MODELO DE ANÁLISIS DE CONFIABILIDAD BASADO EN GESTIÓN DE RIESGOS, APLICADO AL PROCESO DE VOTACIÓN ELECTRÓNICA EN COLOMBIA

ANDREA MILENA ACEVEDO LIPES

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE INGENIERÍAS FISICO-MECÁNICAS

ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

BUCARAMANGA

2009

MODELO DE ANÁLISIS DE CONFIABILIDAD BASADO EN GESTIÓN DE RIESGOS, APLICADO AL PROCESO DE VOTACIÓN ELECTRÓNICA EN COLOMBIA

ANDREA MILENA ACEVEDO LIPES

INGENIERA ELECTRÓNICA

Trabajo de Investigación presentado como requisito parcial

Para optar por el título

Magíster en Ingeniería Electrónica

Director: RICARDO LLAMOSA VILLALBA, PhD

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE INGENIERÍAS FISICO-MECÁNICAS

ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

BUCARAMANGA

2009

DEDICATORIA

Dedico este proyecto principalmente a Dios.

A mi padre(q.e.p.d) quien me enseñó la importancia de la disciplina y la constancia para alcanzar las metas propuestas y mi madre, que con su cariño, entrega y paciencia siempre me animó a finalizar esta etapa.

AGRADECIMIENTOS

A la Universidad Industrial de Santander y la escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones por brindarme la oportunidad de formarme como magíster y ser mi segundo hogar durante estos últimos 10 años.

Al Centro de Innovación y Desarrollo para la Investigación en Ingeniería del Software-CIDLIS, en cabeza del profesor Ricardo Llamosa Villalba, quien me brindó la oportunidad de participar en varios proyectos y desarrollar mi investigación.

Al equipo de e-voting, Hugo Martínez, Herly Herrera, Carlos Pachón y Sergio Méndez, con quienes viví una de las experiencias más emocionantes hasta el momento, en mi vida profesional, la prueba Piloto de Votación Electrónica.

A Houseman, a toda mi familia y amigos quienes siempre creyeron en mí y me apoyaron hasta el final.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

RESUMEN

TÍTULO: Modelo de Análisis de Confiabilidad Basado en Gestión de Riesgos Aplicado al Proceso de Votación Electrónica en Colombia [*]

AUTOR: Andrea Milena Acevedo Lipes [**]

PALABRAS CLAVE: Modelo de análisis, Confiabilidad, Voto Electrónico, Gestión Probabilística, Riesgos.

CONTENIDO: Los procesos electorales en las democracias son eventos críticos e importantes de toma de decisión ciudadana, en la elección de dirigentes de estado de las naciones. En Colombia, las autoridades electorales como la Comisión Electoral y la Registraduría Nacional del Estado Civil, velan por los derechos democráticos, y para ese logro optan por apoyarse en herramientas de Información y Telecomunicación para optimizar y mejorar la prestación de sus servicios. En este contexto, la prueba piloto del voto electrónico del 27 de Octubre de 2007, realizada por la Registraduría Nacional, con el apoyo del Centro de Innovación y Desarrollo para la Investigación en Ingeniería del Software-CIDLIS de la Universidad Industrial de Santander, permitió conocer el impacto de las nuevas tecnologías en un escenario real. En esta prueba se realizaron diferentes mediciones, para llevar a cabo un análisis cualitativo de gestión de riesgos respecto a los aspectos críticos del sistema, como identificación, autenticación y votación.

Una de las conclusiones más importantes obtenidas del piloto, fue la necesidad de llevar a cabo un análisis más profundo y objetivo de los riesgos que pueden afectar el proceso de votación electrónica en Colombia, justificado en la importancia del proceso electoral para la democracia del país. Para llevar a cabo este análisis era necesario crear y aplicar herramientas que permitieran no solo conocer, sino también cuantificar los riesgos de cada etapa del proceso, para crear controles y estrategias de prevención y mitigación.

Concretamente, se propuso un modelo para análisis cuantitativos que sirviera como herramienta para hallar la confiabilidad del proceso de votación electrónica en Colombia, basado en el análisis causa-efecto de los eventos que pueden generar fallas o errores en la etapa de votación, en sus aspectos: Estratégicos, tácticos, operativos y de logística.

---

[*] Tesis de Grado

[**] Facultad de Ingenierías Físico mecánicas. Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones. Universidad Industrial de Santander. Director: Ricardo Llamosa Villalba.

ABSTRACT

TITLE: Reliability Analysis Model Based on Risk Management Applied to Electronic Voting Process in Colombia [*]

AUTHOR: Andrea Milena Acevedo Lipes [**]

KEY WORDS: Analysis model, Reliability, Electronic Voting, Probabilistic Risk Management.

DESCRIPTION: Elections in democracies are critical events and important civic decision-making, in the choice of state leaders of nations. In Colombia, electoral authorities as the Electoral Commission and the National Registry, ensure democratic rights, and for this achievement choose to rely on information and telecommunication tools to optimize and improve the delivery of their services. In this context, the Pilot of Electronic Voting on 27 October 2007, conducted by the National Registry, with support from the Innovation and Development Center for Research in Software Engineering-CIDLIS from Industrial University of Santander, allowed to assess the impact of new technologies in a real scenario. In this test, various measurements were made to carry out a qualitative analysis of risk management on critical aspects of the system, such as identification, authentication and vote.

One of the most important conclusions obtained from the pilot, was the need to conduct a more thorough and objective analysis of risks that may affect the electronic voting process in Colombia, justified by the importance of the electoral process for democracy in the country. To perform this analysis, was necessary to create and use tools that allow not only discover but also to quantify the risks of each stage of the process in order to create controls and strategies for prevention and mitigation.

Specifically, It was proposed a model for quantitative analysis to serve as a tool for finding the reliability of electronic voting process in Colombia, based on cause-effect analysis of events that can generate faults or errors in the voting phase, from Strategic, tactical, operational and logistics points of view

---

[*] Degree Thesis

[**] Physical Mechanical Engineering Faculty. Electrical, Electronic and Telecommunication engineering School. Industrial University of Santander. Director: Ricardo Llamosa Villalba.

CAPÍTULO I: INTRODUCCIÓN

Desde los inicios de la civilización, ha habido el interés por predecir eventos y situaciones. Actualmente, en las empresas y en el gobierno, en general, anticipar sucesos es la línea base para planificar estrategias preventivas y de mitigación, para garantizar la continuidad de la actividades de sus negocios.

A pesar que las estrategias de gestión de riesgos y de confiabilidad se emplean desde hace varias décadas, su uso ha tomado un renovado significado después de los ataques del 9-11 a las torres gemelas.

Es por esto que este proyecto de investigación se desenvuelve en el entorno cualitativo y cuantitativo del riesgo y la confiabilidad del voto electrónico considerando que:

- El análisis cualitativo se emplea en proyectos sencillos, caracterizados porque no se hace necesaria la precisión de la predicción de los eventos indeseables ó porque en tales proyectos sólo prima la subjetividad y la opinión de expertos que en ocasiones produce re-procesos importantes.

- El análisis cuantitativo se emplea en proyecto o actividades complejas de alta prioridad y riesgo. Es necesaria la precisión en el establecimiento de eventos en escenarios que puedan afectar grandes inversiones, o la seguridad y estabilidad humanas.

- El proyecto de prueba piloto de voto electrónico, es el escenario de este proyecto de investigación en el que el análisis de confiabilidad, seguridad y gestión de riesgos en torno a las Tecnologías de Información y Comunicación, es fundamental para el logro del resultado estratégico de selección de dirigentes en un país.

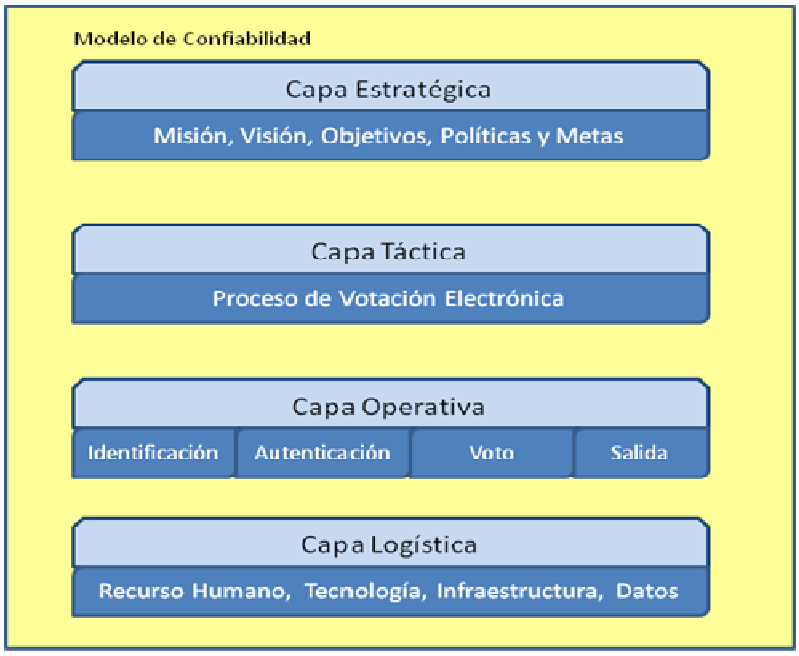
1.1 FORMULACIÓN/DECLARACIÓN DEL PROBLEMA

Los procesos electorales en las democracias son eventos críticos e importantes de toma de decisión ciudadana, en la elección de dirigentes de estado de las naciones. En Colombia, las autoridades electorales como la Comisión Electoral y la Registraduría Nacional del Estado Civil, velan por los derechos democráticos, y para ese logro optan por apoyarse en herramientas de Información y Telecomunicación para optimizar y mejorar la prestación de sus servicios. En este contexto, la prueba piloto del voto electrónico del 27 de Octubre de 2007, realizada por la Registraduría Nacional, con el apoyo del Centro de Innovación y Desarrollo para la Investigación en Ingeniería del Software-CIDLIS de la Universidad Industrial de Santander, permitió conocer el impacto de las nuevas tecnologías en un escenario real. En esta prueba se realizaron diferentes mediciones [1], para llevar a cabo un análisis cualitativo de gestión de riesgos respecto a los aspectos críticos del sistema, como identificación, autenticación y votación [1], con el fin de establecer estrategias y controles que permitieran la ejecución adecuada del proceso.

Una de las conclusiones más importantes obtenidas del piloto de votación electrónica [1], fue la necesidad de llevar a cabo un análisis más profundo y objetivo de los riesgos que pueden afectar el proceso de votación electrónica en Colombia, justificado en la importancia del proceso electoral para la democracia del país. Para llevar a cabo este análisis es necesario crear y aplicar herramientas que permitan no solo conocer, sino también cuantificar los riesgos de cada etapa del proceso, para crear controles y estrategias de prevención y mitigación. Concretamente, se propone realizar un análisis cuantitativo que sirva como herramienta para formular un modelo de confiabilidad del proceso basado en el análisis causa-efecto de los eventos que pueden generar fallas o errores en el proceso de votación electrónica, en sus aspectos: Estratégicos, tácticos, operativos y de logística(Ver figura 1).

A partir del modelo de confiabilidad se pretende hallar el nivel de confiabilidad que presenta actualmente el proceso electrónico electoral, para el cual se ha establecido como hipótesis principal, que su confiabilidad será bastante baja, debido a la poca experiencia y madurez de los procesos electorales electrónicos en el país.

Figura 1: Cobertura de análisis en el modelo de Confiabilidad del proceso de votación electrónica en Colombia.



Fuente: Autor

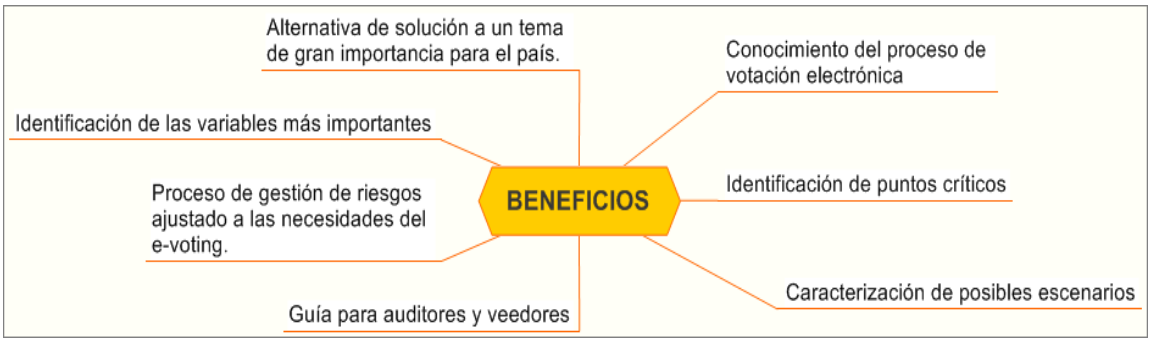
1.2 MOTIVACIÓN Y JUSTIFICACIÓN

Contar con un modelo de confiabilidad del proceso de votación electrónica, que identifique los puntos críticos del sistema, permitiría establecer controles adecuados garantizando la seguridad y continuidad del mismo y obtener así un ejercicio democrático y trasparente en el cual haya un nivel alto de confianza por parte de la ciudadanía, las entidades y partidos políticos en general. Además de esto, también garantizaría una mejor distribución de los presupuestos asignados para la realización de las elecciones ya que cada control establecido tendría una justificación evitando el despilfarro o la mala utilización del presupuesto.

El modelo propuesto, también crearía un punto de referencia para toma de datos en procesos futuros, proveyendo de información a auditores y veedores del proceso, acerca de los problemas que podrían surgir en la ejecución del mismo.

En la figura 2 se resumen los beneficios que traería consigo la ejecución del proyecto:

Figura 2:Beneficios de la ejecución del proyecto



Fuente: Autor

1.3 PROPUESTA DE INVESTIGACIÓN

1.3.1 *OBJETIVO GENERAL*

Proponer un modelo de confiabilidad, aplicado al proceso de votación electrónica en Colombia, que permita la identificación de los puntos críticos en la etapa de emisión del voto.

1.3.2 *OBJETIVOS ESPECÍFICOS*

1. Identificar los procesos, variables, eventos y riesgos del proceso de votación, a partir de la experiencia de la Prueba Piloto de votación electrónica realizada el 27 de octubre de 2007.

2. Formular un modelo de confiabilidad basado en gestión cualitativa y cuantitativa de riesgos que permita identificar y analizar los puntos críticos del sistema.

3. Aplicar el modelo de confiabilidad al proceso de votación electrónica en Colombia, en su instancia de emisión del voto.

4. Proponer controles preventivos y/o correctivos que se ajusten a la naturaleza del riesgo y garanticen mayor confiabilidad en el proceso.

1.4 ORGANIZACIÓN DEL DOCUMENTO

Este documento está organizado en ocho capítulos y cuatro anexos. El capítulo 1 contiene la introducción al documento, el planteamiento del problema, la justificación de la investigación y los objetivos del proyecto.

El capítulo 2 describe el estado del arte de la votación electrónica en el mundo y en Colombia, haciendo énfasis en los resultados obtenidos en la prueba piloto de votación de octubre de 2007, los cuales sirvieron como base para plantear las hipótesis que originaron el desarrollo de la presente investigación.

El capítulo 3 expone el modelo cuantitativo y cualitativo de gestión de riesgos propuesto de acuerdo los resultados de la prueba descrita en el capítulo 2 .

El capitulo 4 describe la aplicación y prueba del modelo para (expuesto en el capítulo 3), verificar su validez.

El capitulo 5 Describe los controles que deben implementarse para mitigar ó evitar la materialización ó presencia de eventos que puedan afectar la continuidad del proceso de voto electrónico.

El capitulo 6 contiene las conclusiones y recomendaciones derivadas de la investigación.

El capítulo 7 contiene la bibliografía consultada y que sirvió de apoyo para el desarrollo del proyecto.

El anexo A presenta la normatividad actual del voto electrónico en Colombia.

El Anexo B describe las amenazas y matrices de riesgo elaboradas para el piloto de votación electrónica.

El anexo C presenta el análisis a través de sistemas de inferencia fuzzy, realizado para obtener datos de entrada adecuados para probar el sistema propuesto.

CAPITULO II: ESTADO DEL ARTE Y MARCO TEÓRICO

A medida que las tecnologías de Información y Comunicación (TIC) cambian dramáticamente las vidas de las personas, los gobiernos deben desarrollar estrategias que permitan mejorar la relación de los ciudadanos con el estado. A los procesos y herramientas concebidas para la mejora de esta relación se le conoce como Gobierno Electrónico o E-Government., las cuales permiten el acceso telemático a los servicios ofrecidos por una administración, tanto para tramitación como para consulta. E-government exige una adaptación y evolución de los sistemas de información actuales, de tal forma que puedan cumplirse características importantes como: Accesibilidad, Conocimiento, Eficacia, Solidez y Democracia.

Uno de los objetivos primarios del e-Government es la mejora de los procesos democráticos del estado, mejorando la accesibilidad y confiabilidad de los mismos, utilizando la tecnología como herramienta mas no como un fin. Asi surge lo que se conoce como e-Democracia o e-Democracy, cuyo elemento más importante y representativo son las votaciones o proceso electoral, conocido como e-Voto o e-Voting.

El e-Voto se trata principalmente del uso de las TIC's para el mejoramiento del proceso electoral. Para esto, se ha tomado el modelo básico de votación –identificación manual, urnas de cartón, tarjetones, y conteo manual – y se ha reemplazado por identificación y autenticación a través de dispositivos conectados a bases de datos, urnas electrónicas, transmisión automática de resultados, etc . Entonces, de forma más directa, se podría considerar al voto electrónico como la incorporación de recursos informáticos en cualquier parte del proceso electoral, ya sea en el registro de ciudadanos, el ejercicio del voto, el escrutinio y/o la transmisión de resultados. Actualmente el voto electrónico, es uno de los instrumentos de apoyo a la e-Democracia en Suramérica [3], Norteamérica [5] y en casi toda Europa [4], cuyos resultados en general se pueden considerar como positivos aunque existen muchos aspectos por mejorar.

En Colombia el proceso de desarrollo tecnológico electoral ha cubierto la actualización de recursos informáticos, el estudio de requerimientos de innovación y el desarrollo de procesos y tecnologías de codificación electrónica segura de la identidad ciudadana (e-cédula). Actualmente, el proceso de desarrollo se encuentra en una segunda fase, en la que se está modernizando el registro civil y el sistema de identificación ciudadana (PMTII) [23]. La última fase de este desarrollo, incluirá el proceso electoral, hecho que está previsto para su implementación en el año 2010.

Existen principalmente dos tipos de voto electrónico: remoto y presencial. El voto remoto, es conocido también como voto por internet y aunque no es el caso de estudio en este proyecto de investigación pues su implementación, riesgos y beneficios son diferentes al voto presencial, vale la pena mencionarlo como una de las opciones disponibles. Por otro lado, el voto electrónico presencial, puede llevarse a cabo utilizando alguno de los mecanismos de votación que se han clasificado en dos grandes grupos: a) Los sistemas de recuento automático de votos mediante el reconocimiento óptico de las marcas realizadas por los ciudadanos en los tarjetones. b) Los sistemas de registro directo electrónico o DRE conocidos como urnas electrónicas.

Un sistema de votación electrónico es una combinación de dispositivos electromecánicos o electrónicos que incluyen el software requerido para programar, controlar y brindar soporte al equipo utilizado para almacenar los votos, realizar el conteo y reportar los resultados de la votación. El sistema de votación también puede incluir la transmisión de datos a través de una red de comunicaciones. En un amplio sentido, un sistema de voto electrónico hace referencia a la tecnología que es viable utilizar en diferentes fases de un proceso electoral (registro de electores, administración electoral, verificación de identidad, emisión de voto, recuento de votos, transmisión de resultados).

El voto electrónico, en todas sus formas (presencial, remoto) ya tiene un amplio lugar en la historia de las democracias. Países como Brasil, Bélgica, Costa rica, Francia, Venezuela, Perú, Ecuador, Paraguay, Argentina [2], Estados Unidos [6], Reino Unido [7], Australia, México, España [8] e India ya lo han implementado.

A pesar que la votación electrónica ha arrojado resultados positivos en la mayoría de los países que lo han implementado, todavía existen grandes riesgos de fraudes debido a que en algunos casos, la transmisión de votos hacia los centros de acopio no es totalmente automática, sino que intervienen funcionarios al final de la jornada recogiendo los resultados en discos magnéticos y en general, otros aspectos que introducen huecos de seguridad en el sistema. En lo referente a riesgos en voto electrónico, se puede consultar los resultados reportados por Thomas W. Lauer [9] quien desde un enfoque de gestión, realiza una comparación y análisis cualitativo de riesgos del voto electrónico con DRE(Direct Recording Electronic o Registro Electrónico Directo del voto)y voto a través de internet. Lauer propone a OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), el cual es un proceso para identificar riesgos asociados a sistemas de la información, como herramienta principal para identificar los riesgos asociados al proceso. Las misiones de observación de elecciones, también realizan publicaciones de sus hallazgos, como por ejemplo las de Escocia e Inglaterra [24], quienes realizaron un reporte de lo observado en las elecciones de 2007 en estos países.

En el ámbito europeo, el gobierno Belga es el pionero en la aplicación de sistemas de voto electrónico en el mundo. Comenzó su camino en 1989 con un estudio de sustitución del sistema tradicional por otros procesos con tecnologías avanzadas para la época y el 8 de Octubre del 2000 el sistema de voto electrónico fue ampliamente utilizado por la población, el 44% realizó el proceso electrónicamente.

Por otro lado, en el ámbito Latinoamericano, más específicamente en Colombia, el 27 de Octubre de 2007, se realizó el más reciente piloto de votación electrónica. El plan piloto fue una prueba no vinculante que buscó la identificación, operatividad y funcionalidad de tecnologías en un entorno ficticio de votación, pero con características asociadas a una votación real y de carácter oficial, respecto a etapas predefinidas de identificación, autenticación, entrenamiento, voto, consolidación, divulgación y cierre. Con el fin de dar pluralidad al concepto de utilización de tecnologías se convocó a varios proveedores de votación electrónica con experiencias nacional e internacional en la

materia, de manera que permitiera una visión integral desde puntos de vista diferentes representados en sus tecnologías. De esta manera una vez realizada la convocatoria respondieron al llamado, cuatro proveedores: Dominion Voting(Canadá), Voting Solutions(EU), Indra(España) y Smartmatic(Venezuela).

La prueba piloto se realizo en las ciudades de Bogotá, San Andrés y Pereira, en tres centros comerciales de cada ciudad. En cada centro comercial de cada ciudad se utilizaron dos máquinas de votación electrónica por proveedor de tecnología participante, en total por ciudad se utilizaron 24 máquinas de votación y un total de 72 máquinas de votación en el país. Las ciudades fueron elegidas de acuerdo a las disposiciones de la RNEC, y los centros comerciales como una muestra representativa de estratos y por la afluencia de personas que garantizaran una buena participación en la prueba. La ubicación de las máquinas de votación en cada centro comercial se realizó teniendo en cuenta condiciones físicas y de infraestructura mínima, como buen suministro de electricidad, infraestructura de comunicaciones, y cubiertos. La participación del ciudadano fue de carácter voluntario y teniendo en cuenta que no existía una experiencia anterior en el uso de las tecnologías ofrecidas por los proveedores no pudo predecirse con exactitud el número de personas que contribuirían en la realización del piloto, sin embargo, el tamaño de la muestra obtenido ofrece confiabilidad a las inferencias que se realizaron a partir de los resultados derivados.

2.1 CARACTERÍSTICAS DE LA PRUEBA PILOTO

A pesar que la prueba fue totalmente independiente de un proceso electoral oficial, el ciudadano que deseaba participar debía cumplir el requisito básico de portar la cédula de ciudadanía. Una vez el ciudadano ingresaba al centro de votación, debía ser identificado, registrado y autenticado en la mesa de inscripción para la prueba. En esta mesa se le indicaba a cual proveedor de tecnología debía dirigirse para realizar la votación. Una vez el ciudadano accedía a la máquina asignada se le capacitaba para su uso.

Al finalizar la votación, el ciudadano debía responder un cuestionario, que permitió medir el impacto del uso de tecnologías de voto electrónico y como percibe estas tecnologías comparadas con el proceso electoral tradicional.

2.1.1 PUNTOS GENERALES DE EVALUACIÓN

Para la prueba piloto, se evaluaron 4 aspectos principales y considerados como críticos en el funcionamiento del proceso:

1. Tiempos de votación de la ciudadanía (tiempo de utilización de la máquina), tiempos de entrenamiento realizados por los proveedores a los ciudadanos y tiempos de Identificación, Registro y Autenticación.
2. Encuesta para medir características como conocimiento, actitud y percepción de los ciudadanos ante el uso de las tecnologías de votación electrónica.
3. Características de los ciudadanos participantes como género, escolaridad, y edad que permitieran la clasificación e interpretación de resultados organizados por criterios.
4. Vulnerabilidades y riesgos que introducen las nuevas tecnologías de votación electrónica.

2.1.2 CONDICIONES IMPRESCINDIBLES

Para la prueba, las tecnologías de cada proveedor debía brindar una evidencia física que mostrara en el inicio de la prueba, las características de registros en cero y al final, la cantidad de votos registrados en las máquinas de votación. Estas evidencias se enmarcaron en al acta de inicio (boletín cero) y el acta de cierre (registro de votos). Lo anterior era necesario para cumplir con las evidencias requeridas por el proceso electoral colombiano. También se establecieron los criterios básicos con los que debía cumplir la prueba para garantizar los principios de democracia y anonimato que debe tener el voto[25]:

- No debe existir trazabilidad del votante entre la etapa de identificación, registro y autenticación y la etapa de voto.

- El voto será de carácter presencial.
- El tarjetón electoral basado en el modelo ficticio fue el mismo para cada uno de los proveedores con el fin de asegurar igualdad de condiciones en el proceso.
- Se aceptaron los tres tipos de cédulas existentes teniendo en cuenta que los ciudadanos que portaban cédulas de tercera generación en la etapa de autenticación, pudieron ser autenticados a través del Morpho Touch.
- El mecanismo electrónico de votación debía asegurar el secreto y la inviolabilidad del voto del ciudadano.

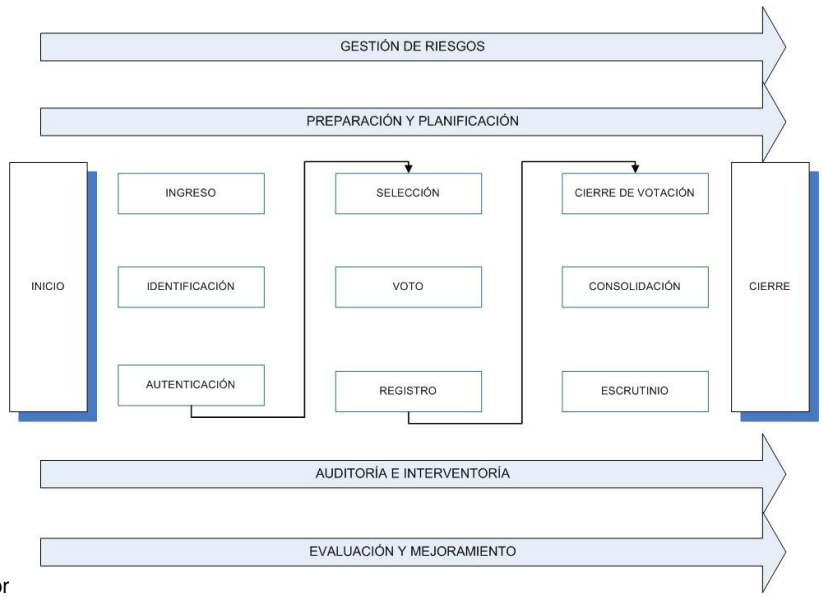
2.2 ESTRUCTURACIÓN DEL PROCESO DE VOTO ELECTRÓNICO

Para realizar la prueba piloto, debía establecerse claramente el orden de procesos y actividades que se llevarían a cabo. Por esto que se creó un modelo basado en experiencias externas , que sirvió de guía para la planificación y ejecución de la prueba piloto.

2.2.1 ACTIVIDADES QUE CONFORMARON EL PROCESO DE VOTACIÓN ELECTRÓNICA

La votación electrónica está compuesta de varias sub-etapas que se pueden observar en la figura 3 y se describen a continuación.

Figura 3:Diagrama de Flujo del Proceso de Votación Electrónica, implementado en el piloto



Fuente:Autor

i. **Inicio y preparación:** Esta actividad se compone de las actividades de formalización del contrato y preparación de los recursos que se deben utilizar el día de las elecciones, incluyendo los simulacros y pruebas al sistema.

Inicio del contrato: esta etapa implica realizar formalmente el perfeccionamiento y firmado del mismo; después de este evento, la empresa debe empezar a prepararse (el mobiliario, los sistemas que intervienen) para la realización del proceso, los simulacros y el día de elecciones.

Acta de Inicio del proceso: Se realiza el acta de inicio de la votación electrónica de manera formal el día previo a las elecciones. Deben establecerse garantes que garanticen la transparencia de esta etapa.

Acta de Congelamiento: Se establece en este procedimiento las condiciones iniciales del sistema (Incluye maquinas, servidores, procesos, logística, Software con contadores y registros en cero), las cuales deben garantizar que ninguna entidad o unidad

funcional sea modificada antes del proceso de descongelamiento, guardando su evidencia en medios magnéticos y/o papel.

Emisión boletín CERO: Corresponde a un acta en la cual se verifica y valida que todos los sistemas relacionados en el acta de congelamiento se encuentran en condiciones iniciales con contadores en cero. Técnicamente el proceso de consolidación (total del sistema y maquinas) debe emitir un boletín con su registro sin votos que sea almacenable y/o permita evidenciar los resultados.

Acta de descongelamiento: Se verifica y valida que las condiciones del sistema establecidas en el acta de congelamiento y boletín CERO, se mantengan inalteradas. Luego del proceso de verificación se dará apertura a la jornada electoral.

Inicio de la votación: En esta etapa se da inicio formal al proceso electoral de acuerdo a las instrucciones impartidas por la registraduría.

ii. Ingreso:

En este paso del proceso de elecciones, se controla el acceso de los votantes (con el apoyo de la fuerza pública), de manera ordenada y con el requisito de portar su documento de identidad.

iii. Identificación:

En este paso el votante acredita su identidad ante el jurado de mesa a través de la cedula de ciudadanía, y el jurado también verifica (leyendo la cedula con un lector de código de barras) que el votante se encuentra habilitado para

votar. Cabe mencionar que este paso debe darse simultáneamente con la autenticación

iv. Autenticación:

En la etapa de autenticación, el votante coloca su dedo índice en el 'Morpho Touch' para validar su identidad. La autenticación se realiza electrónicamente por comparación de la lectura del código de barras de la cedula con la lectura de la huella del votante, realizada con el sistema 'Morpho Touch' y de la base de datos del registro de ciudadanos. El proceso de autenticación es independiente del proceso de votación. Inmediatamente se autentica la identidad del votante, se habilita la maquina y se le da ingreso al cubículo de votación para que este realice su voto.

v. Selección:

En este paso, el votante busca en los listados de los archivos de la maquina, su candidato de preferencia.

vi. Voto:

El votante revisa y confirma su elección, la cual es contabilizada en el sistema.

vii. Registro:

En este paso, el votante recibe el comprobante de votación impreso automáticamente por la máquina, luego lo retira, verifica y lo deposita en la urna dispuesta para tal fin. Cabe aclarar que la impresión del voto se realizó para esta prueba, pero es un tema que debe estudiarse detenidamente antes de ser implementado en votaciones de carácter oficial.

viii. Cierre de la votación:

Cierre de la mesa. Se finaliza el ingreso de personal autorizado para votar y corresponde al final del día electoral.

ix. Consolidación y divulgación WEB:

En esta etapa, las maquinas de los puestos de votación operadas por los jurados, realizan automáticamente el conteo electrónico de los votos y transmiten la información consolidada a las sedes departamentales de la RNEC o a los centros de computo dispuestos para tal fin para ser publicados.

Al culminar esta etapa se debe levantar un acta firmada por los jurados y los delegados de la RNEC y de los organismos de vigilancia y control, especificando la hora, las observaciones del proceso y dando por escrito la terminación del proceso, incluido el cierre del sistema.

x. Escrutinio:

La etapa de escrutinio se realiza de acuerdo a instrucciones que imparta la Registraduría (especialmente lugar y fecha) y consiste en contabilizar los votos impresos por las maquinas y depositados en las urnas, los cuales han sido transportados en unas condiciones de estricta seguridad a los sitios asignados para tal fin.

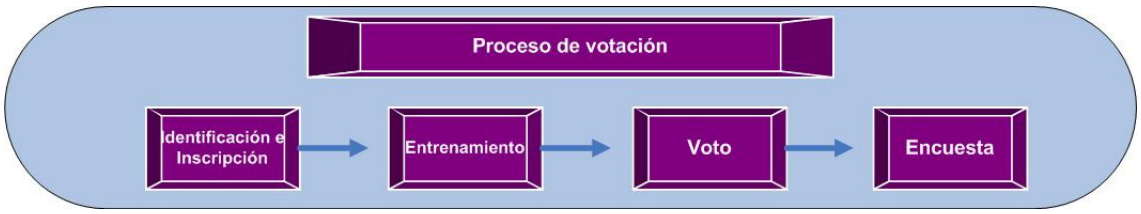
Es necesario levantar actas para el cierre de esta etapa, en la cual deben participar delegados, veedores de los partidos y movimientos políticos, así como los organismos de vigilancia y control.

2.3 PLAN DE GESTION DE RIESGOS DE LA PRUEBA PILOTO

Para la prueba piloto de voto electrónico se elaboró un plan de riesgos, en el cual se identificaron los riesgos propios de la ejecución del proyecto y los relacionados a la votación electrónica(ver anexo B). El plan diseñado, abarcó todos los procesos, procedimientos y productos asociados a la prueba de tal forma que permitieran anticipar, mitigar y controlar los diferentes eventos. Se

adoptaron las recomendaciones de la norma Australiana AS/NZ[19], el modelo CobIT[15], ISO 27000/17799[13] y el modelo PMI(Project Management Institute). En la figura 4 se ilustran los cuatro subprocesos principales de la votación y a los cuales se les identificaron los riesgos asociados

Figura 4:Procesos de votación de la prueba piloto de voto electrónico realizada el 27 de Octubre de 2007

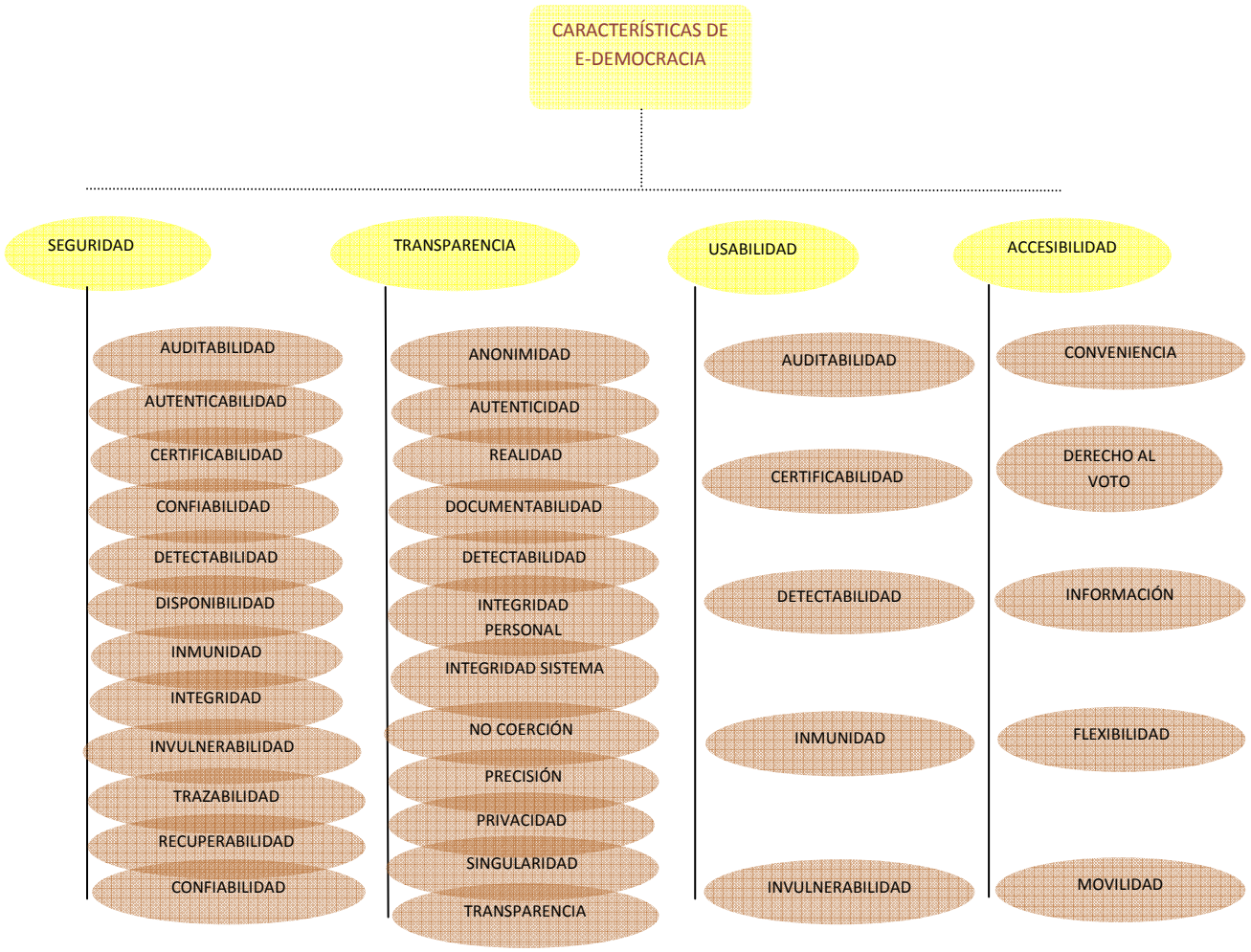


Fuente: Autor

2.3.1 OBJETIVO DE LA IDENTIFICACIÓN DE RIESGOS PARA LA PRUEBA PILOTO DE VOTO ELECTRÓNICO:

La finalidad del proceso de gestión de riesgos fue identificar amenazas y riesgos asociados al proceso y al uso de tecnologías en el proceso electoral colombiano para recomendar controles que permitan el desarrollo adecuado de procesos futuros de votación electrónica.. Los controles actuales utilizados para la seguridad del proceso de votación electrónica están enfocados en preservar las características que debe tener el voto: Libre, secreto, universal, directo y en igualdad de condiciones para todos los votantes(ver figura 5). El votante debe ejercer su voto de forma confidencial y sin coerción. Por tanto, desde el punto de vista tecnológico, el sistema de votación electrónica debe asegurar que no existe ningún enlace entre el voto y su emisor. Es decir, el voto debe ser secreto durante todas las etapas del proceso y la confidencialidad debe ser garantizada. Además de lo anterior, el votante no debe tener la capacidad de probar su voto de ninguna forma, esto es, para prevenir coerción y compra de votos.

Figura 5:Características del proceso de voto electrónico



Fuente:Autor

A partir de la experiencia del piloto, se estableció la necesidad de la identificación de los puntos críticos del sistema de votación a través de una gestión de riesgos más profunda y que permita la obtención final del nivel de confiabilidad del sistema a través de auditorías más rigurosas y precisas. Los análisis de confiabilidad de sistemas para mejorar su diseño, se viene empleando fuertemente desde la década de los 60's, cuando la exploración espacial y el uso de energía nuclear se potenciaron. La NASA realiza estudios de confiabilidad y gestión probabilística de riesgos [10] de los componentes más críticos de sus naves espaciales y tripulación [11], antes de realizar un lanzamiento, para conocer las probabilidades de éxito de la misión y tomar decisiones importantes. Para esto, toma datos históricos y los utiliza para predecir el comportamiento de los componentes del sistema.

El estudio de confiabilidad, se basa en el descubrimiento y conocimiento de los riesgos y sus probabilidades de ocurrencia para el cálculo anticipado de la

confianza en el correcto funcionamiento de un sistema. Es aquí donde entra a jugar un papel importante la gestión probabilística de riesgos, que a su vez se vale del modelado del sistema a través de los árboles de fallas [12] para conocer la cadena de eventos que llevan a la ocurrencia de los riesgos y las razones por la cuales estos se materializan. Luego de identificar y caracterizar los posibles riesgos del sistema, éstos se deben gestionar. La gestión de riesgos es un proceso cíclico que ha cobrado gran importancia después de los ataques del 9/11, de donde se concluyó que en cuanto a seguridad no todo está dicho. Por lo anterior, se han popularizado estándares y normas de seguridad de la información y Gestión de riesgos como ISO 27001 [13], SSE-CMMI [14], CobIT [15], ITIL [16], Coso ERM [17], AAIRM [18], AS/NZ 4360 [19], M_o_R(Management of Risk) [20] e ISO 31000(draft) [21], que dan a conocer mejores prácticas asociadas al buen manejo de los Sistemas de Información.

A partir de esta experiencia en gestión de riesgos en la prueba piloto, se concluyó que a pesar que la gestión cualitativa realizada presentó resultados aceptables que permitieron la gestión adecuada del proyecto, este tipo de análisis no sería suficiente para la identificación de riesgos para un proceso electrónico electoral real, porque es muy subjetivo y está sujeto a arrojar resultados que no se ajustan a la realidad debido a:

- Las probabilidades de ocurrencia de los riesgos fueron asignadas por estimaciones de un grupo pequeño de personas que solo contaban con información de experiencias de votación electrónica en otros países. Además, estos datos eran de tipo cualitativo, que debían interpretarse según la percepción de cada integrante del proyecto.

- Solo se hicieron mediciones cuantitativas, en los puntos considerados como importantes en ese momento por la Registraduría Nacional, como tiempos de votación, número de participantes y su opinión acerca de las tecnologías experimentadas. No se cuantificaron fallos de dispositivos, fallos de seguridad, personas que necesitaron asistencia para ejercer su voto, máquinas averiadas, etc, pues en el momento de la ejecución de la prueba, no se tenía clara la importancia de estos aspectos en el caso de un proceso real

- La naturaleza y extensión del piloto no permitió hacer mediciones sobre la seguridad ofrecida por la red de datos que utiliza la registraduría, pues la transmisión se realizó por un canal soportado por la empresa de telecomunicaciones UNE y no por la red que normalmente utiliza la registraduría para los procesos electorales.

- Debido a las condiciones de participación de los proveedores, solo fue posible realizar algunas pruebas de caja negra al software de las máquinas de votación, lo que dejó sin posibilidad el conocimiento del código que ejecutan estos dispositivos.

Por lo anterior, se identificó la necesidad de implementar un método de gestión que lograra integrar el análisis cualitativo existente con el análisis cuantitativo, esto es, identificar puntos importantes en el proceso para tomar datos numéricos que sirvan como entradas a un modelo que indique el nivel de confiabilidad del proceso y los puntos que deben monitorearse.

