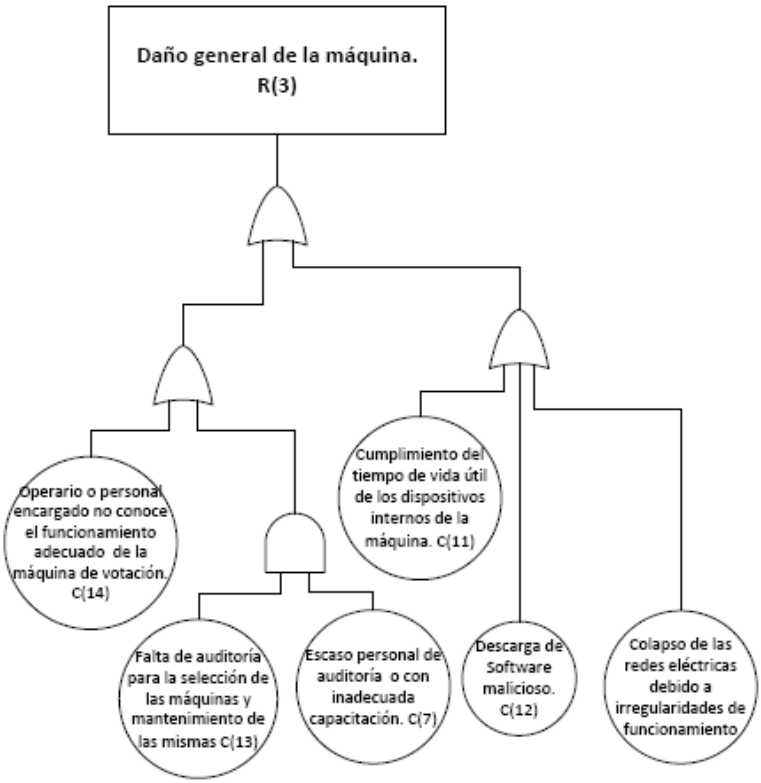
[16] Prince Alejandro, Et.Alt. “Consideraciones, aportes y experiencias para el Voto electrónico en Argentina”. Investigación periodística Enrique Garabetyan. Buenos Aires, 2005.
[17] República argentina. Ministerio del interior de la nación. Dirección nacional electoral. Grupo de trabajo nuevas tecnologías y procesos electorales. “Sistemas Electrónicos de Votación Fortalezas y Debilidades”, Versión Abril 2005.
[18] Código Electoral colombiano disponible en: http://200.31.213.136/videos/elecciones2010/dto_2241_1986.pdf, visitado por última vez 20 Mayo de 2010
[19] Calidad en la prestación del servicio publico de energía eléctrica, disponible en: http://basedoc.superservicios.gov.co/ark-legal/SSPD/details;jsessionid=076F022E293700028C1C000CDB4A7787?docId=cb360c1d-02ab-49d8-ae57-6049074995e9&channel=/C/CALIDAD+DEL+SERVICIO+Y+TARIFAS+DE+ENERGIA+ELECTRICA+Y+DE+GAS+NATURAL&subEspacio=, visitado por última vez 20 Mayo de 2010
[20] Análisis probabilístico de riesgos: Metrología del “Árbol de fallas y errores” Disponible en: http://fete.ugt.org/PRL/p_preventivo/pdf_ntp/ntp_333.pdf visitado por última vez 20 Mayo de 2010
[21] Página Web oficial SysML: **http://www.sysmlforum.com/tools.htm**, visitado por última vez 20 Mayo de 2010.