CAPÍTULO III: MODELO DE CONFIABILIDAD BASADO EN GESTIÓN CUALITATIVA Y CUANTITATIVA DE RIESGOS

INTRODUCCION

En el presente capitulo se propone un modelo de análisis de confiabilidad, que se basa principalmente en la gestión cualitativa y cuantitativa de riesgos. El capitulo inicia con la definición del riesgo, siguiendo con la descripción de las etapas de gestión, en donde se hace énfasis en la identificación y análisis de los riesgos, ya que se propone una metodología para evaluar la confiabilidad de un sistema, a partir de la detección de los eventos iniciales que son amenaza para el cumplimiento de los objetivos del proceso.

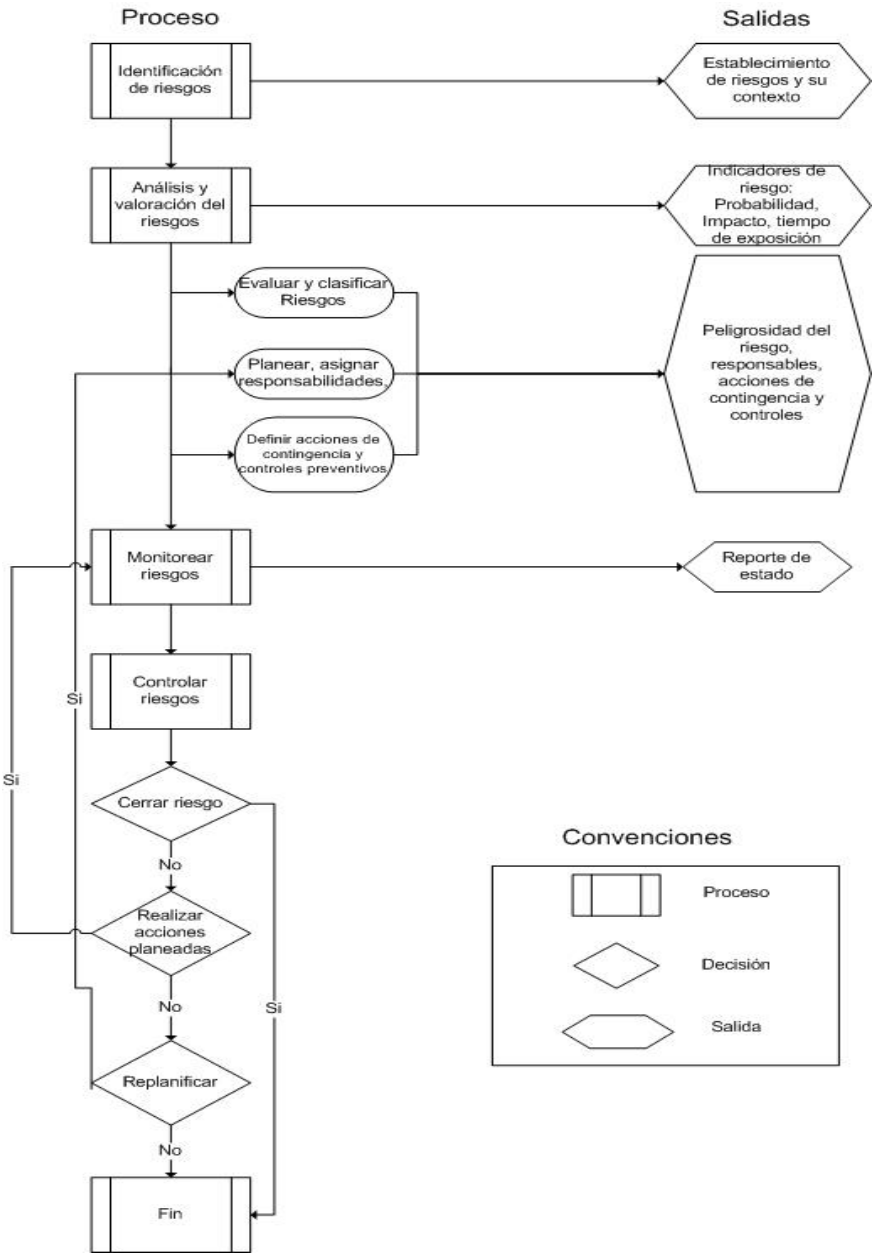
3.1 GESTION CONTINUA DEL RIESGO

La Gestión Continua de Riesgo (Continous Risk Management-CRM) es una metodología para gestionar los riesgos y escenarios de falla identificados. CRM es una práctica de gestión que provee un enfoque documentado y organizado que se ejecuta durante todo el ciclo de vida de un proceso o proyecto. Es principalmente implementado por la NASA en los proyectos para el lanzamiento de transbordadores espaciales.

Además de CRM, se han contemplado las recomendaciones de otras normas y estándares igual de importantes como: la Norma Australiana AS/NZ: 4360-NTC 5254 [19], CobIT (Modelo de control de TI) [15], ISO 27000/17799Seguridad en TI [13] y PMBOK (Project Management Body of Knowledge), las cuales se fusionaron al modelo propuesto.

El modelo de gestión del riesgo está comprendido por una serie de etapas que se ejecutan de forma iterativa (Ver figura 6). El ciclo inicia con la familiarización y contextualización del sistema, luego con la identificación y análisis de los riesgos, planeación, medición y por último el control.

Figura 6:Diagrama de flujo de CRM.



Fuente: Autor

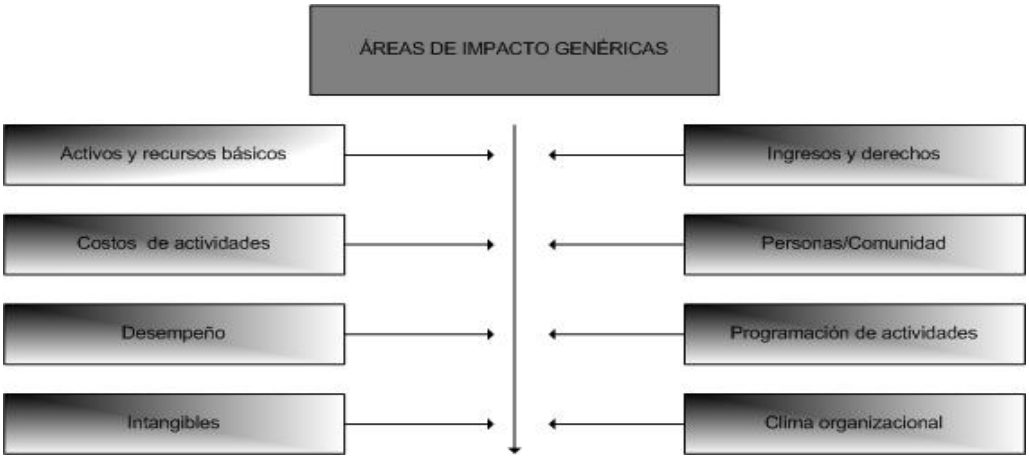
3.2.1 CONTEXTUALIZACIÓN DEL SISTEMA

La primera etapa del todo el proceso es establecer el contexto del sistema de administración del riesgo o el entorno de proceso. Para esto se debe conocer su organización y naturaleza y establecer sus objetivos, metas, extensión, localización y tiempo.

Con relación al análisis de riesgos, también se deben establecer sus objetivos, el porqué y para que se realiza esta actividad y que se espera obtener.

Se debe establecer claramente las áreas de impacto[1]. En la figura 7 se observan algunas genéricas, entre las que se consideran más importantes a los activos del proceso, los cuales deben identificarse plenamente para tener en cuenta los más críticos y protegerlos adecuadamente.

Figura 7:Áreas de impacto genéricas



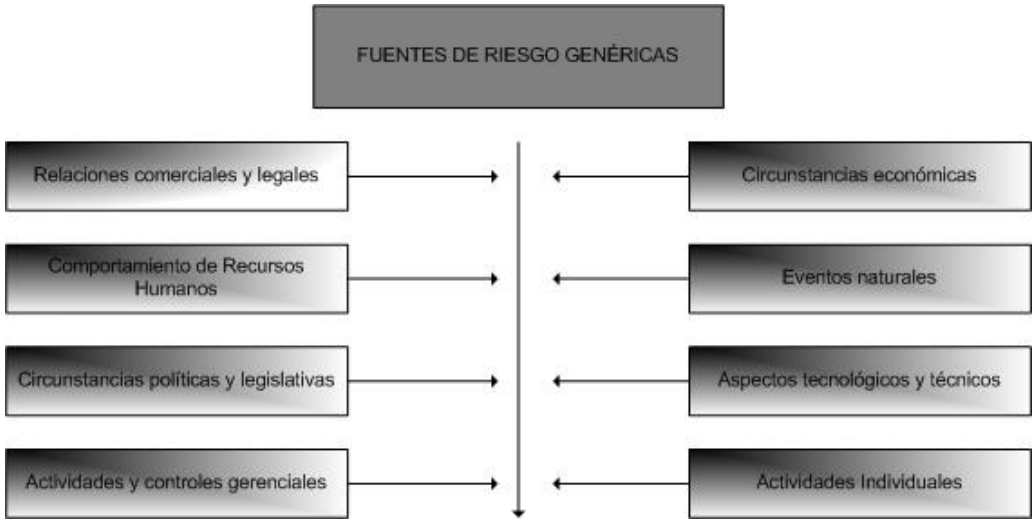
Fuente: Autor

También es importante identificar las *fuentes de riesgo* [2] a las cuales en el proceso de análisis, se le identificarán los eventos iniciales o triggers. En la Figura 8 se observan algunas fuentes de riesgo genéricas.

[1]Todo recurso bien u oportunidad a la cual el proyecto debe asignar un valor y su afectación podría comprometer el cumplimiento de los objetivos y metas y por lo tanto deben ser protegidas.

[2] son los individuos, grupo humano, entidad, elemento físico, o fenómeno del entorno de los cuales se pueden derivar eventos que podrían afectar las áreas de impacto (objetos en riesgo) del proceso

Figura 8:Fuentes de riesgo genéricas



Fuente: Autor

3.2.2 ANÁLISIS Y VALORACIÓN DEL RIESGO

En esta etapa se realiza principalmente la estructuración del problema, es decir, se construye un modelo físico de la situación actual del sistema. A este modelo se le conoce como *"escenario"* y se crea con base en observaciones y suposiciones del proceso.

Debido a que muchos fenómenos cotidianos no pueden ser modelados a través de expresiones determinísticas, por ejemplo las veces en las que una persona se equivoca o falla en la elección de una opción en una máquina de votación, se utiliza la probabilidad incluyendo la incertidumbre como componente principal.

Para construir el modelo se utilizan principalmente árboles de fallas. La característica esencial de este método de desarrollo de escenarios es que permite mapear una realidad compleja en un grupo de relaciones lógicas que pueden ser analizadas de forma manual o computarizada, todo esto dependiendo de la cantidad de cálculos a realizar.

Como resultado final del análisis en esta etapa se deben presentar una serie de escenarios de falla, frecuencias y consecuencias, de tal forma que permitan la toma de decisiones y la asignación de recursos para prevenir la materialización de los riesgos.

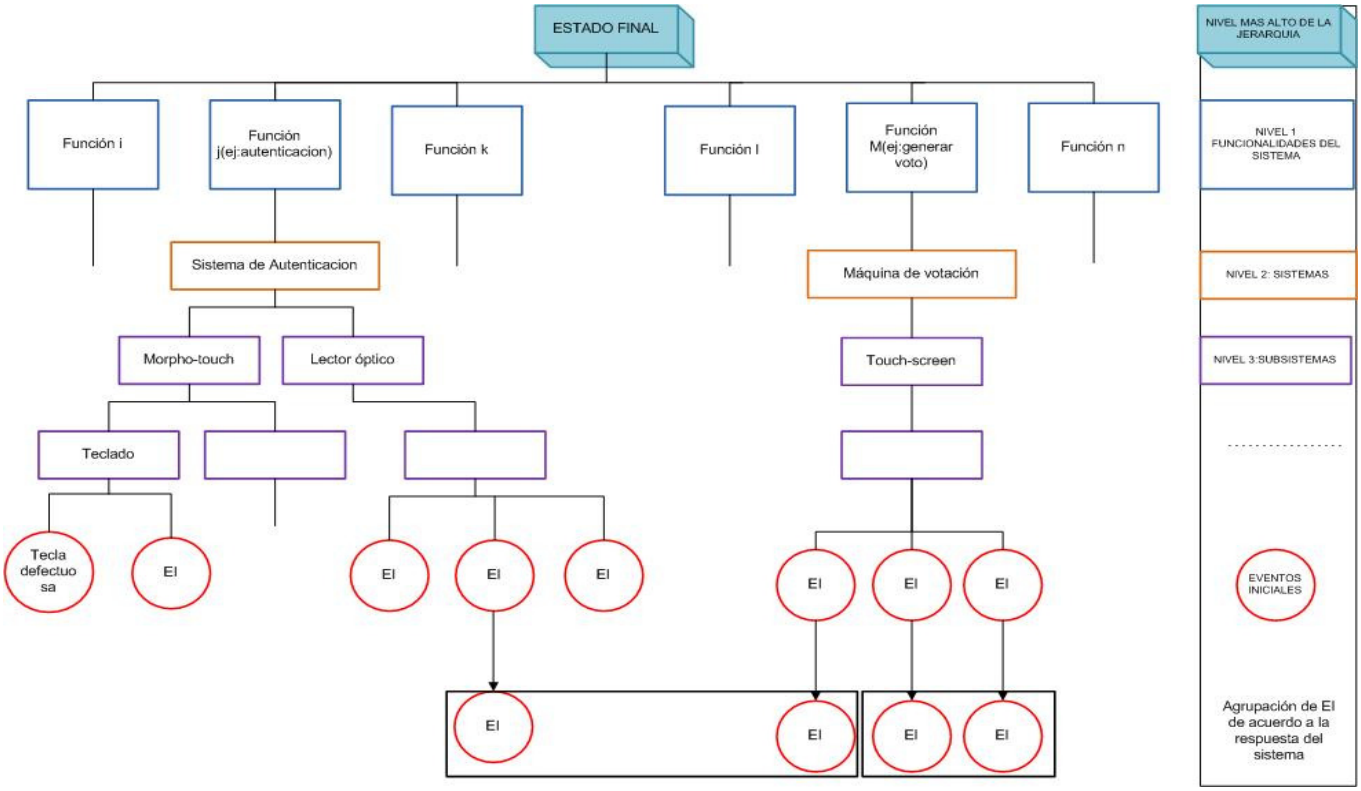
Un escenario está compuesto principalmente por eventos iniciales y uno o más eventos que conllevan a un estado final indeseable (riesgo a evitar). El evento inicial (**EI**) es una perturbación al sistema y usualmente requiere una respuesta rápida por parte de los operadores del mismo. Los siguientes eventos, son las respuestas que se generan como consecuencia de la aparición del **EI**, y por último, el desenlace indeseable o estado final que son aquellos riesgos que ponen en peligro el cumplimiento de los objetivos del proceso que se está ejecutando.

1.3.1.1. Identificación de eventos iniciales(EI)

Para la identificación de eventos iniciales, se propone utilizar una herramienta llamada Diagrama Lógico (DL). El DL es una organización jerárquica que muestra en la parte superior el estado final, siguiendo con las instancias intermedias y en la parte inferior los eventos iniciales. El objetivo del DL no es solo dar soporte a la identificación de los EI, sino también agruparlos de acuerdo al grado de esfuerzo que se debe hacer para mitigar el evento indeseable que generan y a la parte del sistema que afectan. En la figura 9 se observa un ejemplo de diagrama lógico y una muestra de cómo podría implementarse para la identificación de los eventos iniciales del proceso de votación electrónica. En el nivel 1: Funcionalidades del sistema, se identifican los diferentes subprocesos que se realizan y conforman el gran proceso de votación electrónica. En el nivel 2: se identifican los sistemas que intervienen en los subprocesos y que son críticos para el funcionamiento. De ahí en adelante estos sistemas pueden ser descompuestos en tantos niveles se desee, esto depende del nivel de detalle requerido para el análisis. Por último, se llega a los eventos

iniciales, los cuales pueden ser agrupados de acuerdo a sus efectos sobre el sistema.

Figura 9:Esquema de Diagrama Lógico (DL).

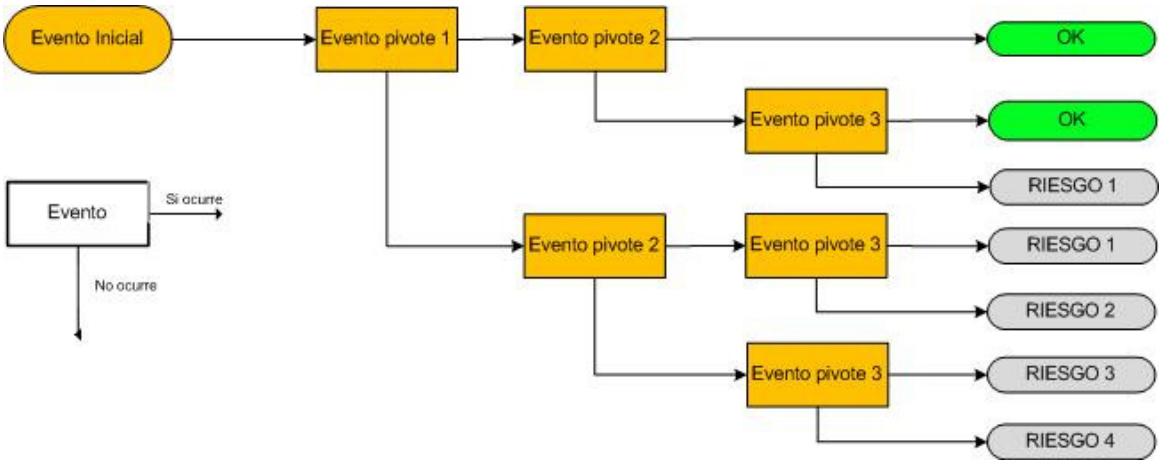


Fuente: Autor

1.3.1.2. Diagramas de secuencias de eventos

Luego de la identificación de los eventos iniciales, se sigue el desarrollo de los escenarios a través de los diagramas de secuencias de eventos (DSE). El DSE es un diagrama de flujo con caminos que llevan a diferentes estados del sistema. Cada camino, es un escenario, que está comprendido por evento inicial y a lo largo de este se enumeran una serie de eventos que se les llamarán eventos pivote, que pueden suceder o no, y generarán un nuevo estado del sistema. De manera general el DSE reflejará el diseño del sistema. Un ejemplo se puede observar en la figura 10:

Figura 10:Diagrama de Secuencia de Eventos



Fuente:Autor

Los diagramas de secuencias de eventos, también pueden representarse como árboles de eventos, en donde los eventos se reemplazan por nodos, indicando la ocurrencia o no del mismo (Ver figura 10). A partir de aquí se pueden deducir las ecuaciones lógicas que describen la secuencia de eventos. A continuación se pueden observar las ecuaciones extraídas del árbol de la figura 10:

SECUENCIA	EXPRESIÓN BOOLEANA
1	$Ie \cap P1 \cap P2 \cap P3$
2	$Ie \cap P1 \cap P2 \cap \overline{P3}$
3	$Ie \cap P1 \cap \overline{P2}$
4	$Ie \cap \overline{P1} \cap P2 \cap P3$
5	$Ie \cap \overline{P1} \cap P2 \cap \overline{P3}$

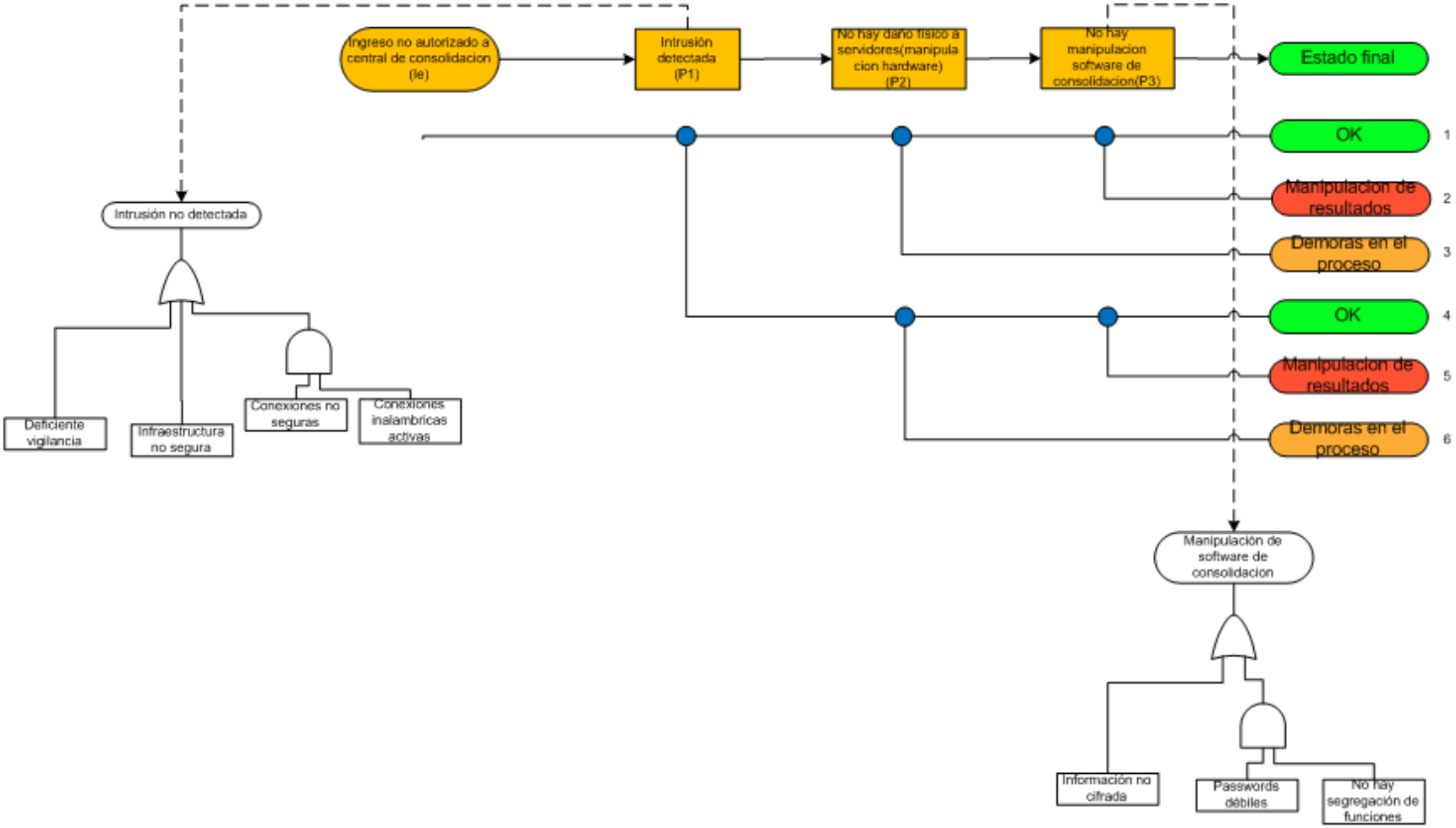
6	$Ie \cap \overline{P1} \cap \overline{P2}$

Tabla 1 : Expresiones booleanas del árbol de eventos de la figura 10

1.3.1.3. Modelado de eventos pivote

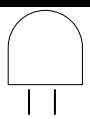
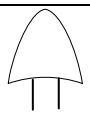
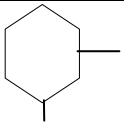
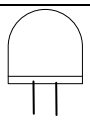
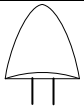
Los eventos pivote deben ser modelados de forma tal que permitan realizar la cuantificación de los escenarios. Para realizar esto, se utiliza una herramienta gráfica y de naturaleza booleana llamada árboles de fallas (AF). Los árboles de fallas muestran las relaciones lógicas de los modos de falla del sistema de tal forma que los eventos pivote se descomponen en eventos más simples o básicos. Los eventos básicos pueden aparecer simultáneamente en otros AF, deben ser cuantificables y estadísticamente independientes. Los eventos básicos, junto con los eventos iniciales son los puntos del sistema donde se debe medir constantemente. Esta herramienta es de tipo deductiva, ya que a partir del evento pivote, se deducen los eventos básicos que llevan a su ocurrencia. En la figura 11 se observa un árbol de eventos al que se le han desarrollado dos árboles de fallas.

Figura 11:Árboles de fallas a partir de diagramas de secuencia

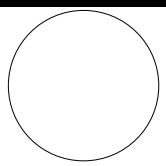
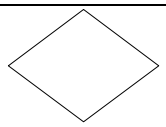
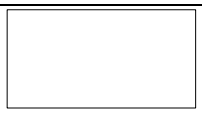
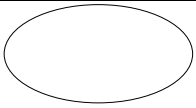
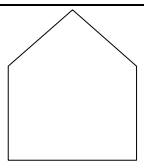
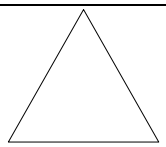


Fuente: Autor

Los árboles de fallas elaborados a partir de los diagramas de secuencias de eventos están compuestos principalmente por compuertas lógicas que establecen una relación entre los eventos básicos. En la tabla 3.2 se encuentran los tipos de compuertas que pueden ser utilizados para expresar este tipo de relaciones.

	COMPUERTA	NOMBRE	RELACION CAUSAL
1		AND	La salida ocurre si todos los eventos de entrada ocurren simultáneamente
2		OR	La salida ocurre si cualquiera de los eventos de entrada, ocurre.
3		CONDICIONAL	La entrada produce una salida cuando el evento condicionante ocurre.
4		AND DE PRIORIDAD	La salida ocurre si todos los eventos de entrada ocurren en el orden de izquierda a derecha
5		OR EXCLUSIVA	La salida ocurre si uno, pero no ambos de los eventos de entrada ocurren.
6		COMPUERTA DE MUESTREO	La salida ocurre si m de los n eventos de entrada ocurren

Fuente: Autor Tabla 2:Compuertas lógicas utilizadas en árboles de fallas.

	SIMBOLO DEL EVENTO	SIGNIFICADO DE SIMBOLO
1		Componente básico. Es el evento de falla inicial que desencadena la serie de eventos que conllevan al desenlace indeseable. Se debe procurar gran cantidad de datos.
2		Evento no desarrollado
3		Estado del sistema
4		Evento condicional
5		Evento House: puede ocurrir o no. Su probabilidad es de 1 o 0.
6		Símbolo de transferencia

Fuente: Autor Tabla 3:Tipos de eventos representados en árboles de falla (AF).

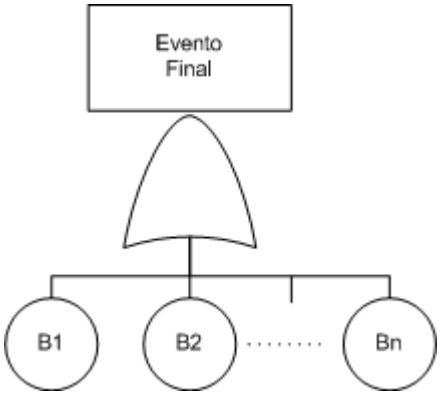
Las compuertas básicas son la AND y OR ya que cualquier otra compuerta siempre se puede expresar en términos de estas dos.

1.3.1.4. Aspectos cuantitativos de la representación de árboles de fallas[11]

- **Compuerta OR:** La ocurrencia simultánea de los eventos básicos $B_1 \ldots \ldots B_n$ da como resultado la ocurrencia del

evento final. Dicho lo anterior, la probabilidad de que se presente el evento final es:

Figura 12:árbol de fallas de compuerta OR



Fuente:autor

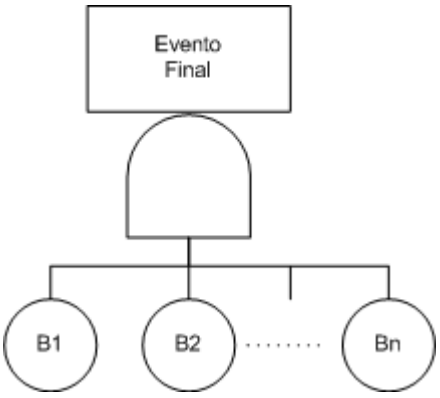
$$Q_s = P_r\{B_1 \cap B_2 \cap \ldots \cap B_n\} \quad \text{Ec(1)}$$

$$Q_s = P_r\{B_1\}P_r\{B_2\} \ldots\ldots P_r\{B_n\} \quad \text{Ec(2)}$$

Donde Q_s es la probabilidad de falla del sistema o la ocurrencia del evento final.

- **Compuerta AND:** La ocurrencia de alguno de los eventos básicos $B_1 \ldots\ldots B_n$ da como resultado la ocurrencia del evento final. Por lo tanto su representación en términos de árbol de fallas es la figura 13:

Figura 13:Árbol de fallas de compuerta AND



Fuente:autor

$$Q_s = P_r\{B_1 \cup B_2 \cup \ldots \cup B_n\} \quad \text{Ec(3)}$$

$$Q_s = 1 - [1 - P_r\{B_1\}][1 - P_r\{B_2\}] \ldots [1 - P_r\{B_n\}] \quad \text{Ec(4)}$$

Donde Q_s es la probabilidad de falla del sistema o la ocurrencia del evento final.

La evaluación de un árbol de fallas puede realizarse en dos pasos: reducción y cuantificación. El objetivo de la reducción, como su nombre lo indica, consiste en reducir el árbol de eventos a su mínima expresión o grupo de eventos básicos mínimos con los cuales se produzca el evento final. Esto se realiza aplicando iterativamente las leyes básicas del álgebra booleana hasta obtener una expresión más simple. La cuantificación del árbol de fallas es la evaluación de la probabilidad del evento final en término de las probabilidades de los eventos básicos.

3.2.3 CONTROLES Y PLANIFICACIÓN DE LOS RIESGOS

Los controles son todas aquellas acciones y/o procedimientos encaminados a la prevención, mitigación o a la disminución del impacto causado por los eventos indeseables.

Para el diseño y la identificación de controles, se deben tener en cuenta los siguientes pasos:

- Iniciar el proceso en orden descendente, iniciando por el riesgo de mayor severidad, tomando como referencia cada una de las causas del riesgo.
- No omitir ningún control existente dentro del proceso, para obviar duplicidades y superposiciones con los controles planeados (tratamientos).
- Diseñar o identificar primero los controles de mayor cobertura (que mitigan las causas de mayor probabilidad o reducen significativamente las consecuencias) y que a su vez sean los de mayor efectividad.
- En los riesgos subsiguientes, antes de incluir nuevos controles, identificar y evaluar controles ya descritos y vinculados a los riesgos de mayor severidad.
- Analizar primero si los controles actuales pueden ser optimizados antes de planear nuevos.

Planificación de actividades relacionadas a los riesgos

Los nuevos riesgos identificados son dados a conocer por todo el equipo del proyecto y se toman decisiones acerca del tratamiento a darles.

A medida que se identifican nuevos riesgos, la junta de configuración del proyecto o la persona encargada de gestionar los riesgos debe determinar la acción a tomar con el mismo: mantener el riesgo, transferirlo a un tercero (outsourcing) o transferirlo en la misma organización a algún rol de mayor jerarquía. Ser responsable por un riesgo, significa que la persona debe responder por el estado y mitigación del mismo

El proceso de planificación de actividades relacionadas a los riesgos requiere la creación de planes de acción, aceptación del riesgo, determinar los atributos del riesgo y su estado (definir requisitos de monitoreo) o mitigar el riesgo (Crear un plan de mitigación, asignar tareas) .

3.2.4 MONITOREO DE RIESGOS

Los criterios definidos en la etapa de planificación deben ser monitoreados, recopilados y analizados para observar tendencias y recálculo de métricas si

es el caso. El responsable del riesgo debe proveer una rutina para el monitoreo y el reporte de los mismos, los cuales deben ser ingresados al documento designado para tal actividad. EL periodo de monitorización de los riesgos depende de la probabilidad de aparición de los mismos.

3.2.5 CONTROL DE RIESGOS

El control de riesgos se realiza a través del comité de gestión de proyectos. En este comité se expone el estado de los riesgos y se toman decisiones con base en el estado de los mismos (cerrar el riesgo, acciones de contingencia, replanificación).

3.2.6 COMUNICACIÓN Y DOCUMENTACIÓN DE RIESGOS

En esta etapa de comunican y documentan todos los riesgos analizados y sus respectivos planes, teniendo en cuenta las líneas base establecidas en la etapa de planificación.

CAPÍTULO IV: MODELO DE ANALISIS DE CONFIABILIDAD BASADO EN GESTIÓN DE RIESGOS APLICADO AL PROCESO DE VOTACIÓN ELECTRÓNICA

INTRODUCCIÓN

En el presente capitulo se realiza la implementación del modelo de confiabilidad, descrito en detalle en el capítulo tres, para el caso particular de votación electrónica y lo observado en la prueba piloto de votación realizada el 27 de Octubre de 2007.

Los eventos y estados del sistema que se observarán en el modelo fueron seleccionados a partir de un profundo estudio del estado del arte (Ver anexo 4-Bibliografía), experiencias de votación electrónica en otros países y hallazgos de la experiencia de gestión de riesgos en el piloto.

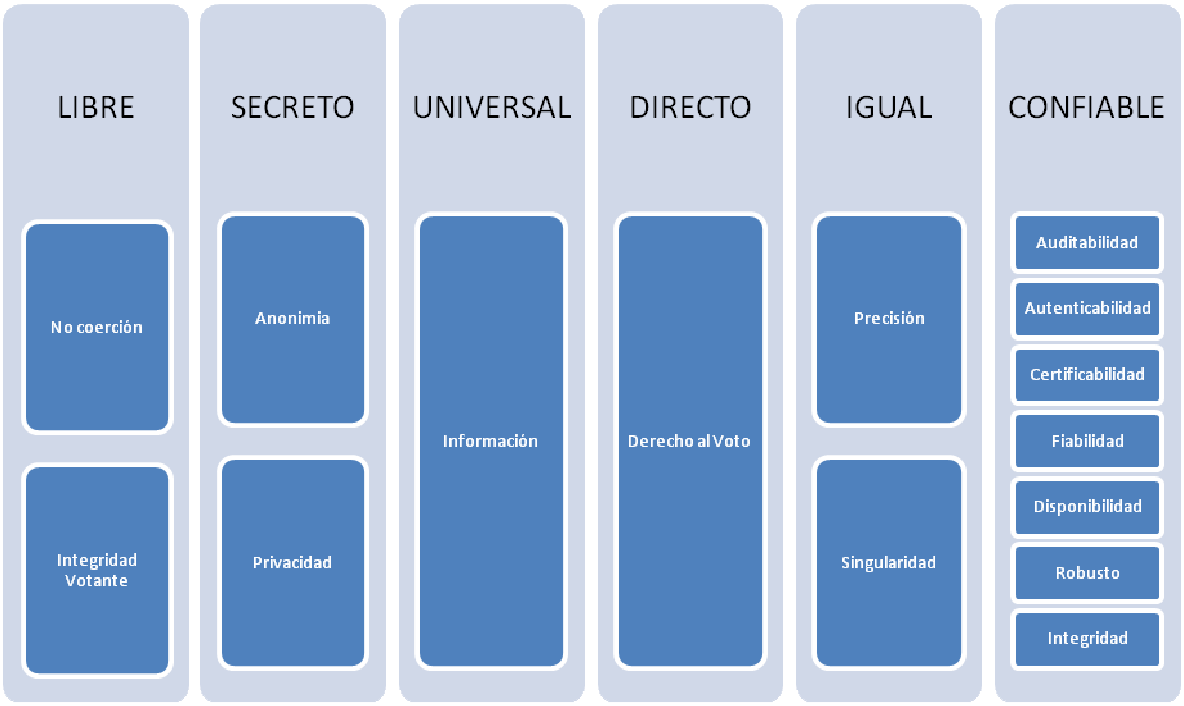
A continuación se hará una contextualización del sistema tal como lo describe la primera etapa del modelo, siguiendo con la identificación y análisis de riesgos que encierra gran parte del análisis propuesto en el modelo, ya que se identifican los eventos iniciales que pueden llevar a la materialización de los riesgos, la integración de estos eventos en un árbol de fallas que finalmente representará gráficamente las relaciones de estos eventos y pruebas del modelo en general, a partir de datos generados con sistemas de inferencia fuzzy que permiten trasladar la experiencia humana a datos probabilísticos.

4.1 CONTEXTUALIZACIÓN DEL SISTEMA

El proceso electoral electrónico tiene como objetivo la realización de las elecciones a través del uso de las nuevas tecnologías para dar mayor agilidad y transparencia al desarrollo de los procesos.

A través de la ley 892 de 2004(Anexo 1), se establecieron las características principales para la puesta en marcha de la votación electrónica en Colombia, que debe garantizar por supuesto, el cumplimiento de las características del voto, propuestas desde la declaración universal de los derechos humanos (Ver figura 14)

Figura 14:Característica del voto



Fuente: Autor

- **No coerción:** No debe existir ningún tipo de presión sobre el votante para que este tome una decisión determinada.
- **Integridad del Votante:** El sistema debe garantizar en todo momento la integridad del votante para que este puede ejercer su voto adecuadamente.
- **Anonimia:** No debe existir vínculo entre el votante y su voto.
- **Privacidad:** Se debe garantizar que el votante ejerza su voto individualmente y de manera privada.
- **Información:** El votante tiene derecho a recibir toda la información requerida para tomar una decisión de voto y realizar el sufragio.
- **Derecho al Voto:** Todo ciudadano que cumpla con las condiciones establecidas por ley, tiene derecho a ejercer su voto.
- **Precisión:** el sistema debe ser preciso al registrar un voto, debe registrar la decisión del votante.
- **Singularidad:** Debe generarse un voto por elector.
- **Auditabilidad:** El sistema debe permitir revisión de cualquiera de sus etapas.
- **Autenticabilidad:** El sistema debe permitir la validación de la identidad del votante, sin realizar trazabilidad de este con su voto.

- **Certificabilidad:** El sistema debe permitir su revisión para establecer su idoneidad.
- **Fiabilidad:** El sistema debe brindar confianza en cuanto a su funcionamiento y desempeño.
- **Disponibilidad:** Se debe garantizar una disponibilidad del 100%
- **Robustez:** El sistema debe funcionar adecuadamente en condiciones extremas de operación.
- **Integridad:** El sistema debe garantizar la integridad de la información que maneja.

4.1.1 ALCANCE Y RESTRICCIONES DE LA IDENTIFICACIÓN DE RIESGOS:

La identificación y valoración de riesgos del proceso electoral electrónico se basó en observaciones realizadas en la prueba piloto realizada el 27 de Octubre de 2007. Por lo tanto, en la identificación de riesgos están incluidos los procesos que se llevaron a cabo en la prueba y en el proceso de votación y no están incluidas otras actividades que se llevan a cabo en un proceso electoral tradicional, como por ejemplo: Supernumerarios, kit electoral, call center, Información a votantes, etc.

4.1.2 LÍMITES FÍSICOS PARA LA GESTIÓN DE RIESGOS

En el análisis de riesgos se tendrán en cuenta todos los dispositivos a utilizar para la prueba piloto de votación electrónica, como las máquinas de votación, dispositivos de autenticación, y en general el escenario físico de votación.

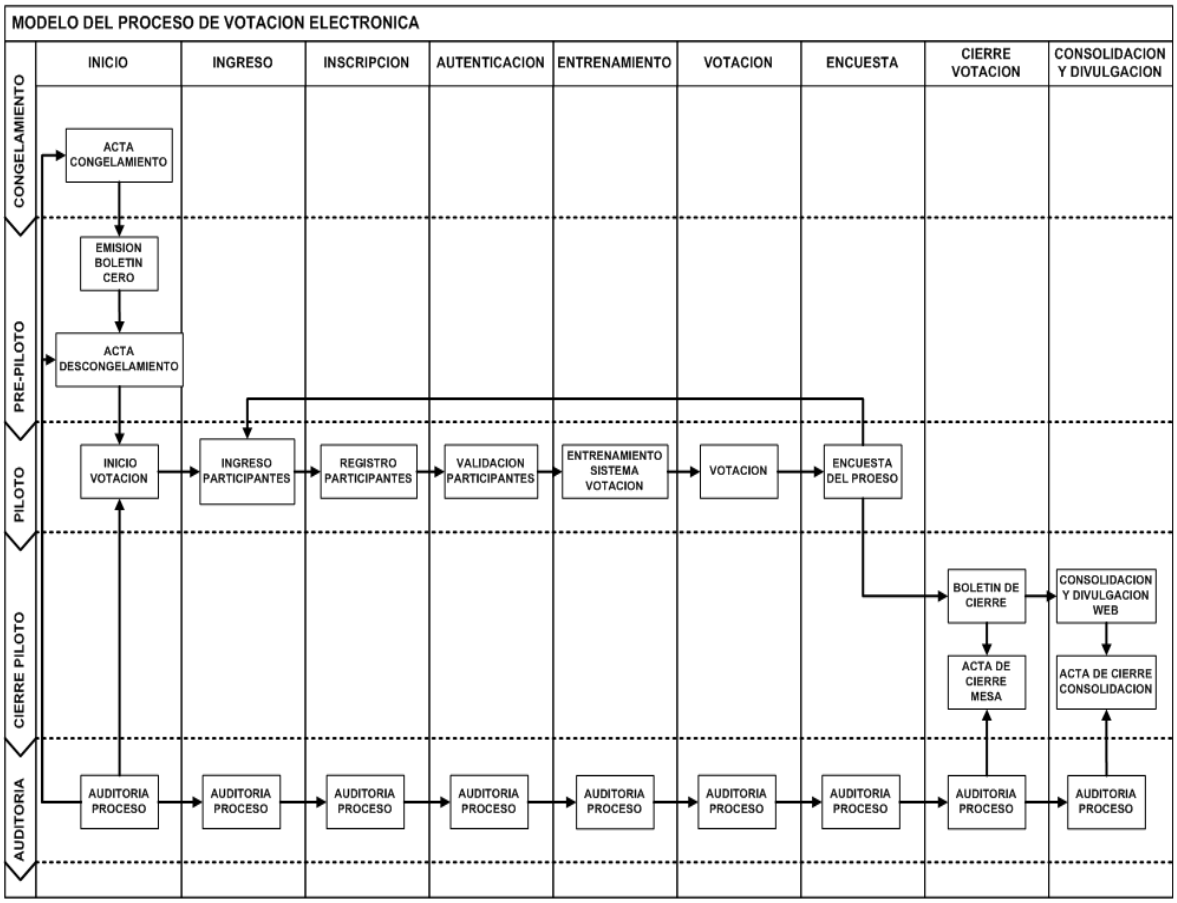
4.1.3 LÍMITES LÓGICOS DE LA GESTIÓN DE RIESGOS:

El análisis de riesgos considerará los aspectos relacionados a los siguientes temas:

- Personal autorizado: Incluyendo personal insuficiente o mal calificado, poca supervisión y entrenamiento.
- Personal no autorizado: Personas con malas intenciones, vándalos, hackers.
- Software malicioso.
- Sistemas de computación: Hardware y software utilizado para la prueba.
- Datos: Almacenamiento.

- Controles existentes para la mitigación de riesgos.
- Procedimientos de seguridad.
- Controles de datos.
- Mantenimientos.
- Controles físicos y lógicos de acceso.
- Arquitectura del sistema

Figura 15:Etapas de la votación electrónica que se analizarán.



4.1.4 OBJETIVO DE LA IDENTIFICACIÓN DE RIESGOS PARA EL PROCESO ELECTORAL ELECTRÓNICO:

Identificar amenazas y riesgos asociados al proceso y al uso de tecnologías en el proceso electoral colombiano para recomendar controles que permitan el desarrollo adecuado de procesos futuros de votación electrónica. Los controles que se adecuen para el proceso de votación electrónica, deben garantizar la preservación de sus características

principales (artículo 21 de la declaración de los Derechos Humanos [25]): Libre, secreto, universal, directo y en igualdad de condiciones para todos los votantes. El votante debe ejercer su voto de forma confidencial y sin coerción. Por tanto, desde el punto de vista tecnológico, el sistema de votación electrónica debe asegurar que no existe ningún enlace entre el voto y su emisor, es decir, el voto debe ser secreto durante todas las etapas del proceso y la confidencialidad debe ser garantizada. Además de lo anterior, el votante no debe tener la capacidad de probar su voto de ninguna forma, esto es, para prevenir coerción y compra de votos.

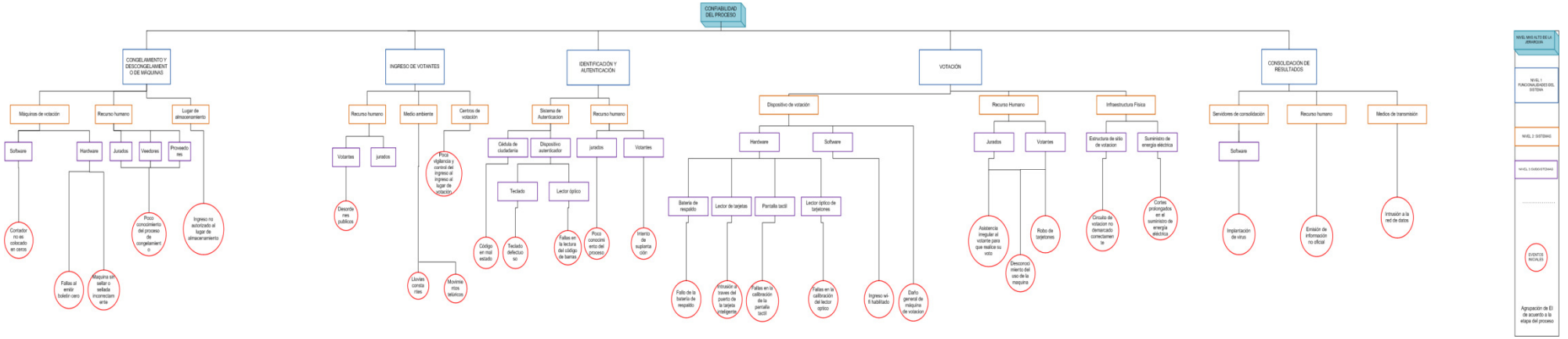
4.2 IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

4.2.1 IDENTIFICACIÓN DE EVENTOS INICIALES:

La identificación de eventos iniciales es la primera parte de la identificación de riesgos. En esta etapa se analiza cada parte del proceso, los activos más importantes y los problemas o eventos que podrían suceder. La figura 16 describe el diagrama lógico resultante del primer análisis del proceso a partir de la experiencia mundial en voto electrónico y la prueba piloto realizada.

En el nivel más alto de la jerarquía se encuentra el riesgo más crítico y representativo del proceso electrónico electoral, la pérdida de confiabilidad, el cual abarca los riesgos asociados a seguridad y continuidad y los relacionados al no cumplimiento de los criterios del voto(Ver Anexo A). Los eventos iniciales que en esta primera etapa se identificaron son:

Figura 16: Árbol de eventos inicilales identificados


CONFIABILIDAD DEL PROCESO
CONGELAMIENTO Y DESCONGELAMIENTO DE MAQUINAS
Máquinas de votación
Recurso humano
Lugar de almacenamiento
Software
Hardware
Jurados
Veedores
Proveedores
Contador no es colocado en ceros
Fallas al emitir boletín cero
Maquina sin sellar o sellada incorrectamente
Poco conocimiento del proceso de congelamiento
Ingreso no autorizado al lugar de almacenamiento
INGRESO DE VOTANTES
Recurso humano
Medio ambiente
Centros de votación
Votantes
jurados
Desorden publicos
Poca vigilancia y control del ingreso al ingreso al lugar de votación
Lluvias constantes
Movimientos teluricos
IDENTIFICACIÓN Y AUTENTICACIÓN
Sistema de Autenticacion
Recurso humano
Cédula de ciudadanía
Dispositivo autenticador
jurados
Votantes
Teclado
Lector óptico
Código en mal estado
Teclado defectuoso
Fallas en la lectura del código de barras
Poco conocimiento del proceso
Intento de suplantación
VOTACIÓN
Dispositivo de votación
Recurso Humano
Infraestructura Física
Hardware
Software
Jurados
Votantes
Estructura de sitio de votacion
Suministro de energía eléctrica
Bateria de respaldo
Lector de tarjetas
Parrralla tactil
Lector óptico de tarjetones
Asistencia irregular al votante para que realice su voto
Robo de tarjetones
Desconocimiento del uso de la maquina
Circuito de votacion no demarcado correctamente
Cortes prolongados en el suministro de energía eléctrica
Fallo de la bateria de respaldo
Intrusión a traves del puerto de la tarjeta inteligente
Fallas en la calibración de la parrallla tactil
Fallas en la calibración del lector optico
Ingreso wi-fi habilitado
Daño general de máquina de votacion
CONSOLIDACIÓN DE RESULTADOS
Servidores de consolidación
Recurso humano
Medios de transmisión
Software
Implantación de virus
Emisión de información no oficial
Intrusión a la red de datos
NIVEL MAS ALTO DE LA JERARQUIA
NIVEL 1 FUNCIONALIDADES DEL SISTEMA
NIVEL 2 SISTEMAS
NIVEL 3 SUBSISTEMAS
EVENTOS INICIALES
Agrupación de El de acuerdo a la etapa del proceso

1. **Proceso de congelamiento y descongelamiento**
    - Contador de la máquina de votación no es colocado en ceros.
    - Fallas al emitir el boletín cero.
    - Máquina sin sellar o sellada incorrectamente.
    - Poco conocimiento del proceso de congelamiento por parte de veedores, jurados y proveedores en general.
    - Ingreso no autorizado al lugar de almacenamiento.
2. **Ingreso de votantes**
    - Desórdenes públicos.
    - Lluvias constantes.
    - Movimientos telúricos.
    - Poca vigilancia y falta de control del ingreso al lugar de votación.
3. **Identificación y autenticación**
    - Cédula en mal estado. No permite la lectura del código de barras.
    - Teclado del dispositivo de autenticacion en mal estado. Presenta fallas.
    - Fallas en la lectura del código de barras por parte del lector óptico del dispositivo de autenticación.
    - Poco conocimiento del proceso por parte de los jurados.
    - Intento de suplantación de votantes.
4. **Votación**
    - Fallo de la bateria de respaldo de la máquina de votación.
    - Intrusión a traves del puerto lector de la tarjeta inteligente(aplica para máquinas con este tipo de tecnología).
    - Fallas en la calibración de la pantalla táctil(aplica para máquinas con este tipo de tecnología).
    - Fallas en la calibración del lector óptico (aplica para máquinas con este tipo de tecnología).
    - Ingreso wi-fi habilitado.
    - Daño general de la máquina de votación. No permite su uso.
    - La asistencia al votante por parte de jurados se realiza de forma irregular.
    - Desconocimiento del uso de la máquina de votación por parte de los jurados y/o votantes.
    - Robo de tarjetones por parte de jurados y/o votantes(aplica para tecnologías que hacen uso de tarjetón físico).
    - Circuito de votación no es demarcado correctamente.
    - Cortes prolongados en el suministro de energía eléctrica.
5. **Consolidación de resultados**
    - Implantación de virus en servidores de consolidacion.
    - Emisión de informacion no oficial.
    - Intrusión a la red de datos.

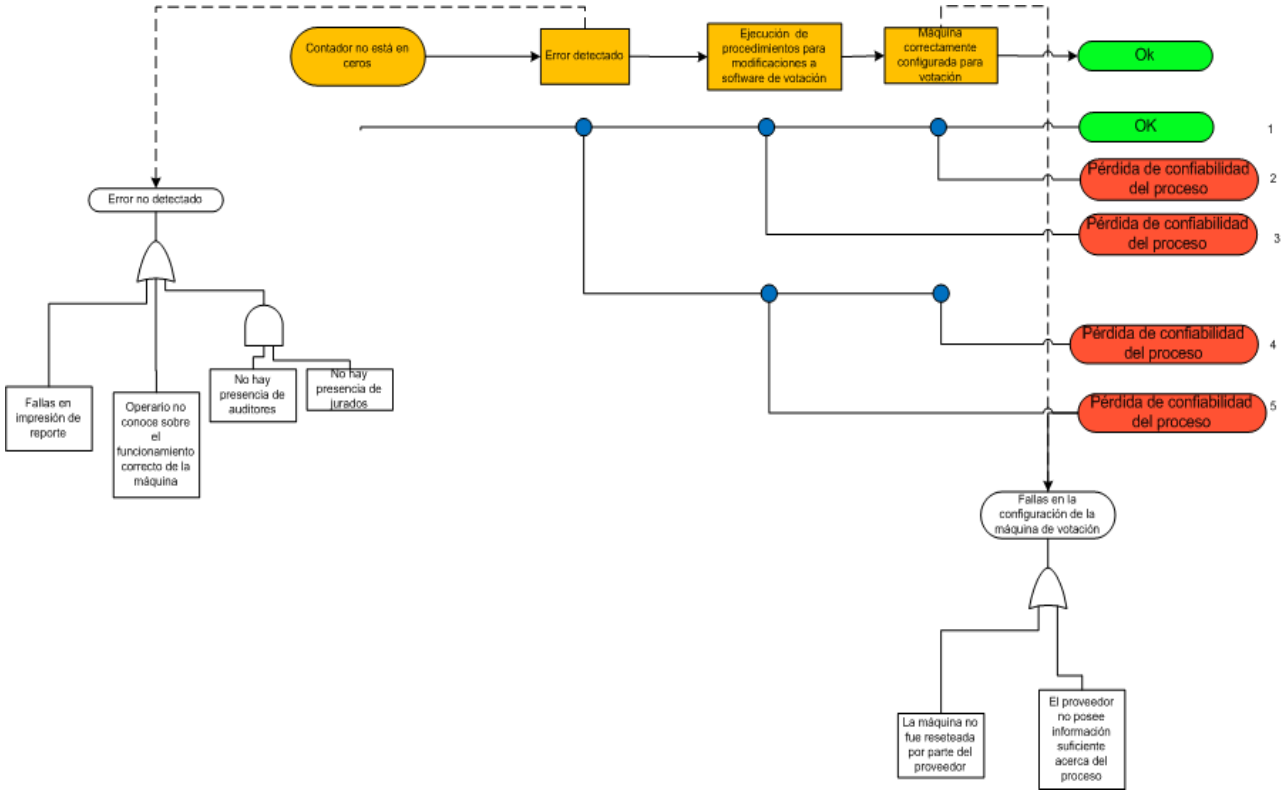
4.2.2 DIAGRAMAS DE SECUENCIAS DE EVENTOS ASOCIADOS A LOS EVENTOS INICIALES IDENTIFICADOS.

A continuación se describirán los árboles de falla creados en el análisis de cada evento inicial. En esta etapa se analizó cada evento inicial, la cadena de eventos que puede generar y su consecuencia final.

i. **Evento inicial: contador de la máquina no es colocado en ceros**

El escenario en el que el proceso tendría buen desenlace a pesar de la ocurrencia del evento inicial **EI,** es que este sea detectado y se ejecuten los procedimientos adecuados, previamente establecidos, para la modificación del software de la máquina de votación y finalmente la máquina es catalogada como apta para hacer parte del proceso. La negación de algunos de estos eventos da como resultado la pérdida de confiabilidad del proceso ya que permitiría manipulación del conteo de votos. Ver figura 17.

Figura 17:Diagrama de secuencia de eventos al EI: contador de la máquina no es colocado en ceros.

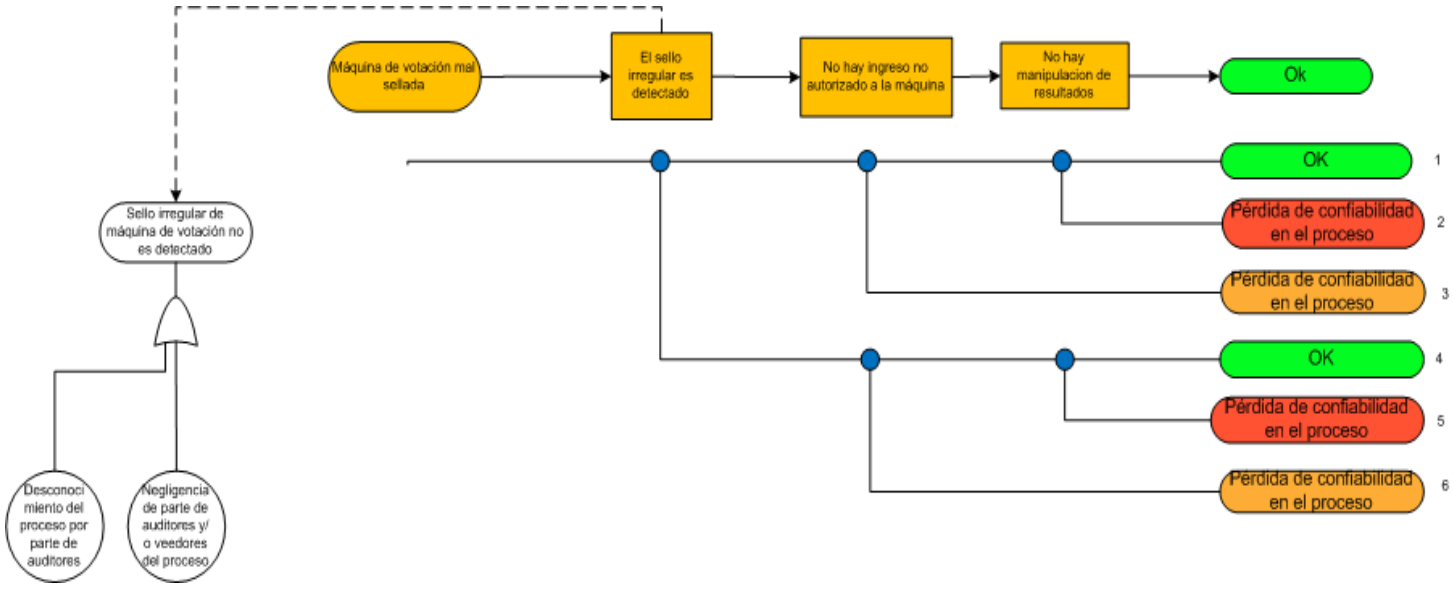


Se elaboraron dos árboles de fallas para error no detectado y fallas en la configuración de la máquina de votación, que a su vez generaron más eventos iniciales.

ii. **Evento inicial: Máquina de votación mal sellada**

El escenario inicia con la ocurrencia del **EI**(Máquina de votación mal sellada), esto se puede presentar en el proceso de congelamiento el día anterior a las elecciones, dado que las máquinas de votación son auditadas y luego dada la conformidad para que la máquina haga parte del proceso, esta se sella con algún mecanismo que permita al día siguiente al inicio de la votación, verificar que no fue accedida físicamente y no se alteró su estado. El escenario correcto sigue con la detección del sello irregular, evitando así el ingreso no autorizado y la manipulación de alguna de sus funcionalidades. En la figura 18 se observa el diagrama de secuencia de eventos en donde se desarrolló un árbol de fallas para el evento de no detección del evento inicial.

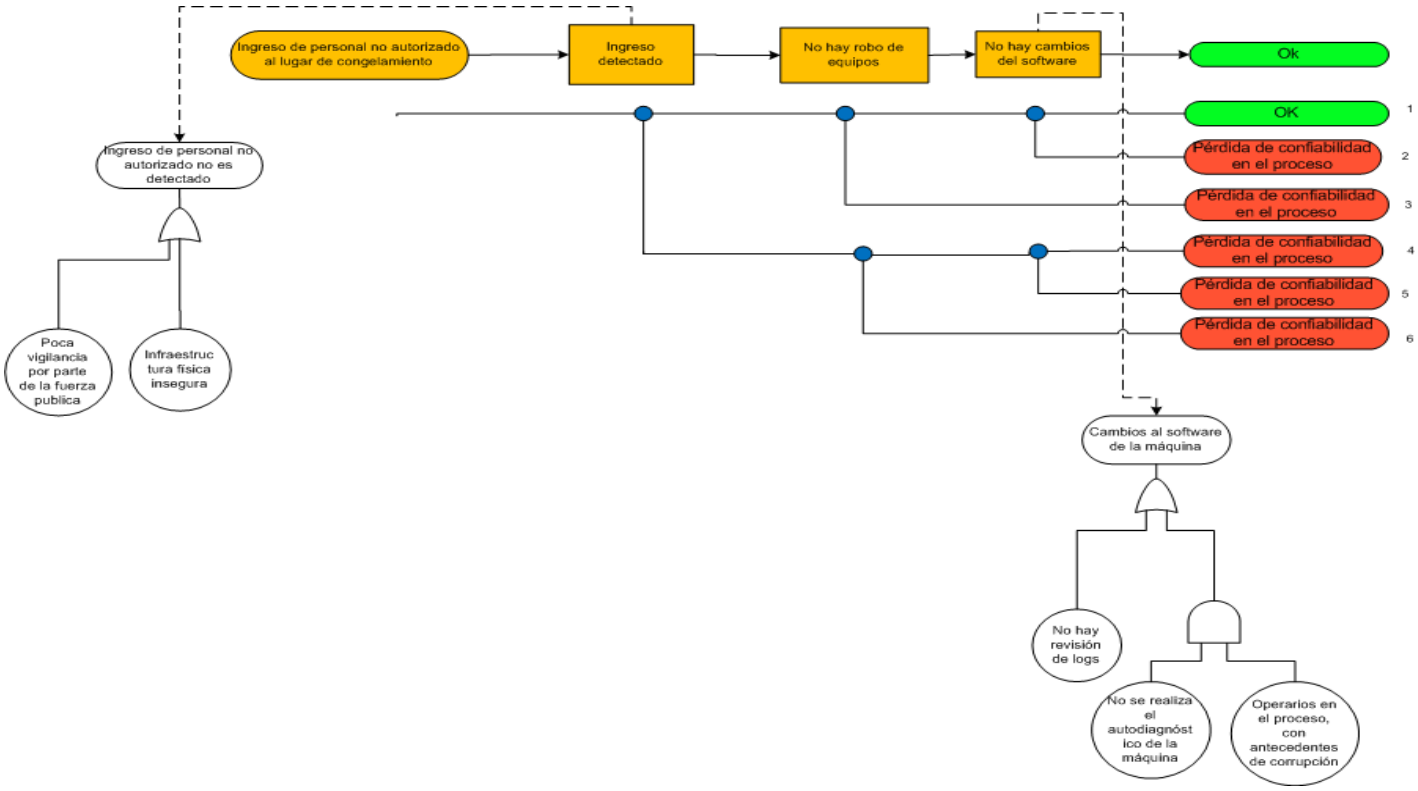
Figura 18:Diagrama de secuencia de eventos del EI: Máquina de votación mal sellada.



iii. Evento inicial: Ingreso de personal no autorizado al lugar de congelamiento

El escenario supone el ingreso de personal no autorizado al lugar de almacenamiento de las máquinas de votación, el ingreso es detectado y por lo tanto no se presenta robo ni manipulacion de software de máquinas. En la figura 19 se observa el diagrama de secuancia de eventos y los dos árboles de falla que se desarrollaron al evento de no detección del ingreso y a la manipulación del software. Se identificaron mas eventos iniciales como la infraestructura insegura de los sitios de congelamiento o votación(generalmente el proceso de congelamiento se lleva a cabo en el mismo lugar de votación), poca vigilancia de parte de la fuerza publica, no revision de logs de las maquinas, operarios con antecedentes de corrupcion y no realizacion del autodiagnóstico de la máquina de votación.

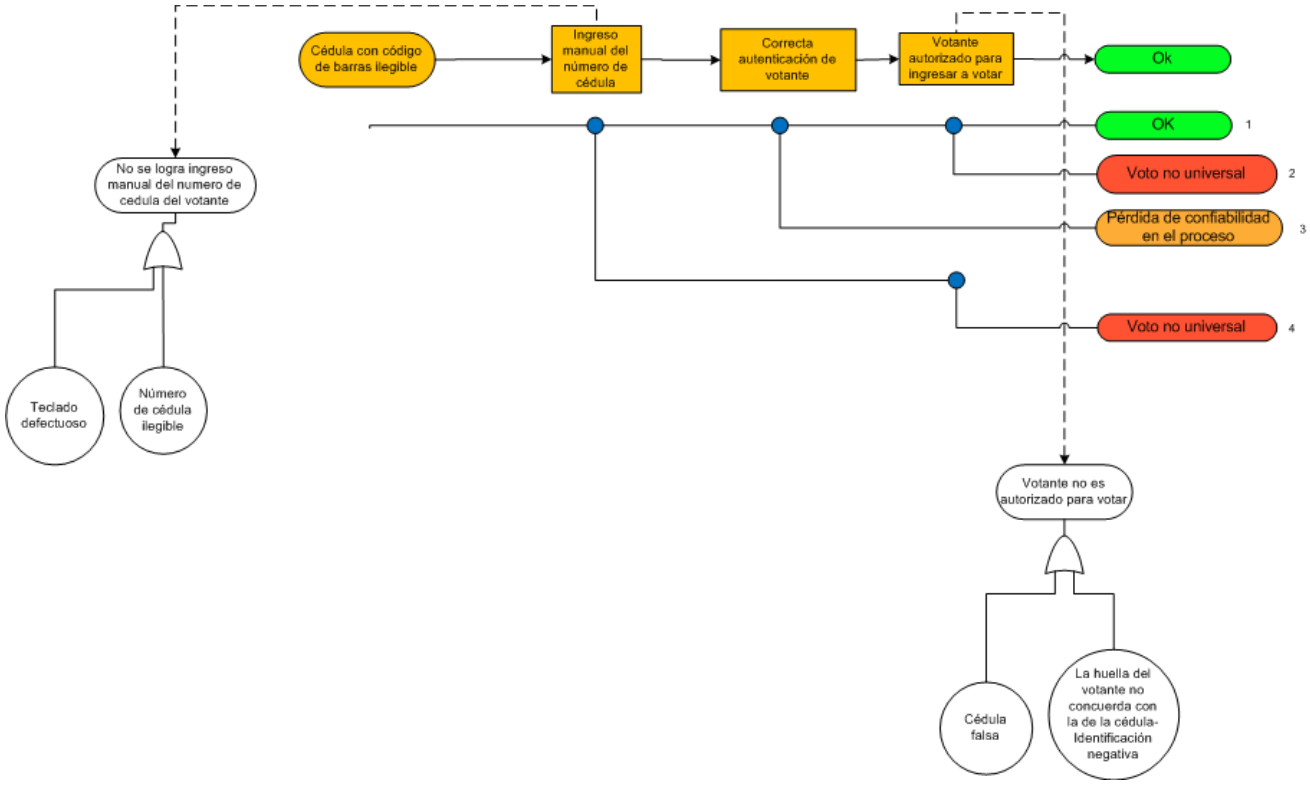
Figura 19:Diagrama de secuencia de eventos del EI: Ingreso de personal no autorizado al lugar de congelamiento.



Evento inicial : Documento de identificación con código de barras ilegible.

El escenario inicia con el evento inicial en el cual no es posible leer el código de barras de la cédula debido a su mal estado. Si este es el caso, se debe ingresar manualmente el número de la cédula para hacer una correcta verificación de votante y autorizarle a ingresar a emitir su voto. El evento 'No se logra ingreso manual del número de la cédula del votante' se descompuso en dos eventos, teclado defectuoso y numero de cedula ilegible. De la misma forma para el evento votante no es autorizado apra ingresar a votar, se le identificaron dos eventos: cédula falsa y no correspondencia de huella del votante con la cédula presentada. Todo lo anterior se puede observar en la figura 20

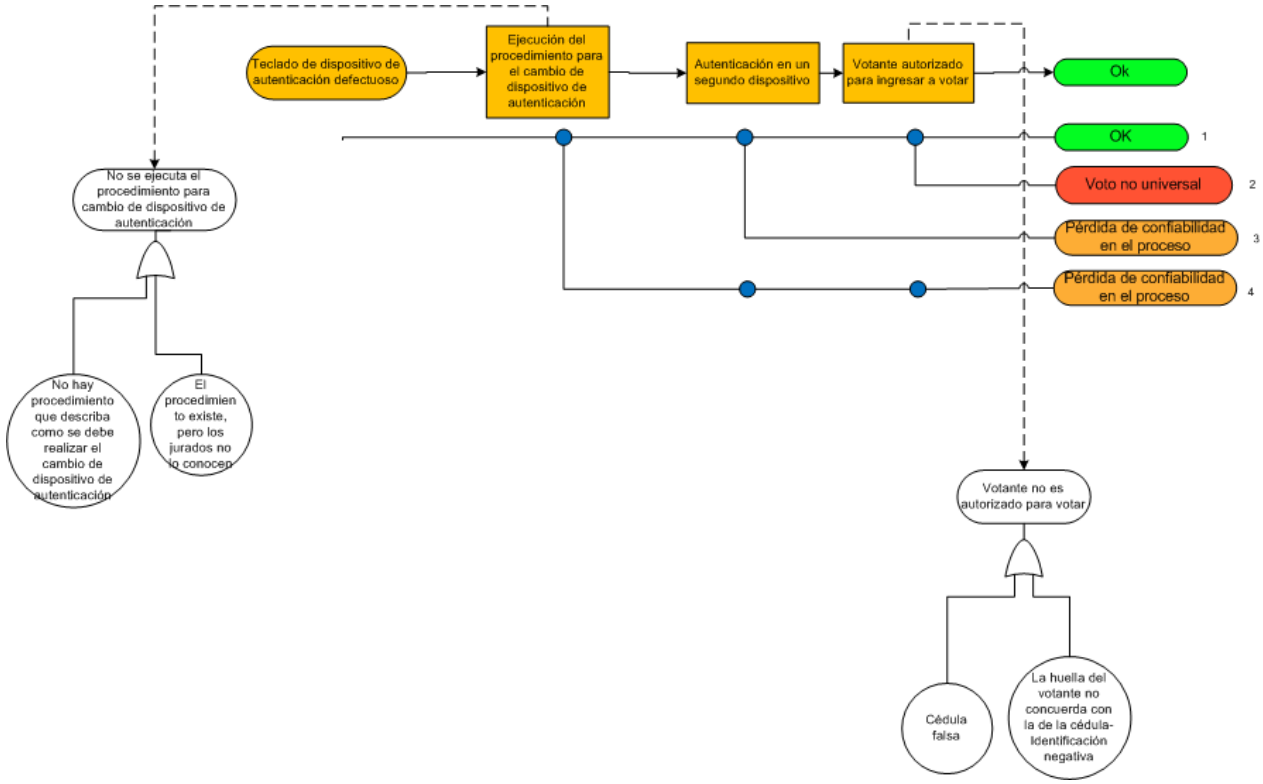
Figura 20:Diagrama de secuencia de eventos del EI: Cédula con código de barras ilegible.



iv. Evento inicial: Teclado de dispositivo de autenticación defectuoso.

En el caso en el que se presente este evento inicial, debe ejecutarse un procedimiento para el cambio de dispositivo de autenticación. La no existencia de este procedimiento puede generar una brecha de seguridad que permitiría el sabotaje o manipulación de datos. La negación de estos eventos da como resultado que el elector no pueda ingresar a votar, propiciando la pérdida de confiabilidad del proceso(ver figura 21).

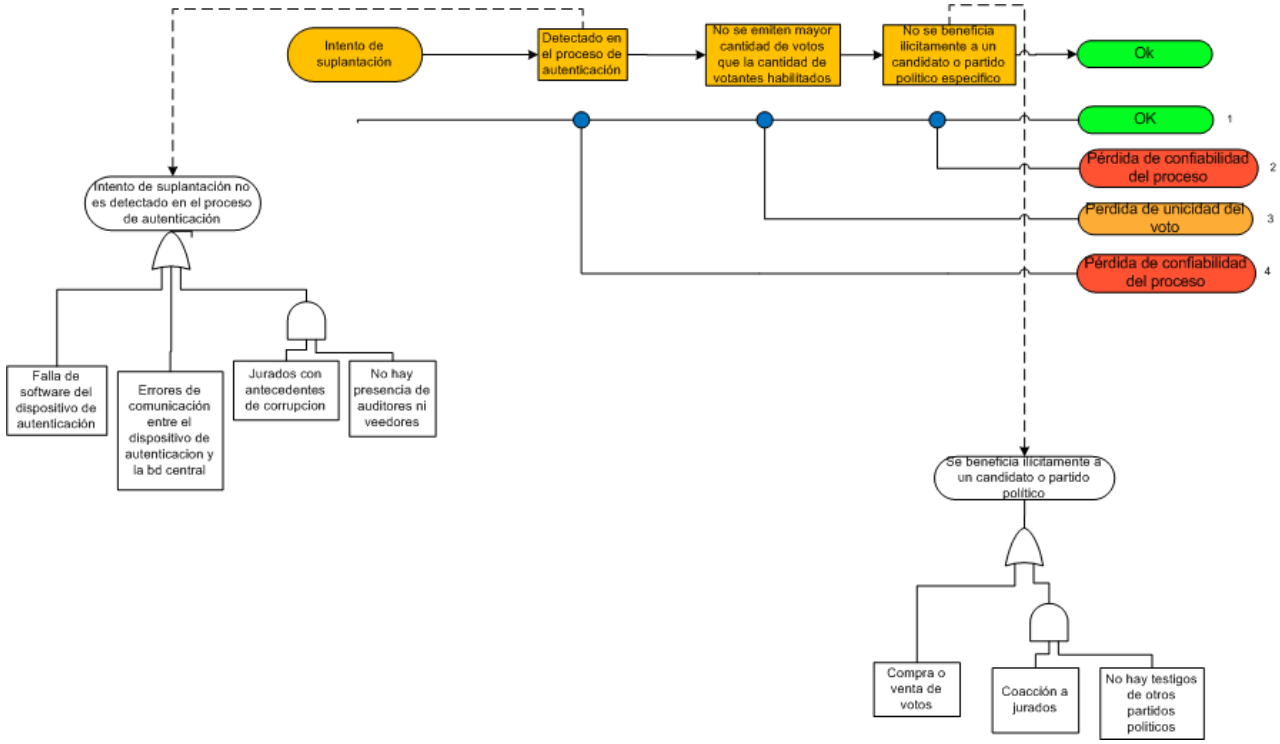
Figura 21:Diagrama de secuencia de eventos del EI: Teclado de dispositivo de autenticación defectuoso.



v. Evento inicial: Intento de suplantación

Los intentos de suplantación se pueden presentar de varias formas. Una persona puede tratar de votar con una cédula robada, una cédula de una persona fallecida o una cédula falsa. En estos tres casos, el sistema de autenticación debe permitir la detección del evento. Si el intento de suplantación no es detectado, se obtendrá mayor cantidad de votos que la cantidad de votantes habilitados, pero esto se sabrá solo después del cierre de la jornada. Por esta razón es tan importante detectar estos casos, ya que si se hace oportunamente, se puede evitar el fraude y dar confiabilidad al proceso de votación (ver figura 22).

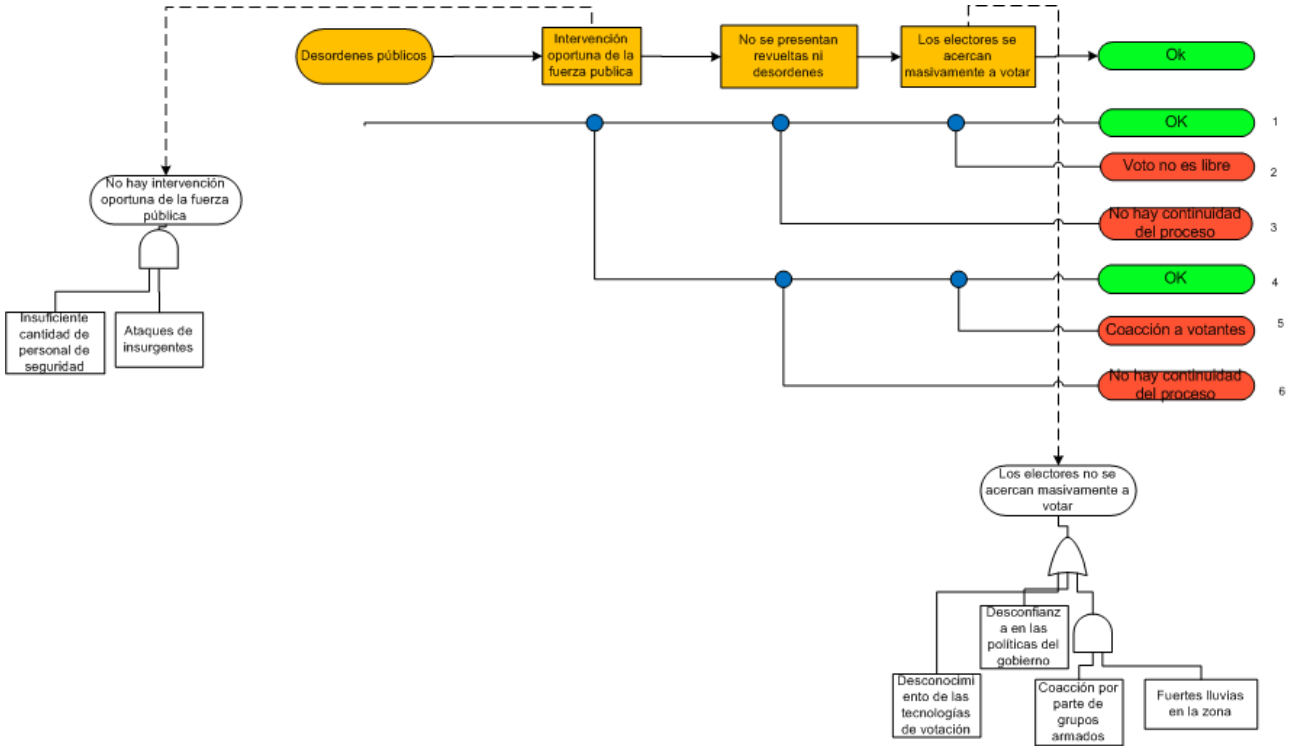
Figura 22:Diagrama de secuencia de eventos del EI:Intento de suplantación.



vi. Evento inicial: Desórdenes Públicos

Los desórdenes públicos, las manifestaciones violentas y las incursiones de grupos armados son eventos que pueden suceder en cualquier tipo de proceso electoral. En la actualidad, a pesar de la madurez del proceso, se presentan desórdenes públicos debido a la delicada situación de orden que vive gran porcentaje de municipios del país. Cuando sucede esto, si hay una oportuna intervención de la fuerza pública, se puede lograr la continuidad de la votación. En caso contrario, se puede presentar desde presiones hacia los electores para que voten por determinado candidato, hasta la suspensión de las votaciones. Todo lo anterior da como resultado gran porcentaje de abstencionismo. Otras causas de abstencionismo son consideradas, como por ejemplo, la desconfianza en las políticas del gobierno, el desconocimiento de las tecnologías de votación y por ende temor de enfrentarse a este tipo de votación (ver figura 23).

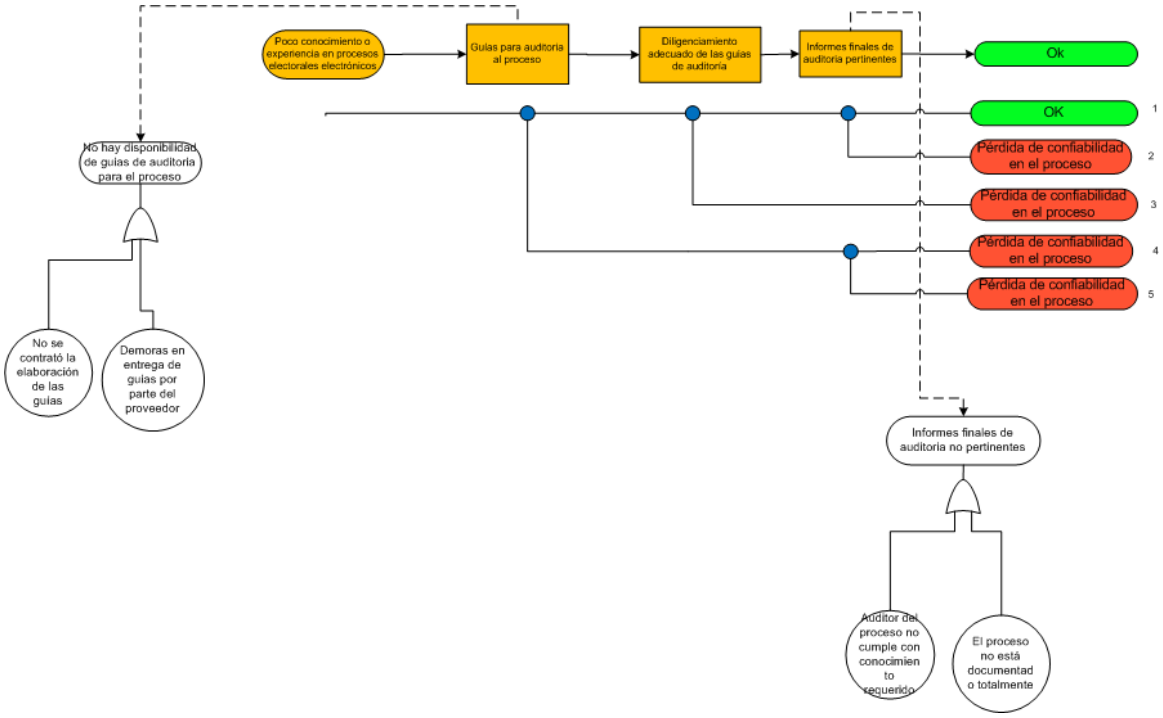
Figura 23:Diagrama de secuencia de eventos del EI: Desórdenes Públicos



vii. Evento inicial: Poco conocimiento o experiencia en procesos electorales electrónicos por parte de los auditores.

Generalmente cuando se escogen los auditores para un proceso electoral electrónico, se busca que tengan experiencia en este tipo de procesos, ya que esto garantiza una auditoría de calidad. Dado la novedad del voto electrónico en Colombia, hay pocos auditores en el país que tienen experiencia en este tipo de eventos, así que es vital que todo esté documentado y se elaboren las guías de auditoría para que el auditor tenga una visión clara de lo que debe medir y sobre lo que debe informar en el reporte final. En las últimas elecciones, los procesos de interventoría y auditoría a las votaciones, los ha realizado la Universidad Industrial de Santander, debido a su experiencia y garantía de imparcialidad y calidad de trabajo. Ahora, en cuanto a voto electrónico se ha logrado un gran avance gracias a la prueba piloto del 27 de Octubre de 2007, pero hay conciencia que se deben realizar más pruebas para caracterizar totalmente el proceso y realizar mediciones de puntos críticos(Ver figura 24).

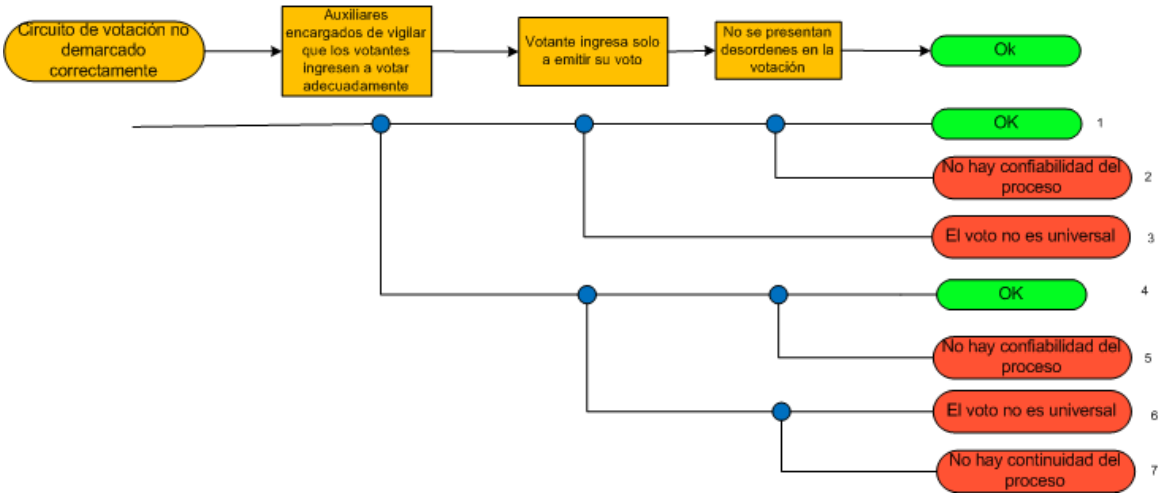
Figura 24:Diagrama de secuencia de eventos del EI: Poco conocimiento o experiencia en procesos electorales electrónicos por parte de los auditores.



viii. Evento inicial: Circuito de votación no demarcado correctamente

La demarcación del circuito de votación es una característica importante del proceso, ya que si no se realiza, genera confusión de los votantes, dando lugar a desórdenes, ingreso de dos o más personas simultáneamente al cubículo de votación y por ende, pérdida de la confidencialidad de la que debe gozar el voto. Este evento puede presentarse no solo en procesos electorales electrónicos, sino también en el tradicional(Ver figura 25).