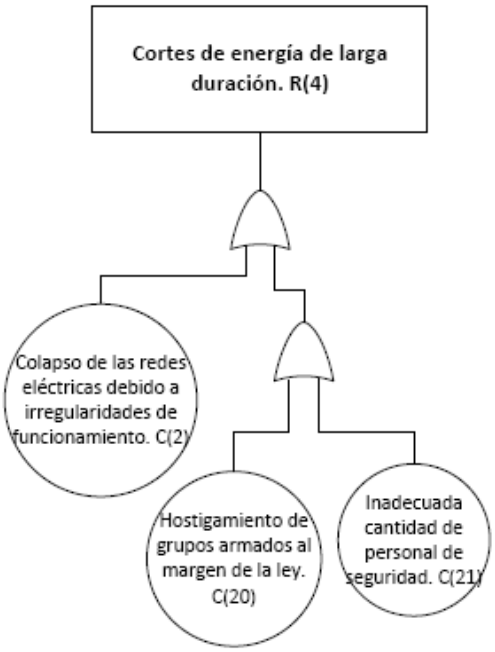
XI. ANEXO

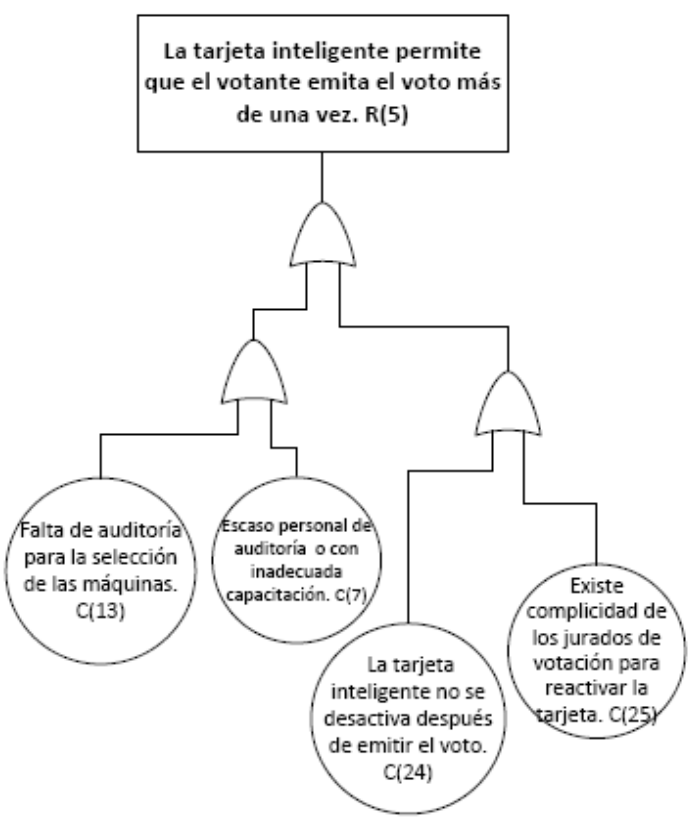
A. ÁRBOLES DE FALLAS DE RIESGOS

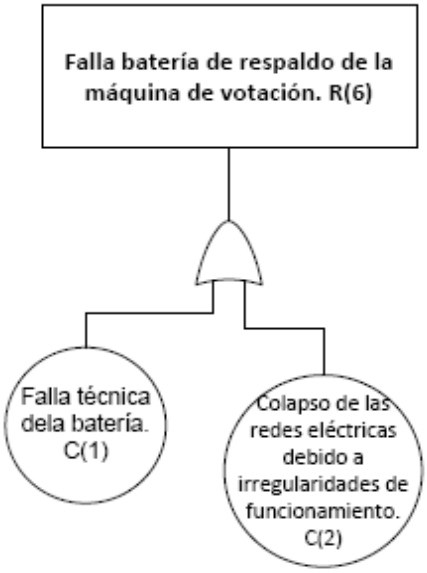


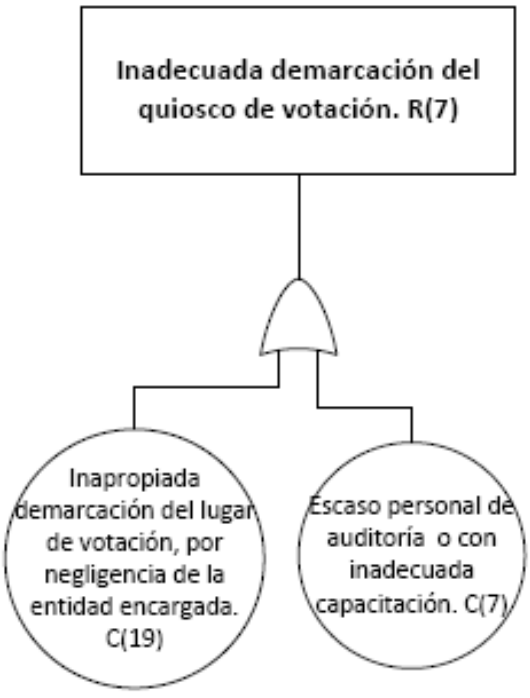


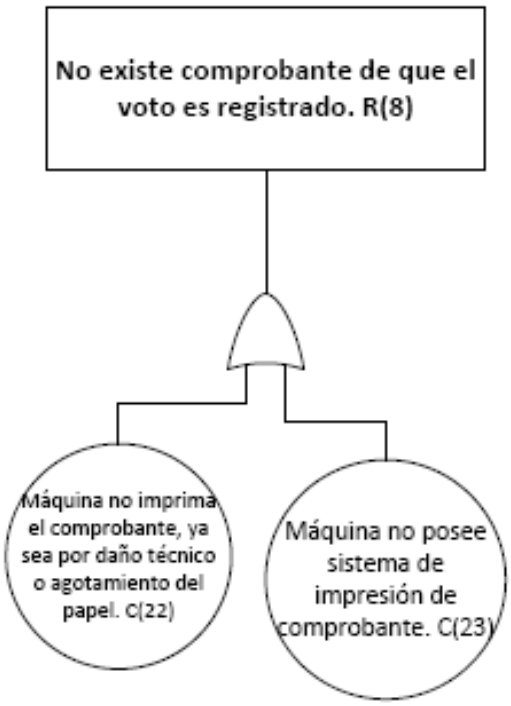


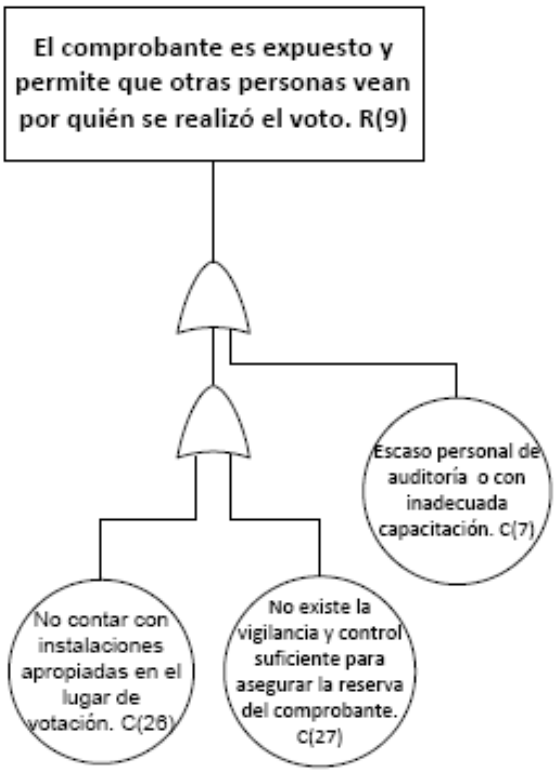


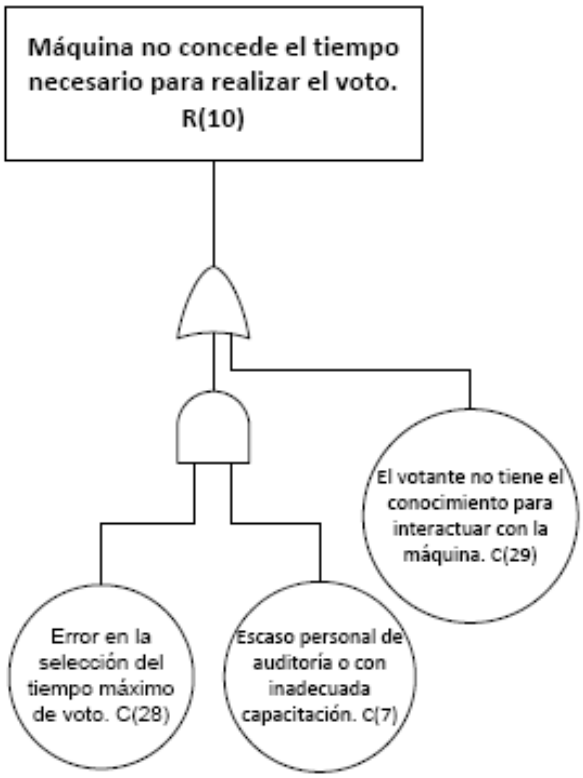

La tarjeta inteligente permite que el votante emita el voto más de una vez. R(5)
Falta de auditoría para la selección de las máquinas. C(13)
Escaso personal de auditoría o con inadecuada capacitación. C(7)
La tarjeta inteligente no se desactiva después de emitir el voto. C(24)
Existe complicidad de los jurados de votación para reactivar la tarjeta. C(25)