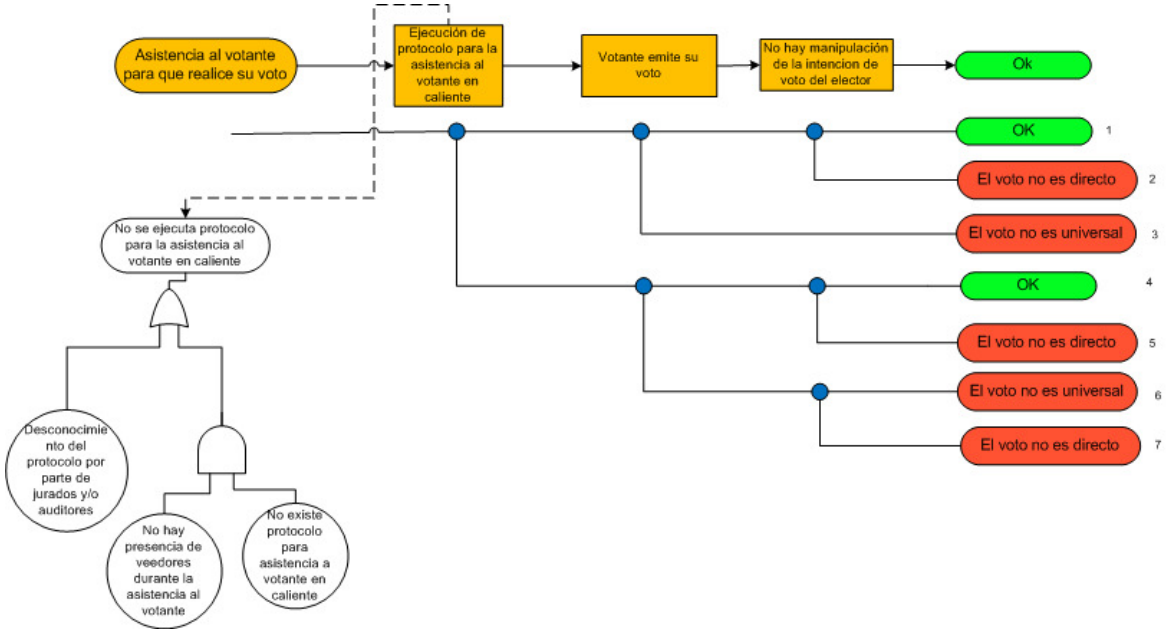
Figura 25:Diagrama de secuencia de eventos del EI: Circuito de votació no demarcado correctamente.



ix. Evento inicial: Asistencia irregular al votante

Este es un evento bastante probable en el proceso electrónico, sobre todo si no hay la suficiente educación a la ciudadanía acerca del funcionamiento de las tecnologías. La asistencia al votante se vuelve crítica en el caso en el que el auxiliar, jurado o el encargado de brindar la asistencia viole las características del voto. Es por esto que es importante que existan protocolos que indiquen lo que se debe hacer en los casos de asistencia a los votantes y evitar irregularidades. (Ver figura 26).

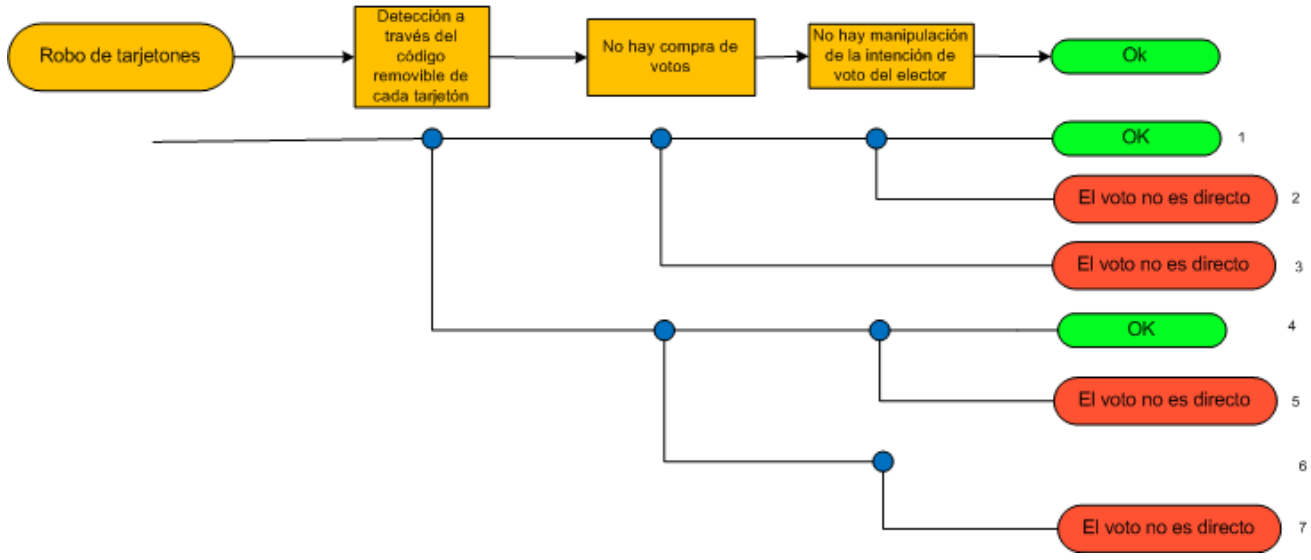
Figura 26:Diagrama de secuencia de eventos del EI: Asistencia irregular al votante.



x. Evento inicial: Robo de tarjetones

El robo de tarjetones se presenta en los casos de uso de tecnologías que aun utilizan el tarjetón físico como medio para que el elector especifique su voto. Generalmente el robo de tarjetones se realiza para comprar votos, en donde la persona que ingresa a votar, ingresa con el tarjetón robado que ya viene marcado y roba el tarjetón que le da el jurado. Asi, logra obtener otro tarjetón para que se siga la cadena. Para evitar estos robos, los tarjetones electrónicos pueden traer consigo un numero que es controlado por el jurado y que es revisado antes que el elector deposite en tarjetón en la urna, de tal forma que pueda saberse si es el mismo tarjetón que se le dio al ingresar. Claramente, antes de depositar el tarjetón en la urna, este número debe ser removido para evitar la trazabilidad del voto con su emisor. Ver figura 27.

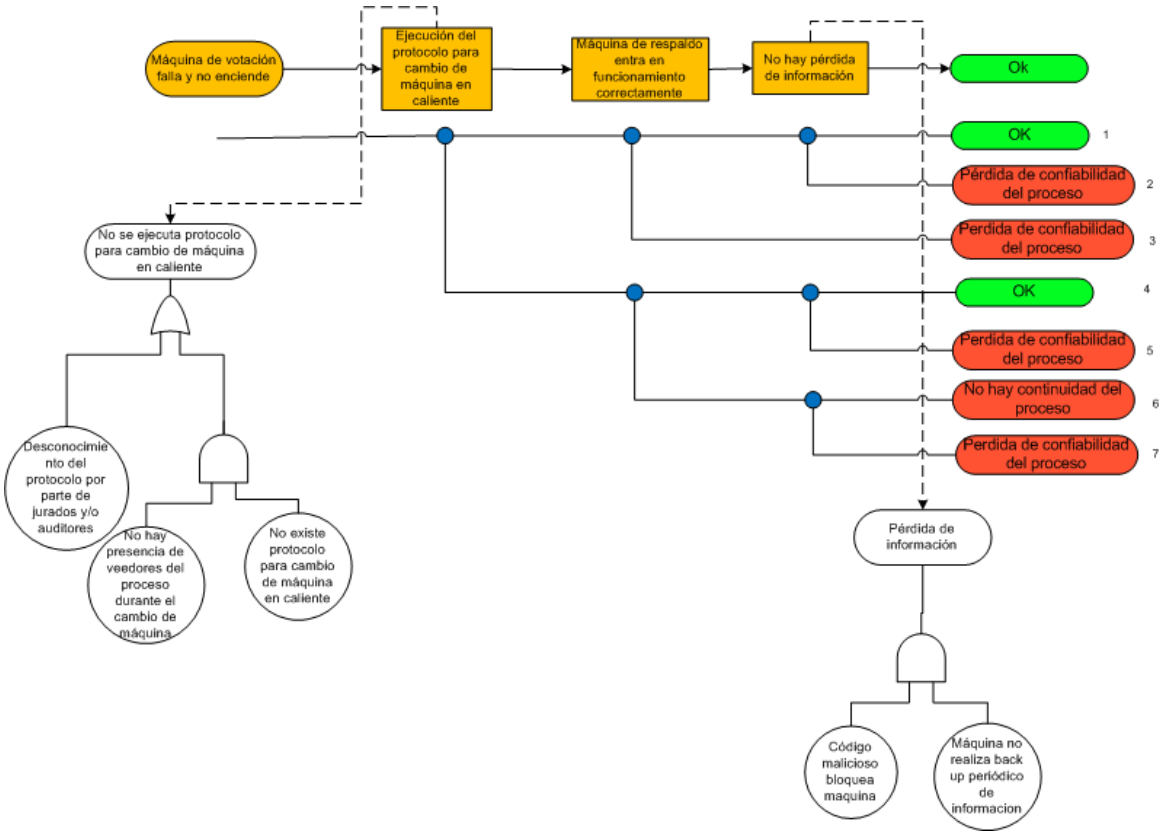
Figura 27:Diagrama de secuencia de eventos del EI: Robo de tarjetones



xi. Evento inicial: Fallo general de la máquina de votación

Uno de los eventos más críticos es el fallo de la máquina en medio del proceso y que esta no pueda volver a operar. Para estos casos, debe establecerse un protocolo de acciones para el cambio de máquina para mantener la transparencia del proceso mientras se garantiza la continuidad del mismo. La no existencia o no ejecución de un procedimiento previamente establecido generaría brechas de seguridad y pérdida de información valiosa. También debe garantizarse suficiente número de máquinas de respaldo y que a su vez funcionen correctamente y estén certificadas para su uso en el proceso. Ver figura 28

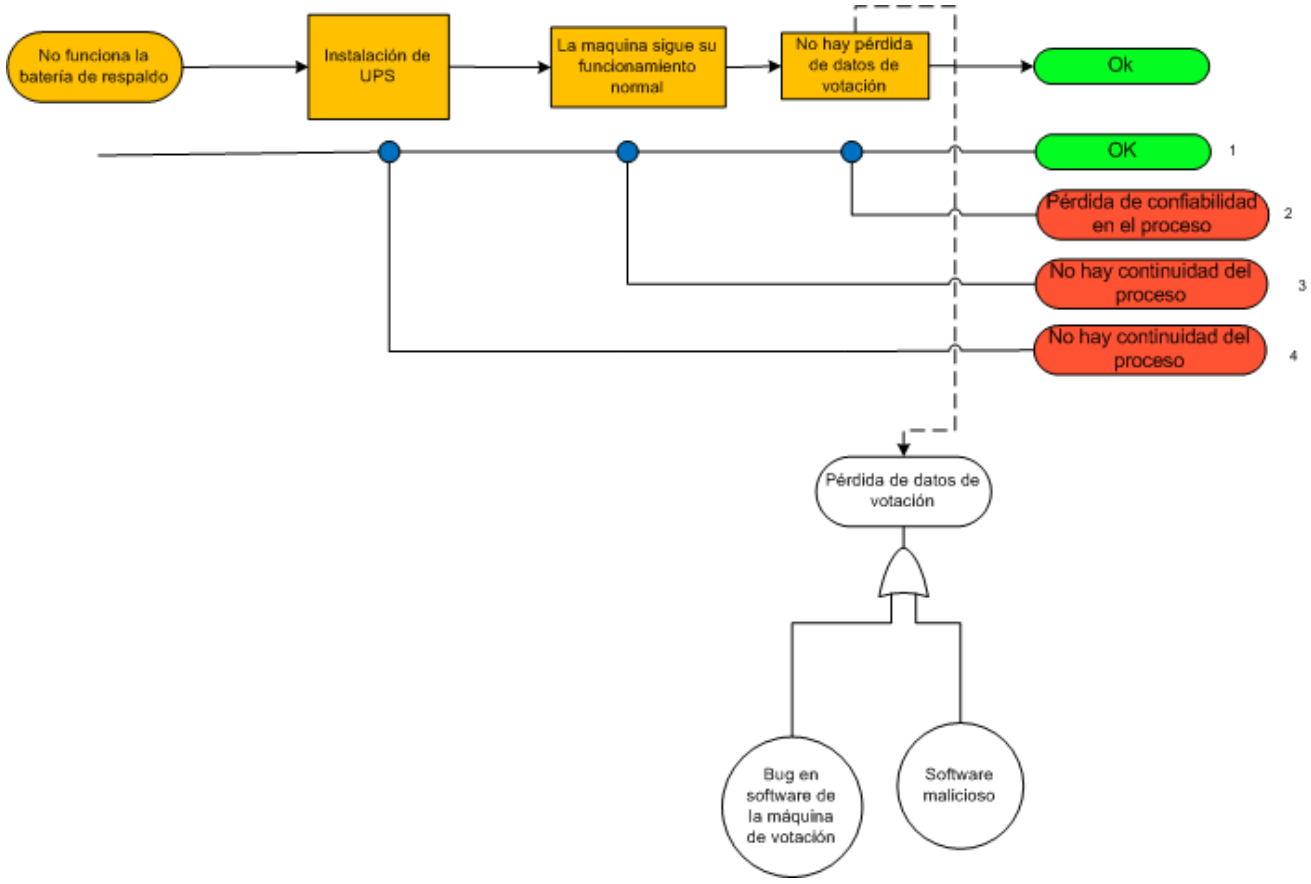
Figura 28:Diagrama de secuencia de eventos del EI: Máquina de votación falla y no enciende.



xii. Evento Inicial: Fallas en la Batería de respaldo de la máquina de votación

Este evento se puede presentar en el caso que haya alguna falta de energía y la batería de respaldo de la máquina deba entrar en funcionamiento pero no lo haga o lo haga por un corto tiempo para permitir la conexión a alguna ups. En estos casos se deben garantizar todas las condiciones para que las máquinas sigan funcionando normalmente a pesar del corte de energía, de lo contrario podría pararse el proceso o pérdida de información. Ver figura 29.

Figura 29:Diagrama de secuencia de eventos del EI: Fallas en la Batería de respaldo de la máquina de votación.



xiii. Evento inicial: Fallas en la calibración del escáner óptico

Este evento se puede presentar con las tecnologías que utilizan tarjetón físico y su lectura se realiza a través de escáner óptico.

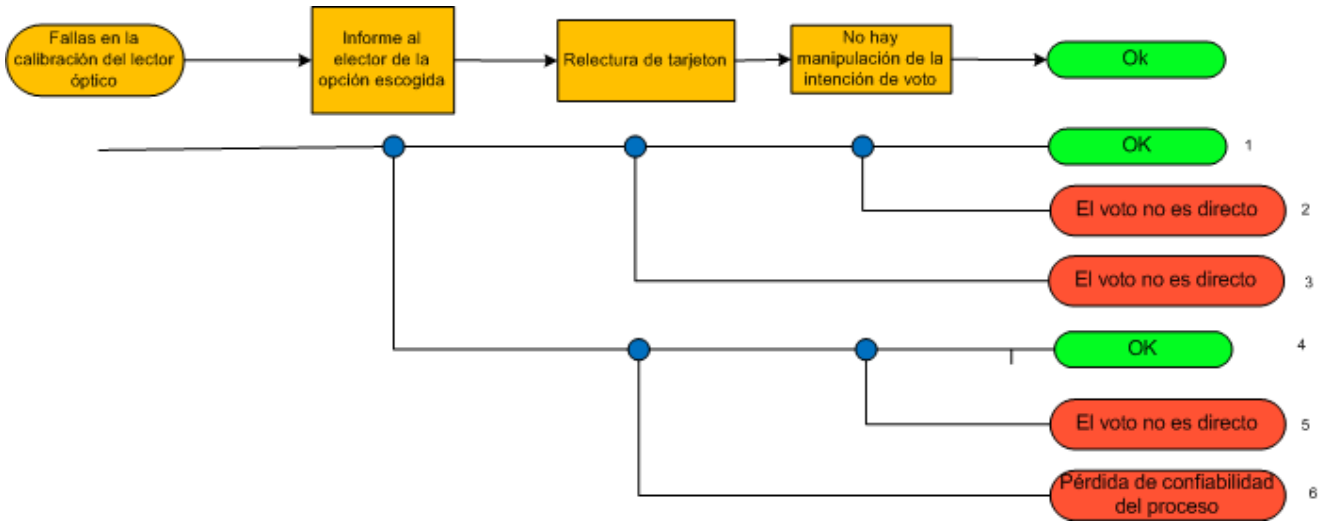
Los sistemas de lectura óptica de votos, poseen un umbral de sensado, esto quiere decir que las marcas en los tarjetones que son más oscuras que el umbral del escáner son consideradas como votos. Las que sean menos oscuras que el valor umbral, no serán contadas como votos.

Debido a que el valor del umbral puede variarse, el sensor del escáner puede ser calibrado de tal forma que solo acepte marcas bastante oscuras o que acepte hasta la marca más débil. Calibrar el escáner significa establecer umbrales de detección de las marcas de los tarjetones de votación de tal forma que los votos sean contados de acuerdo a lo que establece la ley. Idealmente, todos los lectores ópticos utilizados para una votación deben aplicar el mismo estándar que es comparable a una o varias personas examinando los tarjetones de votación para determinar si la marca realizada en él es un voto o no. Los extremos en la calibración de los escaners son perjudiciales. Si se coloca un umbral muy sensible al escáner, este contará puntos, manchas y hasta motas de polvo como votos efectivos. Por otro lado si el umbral del escáner es poco sensible, entonces dejará de contar votos válidos.

La amenaza que genera la mala calibración o la calibración deliberada de un escáner es que los resultados de las votaciones no reflejarán la realidad de la intención de voto y creará confusión. En este tipo de evento es más difícil manipular votos cambiándolos de un candidato a otro, porque el escáner no es inteligente, pero si generará votos o presentará errores donde no los hay. La máquina

de votación debe pedir confirmación al votante acerca de su elección, si es errónea, de debe cancelar el proceso y volver a leer el tarjetón. Si todos estos procesos no son llevados a cabo de forma adecuada por la máquina de votación y el elector, se pueden presentar errores y por ende pérdida de confiabilidad del proceso(Ver figura 30).

Figura 30:Diagrama de secuencia de eventos del EI: Fallas en la calibración del escáner óptico



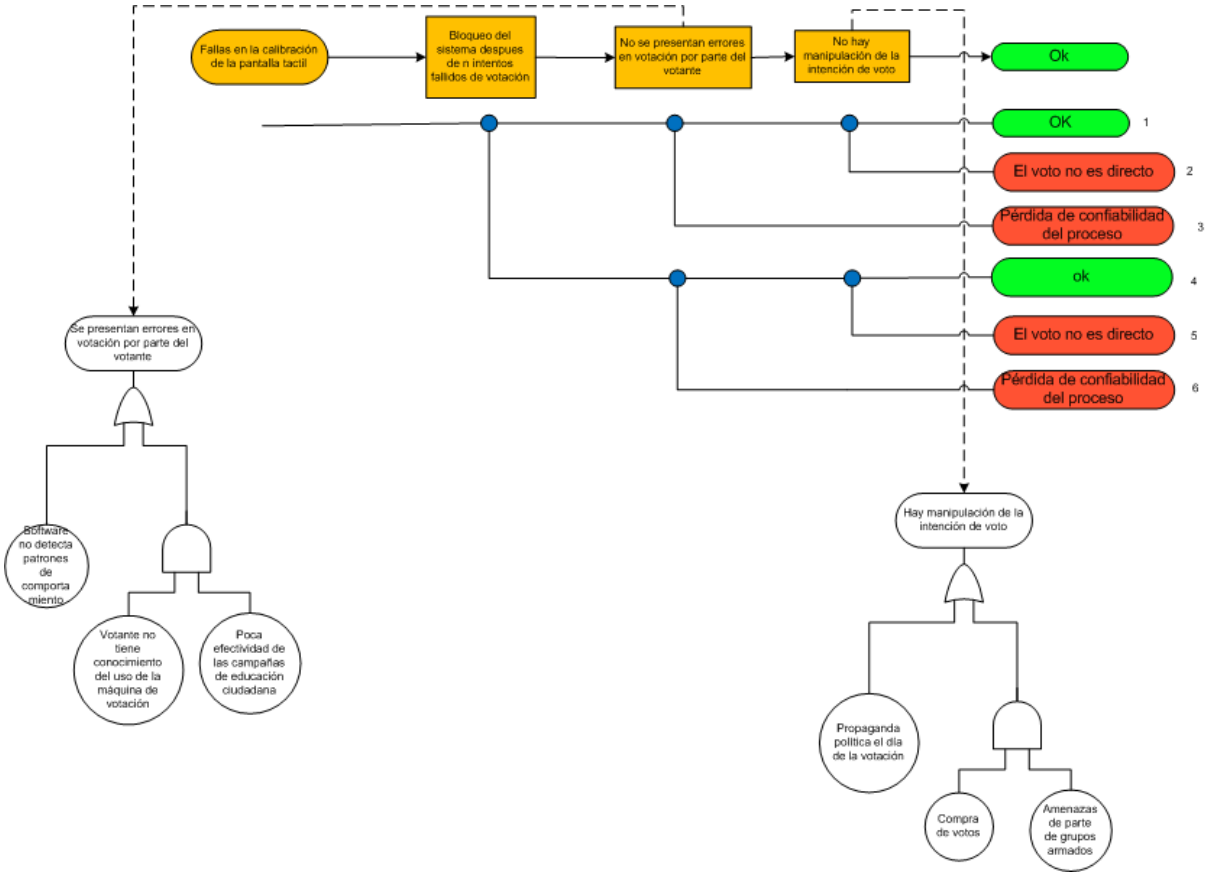
xiv. Evento Inicial: Fallas en la calibración de la pantalla táctil

La amenaza que introduce la pantalla táctil se debe a su naturaleza y diseño. Las pantallas táctiles están conformadas además por otra pantalla que despliega la información, esto quiere decir que el usuario final al utilizar una pantalla táctil o touch screen realmente no entra en contacto con la pantalla sensible al tacto sino que sobre esta hay otra pantalla protectora que despliega la información y es la que realmente hace contacto con el usuario. Como resultado de esto, no hay una relación desde fábrica, entre las coordenadas de un punto de la pantalla que despliega los datos y las coordenadas de la pantalla táctil, ya que son dos dispositivos diferentes. Por esto,

el software que hace de interfaz entre touch screen y la pantalla, debe reconocer cuales puntos en el sensor de la pantalla táctil, recaen sobre qué puntos en la pantalla que despliega los datos. La sincronización de las coordenadas de estas dos pantallas se conoce como calibración del touch-screen o pantalla tactil. Para calibrar la pantalla táctil de la máquina, generalmente se le pide a la persona que toque al menos tres puntos de la pantalla, estos puntos frecuentemente son dos esquinas opuestas y uno central. Si durante la etapa de calibración se tocan deliberadamente otros puntos que no se han indicado, la pantalla quedará mal calibrada.

Si además de la falla de calibración de la pantalla, el sistema no detecta una cantidad determinada de intentos de voto fallidos y emite algún tipo de alarma, se presentarán errores en la votación que conllevarán a la manipulación de la intención de voto del elector.(Ver figura 31)

Figura 31:Diagrama de secuencia de eventos del EI: Fallas en la calibración de la pantalla táctil.

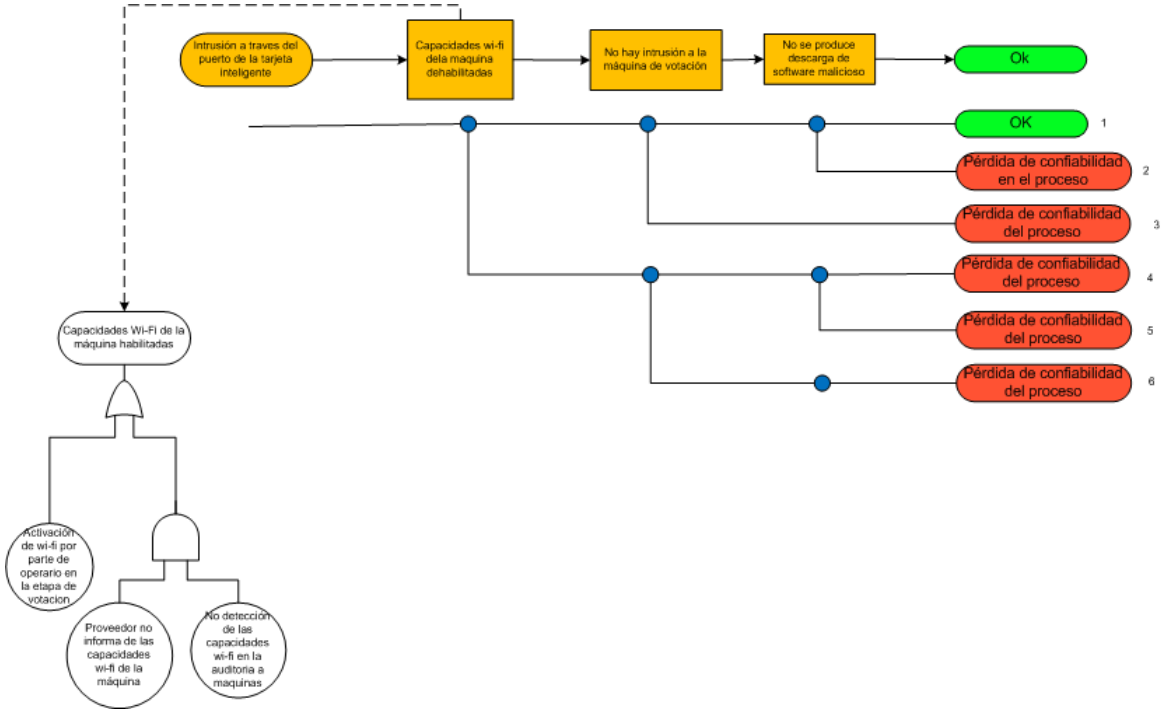


xv. Evento Inicial: Intrusión a través del puerto de la tarjeta inteligente

Este tipo de ataque se puede realizar a través de la creación de una interfaz basada en un software residente en otra máquina. La máquina de votación sería accesada a través del puerto lector de la tarjeta. El objetivo principal sería el controlador de este puerto que normalmente no es revisado debido a que casi siempre es comprado a otro proveedor y este no permite su manipulación o modificación. El atacante solamente coloca el dispositivo en el lector de tarjeta, el cual puede comunicarse con un computador externo a través de una conexión inalámbrica, haciendo mucho más difícil su detección, y descargar todo tipo de código malicioso que pueda modificar los registros de la máquina y cambiar su comportamiento. El impacto de este ataque depende del momento en que se realice. Si el ataque toma lugar en la etapa de programación de las

máquinas, será bastante alto debido a que se pueden manipular mayor cantidad de máquinas. SI el ataque se realiza en el momento de la votación, solo afectará la máquina o máquinas a las que el atacante tenga acceso. Ver figura 32

Figura 32:Diagrama de secuencia de eventos del EI:Ataque a traves del puerto de la tarjeta.

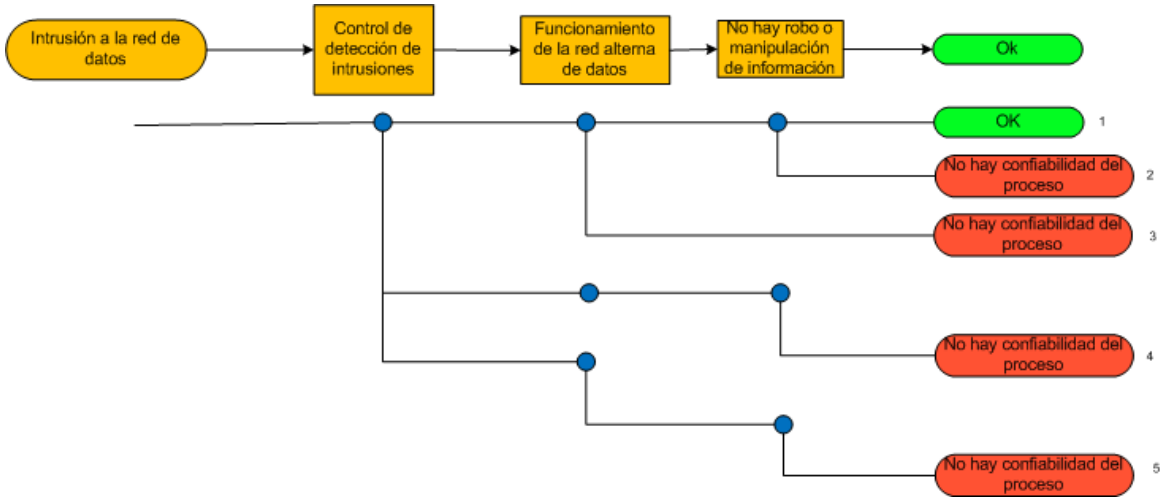


Evento inicial: Intrusión a la red de datos

Uno de los eventos iniciales más críticos es la intrusión a la red de datos, la cual podría causar robo y/o saboteo de la información de votación que es transmitida a la central nacional. Para evitar las intrusiones, se implementan estrategias de seguridad lógica y física en redes de comunicaciones y como medida de contingencia si el evento se presenta, entra en funcionamiento una red de respaldo por donde sigue el flujo de información y se garantiza la transparencia y continuidad del proceso. En las elecciones actuales

se cuenta con buen nivel de seguridad en transmisión de datos debido al buen manejo e implementación de protocolos, herramientas criptográficas y sistemas de gestión de seguridad de la información. En la figura 33 se observa el evento inicial y los demás eventos que son lanzados si se materializa.

Figura 33:Diagrama de secuencia de eventos del EI:Intrusión a la red de datos



4.2.3 INTEGRACIÓN DE EVENTOS INICIALES : ÁRBOL DE FALLAS

Con base en la identificación de eventos iniciales y la cadena de eventos que generarían la ocurrencia de desenlaces indeseables para el proceso de votación electrónica, se construyó el árbol de fallas, que identifica principalmente los puntos de medición del sistema para controlar la ocurrencia de estos eventos que minarían la confiabilidad del proceso. En la imagen del ANEXO D se puede observar el árbol, eventos iniciales o puntos de medición se identifican por estar enmarcados en círculos y son listados en la tabla 4

N°	EVENTO INICIAL
1	Contratación tardía de elaboración de guías.[1]
2	Demora en entrega de Guías por parte del proveedor.[1]
3	Poco conocimiento o experiencia en procesos electorales electrónicos por parte de auditores y/o veedores.[4]
4	Diligenciamiento inadecuado de las guías de auditoría.[1]
5	Teclado de dispositivo de autenticación defectuoso[5].
6	Inexistencia de procedimiento que describa como se debe realizar el cambio de dispositivo de autenticación. [33]
7	No disponibilidad de dispositivos de autenticación de respaldo.[5]
8	Procedimiento de cambio de dispositivo de autenticación no es conocido por el personal encargado del proceso. [33]
9	Número de cédula ilegible.[1]
10	Cédula con código de barras ilegible.[1]
11	Amenazas por parte de grupos armados. [34]
12	Compra/venta de votos.[1]
13	Propaganda política el día de votación.[1]
14	Control inadecuado de tarjetones de votación.[5]
15	No existe protocolo para asistencia a votante en caliente. [33]
16	Desconocimiento de protocolo de asistencia a votantes por parte de jurados y auditores.[33]
17	No hay presencia de veedores durante la asistencia al votante [5].
18	Robo de tarjetones[34]
19	Votante no tiene conocimiento el uso de la máquina de votación.[33]
20	Poca efectividad de las campañas de educación ciudadana.[5]
21	Fallas en la calibración de la pantalla táctil.[5]
22	Fallas en la lectura del escáner óptico de la máquina de la votación.[5]
23	No hay retroalimentación al elector acerca de la opción de voto escogida.[24]
24	Proveedor no informa de las capacidades inalámbricas de la máquina de votación.[1]
25	No hay control de las capacidades inalámbricas en la auditoría a máquinas de votación.[34]
26	Activación de capacidades inalámbricas de máquinas por parte de operario en el proceso de votación.[1]
27	La máquina de votación no fue puesta en ceros por parte del proveedor.[1]
28	El proveedor no posee información suficiente acerca del proceso.[24]
29	Fallas en la emisión del reporte de estadísticas de votación por máquina.[4]
30	El operario no conoce el funcionamiento adecuado de la máquina de votación.[24]
31	Poca presencia de auditores.[24]
32	Poca presencia de veedores.[24]

N°	EVENTO INICIAL
33	Información de votación no cifrada o cifrado débil. [32]
34	Passwords de usuario débiles. [32]
35	No hay segregación de funciones. [32]
36	Desconocimiento de las tecnologías de votación.[33]
37	Desconfianza en las políticas del gobierno.[3]
38	Coacción por parte de grupos armados.[34]
39	Circuito de votación no demarcado correctamente.[1]
40	Poca presencia de encargados de vigilar que los votantes ingresen a la máquina de votación adecuadamente.[1]
41	Insuficiente cantidad de personal de seguridad.[34]
42	Ataques insurgentes.[1]
43	No existe protocolo para cambio de máquinas en caliente.[1]
44	Poca presencia de jurados y/o auditores durante el cambio de máquina de votación.[26]
45	Desconocimiento del protocolo de cambio de máquina por parte de jurados y /o auditores.[26]
46	No funciona la batería de respaldo de la máquina de votación.[8]
47	La máquina de votación falla y no es posible reiniciarla.[8]
48	Brecha de seguridad en el software de votación.[32]
49	Código malicioso bloquea la máquina de votación.[32]
50	Máquina no realiza copia periódica de seguridad de la información de votación.[32]
51	Falla en el software del dispositivo de autenticación[8].
52	Fallas de comunicación entre el dispositivo de autenticación y la bd central.[32]
53	Jurados con antecedentes de corrupción.[8]
54	Poca presencia de auditores y veedores en el proceso de autenticación del votante.[8]
55	Cédula falsa[1]
56	Intrusión en la red de datos [34]

Tabla 4: Listado de eventos iniciales del proceso de votación electrónica.

4.2.4 EXPRESIONES LÓGICAS DEL ÁRBOL DE FALLAS DEL PROCESO DE VOTACIÓN ELECTRÓNICA

A continuación se muestra el desarrollo de las expresiones lógicas que representan el escenario de fallas identificadas en el proceso de votación

electrónica. Los eventos serán representados a través de su número para facilitar la escritura de las ecuaciones.

NÚMERO	ECUACIÓN
1	$P_{E1} = P_r(1) + P_r(2) - P_r(2)P_r(2)$
2	$P_{E2} = P_r(3)P_r(4) + P_{E1} - P_r(3)P_r(4)P_{E1}$
3	$P_{E3} = P_r(5)P_r(6) + P_r(8) - P_r(5)P_r(6)P_r(8)$
4	$P_{E5} = P_r(5)P_r(9)P_r(10)$
5	$X_1 = P_r(55) + P_{E5} + (P_r(53)P_r(54) + P_r(51) + P_r(52) - P_r(53)P_r(54)P_r(51) - P_r(52)P_r(53)P_r(54) + P_r(53)P_r(54)P_r(51)P_r(52))$
6	$P_{E4} = P_r(7) + P_{E3} + X_1 - P_r(7)P_{E3} - P_{E3}X_1 - X_1P_r(7) + P_r(7)X_1P_{E3}$
7	$P_{E6} = P_r(15) + P_r(16)P_r(17) - P_r(15)P_r(16)P_r(17)$
8	$X_2 = P_r(11) + P_r(12)P_r(13) - P_r(11)P_r(12)P_r(13)$
9	$X_3 = P_r(14) + P_{E6} + P_r(18) - P_r(14)P_{E6} - P_{E6}P_r(18) - P_r(18)P_r(14) + P_r(1$
10	$X_4 = P_r(19)P_r(20) + P_r(21) - P_r(19)P_r(20)P_r(21)$
11	$X_5 = P_r(22) + P_r(23) + X_4 - P_r(22)P_r(23) - P_r(23)X_4 - X_4P_r(22) + P_r(22)P$
12	$P_{E7} = X_2 + X_3 + X_5 - X_2X_3 - X_2X_5 - X_3X_2 + X_2X_3X_5$
13	$P_{E8} = P_r(27) + P_r(28) - P_r(27)P_r(28)$
14	$P_{E9} = P_r(31)P_r(32) + P_r(29) + P_r(30) - P_r(31)P_r(32)P_r(29) - P_r(30)P_r(29 - P_r(30)P_r(31)P_r(32)P_r(29)$
15	$P_{E11} = P_r(25)P_r(24) + P_r(26) - P_r(25)P_r(24)P_r(26)$
16	$X_6 = P_r(34)P_r(35) + P_r(33) + P_{E11} - P_r(34)P_r(35)P_r(33) - P_r(33)P_{E11} - P_{E} + P_r(34)P_r(35)P_r(33)P_{E11}$
17	$P_{E10} = P_{E8}P_{E9}X_6 + P_r(56) - P_{E8}P_{E9}X_6P_r(56)$
18	$P_{E12} = P_r(39)P_r(40)$
19	$P_{E13} = P_{E12}P_r(41)P_r(42)P_r(38) + P_r(36) + P_r(37) - P_{E12}P_r(41)P_r(42)P_r(38 - P_r(37)P_{E12}P_r(41)P_r(42)P_r(38) + P_{E12}P_r(41)P_r(42)P_r(38$
20	$X_7 = P_r(43)P_r(44) + P_r(45) - P_r(43)P_r(44)P_r(45)$
21	$P_{E15} = P_r(46)P_r(47)X_7$
22	$P_{E16} = P_r(48)P_r(49)P_r(50)P_{E14}P_{E15}$
23	$X_8 = P_{E1} + P_{E4} + P_{E7} - P_{E1}P_{E4} - P_{E4}P_{E7} - P_{E7}P_{E1} + P_{E1}P_{E4}P_{E7}$
24	$X_9 = P_{E10} + P_{E13} + P_{E16} - P_{E10}P_{E13} - P_{E13}P_{E16} - P_{E16}P_{E10} + P_{E10}P_{E13}P_{E16}$

NÚMERO	ECUACIÓN
25	$P_{E17} = X_8 + X_9 - X_8 X_9$

La ecuación 25 da como resultado la probabilidad de ocurrencia del evento 17: **Pérdida de confiabilidad del proceso**.

Como lo indican las expresiones **23, 24 y 25**:

$$X_8 = P_{E1} + P_{E4} + P_{E7} - P_{E1}P_{E4} - P_{E4}P_{E7} - P_{E7}P_{E1} + P_{E1}P_{E4}P_{E7} \text{ (Ec 23)}$$

$$X_9 = P_{E10} + P_{E13} + P_{E16} - P_{E10}P_{E13} - P_{E13}P_{E16} - P_{E16}P_{E10} + P_{E10}P_{E13}P_{E16} \text{ (Ec. 24)}$$

$$P_{E17} = X_8 + X_9 - X_8 X_9 \text{ (Ec 25)}$$

La no confiabilidad del proceso o la probabilidad de no confiabilidad del proceso, se calcula por la suma booleana de las probabilidades de ocurrencia de eventos iniciales (Ec. 25) relacionados principalmente con las auditorías, ingreso de votantes, manipulación de intención de voto, manipulación de resultados y pérdida de información. Según el modelo obtenido, estos son los principales riesgos presentes en una votación electrónica, que si bien, también son riesgos presentes en votaciones tradicionales, la forma como se presentan en una votación electrónica, es diferente.

Dada la no confiabilidad del proceso, puede calcularse la confiabilidad del mismo, como lo establece la ecuación 26:

$$C_S = 1 - P_{E17} \qquad \text{Ec. 26}$$

Donde C_S representa la confiabilidad del proceso.

4.2.5 PRUEBAS AL SISTEMA

Las pruebas se realizaron a través de un grupo de sistemas de inferencia Fuzzy-Fuzzy Inference System(FIS). Cada sistema representa un evento

inicial como efecto de la evaluación de dos variables que pueden influir en su ocurrencia y, dado un grupo de reglas, que son establecidas a través de la experiencia del piloto de votación, se determina una probabilidad de ocurrencia del **EI.** (ver Anexo C).

La primera y segunda pruebas se realizaron con todas las probabilidades de los eventos iniciales en 0.01 y 0.99 respectivamente, para verificar que el sistema y las ecuaciones que lo representan estuvieran bien formadas. En efecto, al colocar todas las probabilidades iguales a 0.01 la confiabilidad del proceso de votación tiende al 100%. Por otro lado, si todas las probabilidades son colocadas a 0.99, la confiabilidad del proceso tiende a cero 0.

N. Evento	Probabilidad	Confiabilidad sistema
1	0.141	0.01645
2	0.321	
3	0.321	
4	0.2	
5	0.151	
6	0.2	
7	0.254	
8	0.195	
9	0.141	
10	0.141	
11	0.2	

N. Evento	Probabilidad	Confiabilidad sistema
12	0.237	
13	0.5	
14	0.301	
15	0.2	
16	0.486	
17	0.151	
18	0.151	
19	0.2	
20	0.196	
21	0.197	
22	0.151	
23	0.149	
24	0.196	
25	0.181	
26	0.196	
27	0.299	
28	0.322	
29	0.149	
30	0.49	
31	0.151	

N. Evento	Probabilidad	Confiabilidad sistema
32	0.321	
33	0.3	
34	0.3	
35	0.3	
36	0.40	
37	0.321	
38	0.196	
39	0.221	
40	0.221	
41	0.221	
42	0.196	
43	0.499	
44	0.151	
45	0.3	
46	0.151	
47	0.151	
48	0.3	
49	0.3	
50	0.3	
51	0.149	

N. Evento	Probabilidad	Confiabilidad sistema
52	0.149	
53	0.1	
54	0.1	
55	0.1	
56	0.489	

4.2.5.1 Aspectos estadísticos de las pruebas

Asumiendo que las probabilidades de ocurrencia de los eventos iniciales presentan una distribución normal, se obtiene la media y la desviación estándar según las ecuaciones 27 y 28 respectivamente

$$\mu = \frac{\sum_{i=1}^{56} p_{e_i}}{56} \quad \text{Ec. 27}$$

$$\mu = 0{,}23060$$

Donde Pe_i es la probabilidad de ocurrencia del evento i.

$$\delta^2 = \frac{\sum_{i=1}^{56} (Pe_i - \mu)^2}{56} \quad \text{Ec. 28}$$

$$\delta^2 = 0{,}01145$$

Haciendo uso del teorema central del límite, que establece que las medias de muestras aleatorias de cualquier variable siguen ellas mismas una distribución normal con desviación estándar de la población dividida por la raíz de la cantidad de muestras, se puede dar una expresión para el intervalo de confianza(Ec 29.):

$$\left(\mu - \frac{1.96 * \sigma}{\sqrt{56}}, \mu + \frac{1.96 * \sigma}{\sqrt{56}}\right) \quad \text{Ec. 29}$$

$$(0.2276, 0.2336)$$

A partir de este resultado se puede aseverar que se estaría un 95% seguro que la probabilidad media real de los eventos iniciales oscila entre el 0,2276 y 0,2336. Todo esto a partir de los datos obtenidos a través de los sistemas de inferencia fuzzy.

CAPÍTULO V: CONTROLES PREVENTIVOS Y DE MITIGACIÓN DE RIESGOS

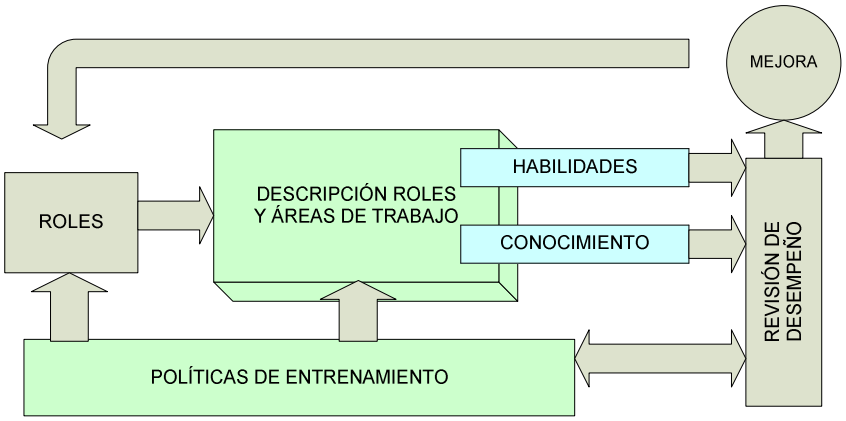
En la gestión de riesgos, se le conoce como control a todas las medidas tanto preventivas como correctivas que permiten prevenir o corregir los efectos de la materialización de los riesgos.

A continuación se proponen controles para prevenir la aparición de los eventos iniciales. Algunos controles presentan un nivel de cobertura amplio(controles estratégicos), con lo cual, con su implementación logran la prevención simultanea de gran cantidad de riesgos. Los demás controles son de tipo táctico y operativo.

5.1 CONTROLES DE NIVEL ESTRATÉGICO

1. **Diseñar, revisar y evaluar procesos para asegurar que los involucrados en el proceso de voto electrónico tengan la habilidad y conocimiento necesario para realizar sus actividades.**

   Figura 34:Capacitación del recurso humano



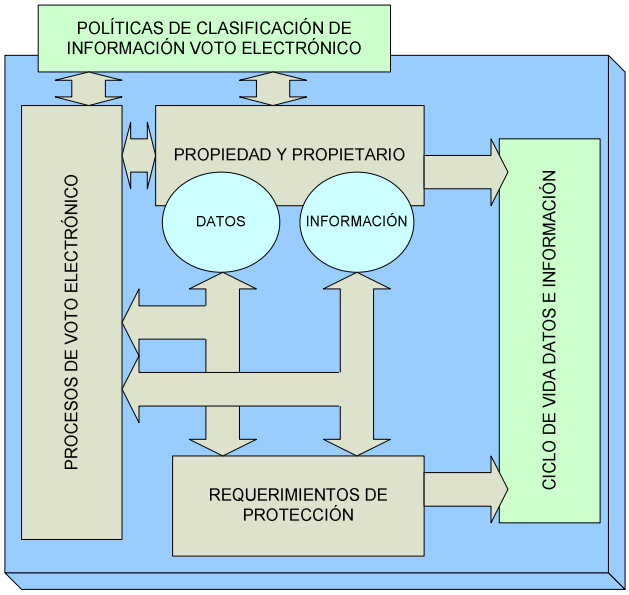
Fuente:Autores

Con base en unas políticas de entrenamiento deben establecerse roles, su descripción y las áreas de trabajo. Lo anterior permitirá la adquisición de conocimiento y desarrollo de habilidades por parte de los funcionarios que desarrollan los procesos de votación electrónica. En conclusión:

a. Se debe asegurar que existen descripciones de los roles para los diferentes actores del voto electrónico, y que estas descripciones son especificas al conocimiento y habilidad requerida para cada área de trabajo. Se debe revisar evidencia de que estas descripciones del trabajo son referenciadas durante la etapa de contratación de personal.
b. Se deben tener políticas de entrenamiento y asegurar que ellas ofrecen la oportunidad de atender a entrenamientos por parte de los empleados e involucrados en el voto electrónico.
c. Se deben contar con procesos de revisión de desempeño y generar evidencia que los involucrados reciben retroalimentación respecto al desempeño que ellos tienen en el proceso de votación electrónica.

2. **Diseñar, revisar y evaluar políticas y procesos para asignar propietarios y encargados de la protección de datos e información de acuerdo a su clasificación y la definición de su ciclo de vida.**

Figura 35: Clasificación de la información.



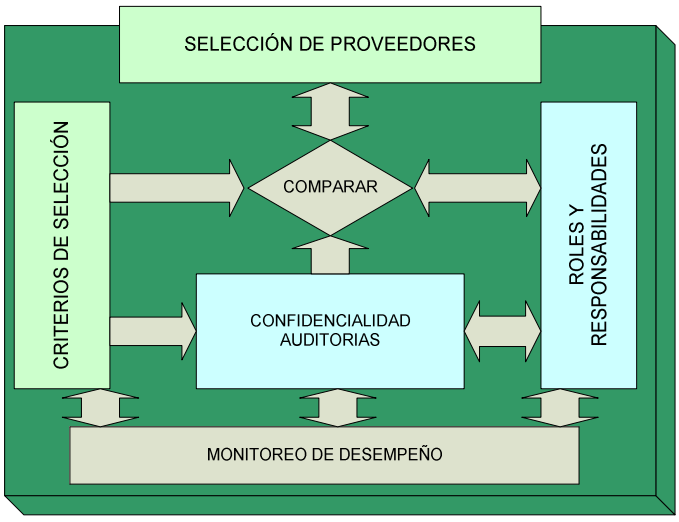
Fuente:autores

Debe existir un marco de trabajo que permita definir el nivel de protección necesario para los datos, basado en su aspecto critico. Para esto:

a. Se debe establecer una política de clasificación de información, esto definirá quien es el propietario de datos e información critica en el proceso de voto electrónico.
b. Implementar un marco de trabajo que clasifique los datos e información basado en su criticidad (confidencial, interna, publica etc.). Este marco de trabajo debe tener definiciones especificas para cada nivel de clasificación con requisitos específicos de cómo cada información y dato deben ser protegido (encriptado, etc)
c. Creación de un ciclo de vida de la información que incluya requerimientos de retención, archivo y destrucción, donde se identifique el tiempo en el que el dato estará activo (online, fácilmente accesible, modificable, back up etc), cuándo y por cuánto tiempo puede ser archivado y cuando debería ser destruido.

3. **Diseñar, revisar y evaluar procesos para gestión de servicios, productos y subprocesos de terceras partes involucrados en el voto electrónico, asegurándose que sus roles y responsabilidades estén bien definidas y acompañadas de un monitoreo de desempeño.**

Figura 36:Gestión de contratación externa



Fuente:Autor

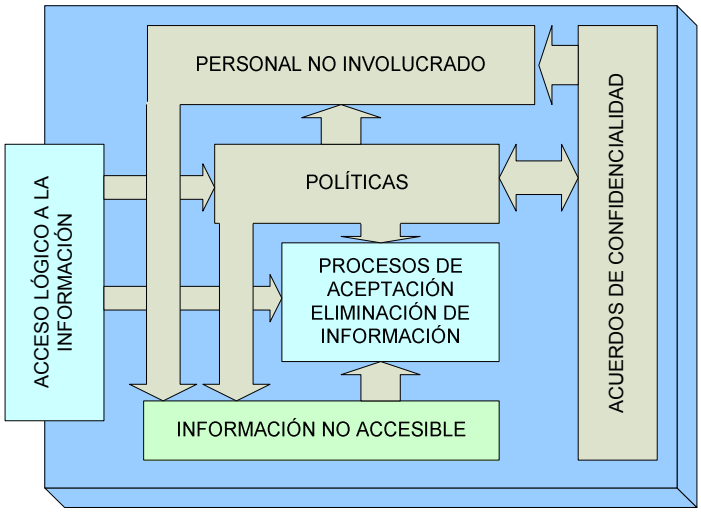
Para realizar el proceso electoral, la Registraduría Nacional evalúa y selecciona propuestas presentadas por proveedores externos que serán los encargados de realizar las diferentes etapas. Para el proceso de voto electrónico también se realizarían

licitaciones para escoger los proveedores que mejor cumplan con los requisitos impuestos por la Registraduría y en general por la Comisión Nacional Electoral . Estos proveedores deberán ajustarse a sistemas de gestión de la calidad y seguridad para garantizar que el proceso de realiza adecuadamente. Para esto se debe:

a. Diseñar y revisar el proceso de selección de proveedores de tecnología incluyendo aquellos relativos a las máquinas de votación electrónica.
b. Comparar cada proveedor participante contra unos criterios definidos incluyendo personal y entidades con conocimiento sobre el tema que ayuden en la negociación del contrato, teniendo en cuenta una investigación acerca de calificaciones atribuibles al proveedor y su estado financiero.
c. Asegurar que los contratos con terceras partes definen los roles y responsabilidades de los mismos y que están incluidos en los acuerdo de nivel de servicios (SLA-Service Level Agreement).
d. Realizar acuerdos de confidencialidad y clausulas de derecho a auditorias de las actividades que son críticas para el proceso de voto electrónico.
e. Establecer procesos de monitoreo de desempeño de los proveedores para tener la visión de los servicios ofrecidos por los mismos.

4. **Diseñar, revisar y evaluar procesos para el control del acceso lógico a información por parte de personal no involucrado en el proceso de voto electrónico.**

Figura 37:Control de Acceso a la información.



Fuente:Autor

En el caso de terceras partes o personal no vinculado al desarrollo del proceso de voto electrónico y deban tener acceso lógico a información del proceso electoral como observadores o elementos de soporte, deben estar gobernados y controlados de manera que los activos e información confidencial no pueda ser expuesta ni alterada.

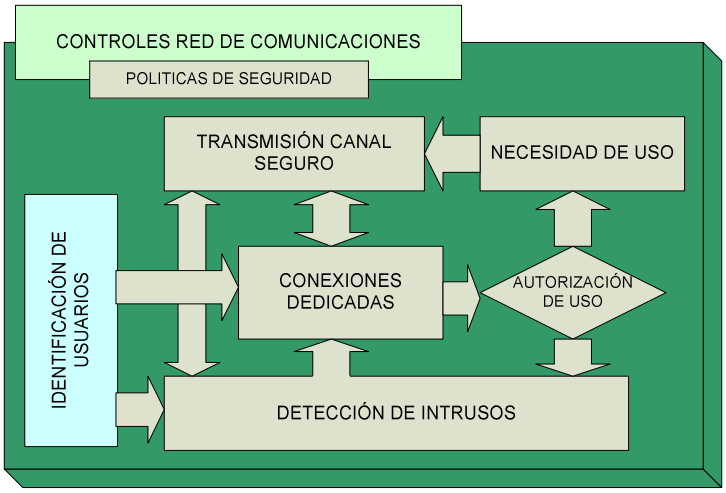
a. Se debe asegurar que las políticas sean explícitas respecto al acceso lógico a información del sistema por parte de personal no empleado en el proceso de voto electrónico.
b. Se debe diseñar procedimientos de comunicación de las políticas (incluyendo las políticas de seguridad) del voto electrónico, a personas ajenas al proceso y que deseen tener acceso lógico a información crítica. Estas personas deben firmar un documento que constate que conocen las políticas, están de acuerdo con ellas y las cumplirán.
c. Se debe asegurar el uso de acuerdos de confidencialidad firmados por los no empleados en el proceso de voto electrónico que permitan proteger legalmente el uso inapropiado de los datos e información del proceso electoral y el voto electrónico.

5. Se debe asegurar que el proceso de voto electrónico cumple con el uso de software legal

Se debe contar con un listado de las licencias de software utilizadas por los involucrados en el voto electrónico y debe desarrollarse un proceso del uso de las mismas de manera tal que cumpla con los términos acordados.

6. **Diseñar, revisar y evaluar controles sobre la red y acceso remoto del proceso de voto electrónico**

Figura 38:Controles de acceso a la red



Fuente:Autor

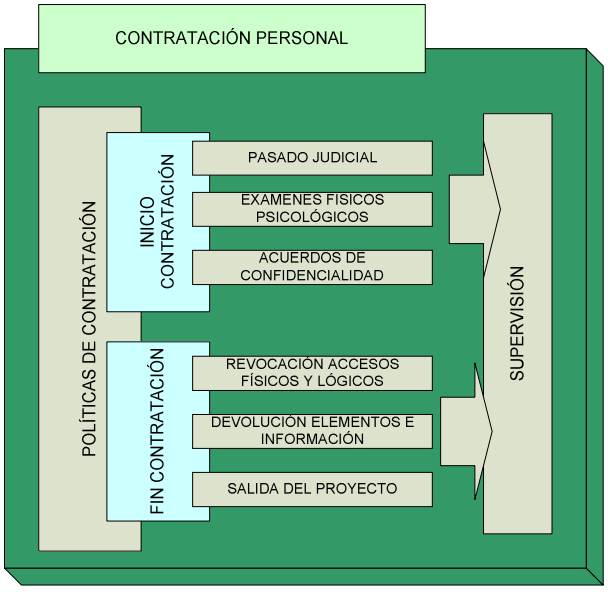
Habilitar el acceso remoto la red de transmisión hace que la red se extienda más allá de los límites establecidos en su diseño para la transmisión de datos del voto electrónico, pasando los controles de perímetro normales (firewalls). Es indispensable crear controles de acceso bastantes r obustos, para prevenir el ingreso no autorizado y ataques a la red. .

a. Asegurar que los usuarios se identifiquen (passwords) para el acceso remoto y que estas credenciales sean transmitidas sobre canales de comunicación seguras (VPN).
b. Establecer controles que aseguren que conexiones externas dedicadas y sean removidas cuando no son utilizadas.
c. Crear controles que aseguren que dispositivos o módems no autorizados o puntos de conexión como VPN's no puedan ser usados en la red y que existan mecanismos de detección de los mismos.

d. Asegurar que todos los dispositivos que accedan remotamente la red cumplan con requerimientos mínimos de seguridad de acuerdo a las políticas.
e. Controlar que los dispositivos que accedan la red de voto electrónico no permitan “puentear” a otras redes.

7. **Crear procedimientos de inicio y de cierre de contratación de personal involucrado en el voto electrónico.**

Figura 39:Políticas de contratación.



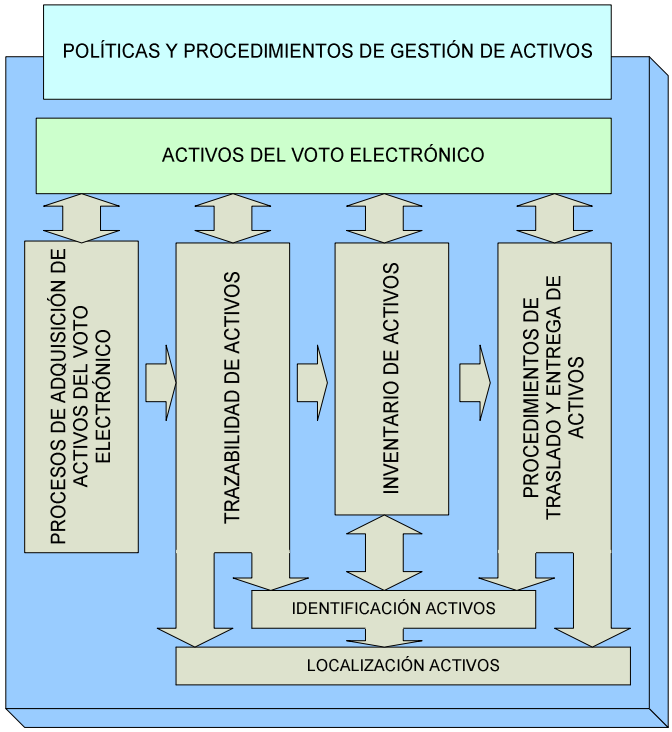
Fuente:Autor

Antes de iniciar labores en el proceso de voto electrónico todo el personal contratado debe pasar por un proceso de contratación que permita valorar su calidad humana, experiencia y conocimiento. Los procedimientos de terminación de contrato son importantes ya que permiten asegurar que el acceso a los activos de información se restringe a los empleados actuales.

a. Los procesos de contratación podrían incluir revisiones al pasado judicial, chequeos de consumos de drogas y acuerdos de confidencialidad.
b. Los procesos de terminación del contrato deben incluir la eliminación de accesos fisicos y logicos de la información del voto electronico, devolución de los equipos utilizados, y supervisión de la salida del personal del proyecto.

8. **Diseñar, revisar y evaluar políticas de uso y traslado de hardware utilizado en el proceso de voto electrónico.**

Figura 40:Políticas de tratamientos de activos.



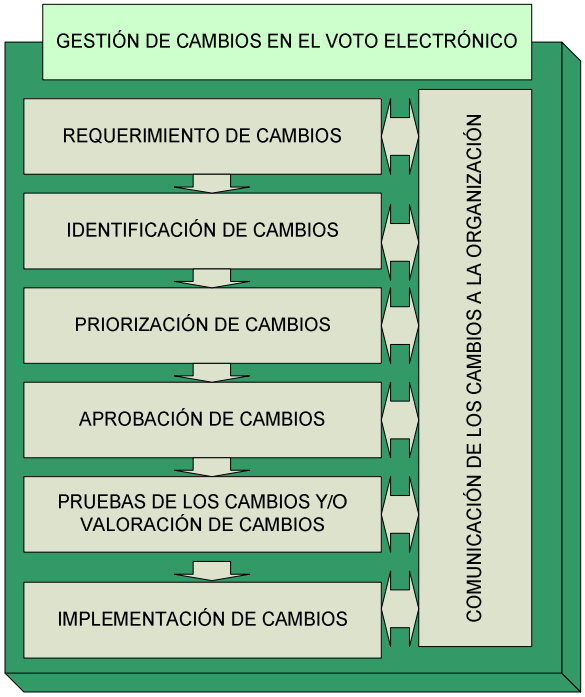
Fuente:Autor

El control, trazabilidad y reporte de los activos son parte importante en el desarrollo de los procesos del voto electrónico porque evitan la pérdida de hardware. Se deben diseñar, revisar y evaluar políticas y procedimientos de gestión de activos teniendo en cuenta las siguientes características:

i. Procesos de adquisición de activos. Estos procesos deben ser aprobados antes de la adquisición de los activos.
ii. Trazabilidad de activos. Se debe asegurar el uso de indicadores de los activos y de una base de datos de su gestión.
iii. Inventario de los equipos. Crear un inventario con el número de cada activo y su localización.
iv. Crear procedimientos de traslado y entrega de activos. Se debe asegurar que los datos en los equipos on totalmente eliminados antes de su entrega.

9. **Asegurar que la configuración de máquinas de votación electrónica y los sistemas empleados en el proceso de voto electrónico son controlados a través de la gestión de cambios para evitar fallas de funcionamiento durante las etapas críticas del proceso.**

Figura 41:Gestión de cambios.



Fuente:Autor

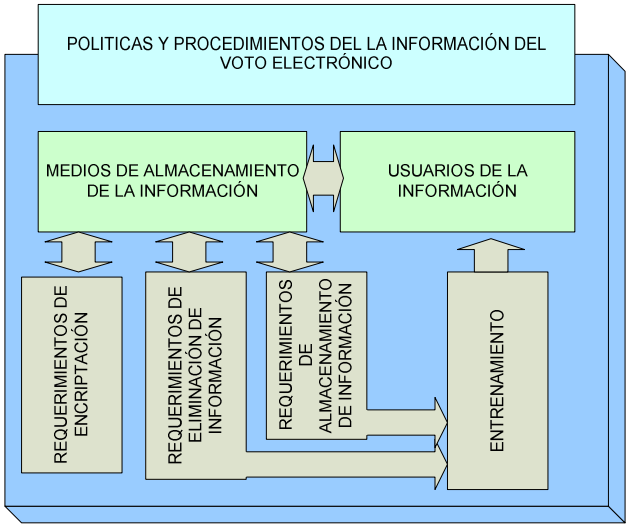
La gestión de cambios asegura que los cambios realizados al sistema de voto electrónico son controlados y traceables con el fin de reducir riesgos que origen mal funcionamiento del sistema. Esto incluye planeación, tiempos y fechas, aplicación y trazabilidad de los cambios realizados al sistema. Los cambios pueden estar asociado a dos áreas: Hardware y Software, se debe asegurar que los procesos de gestión de configuración tenga en cuenta los siguientes puntos.

a. Requerimiento de cambios incluyendo cambios teniendo en cuenta la opinión del ciudadano.
b. Determinación especifica de lo que se debe cambiar
c. Priorización y aprobación de cambios propuestos
d. Calendario de los cambios aprobados

e. Pruebas y aprobación de cambios antes de su implementación
f. Planeación de comunicación de los cambios antes de su implementación
g. Implementación de cambios

10. Se debe asegurar que todos los medios de transporte, almacenaje y entrega de información utilizada en el proceso de voto electrónico son direccionados de acuerdo a las politicas y procedimientos de la organización electoral.

Figura 42:Políticas del manejo de la información.



Fuente:Autor

Se debe asegurar que la información almacenada se conserve confidencial y protegida de deterioro, pérdida o destrucción no apropiada y prematura. Todos los medios de almacenaje y registro de información de importancia para el proceso de voto electrónico como CD's, DVD's, discos duros, máquinas de votación, USB, memorias flash etc, deben ser controladas con el fin de asegurar la privacidad de los datos.

a. Se deben asegurar políticas y procedimiento del uso y no uso de los medios de almacenamiento y registro de información teniendo en cuenta los siguientes puntos:

i. Deben existir requerimientos de encriptación de información sensible antes que esta sea transportada por una tercera parte en el proceso de voto electrónico
ii. Elaborar requerimientos de deformación, trituración, corte o eliminación de información en los medios magnéticos, ópticos que son reutilizados o desechados.
iii. Debe instruirse al recurso humano del proceso electoral acerca del uso y eliminación de medios de almacenaje.

5.2 CONTROLES DE NIVEL TÁCTICO Y OPERATIVO

Establecer los proveedores a participar

- Realizar acuerdos de no corrupción de cada uno de los proveedores participantes en el proceso, teniendo en cuenta sus efectos legales.
- Realizar acuerdos de ética con cada uno de los proveedores participantes, teniendo en cuenta sus efectos legales.
- Realizar acuerdos de no corrupción de cada uno de los proveedores participante en el proceso, teniendo en cuenta sus efectos legales
- Realizar acuerdos de confidencialidad con cada uno de los proveedores respecto a la información relacionada con proceso de voto electrónico
- Desagregar las funciones críticas con cada proveedor respecto a las tareas y actividades que deben desempeñar.
- Diseñar un sistema de control de acceso a personal autorizado con cada proveedor donde se incluyan solo el mínimo de personas necesarias y sus respectivos datos, en cada uno de los lugares críticos en el voto electrónico.
- Debe existir un registro donde cada proveedor liste las personas relacionadas bajo su mando que operarán en el proceso de voto electrónico y los datos de cada uno de ellos.

Establecer la seguridad física de los lugares de votación

- Debe existir presencia del personal oficial de seguridad en los diferentes sitios de votación
- Debe existir control de acceso a los diferentes sitios de votación electrónica
- Diseñar un sistema de control de acceso a personal autorizado en las etapas críticas donde se incluyan solo el mínimo de personas necesarias y sus respectivos datos, en cada uno de los lugares críticos en el voto electrónico
- Debe existir un registro donde cada proveedor u organización liste las personas relacionadas bajo su mando que operarán en el proceso de voto electrónico y los datos de cada uno de ellos
- Establecer vigilancia en los lugares designados para el bodegaje de materiales y/o equipos relativos al voto electrónico.
- Cada evento que esté relacionado con las funciones críticas del voto electrónico debe estar registrado en una bitácora que permita dar seguimiento y control a las diferentes actividades.
- Se deben realizar simulacros que establezcan el funcionamiento de las medidas de seguridad aquí establecidas.
- Debe existir clasificación de la información relativa al voto electrónico en multiniveles que permitan definir si es pública, confidencial o secreta.
- Debe existir un diseño del proceso “in situ” de la votación de tal manera que coexista un orden de entrada-proceso-salida en cada espacio asignado.
- Debe existir un control y registro de las personas autorizadas para manipular equipos y/o máquinas de votación con cada una de los actores involucrados teniendo en cuenta el mantenimiento, asistencia técnica o contingencia de los mismos en cada sitio relativo al voto electrónico.
- Se debe asegurar que solo el personal autorizado para operar en el proceso se encuentra en cada lugar relativo al voto electrónico

- Las máquinas y/o equipos del voto electrónico deben tener medidas que restrinjan el acceso físico por personal no autorizado.
- Las máquinas y/o equipos de votación electrónica deben tener medidas que restrinjan el acceso lógico a las aplicaciones por personal no autorizado.

Recibo de equipos de votación electrónica

- El recibo de los equipos de votación electrónica deben estar enmarcados bajo los acuerdos de confidencialidad establecidos
- Se deben establecer niveles de servicio con las organizaciones que transportan equipos, máquinas y materiales referentes al voto electrónico
- Se deben establecer rutas alternativas de contingencia para el transporte de equipos, máquinas y materiales referentes al voto electrónico
- En el recibo de equipos, máquinas y materiales referentes al voto electrónico debe realizarse un chequeo de las misma (a través de una muestra, o en su totalidad) de manera que permita verificar y validar el buen estado de las mismas.
- Se debe definir un cronograma detallado que permita validar los tiempos de recibo de las máquinas de votación, y debe existir un tiempo de tolerancia que permita recurrir a nuevas estrategias de transporte para el recibo de los equipos, máquinas y materiales.
- Definir un tiempo prudencial para la importación de los equipos, máquinas y materiales referentes al voto electrónico de manera tal que estos sean recibidos dentro de las fechas que el cronograma de actividades establezca.

Chequeo de las máquinas de votación y consolidación

- El chequeo de las máquinas de votación y consolidación debe efectuarse en el marco de los acuerdos de confidencialidad establecidos
- Cualquier evento relacionado con las máquinas de votación y consolidación debe estar relacionado en un registro o bitácora y debe efectuarse un chequeo de las mismas en cada etapa
- Cualquier retraso en el transporte de las máquinas debe estar justificado por su custodio y siempre debe existir una verificación y validación de su buen estado
- La manipulación de máquinas de votación y consolidación debe ser realizado solo por personal autorizado y debe realizarse a puerta cerrada en los tiempos en los que es permitido realizar cambios
- Las máquinas de votación y consolidación deben tener registros de las diferentes pruebas realizadas a las misma con firmas de los responsables sobre dichas pruebas
- En el registro de pruebas debe establecerse el visto bueno de los componentes de hardware y software establecidos por la organización electoral
- Las máquinas de votación y consolidación deben tener interfaces externas deshabilitadas y no deben estar expuestas.
- Se deben identificar las interfaces de las maquinas de votación y consolidación que deben operar y aquellas inoperantes que deben estar deshabilitadas
- Las máquinas de votación y consolidación deben ser compactas de tal manera que el acceso a los componentes al hardware sea difícil y deben existir sistemas de trazabilidad
- Las máquinas de votación y consolidación deben tener mecanismos de control de acceso respecto a su manipulación lógica o de software y deben existir mecanismos de trazabilidad (logs)
- Debe existir un control de cambios respecto a cada evento relacionado con las máquinas de votación y consolidación relacionando el responsable, la causa y consecuencia del cambio.

Establecer condiciones eléctricas de sitios de votación

- Los lugares de votación y consolidación deben estar reglamentados de manera tal que exista energía eléctrica para el funcionamiento de los diferentes componentes
- Deben existir mecanismos de regulación de energía eléctrica en los sitios relativos a la votación de tal manera que disminuyan la probabilidad de daños causados por mala calidad de energía.
- Deben existir fuentes de contingencia de energía como UPS, o plantas generadoras de energía que permitan ofrecer continuidad al proceso

Establecer condiciones de comunicaciones de los lugares de votación

- Se deben establecer los medios de comunicación de las máquinas de votación con anterioridad en cada uno de los lugares referentes al voto electrónico
- Se deben realizar pruebas que permitan establecer el buen funcionamiento de las comunicaciones en el voto electrónico antes de la realización del proceso
- Se deben establecer con anterioridad, teniendo en cuenta la tecnología de votación electrónica a utilizar, los protocolos utilizados y su compatibilidad con los diferentes componentes.
- Se debe establecer el cronograma de puesta a punto de la red de comunicaciones e incluir un tiempo de tolerancia que permita incluir sistemas de transmisión redundantes y contingentes para la transmisión de datos
- Se deben establecer niveles de servicio con el proveedor de comunicaciones teniendo en cuenta los índices de disponibilidad, eficiencia y eficacia
- Se deben diseñar sistemas de contingencia de los canales de transmisión

Número de maquinas de votación a utilizar

- Se debe tener en cuenta tiempos de votación de las máquinas de votación para realizar el estudio de número de ciudadanos potenciales votantes que puede una máquina de votación soportar en el tiempo requerido para el proceso de votación
- Se deben realizar un estudio que permita definir el número de máquinas de contingencia a utilizar por lugar de votación
- Se debe tener plena seguridad de que las máquinas de votación que se encuentran destinadas a la votación electrónica y su contingencia han sido probadas y certificadas
- Se deben realizar acuerdos de servicio con transportadores de las máquinas de votación donde se especifique las condiciones mínimas para su transporte
- Debe asegurarse que en cada sitio de votación solo existe un número de máquinas establecido con anterioridad, incluyendo las contingencias
- Debe tenerse un registro del número de máquinas establecido por lugar de votación y el responsable o custodio de las mismas

Establecer las fechas de desarrollo del proyecto

- Se debe definir un cronograma de tallado de actividades y tareas, que incluya roles y responsabilidades de cada uno de los actores involucrados en el voto electrónico
- Deben realizarse las firmas de compromiso de participación de proveedores, y actores relacionados en el voto electrónico donde se describa explícitamente su responsabilidad frente el proceso de voto electrónico en los tiempos designado en el cronograma de actividades
- Se debe incluir en el cronograma de actividades los tiempos de tolerancia a fallos en el sistema de voto electrónico, incluyendo fallas en la transporte, importación, diseño de políticas alineación estratégica, puesta a punto y pruebas.

- Cualquier cambio en el cronograma de actividades debe estar realizado bajo un control y seguimiento y con la aprobación de la organización electoral.
- Debe existir un versionamiento de los cambios efectuados al cronograma de actividades

Contratación de personal

- Toda contratación de personal debe ser efectuada bajo el marco de confidencialidad establecido con anterioridad en el proceso de voto electrónico.
- Deben establecerse sistemas de control de acceso físicos y lógicos a los lugares relativos al voto electrónico sobre el personal vinculado al proceso, de tal manera que solo estos tengan permisos para operar en los puntos críticos del proceso.
- Se debe clasificar la información relativa al voto electrónico en capas multinivel y se deben asignar los custodios responsables sobre la misma.
- Al contratar el personal se deben tener medidas de seguridad incluyendo revisión del pasado judicial y referencias.
- Debe asegurarse que cada uno de los participantes involucrados en el desarrollo del voto electrónico han sido registrados con los datos que se consideren necesarios.
- Se debe tener una lista de personal de contingencia que permita reemplazar la ausencia de los actores involucrados en voto electrónico bajo diferentes formas.

Transmisión de datos

- Los equipos de comunicaciones empleados en la transmisión de datos deben haber sido probados y certificados para su operación en el proceso del voto electrónico

- Se debe asegurar que los equipos de transmisión de datos permitan ser compatibles con las especificaciones de las tecnologías de votación electrónica empleadas
- Se debe asegurar que los equipos de transmisión de datos cumplen y operan bajo los protocolos de comunicación establecidos por las tecnologías de votación electrónica
- Se debe cumplir a cabalidad el cronograma establecido para la puesta a punto de la red de comunicaciones
- Se deben realizar pruebas de comunicación con anterioridad para verificar y validar el funcionamiento del sistema
- Se deben tener conectividad alterna o de contingencia respecto a la transmisión de datos
- Se deben establecer los acuerdos de nivel de servicio que permitan verificar la disponibilidad, eficiencia y eficacia de los medios de transmisión de datos

Servidores de Consolidación

- Se deben realizar pruebas en los servidores de consolidación con el tiempo suficiente de tal manera que se puedan realizar cambios en el software sin interrumpir el normal desarrollo del proceso
- Se deben realizar pruebas en los servidores de consolidación que incluyan los equipos de comunicaciones y la transmisión de datos.
- Se deben tener equipos de consolidación de contingencia ante el mal funcionamiento de los mismos.
- En el mejor de los casos las contingencias de los equipos de consolidación deben estar en alta disponibilidad

Back-up de información relativa al voto electrónico

- Se debe clasificar la información en capas multinivel asignando un custodio de la misma con sus respectivas responsabilidades.
- La información clasificada como crítica debe ser almacenada y se debe realizar un “back-up” de la misma.

- Se debe tener redundancia y contingencia para el envío de información desde los diferentes lugares de votación y en el centro de consolidación
- Se debe establecer un plan de comunicaciones que permita el flujo de información de control y seguimiento del proyecto de una manera adecuada.
- Además de la información transmitida a consolidación, se deben tener verificar y validar los registros en memorias individuales de cada una de las máquinas de votación.
-

Método de autenticación

- Debe establecerse un sistema de control de acceso a la etapa de autenticación del proceso.
- Los métodos de autenticación empleados deben ser probados, verificados, validados y certificados por la organización electoral.
- Los equipos de autenticación empleados deben tener un custodio o responsable sobre la operación y buen funcionamiento del mismo.
- Los equipos utilizados en la etapa de autenticación deben realizar solo las funciones establecidas por la organización electoral.
- Los equipos deben tener habilitadas solo las interfaces necesarias para su correcta operación.
- Los equipos utilizados en la etapa de autenticación deben tener control de acceso lógico para su operación y debe tener un sistema de trazabilidad de los eventos realizados en el mismo.
- Deben ser operados solo por personal autorizado para ello.

Control de actividades

- La información debe ser clasificada en capas multinivel para la ejecución de cada una de las actividades de los actores involucrados en el voto electrónico

- En la firma de compromiso por parte de los proveedores se debe hacer énfasis en la responsabilidad sobre cada una de las actividades que deben ejecutar
- El cronograma de actividades debe incluir tiempos de tolerancia y su control ante retrasos originados por los proveedores encargados del transporte de máquinas, equipo y materiales del voto electrónico.
- Todo cambio debe ser registrado y debe ser incluido en el sistema de control de actividades planificado en el plan de gestión.
- El control de actividades debe llevar registro del mal funcionamiento de las máquinas y del accionar de las contingencias establecidas.

Autenticación

- Debe existir presencia de personal de seguridad que mitigue las incidencias de personal violento en los lugares de votación
- Las personas o custodios de la etapa de autenticación deben estar soportadas por personal contingente que cumpla con los mismos requerimientos y que han sido entrenados para operar de la misma manera en el proceso

Entrenamiento al ciudadano

- El entrenamiento del ciudadano debe verificar y validar que este comprende el modo de votación y debe responder ante cualquier inquietud del votante
- El entrenamiento al ciudadano debe efectuarse en el mejor de los casos con una máquina de votación igual y en las mismas condiciones que una máquina de votación oficial

Votación

- El proceso de votación debe realizarse en un espacio aislado garantizando anonimidad del sufragio
- El proceso de votación es responsabilidad únicamente del elector que ya ha sido entrenado anteriormente
- Debe existir personal técnico que soporte las fallas presentadas en las máquinas de votación.
- El software de aplicación de las máquinas de votación debe haber sido probado, verificado y validado

Consolidación

- Deben existir pruebas del proceso de consolidación incluyendo los equipos de telecomunicaciones que permitan detectar acciones de mejora al proceso.
- El proceso de consolidación debe minimizar los efectos de interrupción del servicio por fallas eléctricas.
- Se deben tener contingencias para los equipos involucrados en la consolidación del proceso.
- Debe existir personal de soporte al proceso de consolidación que mitigue las fallas causada por ausencia de personal de operación.
- La configuración de los equipos de consolidación deben haber sido probados, verificados, validados y certificados por la organización electoral.
- El proveedor custodio de la consolidación debe seguir al detalle la especificación de cálculo de consolidación establecido por la organización electoral.

Especificación del sistema

- Todo cambio por parte de la organización electoral al contrato debe ser registrado y seguido con control de cambios.
- La especificación del sistema se diseña teniendo en cuenta las limitaciones declaradas por cada uno de los participantes

- La información sobre la especificación del sistema solo debe ser entregada a los proveedores que han firmado el acuerdo de participación en el proyecto
- El modelo de votación debe estar incluido en la especificación del sistema y debe ser aprobado por la organización electoral
- El sistema de cálculo de resultados debe ser aprobado por la organización electoral y todo cambio realizado al mismo debe ser registrado con los datos de causa, responsable y consecuencia

Auditorias

- Debe existir presencia de auditores que observen el desarrollo del proceso del voto electrónico
- El auditor debe establecer especial énfasis en el comportamiento de los actores involucrados en el proceso como proveedores, jurados, personal de soporte.
- La auditoria debe estar incluida dentro de las políticas diseñadas para el voto electrónico
- La auditoría debe tener registro de las personas que se encuentran operando el proceso del voto electrónico en sitio
- La auditoría debe ser entrenada con anterioridad sobre el diseño del proceso, el análisis de puntos críticos y medidas a tener en cuenta en la observación

Educación al ciudadano y/o votante

- Los ciudadanos deben ser entrenados en el uso de nuevas tecnologías de votación electrónica.
- El ciudadano debe estar informado sobre los posibles consecuencias legales de actos indebidos que interrumpan el proceso.
- El ciudadano debe entender que cualquier manipulación de equipos sin autorización está totalmente prohibida.

- El ciudadano debe ser informado y entender sobre el flujo del proceso de votación electrónica y los pasos a seguir.
- El ciudadano debe ser informado sobre las reglas establecidas para poder efectuar el sufragio.
- Debe existir medios y puestos de información al elector.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Los resultados de confiabilidad obtenidos a través de las pruebas con el modelo propuesto, dieron como resultado una no confiabilidad del proceso del 98%. Este resultado se ajusta a la realidad actual del voto electrónico en Colombia, ya que aun no existen procedimientos que regulen esta práctica y la ley existente no considera temas vitales como características del software de las máquinas de votación, deberes y derechos de proveedores de tecnologías de votación, el papel de la Registraduría y el Consejo Electoral en el escenario de votación electrónica, nivel de educación ciudadana para asumir el cambio, penalizaciones en casos de irregularidades en los sistemas electrónicos, etc. Este porcentaje muestra que aún hay mucho camino por recorrer en búsqueda de un proceso de votación electrónica confiable en Colombia.

- Los eventos que más aportan a la falta de confiabilidad del proceso son los relacionados a la gestión de los procesos, a la forma como las personas deben hacer su trabajo. Esto demuestra que la tecnología juega un papel importante en el proceso, pero si no es acompañada de buenas prácticas de gestión de procesos y de seguridad de la información, se podría perder toda la confianza ganada con las elecciones tradicionales y generar incertidumbre y desconfianza en las instituciones del gobierno.

- Los eventos relacionados a la falta de disponibilidad de materiales de auditoría al proceso, irregularidades en la autenticación del votante, manipulación de la intención de voto del elector, manipulación de resultados, altos niveles de abstencionismo y pérdida o robo de información son los más críticos en el proceso pues atentan directamente contra los objetivos del proceso electoral y la naturaleza del voto.

- La educación ciudadana juega un papel preponderante en la ejecución satisfactoria de la votación electrónica, pues garantiza la asistencia masiva de electores a las urnas y confianza en los resultados que se obtengan. Es

necesario reducir el analfabetismo digital para que la votación electrónica permee todos los niveles de la sociedad.

- Se espera que el modelo propuesto sea retomado para realizar análisis no solo de la instancia de votación, sino del todas la etapas que comprenden un proceso electoral. Para esto, se debe designar todo un equipo de trabajo que realice la identificación, valoración de los riesgos y modelado de los datos para concluir acerca del estado del proceso.
- Cada evento inicial identificado es un punto de medición en el sistema, para lo cual debe designarse personal adecuado para la toma de datos durante la ejecución del proceso.

6.2 RECOMENDACIONES

- Es necesario crear un debate político y social que clarifique las normas, desafíos y estrategias de cambio nacional para implementar procesos de votación electrónica.

- Se debe redefinir el concepto de voto electrónico adaptándolo a las tecnologías emergentes de votación electrónica.

- Se debe establecer un ente de gestión multidisciplinario encargado de la estandarización y certificación del proceso de votación electrónica para Colombia. Este aspecto es muy importante dado que la mayoría de los eventos iniciales causantes de riesgos se deben a la falta de creación y estandarización de procesos ajustados a la votación electrónica

- Es importante recalcar que el modelo obtenido no es estático, se irá refinando a medida que se puedan realizar más pruebas y obtener datos reales del proceso. Para esto es de suma importancia que el gobierno se concientice de la necesidad de la ejecución de más pruebas piloto.

- Determinar si existen mapas de ruta de tecnología y aplicaciones, además de evaluar procesos para planeación tecnológica a largo y mediano plazo.

- Diseñar y/o revisar medidas e indicadores de desempeño de los procesos de votación electrónica y de los procesos de modernización tecnológica. Asegurar que los procesos y métricas están relacionados para medir el desempeño de actividades y la trazabilidad del desarrollo de los objetivos del voto electrónico contra las necesidades del país y los requerimientos operacionales en los procesos electorales.

- La existencia de fenómenos como la brecha digital y el analfabetismo digital, demuestran la necesidad de una apertura de la sociedad a las nuevas tecnologías, así como la formación e información de todos los ciudadanos para el ejercicio democrático y el aprovechamiento de los mecanismos y escenarios surgidos por la democracia electrónica con el fin de optimizar su participación.

- Asegurarse que existen políticas de seguridad de la información y que estas cubren los requerimientos de seguridad del ambiente electoral. Determinar como estas políticas son comunicadas y como el cumplimiento es monitoreado y reforzado.

- Revisar y evaluar los procesos de valoración de riesgos para el voto electrónico y la organización electoral.

- Se deben diseñar, revisar y evaluar procesos para asegurar que los involucrados en el proceso de voto electrónico tengan la habilidad y conocimiento necesario para realizar sus actividades, tareas y trabajos.

- La implementación de proyectos de base tecnológica tan sensibles como los de votación electrónica requiere de la implementación de mecanismos que aseguren la calidad y gestión de los procesos y productos de la votación.

- Se deben asegurar mecanismos de administración del proceso electoral electrónico que garanticen la continuidad del servicio y recuperación de desastres basado en la gestión de riegos.

- Revisar la estructura organizacional general del voto electrónico y asegurar que existe una autoridad y responsabilidad sobre las operaciones y actividades y que estas están segregadas en tareas específicas.