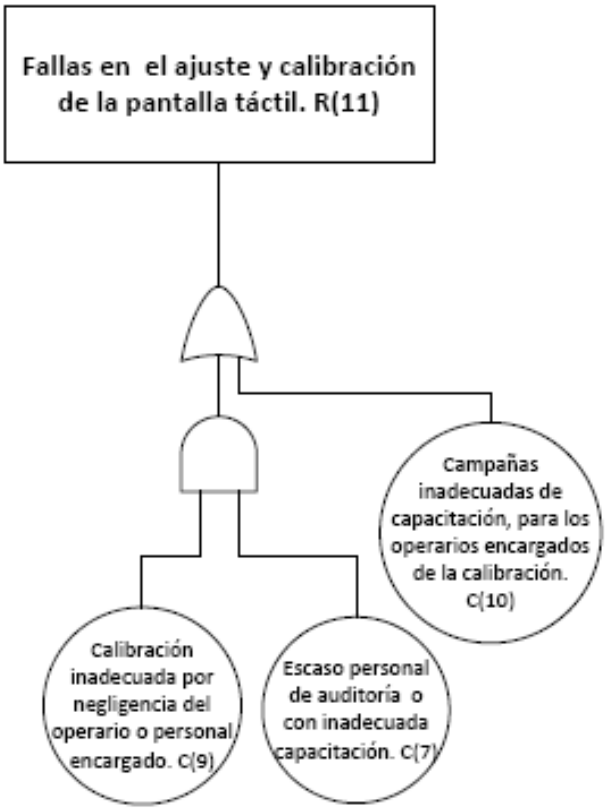

Falla batería de respaldo de la máquina de votación. R(6)
Falla técnica dela batería. C(1)
Colapso de las redes eléctricas debido a irregularidades de funcionamiento. C(2)

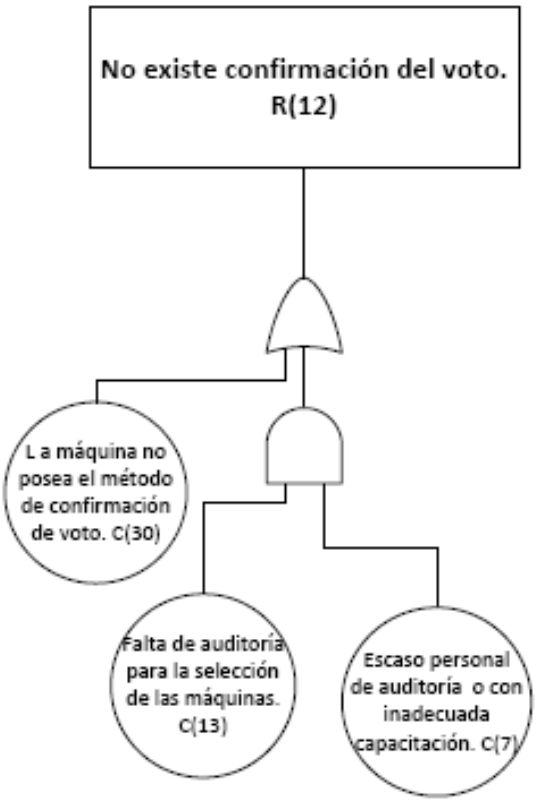

Inadecuada demarcación del quiosco de votación. R(7)
Inapropiada demarcación del lugar de votación, por negligencia de la entidad encargada. C(19)
Escaso personal de auditoría o con inadecuada capacitación. C(7)


No existe comprobante de que el voto es registrado. R(8)
Máquina no imprima el comprobante, ya sea por daño técnico o agotamiento del papel. C(22)
Máquina no posee sistema de impresión de comprobante. C(23)


El comprobante es expuesto y permite que otras personas vean por quién se realizó el voto. R(9)
Escaso personal de auditoría o con inadecuada capacitación. C(7)
No contar con instalaciones apropiadas en el lugar de votación. C(26)
No existe la vigilancia y control suficiente para asegurar la reserva del comprobante. C(27)


Máquina no concede el tiempo necesario para realizar el voto. R(10)
El votante no tiene el conocimiento para interactuar con la máquina. C(29)
Error en la selección del tiempo máximo de voto. C(28)
Escaso personal de auditoría o con inadecuada capacitación. C(7)


Fallas en el ajuste y calibración de la pantalla táctil. R(11)
Campañas inadecuadas de capacitación, para los operarios encargados de la calibración. C(10)
Calibración inadecuada por negligencia del operario o personal encargado. C(9)
Escaso personal de auditoría o con inadecuada capacitación. C(7)


No existe confirmación del voto. R(12)
L a máquina no posea el método de confirmación de voto. C(30)
Falta de auditoría para la selección de las máquinas. C(13)
Escaso personal de auditoría o con inadecuada capacitación. C(7)