CAPITULO VII: BIBLIOGRAFÍA

1. Acevedo L. Andrea, Martinez A. Hugo, Pachón F. Carlos, Herrera Herly J. 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. Informe Preliminar: www.mininterior.gov.ar/elecciones/archivos_doc_pdf/InformePreliminar14abr05.pdf. 2005 Electronic Voting Pilot, Buenos Aires-Argentina. Fecha de última consulta: Julio 10 de 2008.
3. http://www.observatorioelectoral.org/informes/analisis/. Página Web. Fecha de última consulta: Julio 10 de 2008.
4. http://www.votobit.org/. Página Web. Fecha de última consulta: Julio 10 de 2008.
5. http://www.votingtechnologyproject.org/index.html. Página web Fecha de última consulta: Julio 10 de 2008.
6. http://www.notablesoftware.com/Papers/CACM1102.html. "Florida 2002: Sluggish Systems, Vanishing Votes". Working paper. Fecha de última consulta: Julio 10 de 2008.
7. http://www.j-dom.org/h/n/WRITING/evoting/ALL///. "May 2007 Election Report: Findings of the Open Rights Group, Election Observation Mission in Scotland and England". Reporte final. Fecha de última consulta: Julio 10 de 2008.
8. www.votoelectronico.es/Archivos/PruebaArgentina/ExperienciasInternacionalesPruebaPilotodeVotoElectronico.pdf. Fecha de última consulta: Julio 10 de 2008.
9. Lauer, Thomas W. "The Risk of e-Voting". Electronic Journal of E-Government, Volume 2, Issue 3, 2004(177-186). School of Bussiness Administration, Oackland University, Rochester, USA.
10. Stamatelatos, Michael, et al. "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners". Office of Safety and Mission Assurance, Nasa Headquarters. Manual de procedimientos. Washington D.C. Agosto de 2002.
11. Kumamoto, Hiromitsu. Henley, Ernest. "Probabilistic Risk Assessment and Management for Engineers and Scientists". Second Edition. ISBN 0-7803-6017-6.IEEE Reliability Society- IEEE PRESS. New York, EE.UU. 1996.
12. W. E. Vesely, F. F. Goldberg, N. H. Roberts, D. F. Haasl. "Fault Tree Handbook". U.S Nuclear Regulatory Commission. Nureg-0492. Washington D.C. 1992.
13. BS ISO/IEC 27001:2005. Information Technology-Security Techniques-Information Security Management Systems-Requirements. British Standars. Versión Electrónica. 18 de Octubre de 2005.
14. "Systems Security Engineering Capability Maturity Model". SSE-CMM. Versión 3.0. Carnegie Mellon University. Junio 15 de 2003. http://www.sei.cmu.edu/.
15. CobIT 4.1. IT Governance Institute. ISBN 1-933282-72-2. United States. 2007. www.isaca.org
16. CobiT Mapping: Mapping of ITIL with CobIT 4.0. IT Governance Institute. ISBN 1-933284-77-3. United States. 2007. www.isaca.org
17. Enterprise Risk Management Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission-COSO. 2004. www.isaca.org
18. Association of Insurance and Risk Managers (AIRMIC), ALARM(National Forum for Risk Management in the Public Sector) and Institute of Risk Management(IRM), A risk Management Standard, Londres, 2002.
19. AS/NZ 4360:2004. Risk Management systems Standard. Australia and New Zealand. 2004.

20. Williams, Graham. “Management of Risks(M_o_R):The facts v1.0. Office of Government Commerce. U.K 2007.

21. ISO/TMB WG on Risk Management- Guidelines on Principles and Implementation of Risk Management. Junio de 2007.

22. Yang. Guangbin, “ Life Cycle Reliability Engineering” John Wiley and Sons, Inc, 2007, pág 13.

23. www.registraduria.gov.co/ Avances PMTII. Registraduría Nacional del Estado Civil.

24. “May 2007 Election Report. Findings of the Open Rights Group. Election Observation Mission in Scotland and England”. Open Right Group(www.openrightsgroup.org). 2007

25. http://www.un.org/es/documents/udhr/index.shtml#a20. Declaración Universal de los Derechos Humanos.

26. “Implicaciones de la adopción del voto electrónico en Colombia” Departamento Nacional de Planeación, Dirección de Justicia y Seguridad, Grupo de estudios de Gobierno y asuntos internos. Informe Final. Mayo 2003.

27. SafeVote-Internet Voting Requirements, The Bell, Vol. 1 No 7, p.3 Noviembre 2000. ISSN 1530-048X. Available at: http://www.thebell.net/archives/thebell1.7.pdf

28. “Voto Electrónico. Riesgos de una illusion.” Fundación Via libre(http://www.vialibre.org.ar) Fundación Heinrich Boll(http://www.boell-latinoamerica.org) ISBN 978-987-22486-5-9. 2008.

29. “Assessing the impact of voting technologies on multy-party electoral outcomes: the case of Buenos Aires’ 2005 Congressional Election”. Katz. Gabriel, Alvarez. Michael. Caltech/MIT-Voting Technology Project. Working Paper. Abril 2008.

30. “Are Americans confident their ballots are counted?”. Alvarez. Michael, Llewellyn. Morgan. Caltech/MIT-Voting Technology Project. Working Paper. Julio 2006.

31. “El voto electrónico en Colombia: Antecedentes, rasgos y factores de desconfianza”. Ibañez Parra, Oscar. XIII Congreso Internacional del CLAD sobre la reforma del estado y de la administración pública, Buenos Aires, Argentina,2008.

32. “Analysis of an Electronic voting System” Tadayoshi Kono, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach. IEEE Symposium on Security and Privacy 2004.

33. “Residual Votes Attributable to technology: An assessment of the reliability of existing voting technology” Caltech/MIT Voting Technology Project. Marzo 30, 2001.

34. “Threats to Voting Systems”. Jones. Douglas, University of Iowa. A position paper for the NIST workshop on threats to voting systems. Octubre 7 de 2005.

35. “A Better Ballot Box? New electronic voting systems pose risks as well as solutions” Rebeca Mercury. IEEE Spectrum. Octubre 2002.

36. “Implementación de Mecanismos de Votación Electrónica en Colombia”. Rebellón Rodríguez, Orus Andrés. Monografía para optar por el título de Politólogo. Facultad de Ciencias Políticas. Pontificia Universidad Javeriana. Bogotá, 2005.

37. “The Perils of Polling” Steven Cherry. IEEE Spectrum, Octubre 2004.

38. “Guía de democracia electrónica local: e-participación en la formulación de políticas públicas.” Convenio UNESCO – Primera edición, Bogotá, Agosto de 2005.

39. “La democracia electrónica: un análisis desde la teoría política”. García Guitián, Elena. VII Congreso Español de Ciencia Política y de la Administración. UAM. Madrid 2005.

40. “Del voto electrónico al voto telemático: clasificación y valoración de las propuestas existentes”. Gómez A. Cariacedo J. Departamento de Ingeniería y Arquitecturas Telemáticas. Universidad Politécnica de Madrid. Artículo presentado en VI Congreso AECPA, Barcelona 2003.

41. “Diseño de una plataforma de Democracia Digital”. Gómez A., Sánchez S. et all. Departamento de Ingeniería y Arquitecturas Telemáticas. Universidad Politécnica de Madrid. Junio 2005. Articulo disponible en www.votobit.org

42. “Plataformas telemáticas para la participación ciudadana municipal en países en desarrollo”. Prieto Martín, Pedro. Proyecto de Tesis de Doctorado. Universitat Oberta de Catalunya, Febrero 2005.

43. “El debate sobre la democracia electrónica como síntoma: hacia un replanteamiento del problema”. Conferencia Internacional sobre "La contribución de las Tecnologías de la Información y la Comunicación (TIC) a las instituciones representativas: e Democracia.” Universidad del País Vasco. Bilbao 2003.

44. IEEE Spectrum NA, “The next voting debacle?”. Agosto 2006.

45. Carina Perelli-DAE, Almabeatriz Rengifo-RNEC, Luis Alfonso Hoyos-ACCI, Alfredo Witschi-ONU, “Proyecto Integral para la Modernización del Sistema Electoral Colombiano”, Estudios base, Bogotá 2005.

46. Information Systems Audit and Control Association, *Control Objectives for Information and Related Technology*, 4.1: Edicion, 2007.

47. “Who does better with a Big Interface? Improving voting performance of reading for disbled voters”. Ted selker, Jonathan Goler, Lorin Wilde. MIT Research Laboratory of Electronics(VTP Working Paper). Febrero 2005.

48. http://www.fisterra.com/mbe/investiga/distr_normal/distr_normal.asp. Sitio web. Última revisión: Febrero 2009.

ANEXO A: NORMATIVIDAD DEL VOTO ELECTRÓNICO

El marco normativo referencial en Colombia, sobre el cual se sustenta y reglamenta el proyecto y la implementación del voto electrónico corresponde a la ley 892 de 2004 (Julio 7), que establece el mecanismo electrónico de votación e inscripción para los ciudadanos colombianos y en la cual se destacan:

Artículo 1º.- Establézcase el mecanismo electrónico de votación e inscripción para los ciudadanos colombianos.

Para tales efectos, la Organización Electoral diseñará y señalará los mecanismos necesarios para que el voto electrónico se realice con la misma eficacia para los invidentes, discapacitados o cualquier otro ciudadano con impedimentos físicos.

PARÁGRAFO 1º. - Se entenderá por mecanismo de votación electrónico aquel que sustituye las tarjetas electorales, por terminales electrónicos, que permitan identificar con claridad y precisión, en condiciones iguales a todos los partidos y movimientos políticos y a sus candidatos.

PARÁGRAFO 2º.- Las urnas serán reemplazadas por registros en base de datos, los dispositivos y las herramientas tecnológicas que garantizarán el voto deben organizarse en cubículos individuales separados donde el ejercicio electoral sea consolidado, de manera tal, que se cumplan las normas establecidas constitucionalmente. El sistema debe constar de los siguientes módulos: reconocimiento del votante, Intefax para escogencia electoral y comunicación con la central de control.

PARÁGRAFO 3º.- El sistema debe asegurar la aceptación de los tres tipos de cédulas existentes, en orden cronológico. De la primera cédula se tomará el número para alimentar la base de datos de los electores, de la segunda y tercera generación de cédulas se toma el código de barras por medio de censores láser o infrarrojos los cuales permitan reconocer dicho código y convertirlo en un registro para confrontarlos con la base de datos del sistema electoral. Cada entrada al sistema debe quedar registrada por el mismo.

PARÁGRAFO 4º.- Este mecanismo debe incluir, como requisito mínimo, la lectura automática del documento de identidad, captura de huellas dactiloscópica u otros

métodos de identificación idóneos que validen y garanticen la identidad de la persona al instante de sufragar.

PARÁGRAFO 5º.- Los electores podrán obtener el certificado electoral a través de una página web determinada por la Registraduría Nacional en la cual se publicarán las cédulas que efectivamente sufragaron. La Registraduría podrá determinar otros mecanismos para evitar la suplantación de la persona al momento del sufragio.

Artículo 2°. Para los ciudadanos colombianos domiciliados en el exterior la Organización Electoral implementará el mecanismo electrónico de inscripción y votación con la cobertura que facilite su participación en los comicios electorales.

Artículo 3°. La implementación del nuevo mecanismo se realizará antes de cinco años, sin embargo, la Organización Electoral deberá, en un plazo no mayor de seis meses, dar inicio a los planes pilotos de votación con el nuevo sistema.

PARÁGRAFO 1º. Dentro de la reglamentación se exigirá que el aplicativo o software y la base de datos posean el código fuente debidamente documentado, descartará los votos que presenten identificación y/o huellas repetidas, así como los votos sufragados en una circunscripción diferente a la inscrita cuando los candidatos sean de circunscripción territorial.

PARÁGRAFO 2º. El mecanismo electrónico de votación asegurará el secreto e inviolabilidad del voto.

Artículo transitorio 1º. La Organización Electoral permitirá la coexistencia del sistema convencional de votación en tarjetones de papel, mientras la infraestructura tecnológica de ciertos puntos de votación, no cumpla con los requerimientos mínimos del mecanismo automatizado de inscripción y votación.

Artículo transitorio 2º. Cuando los documentos de identificación no permitan su lectura automática esta se hará mediante la captura del número de identificación por digitación manual, siempre y cuando se verifique la identificación dactilar del ciudadano. El procedimiento anterior, regirá tanto para el proceso de inscripción, como el de votación.

Artículo 4°. Esta ley rige a partir de su sanción y promulgación.

ANEXO B: SISTEMAS DE INFERENCIA FUZZY

La inferencia fuzzy es un método que interpreta los valores de un vector de entrada basado en un grupo de reglas y asigna valores a un vector de salida. Por lo anterior, un sistema fuzzy de inferencia mapea un grupo de entradas y les asigna una salida y relaciona conceptos como funciones de membresía, operadores fuzzy y reglas if-then. Uno de los métodos de inferencia fuzzy más utilizados es el Mandani. Fue propuesto en 1975 por Ebrahim Mandani como un intento de controlar un motor a vapor sintetizando un grupo de reglas lingüísticas obtenidas de la experiencia de los operadores.

El método de inferencia fuzzy está compuesto de cinco etapas: Fuzzificación de las variables de entrada, aplicación de operadores fuzzy(And, Or) en el antecedente, Implicación del antecedente al consecuente, análisis del consecuente a la luz de las reglas y defuzzificación. A continuación se dará una breve descripción de cada una de las etapas.

1. **Fuzzificación de variables de entrada**

   En esta etapa se define el grado de de pertenecía de cada variable de entrada a cada grupo fuzzy a través de funciones de membresía. La entrada es un intervalo de valores o grupo 'crisp' y la salida es una función de membresía con valores entre cero y uno. En conclusión, en esta etapa se asignan valores numéricos a las variables lingüísticas obtenidas de la experiencia. Por ejemplo, si se tienen dos variables de entrada llamadas: Experiencia y Documentación, se definen valores numéricos para las características lingüísticas.

Característica	Valores		
Experiencia	Sin experiencia(0,0.35)	Poca experiencia (0.35, 0.7)	Bastante experiencia (0.7,1)
Documentación	Sin Documentación	Alguna Documentación	Adecuada Documentación

	(0,0.35)	(0,0.35)	(0,0.35)

2. **Aplicar el operador fuzzy**

   El operador fuzzy es aplicado a los valores de la función de membresía de las variables fuzzificadas. Si el antecedente de una regla tiene más de una parte, el operador debe ser aplicado para obtener un número que represente el antecedente de la regla, por ejemplo

   - Experiencia es bastante **OR** la documentación es adecuada
   - Experiencia es 0.9 **OR** documentación es 0.8 => 0.9

3. **Aplicación de método de implicación**

   El método de implicación es aplicado principalmente al consecuente o consecuencia, que en este caso del ejemplo seria: Guías de auditoría elaboradas correctamente. Este consecuente, también es un grupo fuzzy representado por una función de membresía la cual es modificada de acuerdo a una función asociada al antecedente. Entonces, la entrada a esta etapa es un número dado por el antecedente y la salida es un grupo fuzzy. El método se aplica a cada regla definida.

4. **Cómputo de todas las salidas**

   Luego del método de implicación, se obtienen varias salidas (dependiendo de la cantidad de reglas evaluadas). Estas salidas debe ser combinadas de cierta forma para tomar una decisión. La entrada a esta etapa son las funciones obtenidas del proceso de implicación aplicado a cada regla y la salida es un grupo fuzzy por cada variable de salida.

5. **Defuzzificación**

La función fuzzy obtenida en el cómputo de la salida es defuzzificada para obtener finalmente un número, en este caso entre cero y uno que representa la salida final del sistema fuzzy.

Los sistemas de inferencia fuzzy(FIS-Fuzzy Inference System) implementados en la presente investigación, se crearon en la toolbox de lógica fuzzy de matlab, que permite el uso de una interfaz gráfica para esta actividad, permitiendo realizar análisis de manera más rápida y eficiente.

A continuación se describen los sistemas de inferencia utilizados para el análisis de cada uno de los eventos iniciales(**EI**) identificados en el análisis de riesgos. Para cada evento se adjuntan imágenes de las reglas aplicadas, las funciones de salida obtenidas y una tabla con valores de algunos puntos de la función de salida.

Como fue descrito anteriormente, este tipo de inferencia fuzzy permite mapear variables léxicas obtenidas de la experiencia en una actividad en valores entre cero y uno(probabilidades) que permitirán el cálculo de la confiabilidad del sistema propuesto en el presente proyecto.

Todos los eventos fueron representados con funciones de distribución gaussianas principalmente por dos razones:

1. La campana de gauss es una función suve, es decir, no presenta ningún cambio drástico en ninguno de sus puntos.
2. Nunca toma el valor de cero. Esto implica que ninguno de los eventos iniciales considerados, tomaría cero como probabilidad de ocurrencia.

ASPECTOS IMPORTANTES :

- Algunos eventos se encuentran agrupados y representados por las mismas imágenes, esto es debido a que las variables que los afectan son básicamente las mismas y se pueden representar con las mismas funciones de membresía.
- En la figura de las reglas para cada evento se pueden observar las escalas asignadas a cada característica. En todos los casos, la salida puede tener una connotación positiva o negativa.

- En la tabla de valores para cada evento, se podrán observar los valores de salida y su valor negado.

Evento 1**: Contratación tardía de elaboración de guías.**

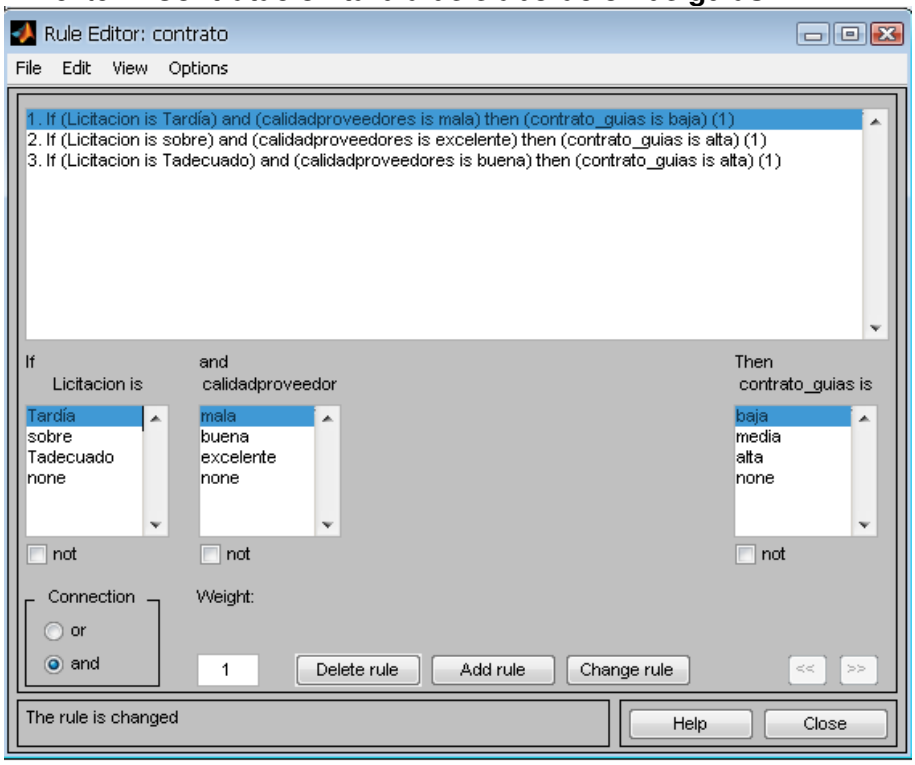


Figura B.1: Reglas para evento 1

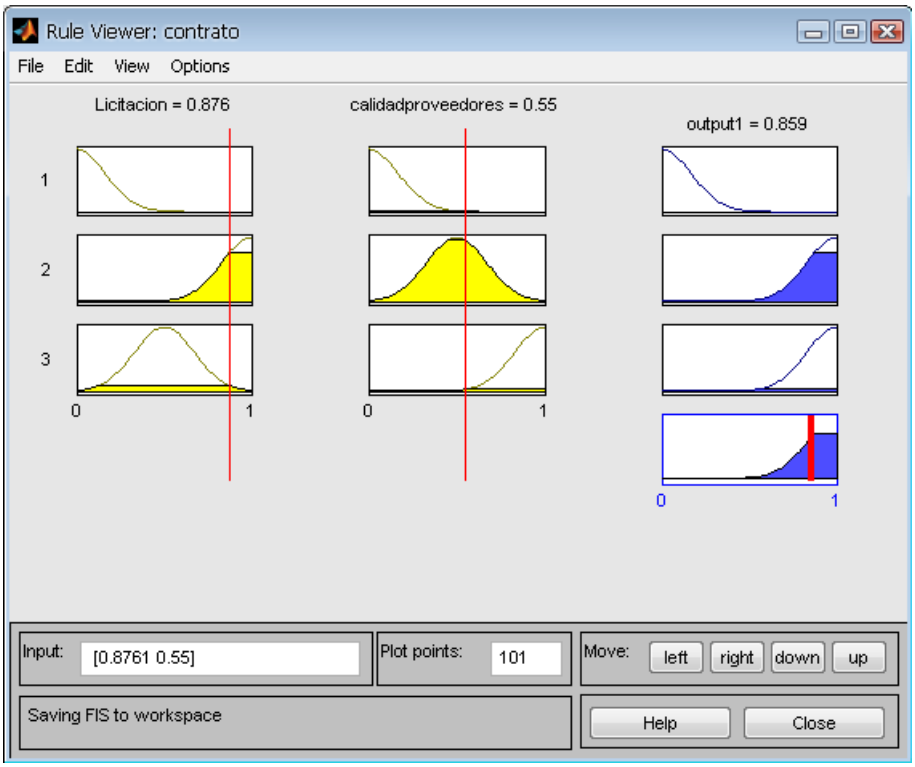


Figura B.2: Entradas y salidas del sistema

Licitación	Calidad Proveedores	Contratación	
0.95	0.832	0.795	0,205
0.876	0.55	0.859	0.141
0.619	0.495	0.769	0.231
0.142	0.268	0.181	0,819

Tabla B.1: Evento 1

Interpretación: En la medida en que la licitación se realice con suficiente tiempo y la calidad de propuestas de los proveedores sea buena, la probabilidad de que la contratación se realice a tiempo es alta, por lo tanto su evento negado, la probabilidad que no se realice a tiempo será baja y aumentará si la licitación no se realiza con el tiempo adecuado y las propuestas de proveedores no son las mejores.

Evento 2: **Demora en entrega de Guías por parte del proveedor**

Evento 3: **Poco conocimiento de procesos electorales electrónicos por parte de auditores y/o veedores.**

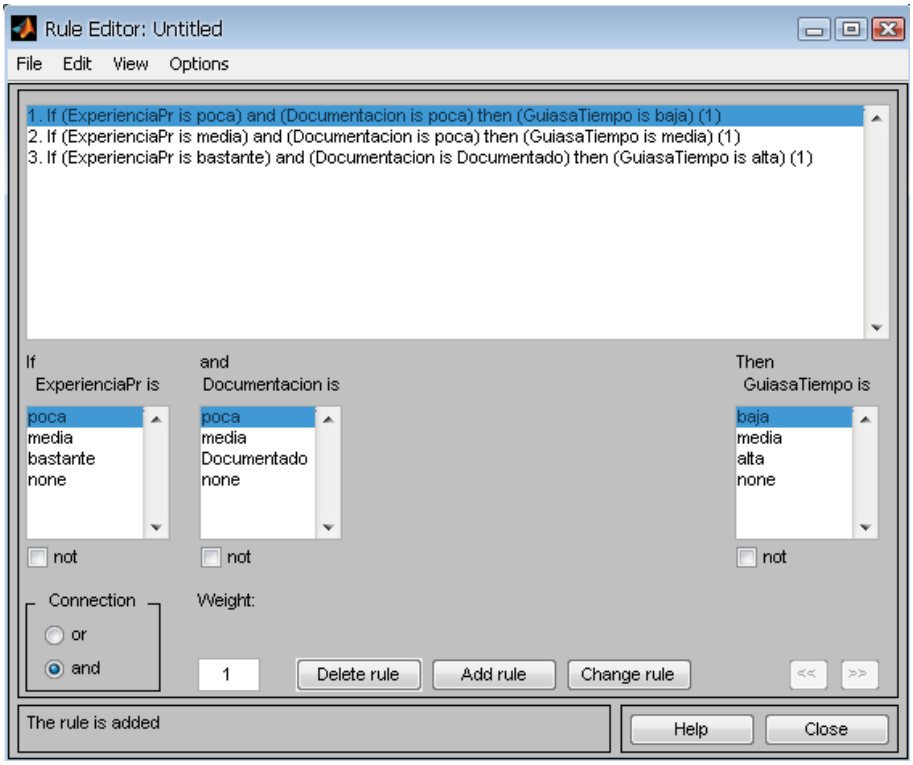


Figura B.3: Reglas para eventos 2 y 3

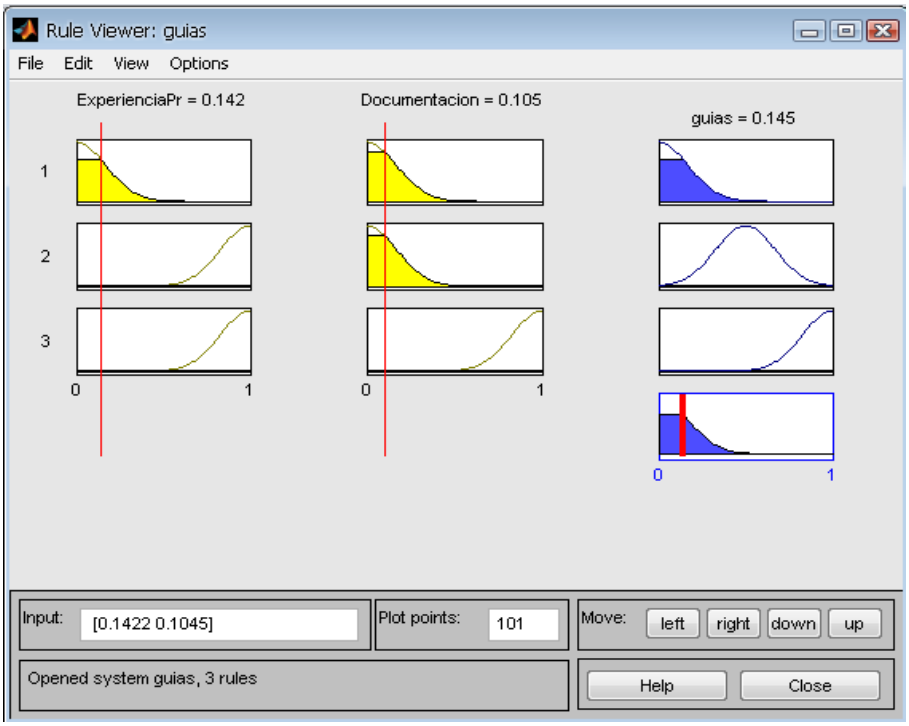


Figura B.4: Entradas y salidas del sistema

Experiencia	Documentación proceso	Guías a tiempo	
0.95	0.832	0.849	0.151
0.876	0.55	0.679	0.321
0.619	0.495	0.5	0.5
0.142	0.268	0.181	0.819

Tabla B.2 : Eventos 2 y 3

Si la experiencia del proveedor encargado de las auditorías es amplia y además el proceso se encuentra documentado adecuadamente, hay una alta probabilidad que las guías de auditoría sean entregadas a tiempo. Si la experiencia del proveedor es poca y el proceso no se encuentra totalmente

documentado o nada documentado, la tarea de auditoría será más compleja y habrá mayores probabilidades que las guías no sean entregadas a tiempo. Lo mismo sucede para el evento 3, el conocimiento del proceso.

Evento 4: **Diligenciamiento inadecuado de las guías de auditoría.**

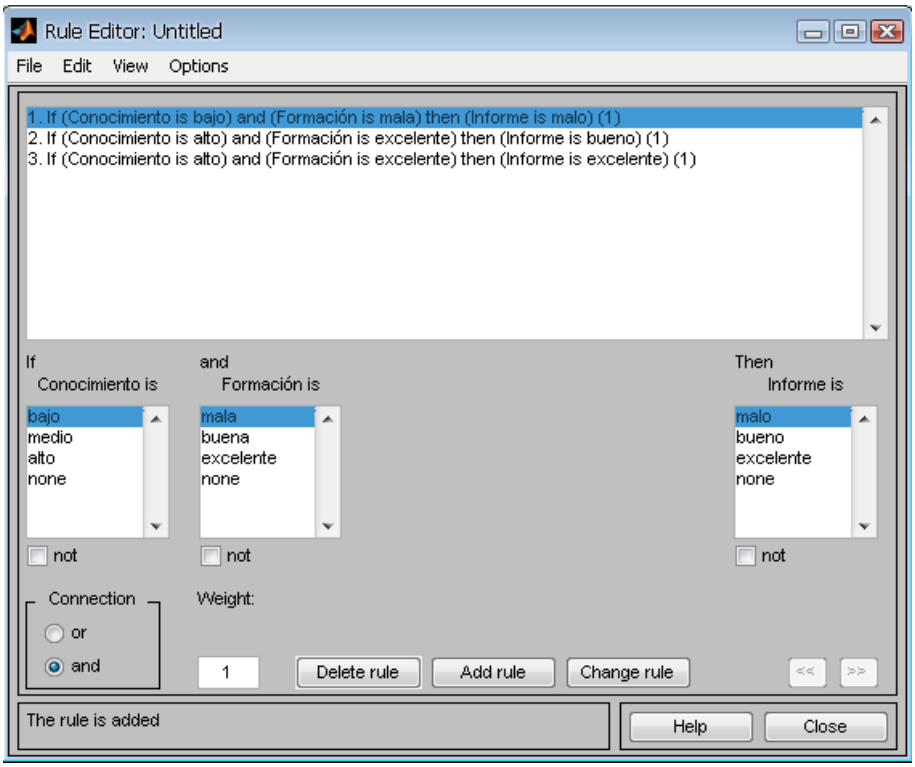
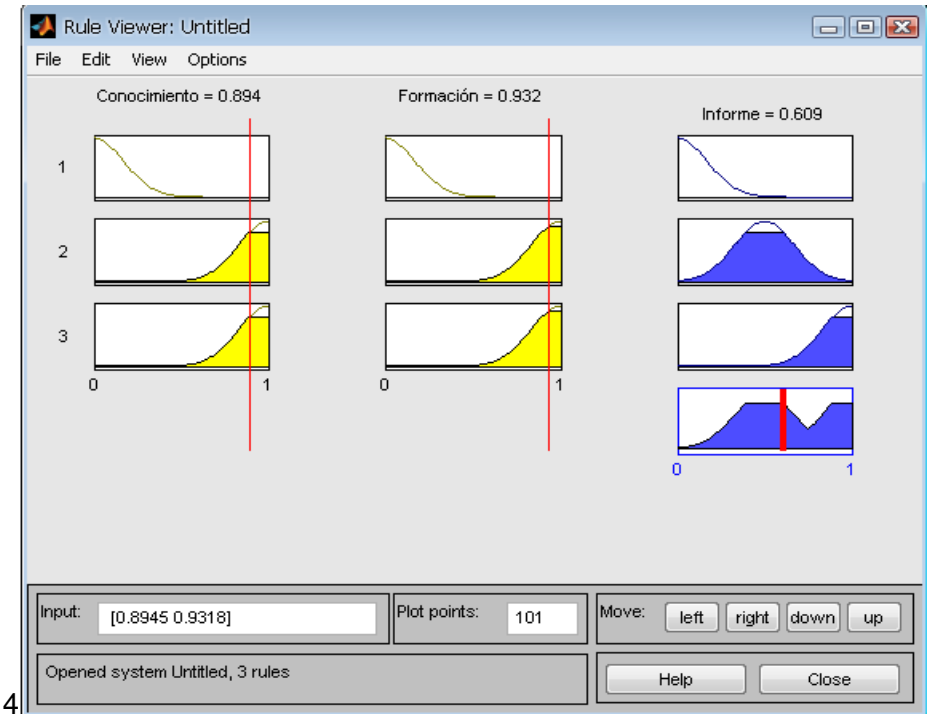


Figura B.5: Reglas para evento



4

Figura B.6: Entradas y salidas del sistema

Conocimiento	Formación como auditor	Informe final-Guías	
0.95	0.832	0.601	0.399
0.876	0.55	0.509	0.491
0.619	0.495	0.5	0.5
0.142	0.268	0.181	0.819

Tabla B.2 : evento 4

Los eventos que influyen directamente sobre el diligenciamiento de las guías son el conocimiento del proceso y la formación que tiene el auditor. Si el auditor tiene gran conocimiento del proceso y buena formación, el informe final y las guías de auditoría serán diligenciadas adecuadamente. Se

presentará el caso contrario si hay poco conocimiento y además la formación como auditor no ha sido buena.

Evento 5: **Teclado de dispositivo de autenticación defectuoso.**

Evento 46: **No funciona la batería de respaldo de la máquina de votación.**

Evento 47: **La máquina de votación falla y no es posible reiniciarla.**

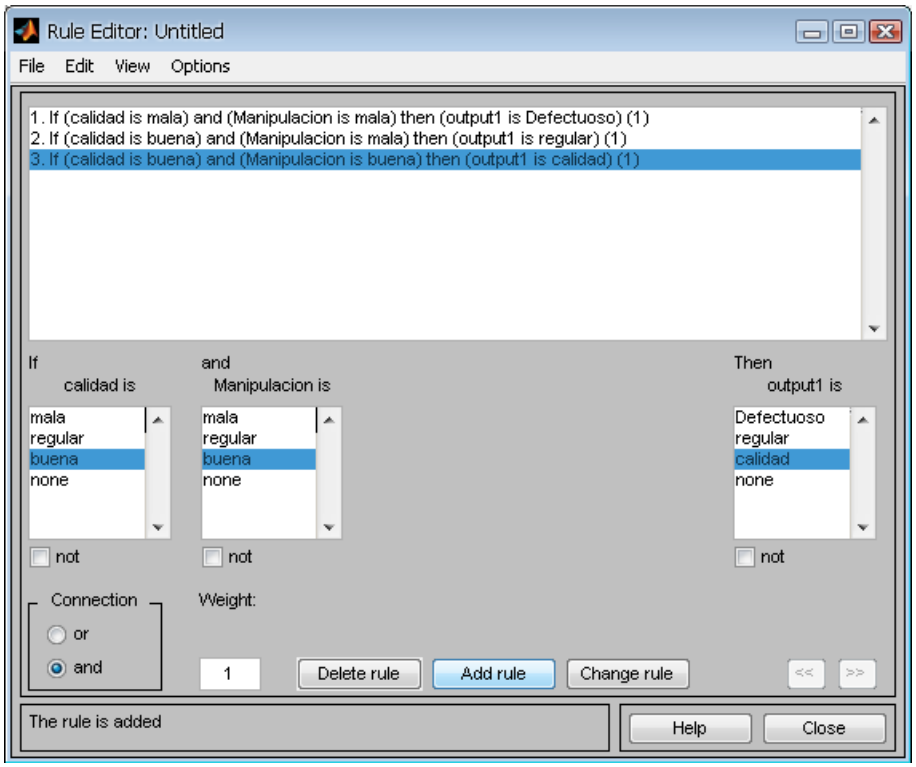


Figura B.7: Reglas para eventos 5, 46,47

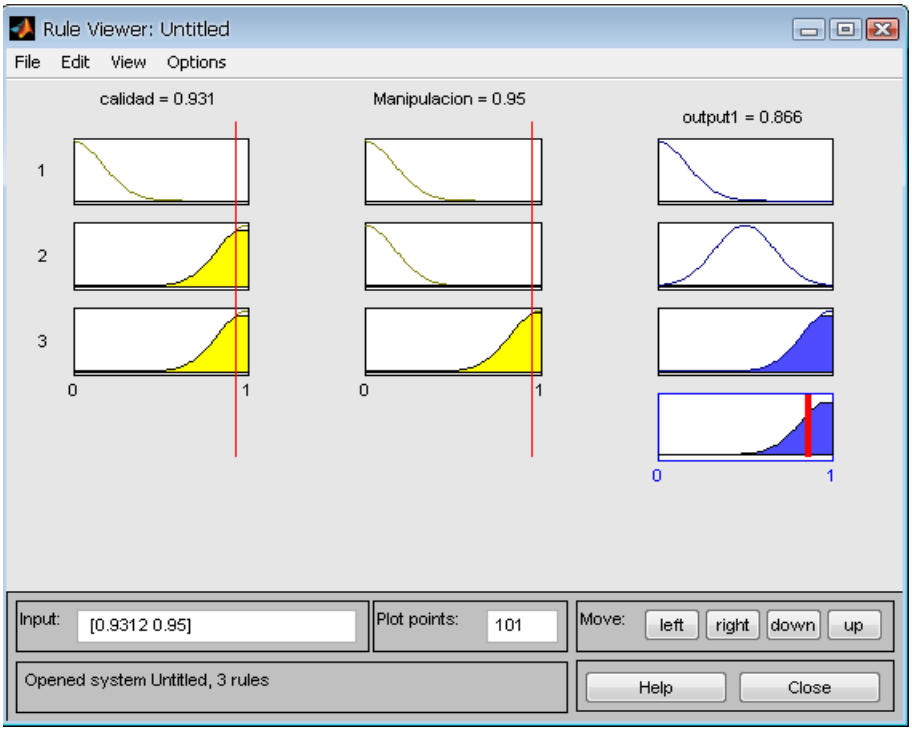


Figura B.8: Entradas y salidas del sistema

Calidad	Manipulación	Buen Desempeño Teclado	
0.95	0.832	0.849	0.151
0.876	0.55	0.679	0.321
0.619	0.495	0.5	0.5
0.142	0.268	0.181	0.819

Tabla B.3 : eventos 5, 46,47

Los eventos iniciales que se analizan en este sistema de inferencia fuzzy tienen que ver con la calidad de los dispositivos físicos involucrados en el proceso, como lo son la máquina de votación, las baterías de respaldo y los dispositivos de autenticación: *Morpho-Touch.* Si la calidad de los elementos y la manipulación es la adecuada, estos tendrán mayor probabilidad de buen desempeño.

Evento 6: **Inexistencia de procedimiento que describa como se debe realizar el cambio de dispositivo de autenticación.**

Evento 15: **No existe protocolo para asistencia a votante en caliente.**

Evento 43: **No existe protocolo para cambio de máquinas en caliente.**

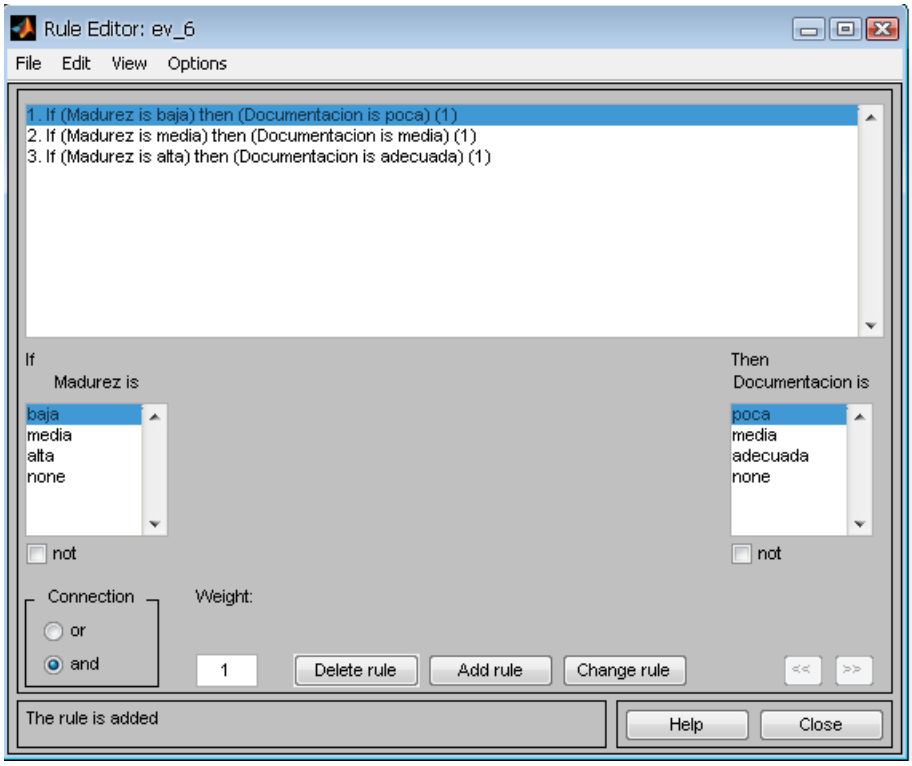


Figura B.9: Reglas para eventos 6, 15,43

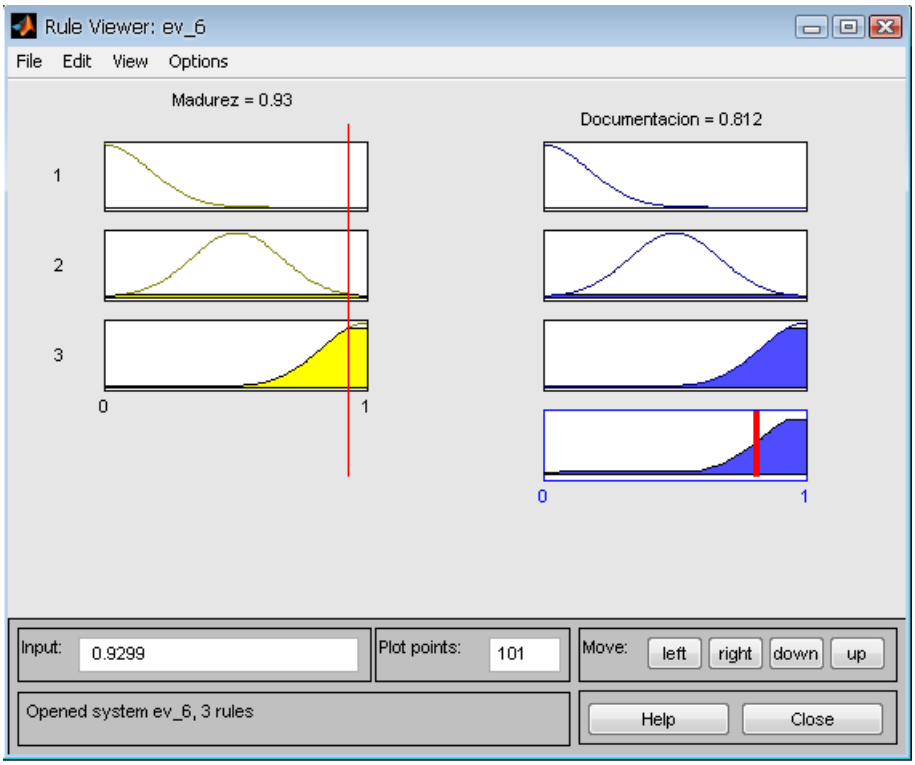


Figura B.10: Entradas y salidas del sistema

Madurez	Documentación	
0.832	0.696	0.304
0.55	0.501	0.499
0.495	0.5	0.5
0.268	0.437	0.563

Tabla B.4 : eventos 6, 15,43

Los eventos iniciales 6, 15 y 43 se analizan con este sistema fuzzy, ya que la existencia de protocolos para cambio de máquinas de votación, cambio de dispositivos de autenticación y asistencia al votante, depende de la

madurez del proceso. Entre más alta sea la madurez, habrá mayor probabilidad de existencia de documentación.

Evento 7: **No disponibilidad de dispositivos de autenticación de respaldo.**

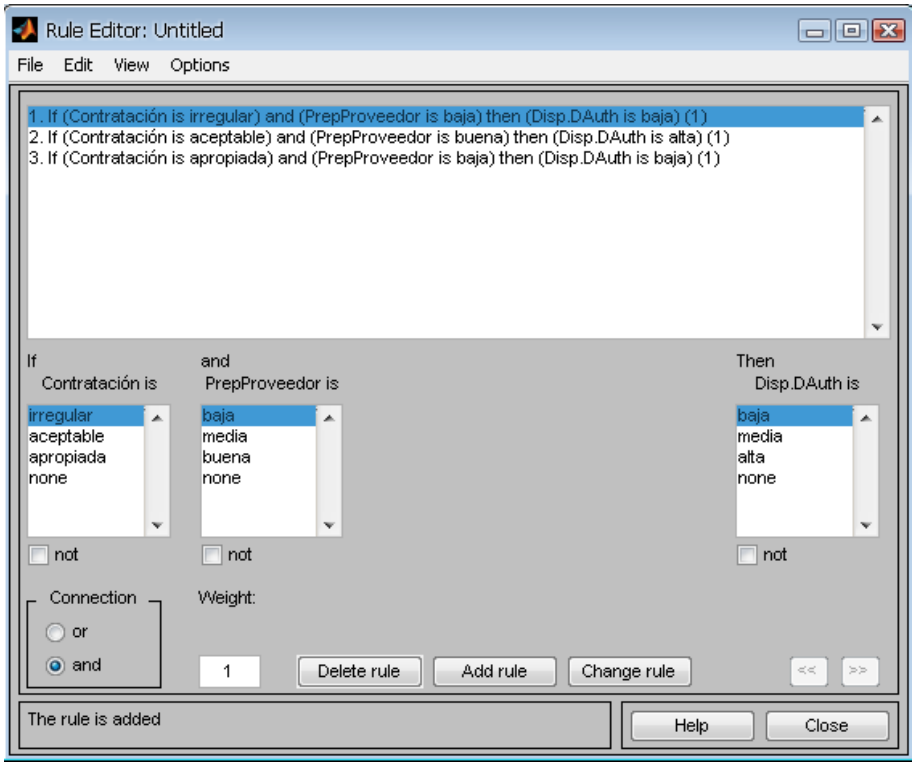


Figura B.11: Reglas para evento 7

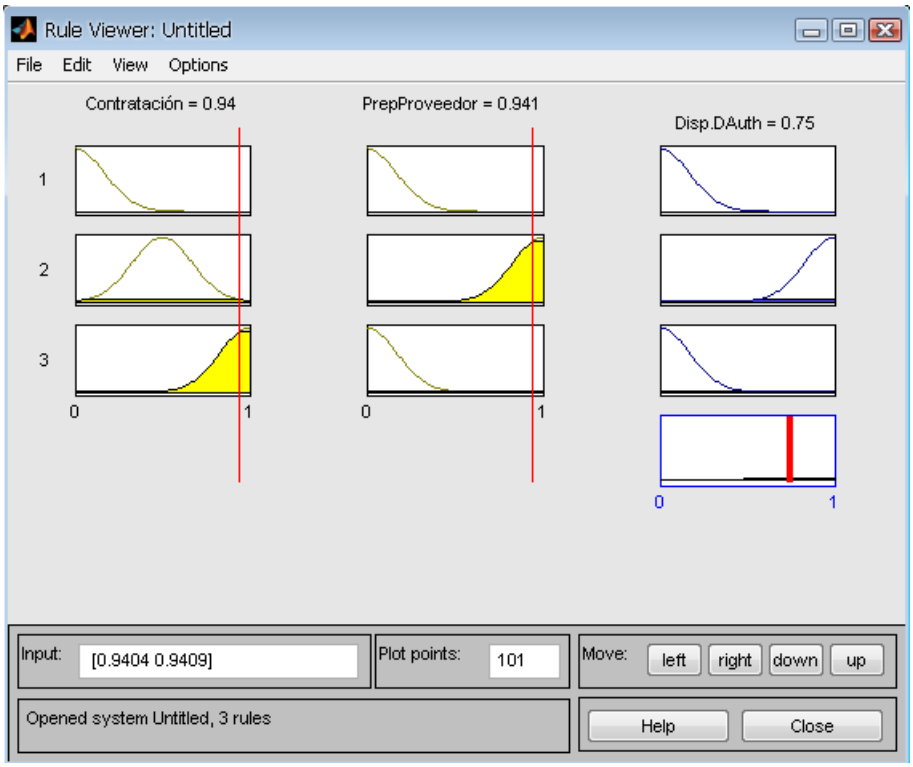


Figura B.12: Entradas y salidas del sistema

Contratación	Prep.Proveedor	Disp.DispAuth	
0.95	0.832	0.746	0.254
0.876	0.55	0.679	0.321
0.619	0.495	0.48	0.52
0.142	0.268	0.181	0.819

Tabla B.5 : evento 7

La disponibilidad de dispositivos de autenticación depende en gran medida de las condiciones de contratación impuestas al proveedor y de la preparación con que cuente este para todas las actividades del proceso. La disponibilidad de dispositivos será más alta en la medida que esto se haya condicionado en la contratación.

Evento 8: **Procedimiento de cambio de dispositivo de autenticación no es conocido por el personal encargado del proceso.**

Evento 16: **Desconocimiento de protocolo de asistencia a votantes por parte de jurados y auditores.**

Evento 45: **Desconocimiento del protocolo de cambio de máquina por parte de jurados y /o auditores.**

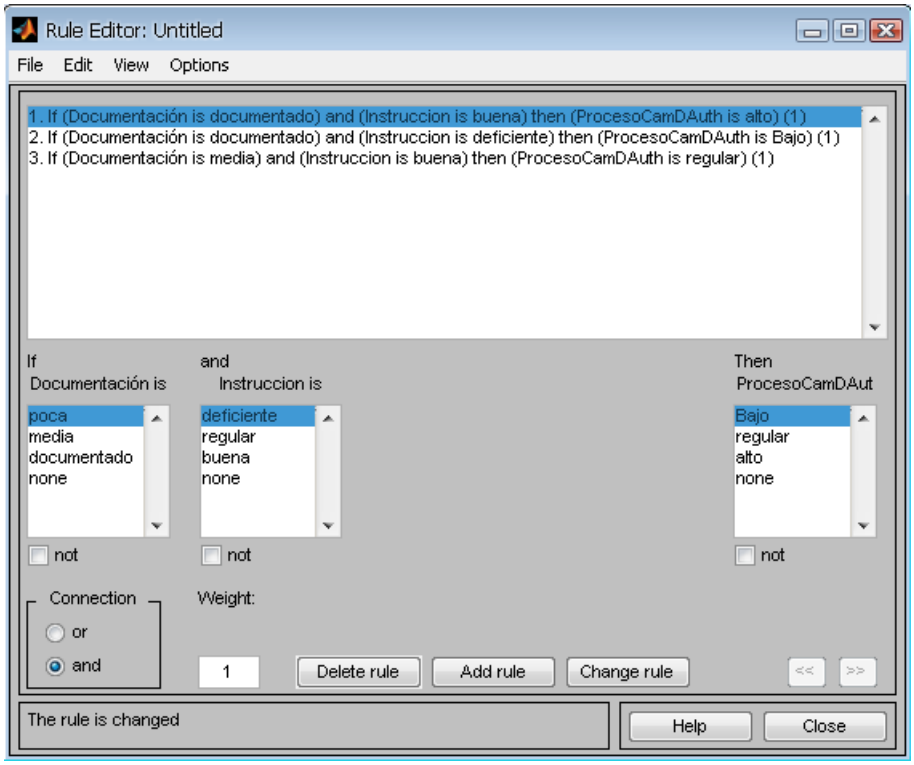


Figura B.13: Reglas para eventos 8,16,45

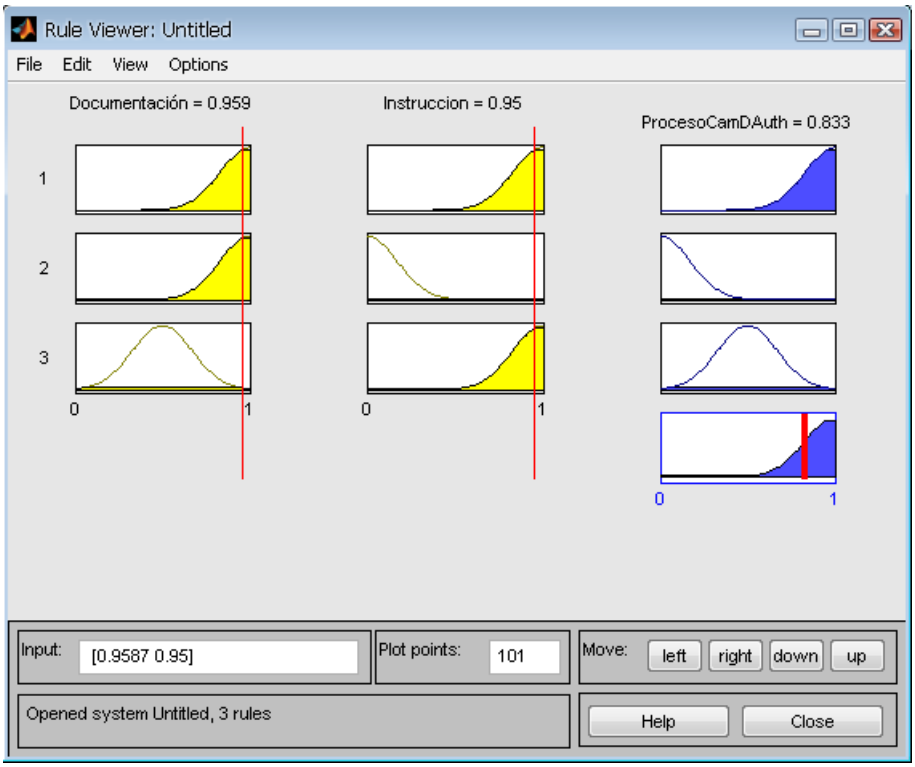


Figura B.14: Entradas y salidas del sistema

Documentación	Instrucción	Proc.CamDAuth	
0.95	0.832	0.805	0.195
0.876	0.55	0.51	0.49
0.619	0.495	0.486	0.514
0.142	0.268	0.5	0.5

Tabla B.6 : evento 7

El conocimiento de todos los procedimientos que se deben ejecutar, depende principalmente de que estos se encuentren documentados adecuadamente y que las personas que deban hacer uso de ellos, reciban la instrucción pertinente. Si estos dos aspectos, documentación e instrucción , se cumplen a cabalidad, habrá buen conocimiento y por tanto, buena implementación de los procesos.

Evento 9: **Número de cédula ilegible.**

Evento 10: **Cédula con código de barras ilegible.**

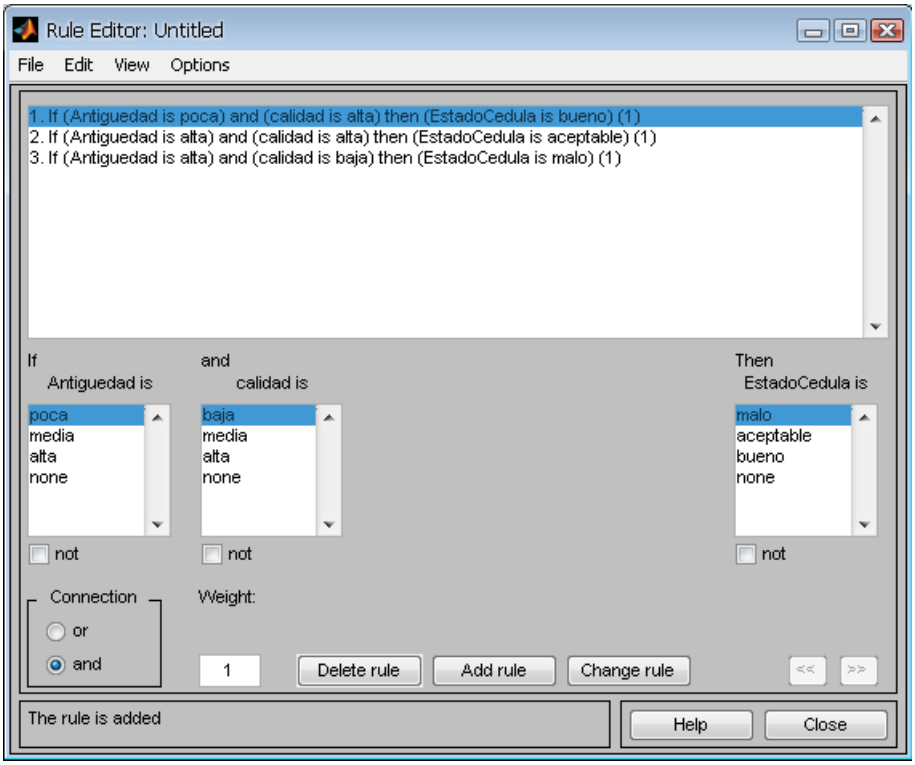


Figura B.15: Reglas para eventos 9, 10

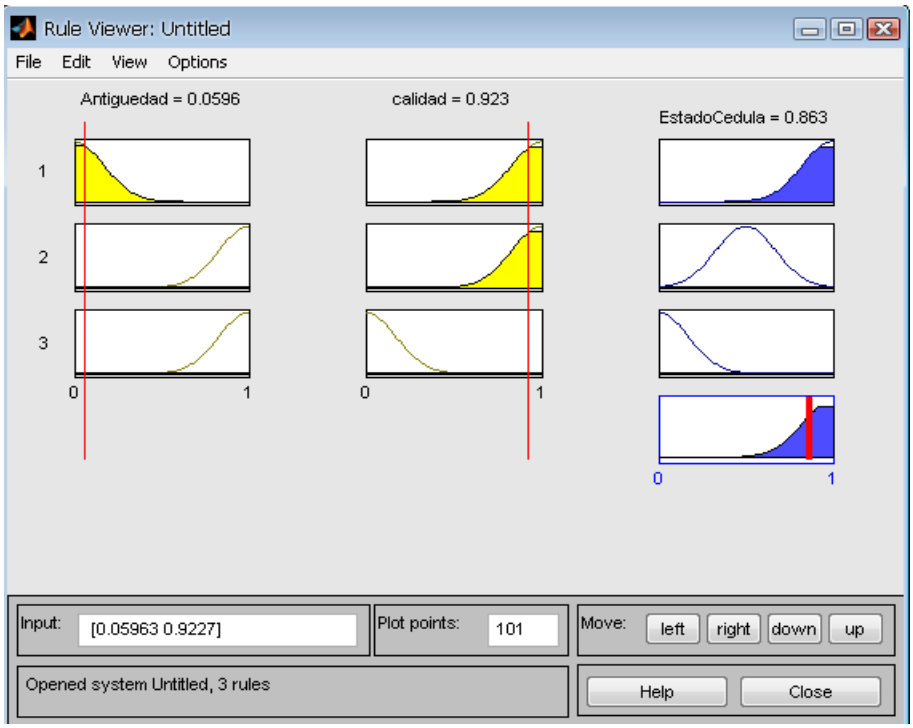


Figura B.16: Entradas y salidas del sistema

Antigüedad	Calidad	BuenestadoCédula	
0.95	0.832	0.5	0.5
0.876	0.55	0.5	0.5
0.619	0.495	0.48	0.52
0.106	0.905	0.859	0.141

Tabla B.7: eventos 9, 10

Este sistema modela como la antigüedad y la calidad pueden influir en el buen estado de la cédula de ciudadanía. En conclusión se puede decir que si el documento es fabricado con buenos estándares de calidad, la cédula presentará un general un buen estado, que permitirá su uso en el proceso de autenticación.

Evento 11: **Amenazas por parte de grupos armados.**
Evento 38 : **Coacción por parte de grupos armados.**
Evento 42 : **Ataques insurgentes.**

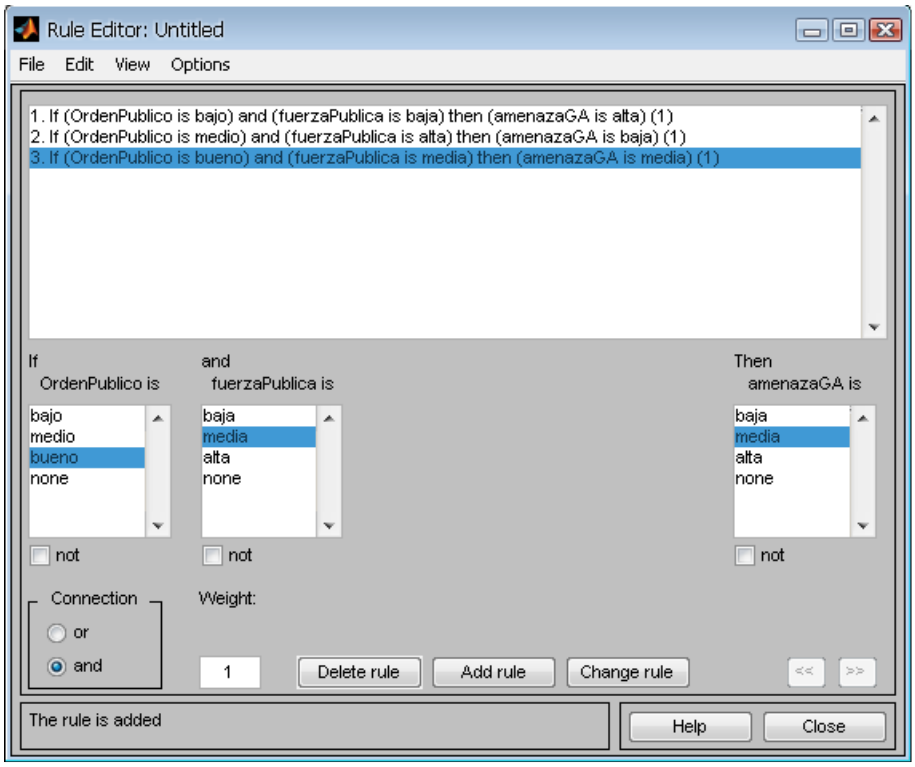


Figura B.17: Reglas para evento 11

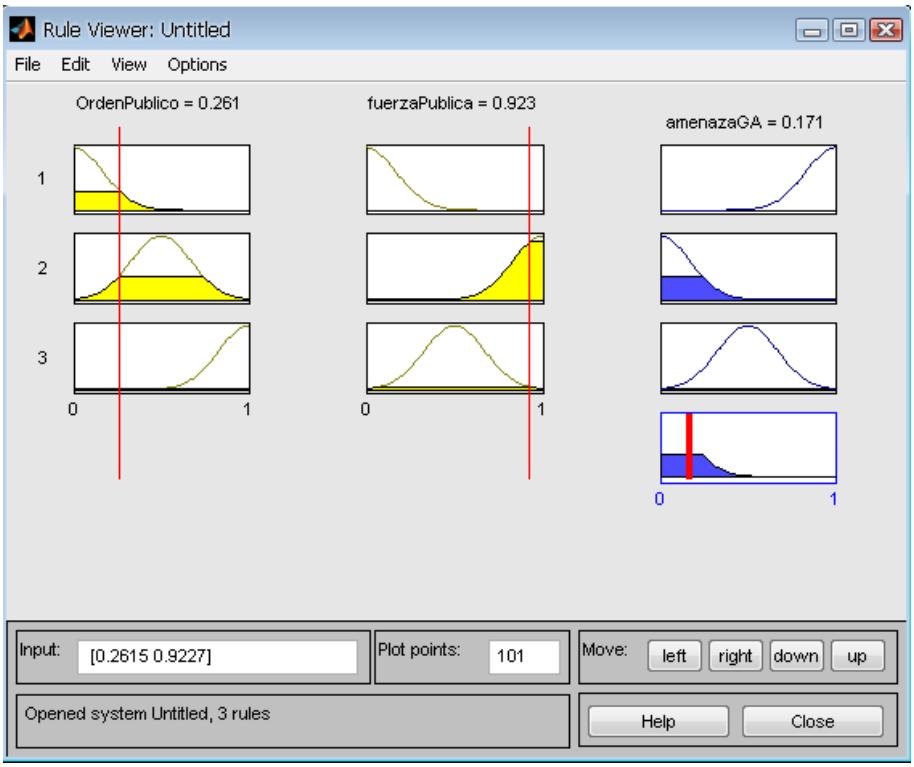


Figura B.18: Entradas y salidas del sistema

OrdenPublico	fuerzaPublica	AmenazaGA	
0.95	0.832	0.498	0.502
0.876	0.55	0.499	0.501
0.619	0.495	0.5	0.5
0.142	0.268	0.819	0.181

Tabla B.8: evento 11

La amenaza de ataques por parte de grupos armados al margen de la ley (guerrilla, paramilitares, delincuencia común) es un evento de gran probabilidad si se tiene en cuenta que depende principalmente del estado del orden público del país y de la presencia y preparación de la fuerza pública para este tipo de eventos. Si el orden público es bueno, y la presencia de la fuerza pública es también evidente, los grupos armados tendrán pocas probabilidades de ejercer presión.

Evento 12: **Compra/venta de votos.**

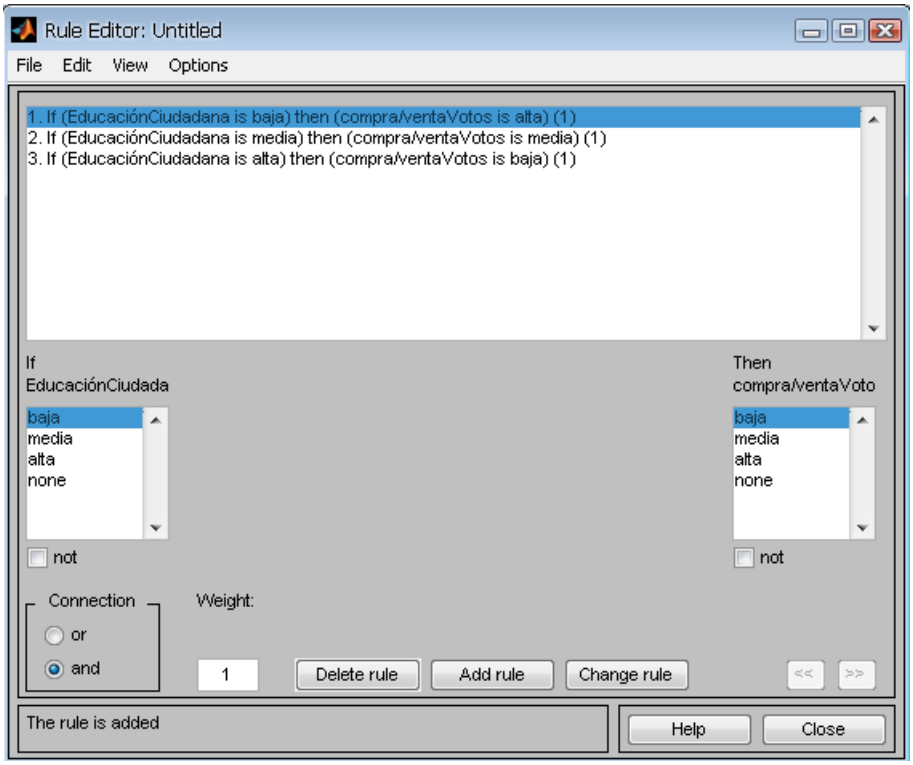


Figura B.19: Reglas para evento 12

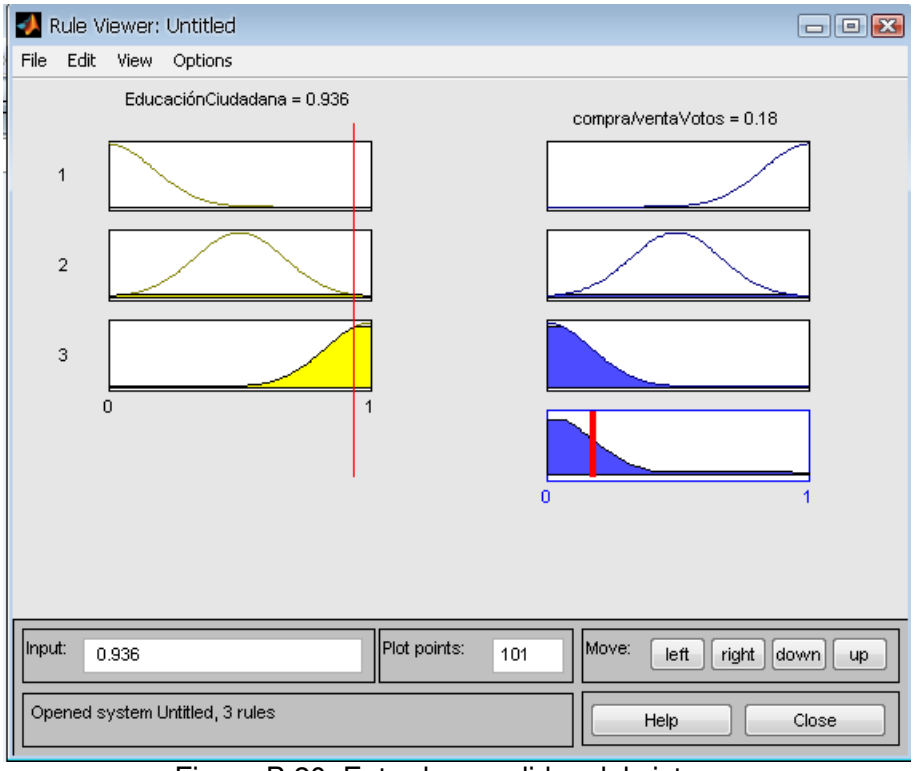


Figura B.20: Entradas y salidas del sistema

EducaciónCiudadana	Compra/venta votos	
0.95	0.171	0.829
0.876	0.237	0.763
0.619	0.489	0.511
0.142	0.737	0.263

Tabla B.9: evento 12

La educación ciudadana es la base principal para evitar la compra y venta de votos, esto quiere decir, que a mayor educación ciudadana, habrá menos compra/venta de votos porque los ciudadanos tendrán más conciencia de la importancia que tiene su voto en la democracia y futuro del país

Evento 13: **Propaganda política el día de votación.**

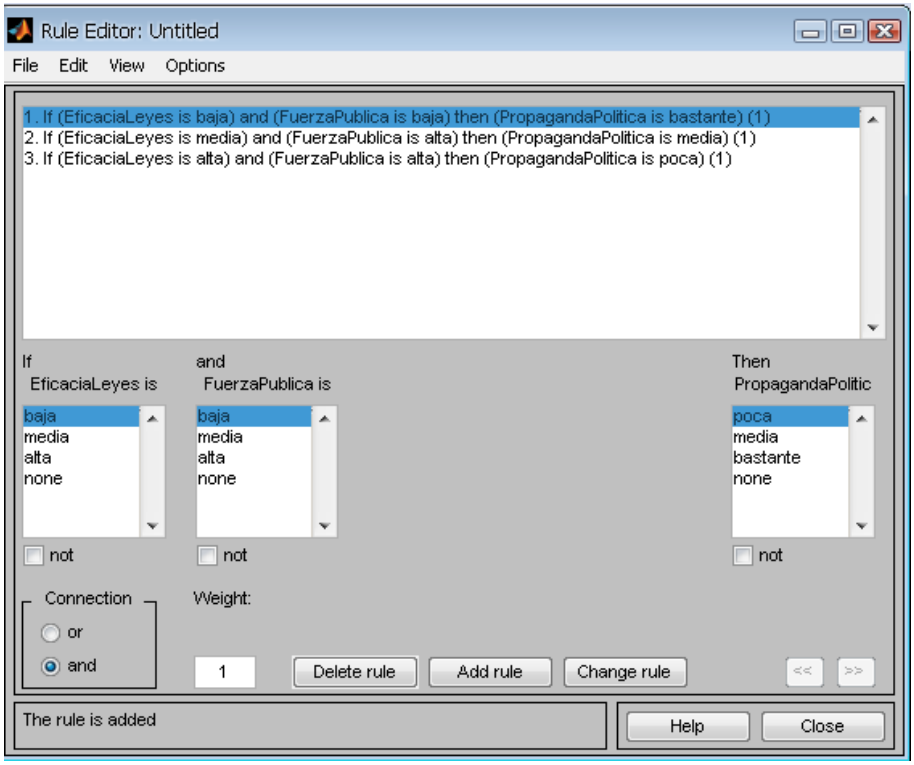


Figura B.21: Reglas para evento 13

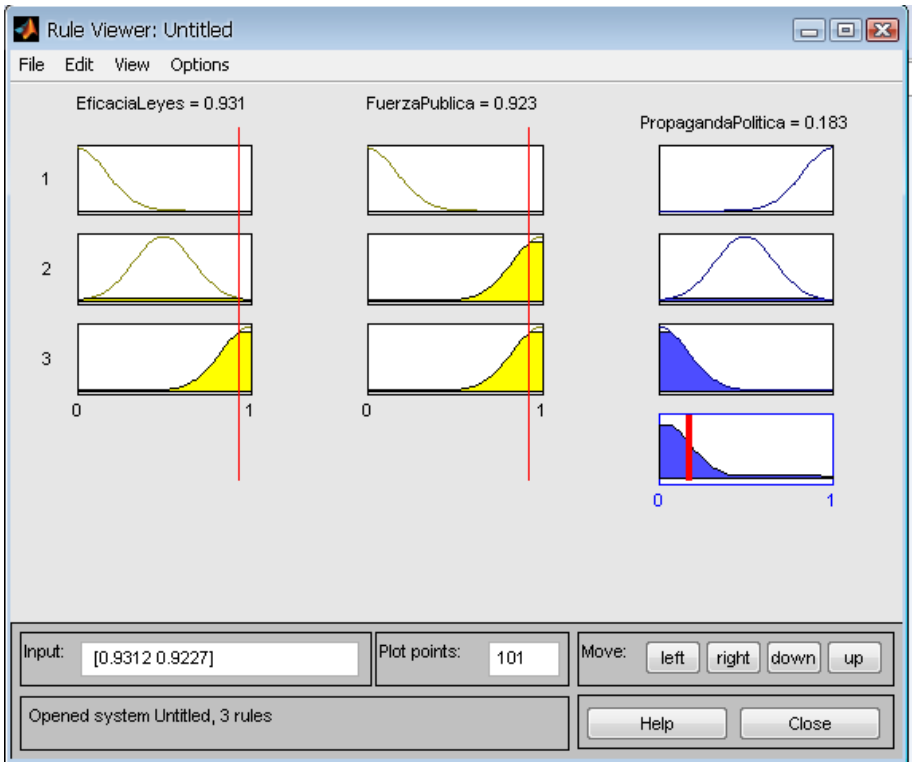


Figura B.22: Entradas y salidas del sistema

EficienciaLeyes	fuerzaPublica	PropagandaPolitica	
0.95	0.832	0.194	0.806
0.876	0.55	0.49	0.51
0.619	0.495	0.5	0.5
0.142	0.268	0.819	0.181

Tabla B.10: evento 13

El día de las elecciones no se debe realizar ninguna actividad de propaganda política, esto para evitar presiones al ciudadano y la compra/venta de votos. Entre más eficientes sean las leyes que prohíben estas prácticas y la presencia de la fuerza pública esté vigilante, habrán menos probabilidades que haya propaganda política y por tanto, se presione al votante a tomar una decisión determinada.

Evento 14: **Control inadecuado de tarjetones de votación.**

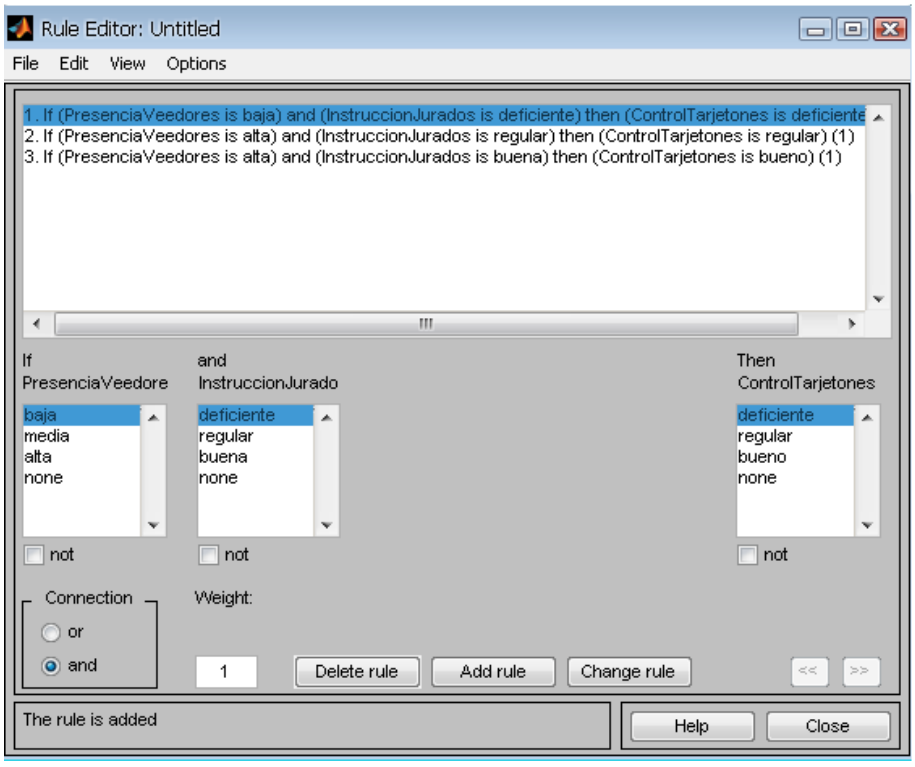


Figura B.23: Reglas para evento 14

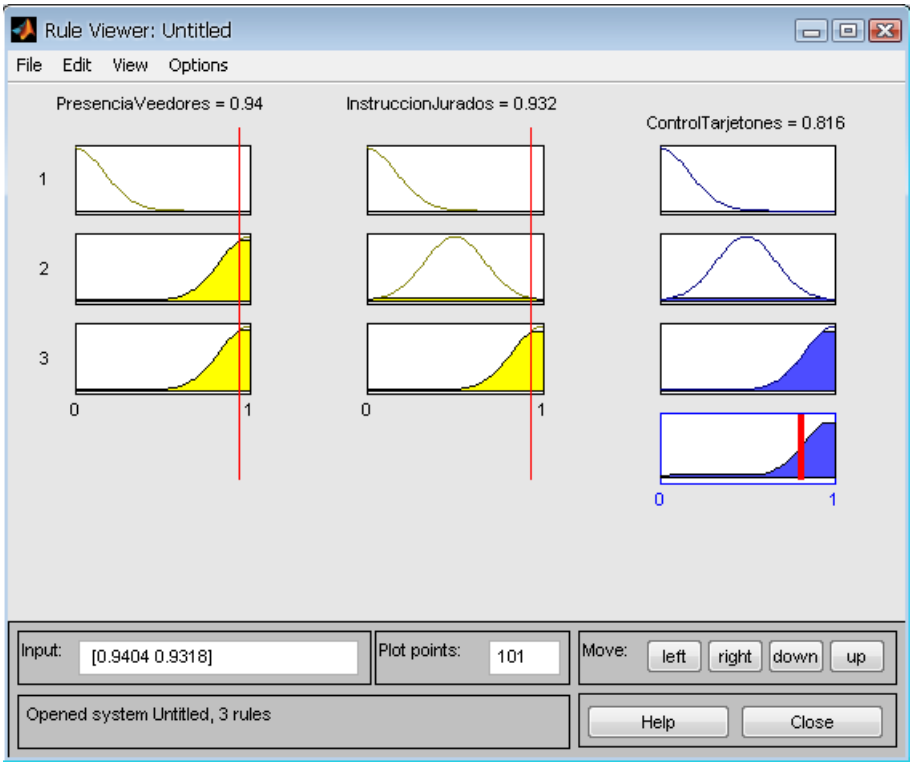


Figura B.24: Entradas y salidas del sistema

presenciaVeedores	InstruccionJurados	controlTarjetones	
0.95	0.832	0.699	0.301
0.876	0.55	0.496	0.504
0.619	0.495	0.496	0.504
0.142	0.268	0.181	0.819

Tabla B.11: evento 14

En la jornada de elecciones, el control de los tarjetones recae principalmente sobre jurados y veedores, quienes deben conocer como realizar el control de

tarjetones y estar presentes en todos los momentos que se realice manipulación de los mismos. Entre más adecuada sea la instrucción a los jurados y los veedores del proceso estén presentes, habrá mejor control de tarjetones.

Evento 17: **No hay presencia de veedores durante la asistencia al votante.**
Evento 44: **Poca presencia de jurados y/o auditores durante el cambio de máquina de votación.**
Evento 54: **Poca presencia de auditores y veedores en el proceso de autenticación del votante.**

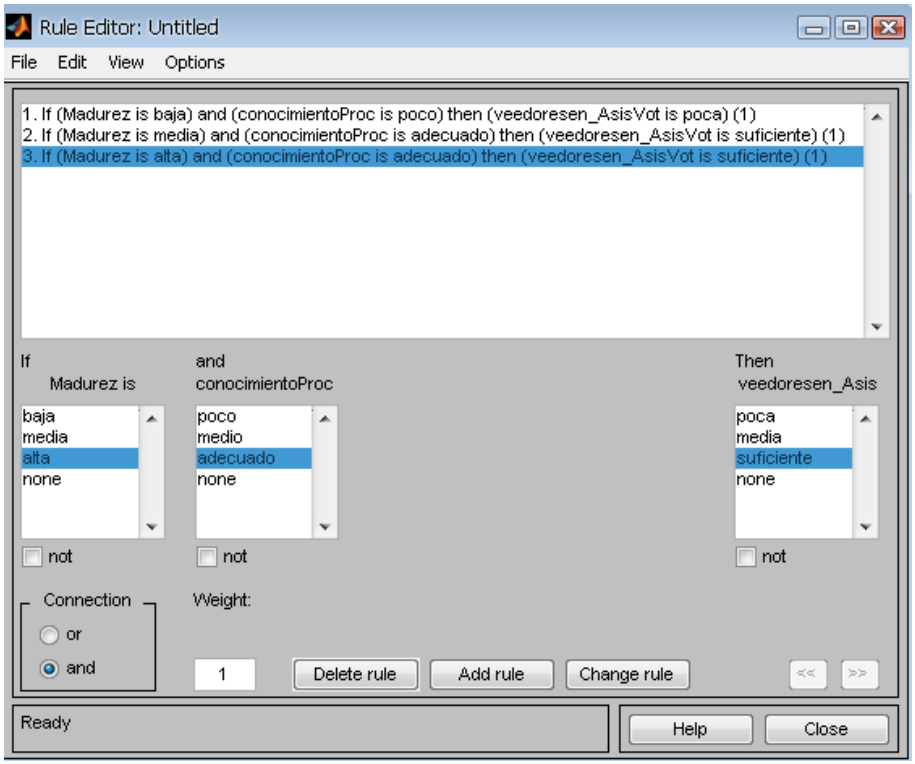


Figura B.25: Reglas para eventos 17,44,54

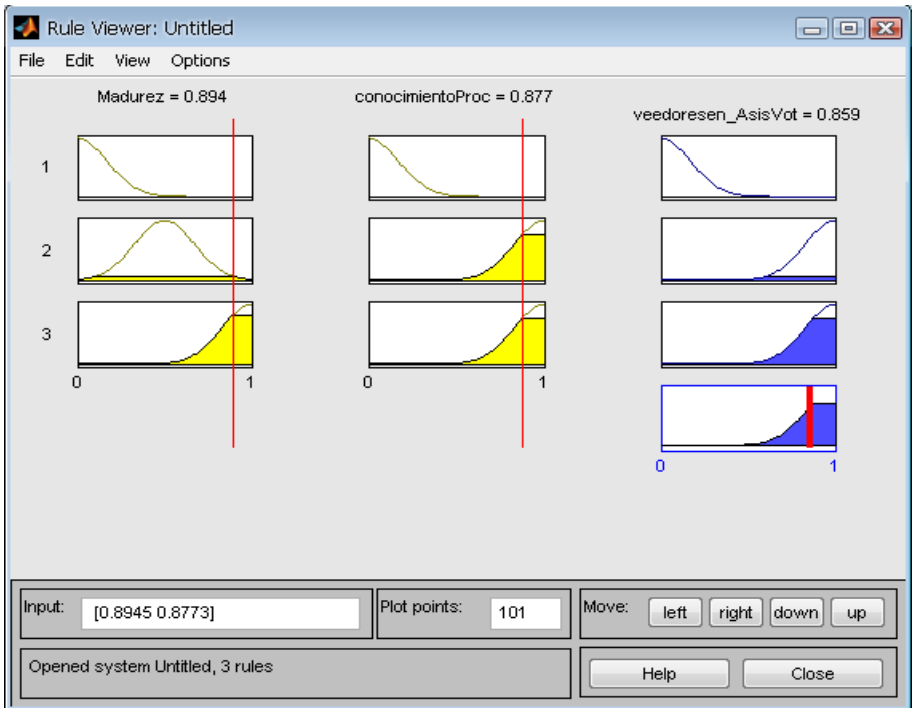


Figura B.26: Entradas y salidas del sistema

Madurez	ConocimientoProc	VeedoresAsistVot	
0.95	0.832	0.849	0.151
0.876	0.55	0.746	0.254
0.619	0.495	0.688	0.312
0.142	0.268	0.181	0.819

Tabla B.11: eventos 17,44,54

La presencia de auditores y veedores en todas las instancias del proceso depende principalmente de la madurez y el conocimiento que los jurados y veedores tengan del mismo. Si el proceso es maduro y los veedores conocen adecuadamente los procesos, se presentarán menos irregularidades.

Evento 18: **Robo de tarjetones**

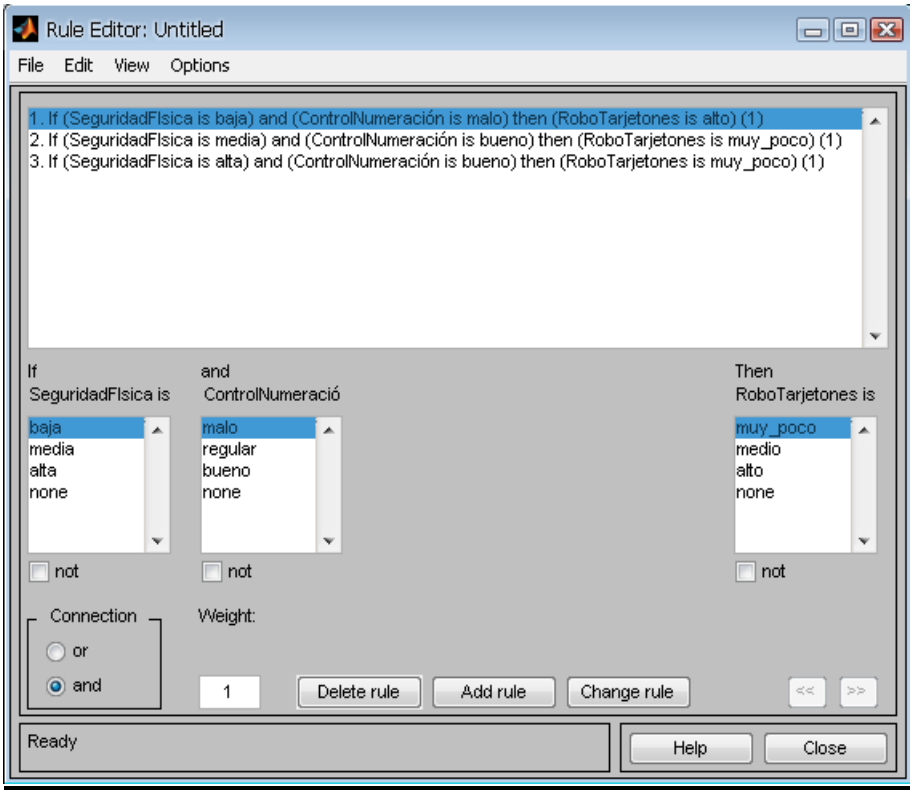


Figura B.27: Reglas para evento 18

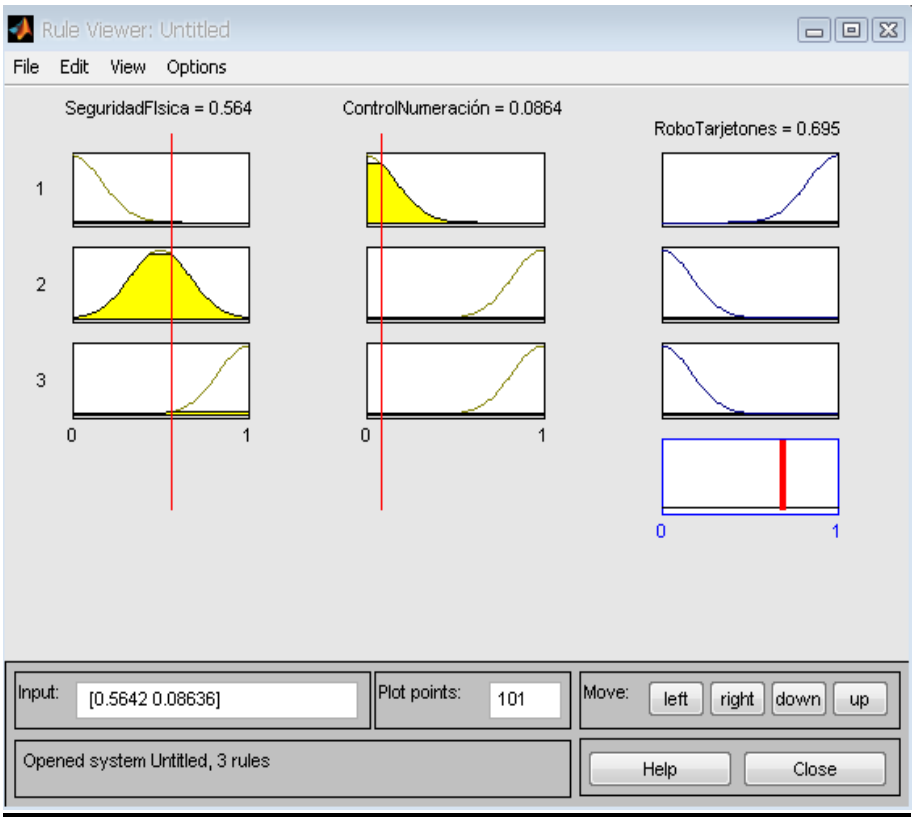


Figura B.28: Entradas y salidas del sistema

SeguridadFisica	ControlNumeracion	Control Tarjetones	
0.95	0.832	0.849	0.151
0.876	0.55	0.746	0.254
0.619	0.495	0.688	0.312
0.142	0.268	0.181	0.819

Tabla B.12: evento 18

El robo de tarjetones durante el proceso electoral es un tema crítico porque si el control no se realiza de manera adecuada, se puede terminar violando los principios de confidencialidad y no trazabilidad del voto. Para los sistemas de voto electrónico que utilizan tarjetón esto seria un

inconveniente que podría solucionarse garantizando buen nivel de seguridad física, es decir, vigilancia y control de la numeración de los tarjetones para evitar el robo o reemplazo de los mismos.

Evento 19: **Votante no tiene conocimiento el uso de la máquina de votación.**

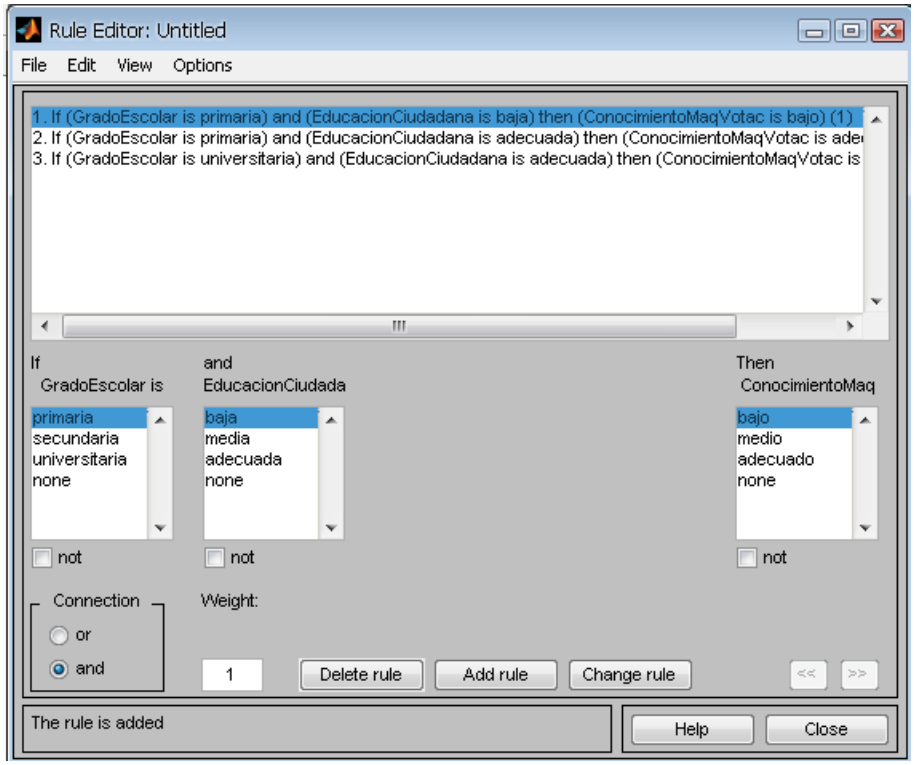


Figura B.29: Reglas para evento 19

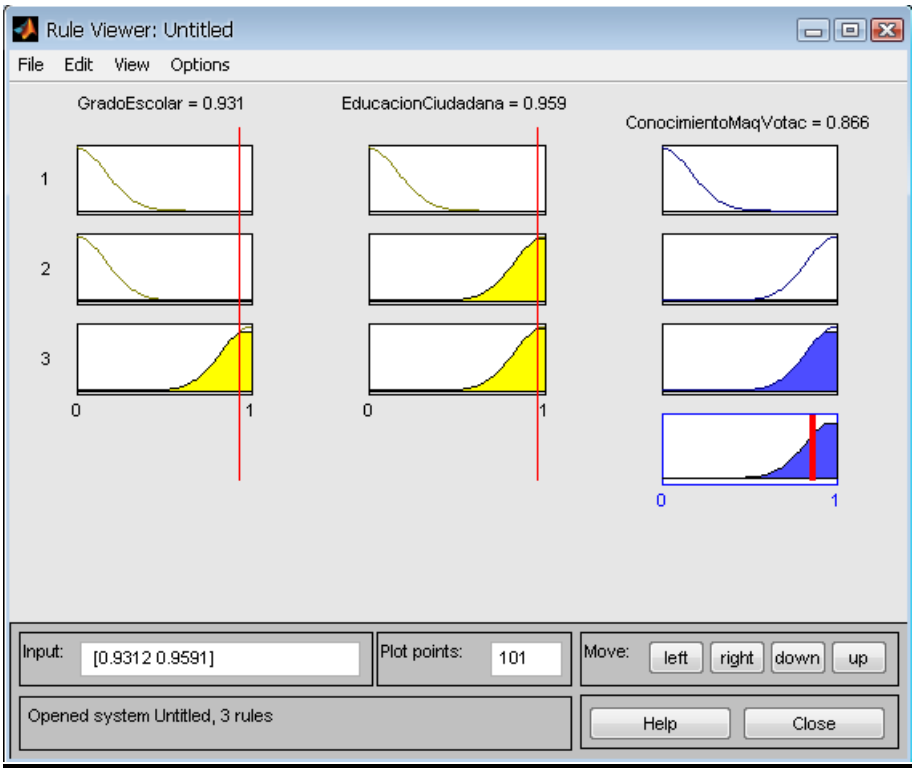


Figura B.30: Entradas y salidas del sistema

GradoEscolar	Eduación Ciudadana	ConocimientoMáq. Vot.	
0.95	0.832	0.849	0.151
0.876	0.55	0.746	0.254
0.619	0.495	0.688	0.312
0.142	0.268	0.181	0.819

Tabla B.13: evento 19

El conocimiento de la tecnología de votación y la destreza en su uso por parte del ciudadano, depende en gran medida de la educación ciudadana

realizada para tal fin y del grado de escolaridad del votante. Entre más alto el nivel de escolaridad[1] y la eficacia de las campañas de educación, el ciudadano conocerá mas la tecnología de votación y podrá por ende ejercer su derecho de manera rápida y eficiente

Evento 20: **Poca efectividad de las campañas de educación ciudadana.**

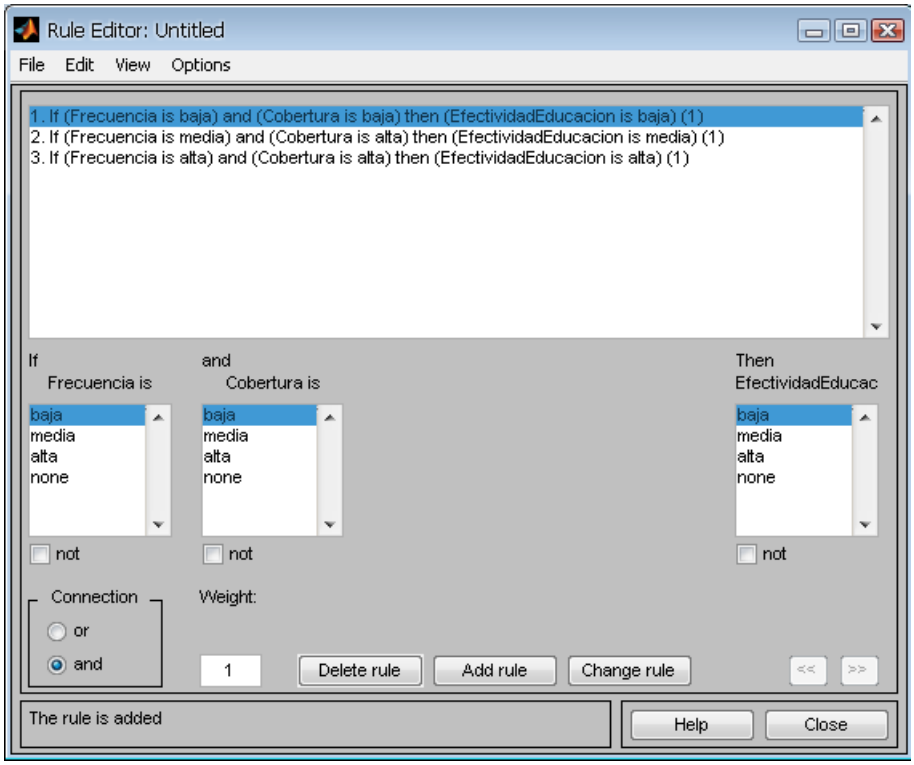


Figura B.31: Reglas para evento 20

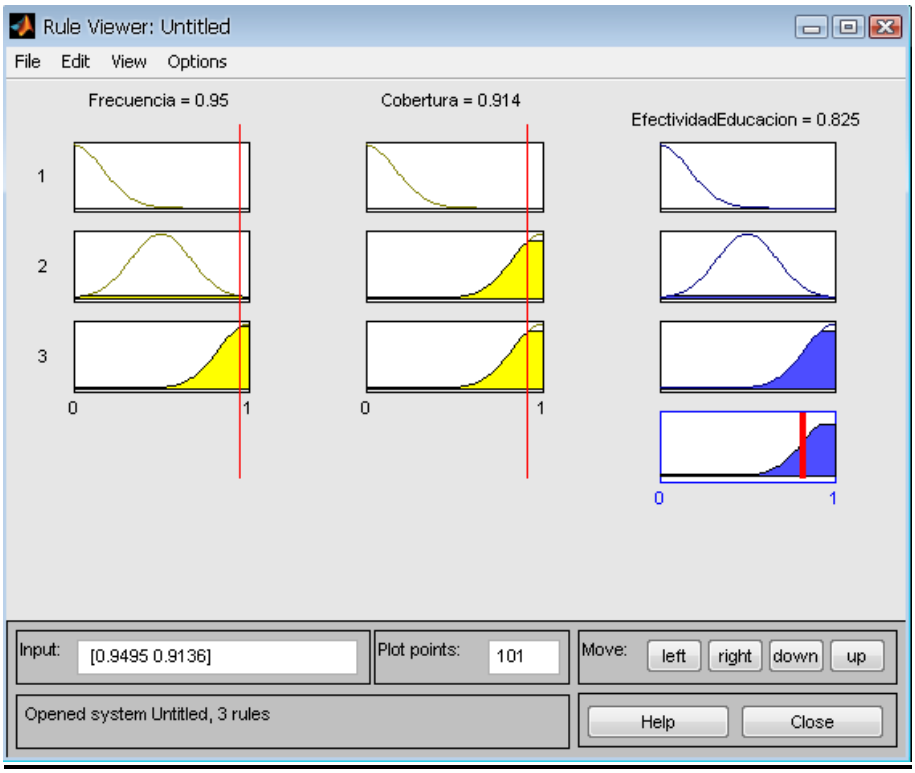


Figura B.32: Entradas y salidas del sistema

Frecuencia	Cobertura	EfectividadEducación	
0.95	0.832	0.804	0.196
0.876	0.55	0.509	0.491
0.619	0.495	0.5	0.5
0.142	0.268	0.181	0.819

Tabla B.14: evento 20

La frecuencia y cobertura de las campañas educativas respecto al voto electrónico, inciden directamente sobre la efectividad de las mismas. A mayor frecuencia y cobertura, habrá mayor efectividad.

Evento 21: **Fallas en la calibración de la pantalla táctil.**

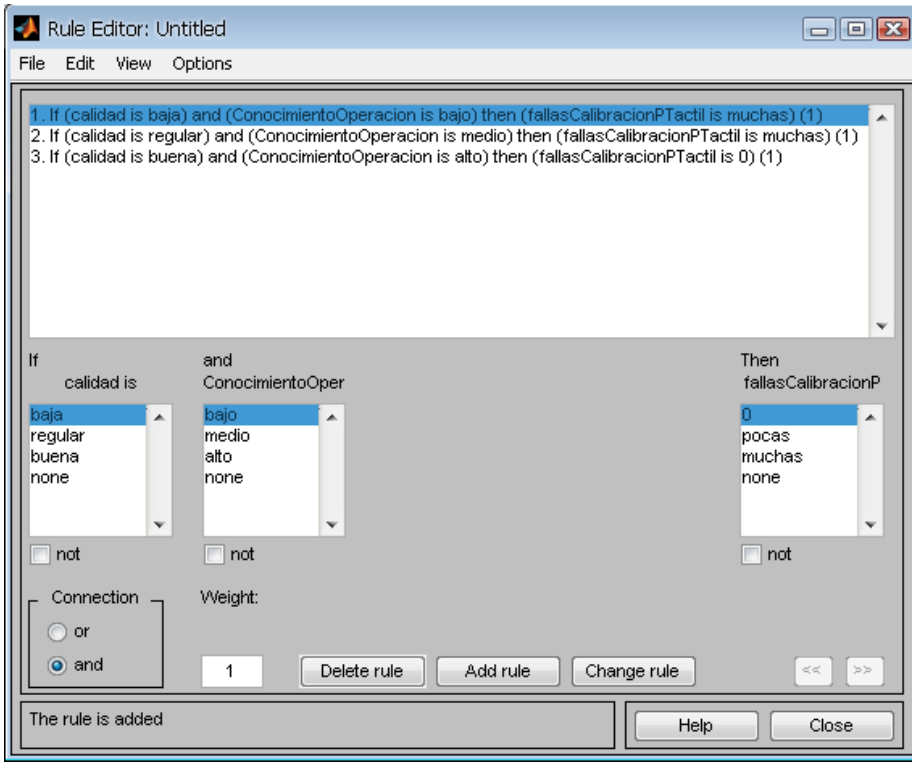


Figura B.33: Reglas para evento 21

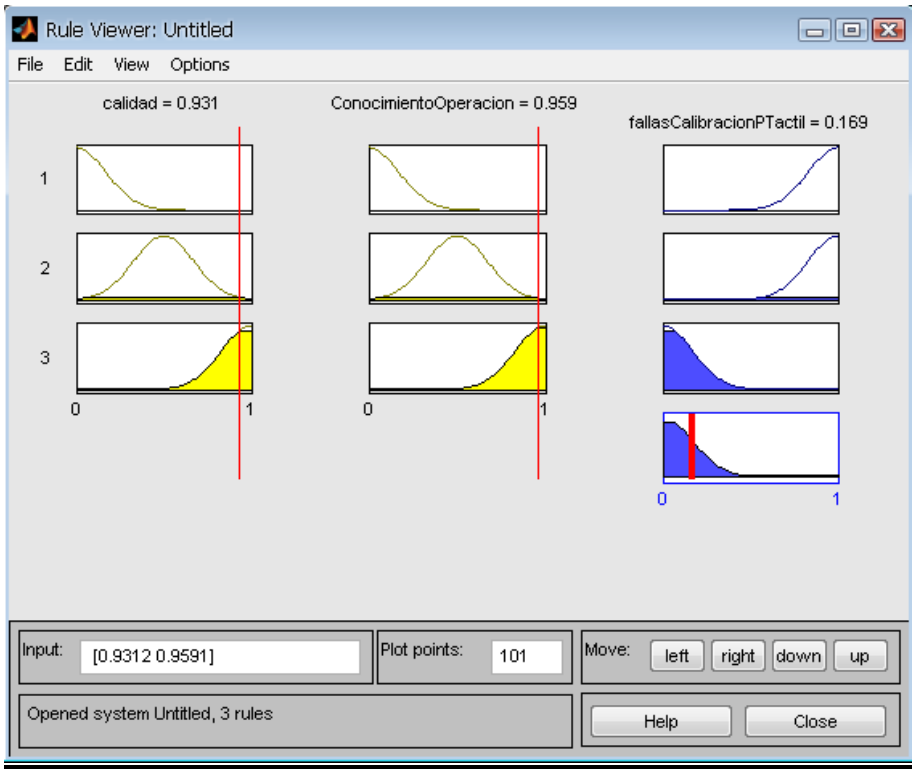


Figura B.34: Entradas y salidas del sistema

Calidad	ConocimientoOper	FallasP.Tactil	
0.95	0.832	0.197	0.803
0.876	0.55	0.632	0.368
0.619	0.495	0.842	0.158
0.142	0.268	0.189	0.811

Tabla B.15: evento 21

Las fallas de la pantalla táctil se pueden originar debido a dos aspectos principales como su calidad y el conocimiento que el operario que la calibra y manipula sea el adecuado. Entre más alta sea la calidad de la pantalla y el operario conozca su funcionamiento, las probabilidades de fallas de la pantalla serán pocas.

Evento 22: **Fallas en la lectura del escáner óptico de la máquina de la votación.**

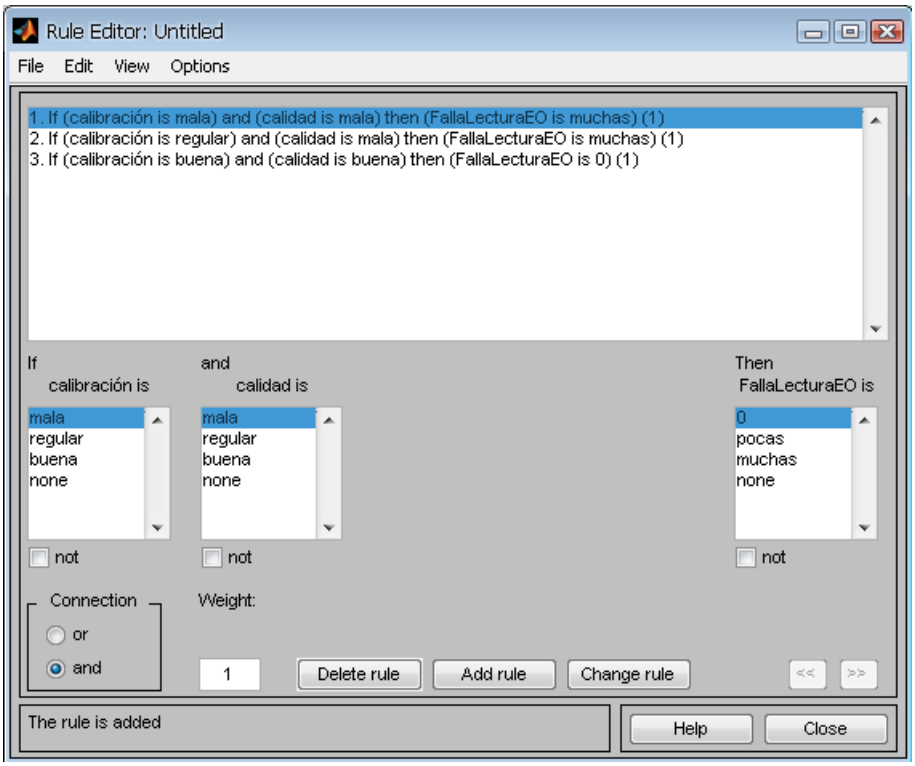


Figura B.35: Reglas para evento 22

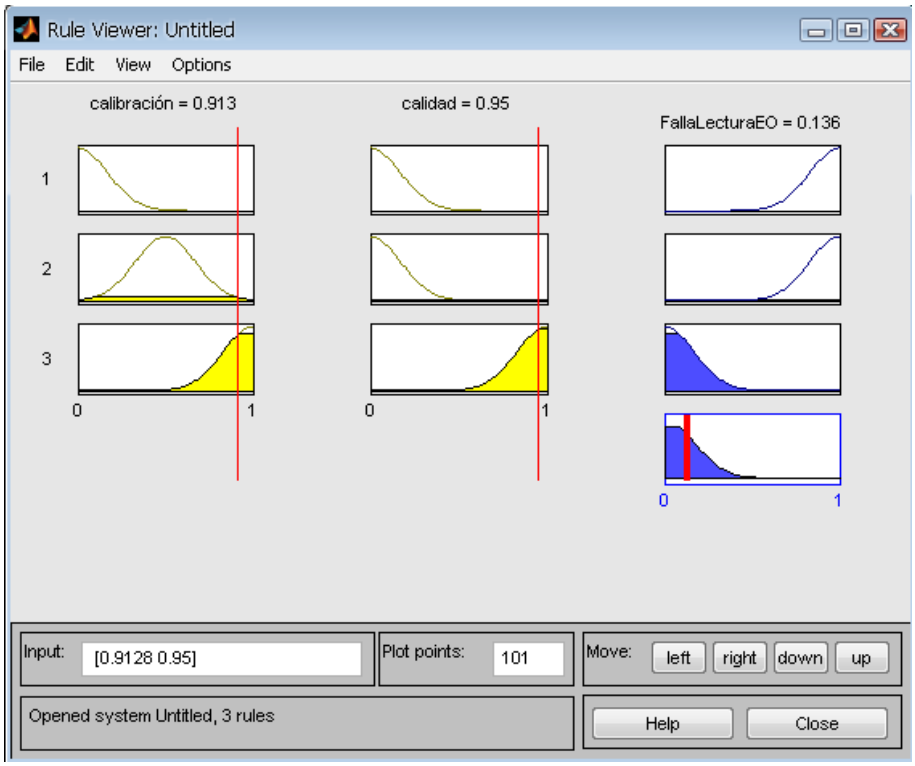


Figura B.36: Entradas y salidas del sistema

Calibracion	Calidad	FallaLecturaEO	
0.95	0.832	0.151	0.849
0.876	0.55	0.321	0.679
0.619	0.495	0.52	0.48
0.142	0.268	0.819	0.181

Tabla B.16: evento 22

Las tecnologías que realizan lectura de tarjetón a través de escáner óptico pueden presentar fallas debido a la calibración del escaner y/o la calidad del mismo. Como se explicó en la identificación de este evento inicial en el capítulo 4 del presente documento, si la calibración no se realiza adecuadamente, pueden presentarse fallas de lectura de tarjetones que incluyen: Sensado de marcas no realizadas por el elector o no sensado de marcas realizadas por el elector. La calidad de fabricación también influye en este tema, ya que si el lector óptico no ha sido probado y certificado previamente, el día del proceso puede presentar fallas.

Evento 23: **No hay retroalimentación al elector acerca de la opción de voto escogida.**

Evento 29: **Fallas en la emisión del reporte de estadísticas de votación por máquina.**
Evento 51: **Falla en el software del dispositivo de autenticación.**
Evento 52: **Fallas de comunicación entre el dispositivo de autenticación y la bd central.**

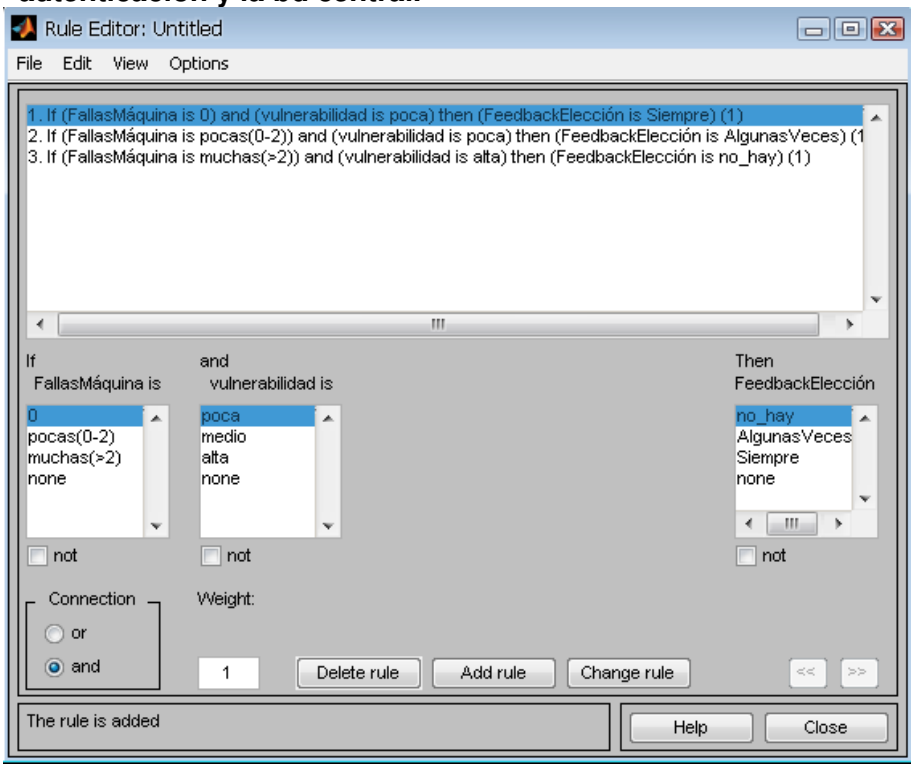


Figura B.37: Reglas para evento 23,29,51,52

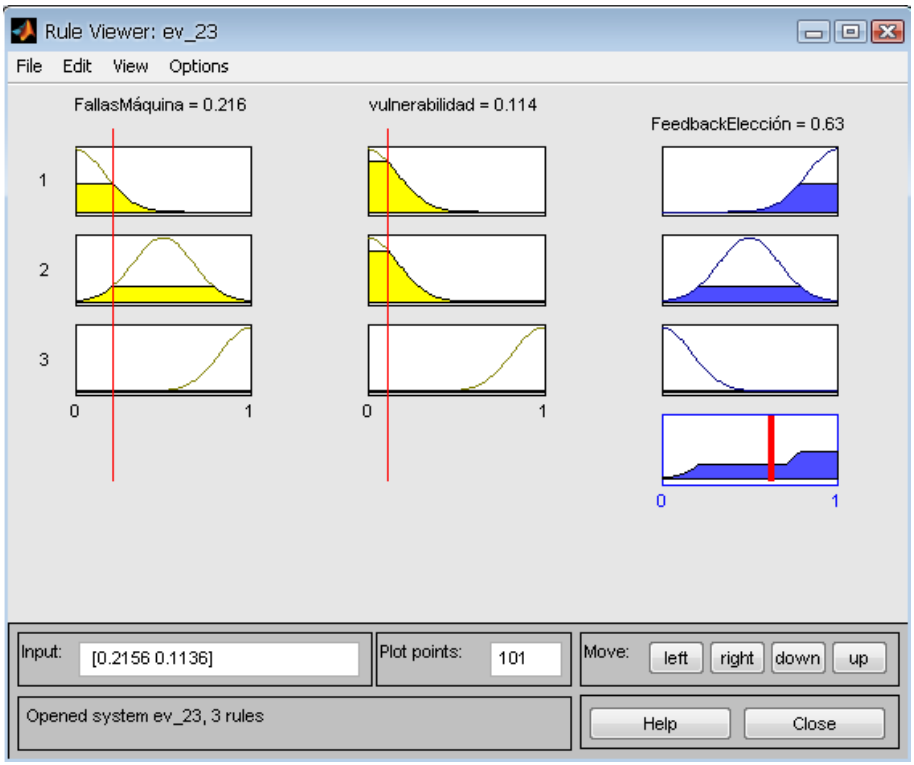


Figura B.38: Entradas y salidas del sistema

FallasMáquina	Vulnerabilidad	FeedbackMáquina	
0.95	0.832	0.149	0.851
0.876	0.55	0.311	0.689
0.619	0.495	0.5	0.50
0.142	0.268	0.653	0.347

Tabla B.17: evento 23, 29, 51,52

Los eventos de falla representados por este sistema pueden ser causados principalmente por fallas(hardware o software) o vulnerabilidad del dispositivo. Las fallas pueden ser causadas por errores en la fabricación o mala manipulación del dispositivo. Entre más vulnerable a ataques sea el dispositivo será mas probable que se presenten este tipo de fallos.

Evento 24 **: Proveedor no informa de las capacidades inalámbricas de la máquina de votación.**

Evento 26 **: Activación de capacidades inalámbricas de máquinas por parte de operario en el proceso de votación.**

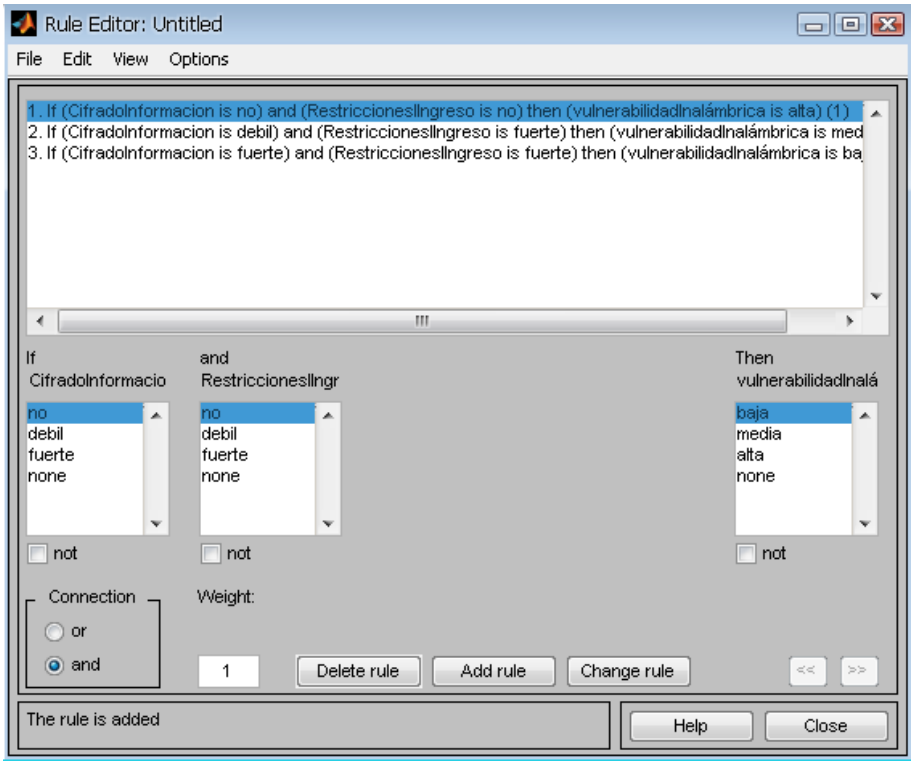


Figura B.37: Reglas para eventos 24,26

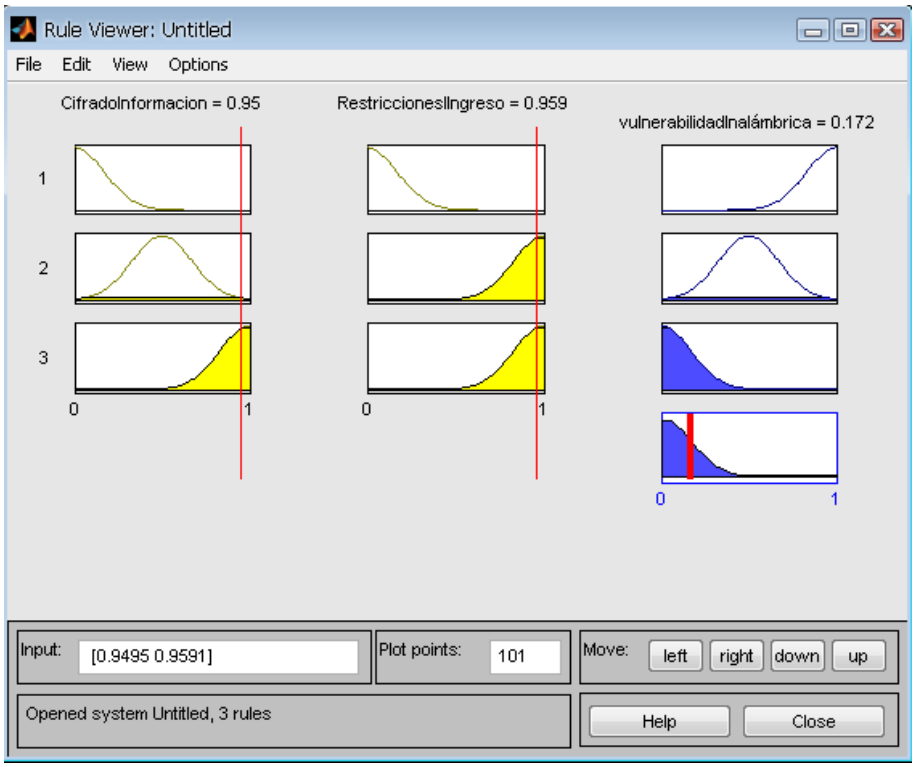


Figura B.38: Entradas y salidas del sistema

CifradoInfo	RestriccionIngreso	VulnerabilidadWireless	
0.95	0.832	0.196	0.804
0.876	0.55	0.491	0.509
0.619	0.495	0.5	0.5
0.142	0.268	0.819	0.181

Tabla B.18: evento 24,26

Entre las capacidades que normalmente tienen estos dispositivos de votación, está la de conectarse a otros dispositivos de manera inalámbrica. Esta utilidad permite al proveedor agilizar el proceso de programación y carga de configuración en gran cantidad de máquinas al mismo tiempo. Pero esta facilidad puede llegar a ser un problema si se encuentra activa en cualquier instante del proceso, ya que si no hay el adecuado control de ingreso a la máquina y además la información no se encuentra cifrada y

protegida, cualquier persona con la herramienta adecuada podría ingresar remotamente a la máquina, robar o cambiar información confidencial.

Evento 25 **: No hay control de las capacidades inalámbricas en la auditoría a máquinas de votación.**

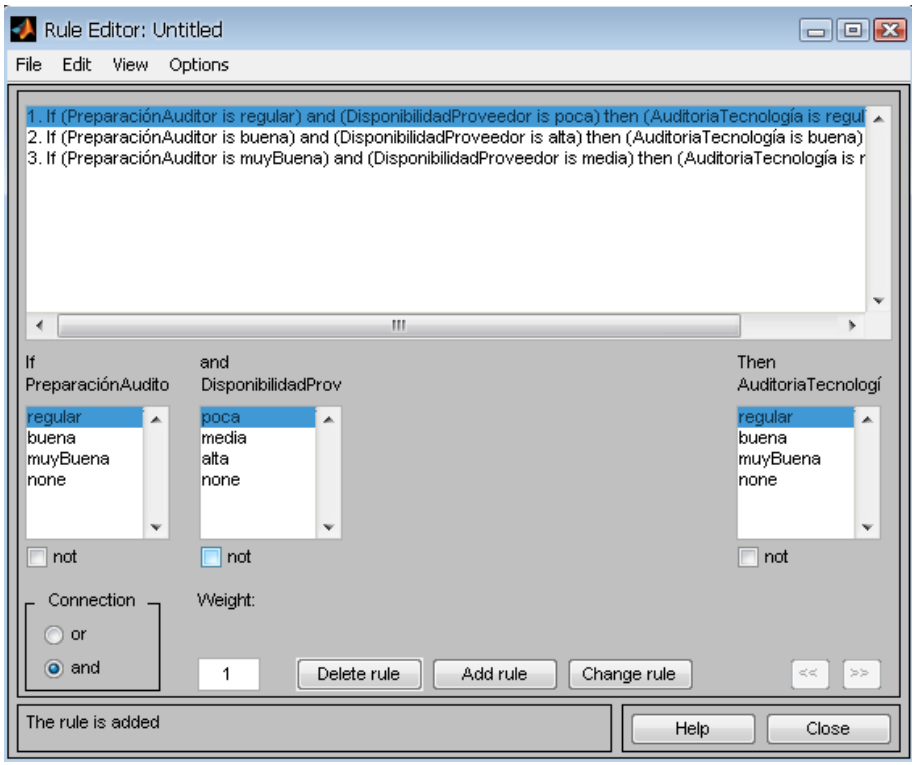


Figura B.39: Reglas para evento

25

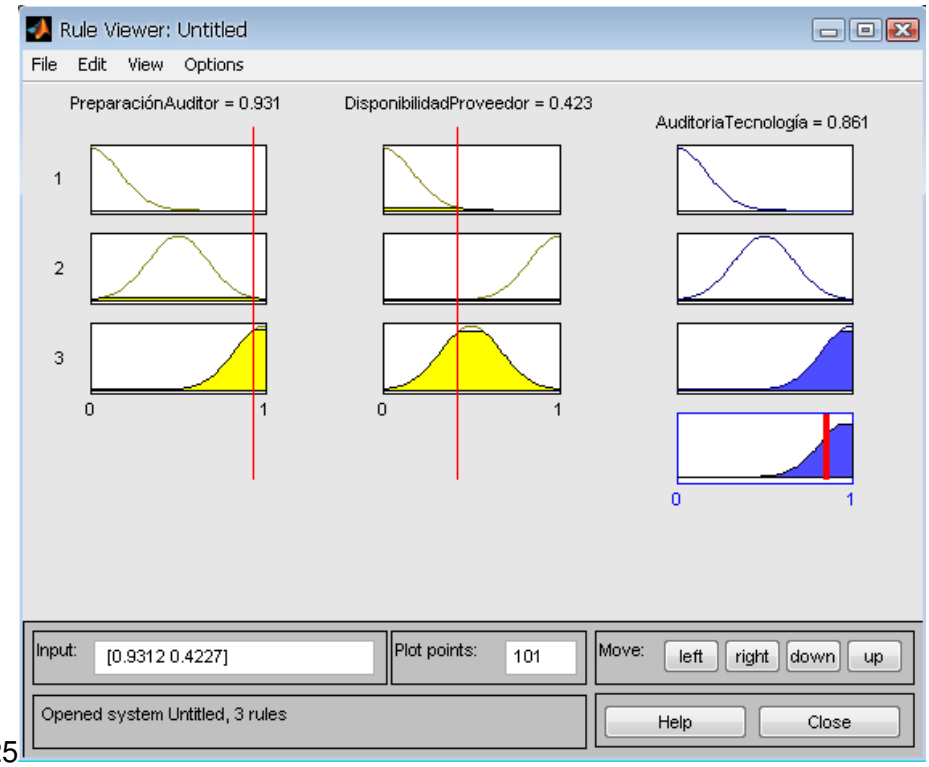


Figura B.40: Entradas y salidas del sistema

PrepAuditor	Disp.Proveedor	CalidadAuditoríaTech	
0.95	0.832	0.688	0.312
0.876	0.55	0.819	0.181
0.619	0.495	0.709	0.291
0.142	0.268	0.181	0.819

Tabla B.19: evento 25

Un auditor de tecnologías para un proceso electoral electrónico debe tener claro que las capacidades inalámbricas de las maquinas de votación deben estar totalmente deshabilitadas, vía hardware y software , preferiblemente. Para realizar esta revisión, el proveedor también debe garantizar las condiciones para esta actividad y proporcionar toda la información que el auditor solicita. Asi , se puede concluir que entre mejor sea la preparación

del auditor y la disponibilidad del proveedor para la auditoría, la calidad y resultados de esta garantizarán un buen desarrollo del proceso.

Evento 27 **: La máquina de votación no fue puesta en ceros por parte del proveedor.**

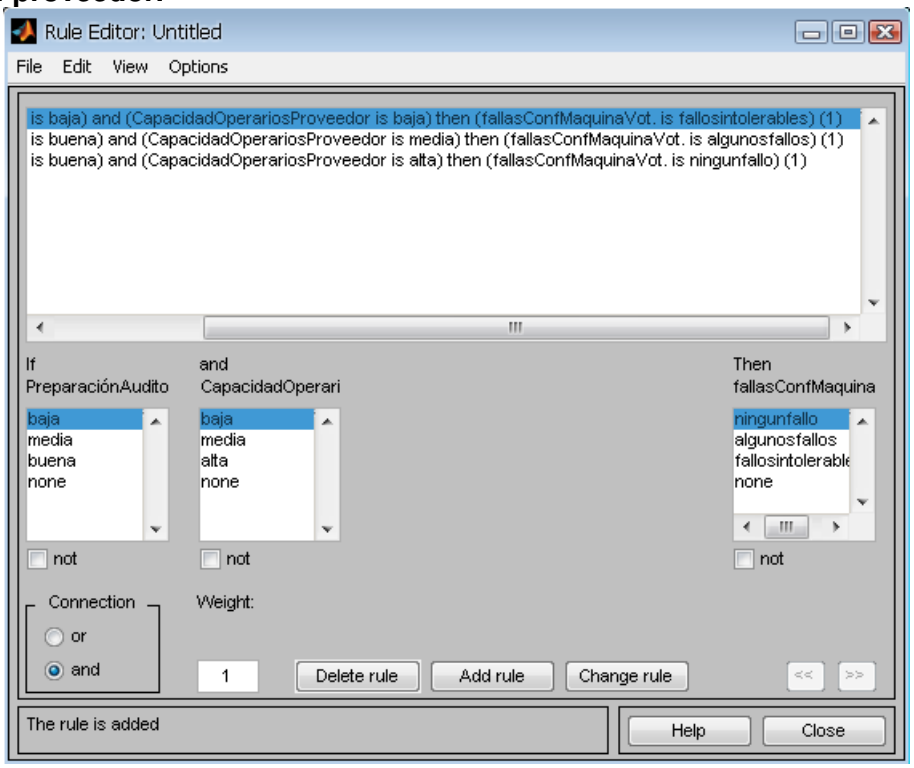


Figura B.41: Reglas para evento 27

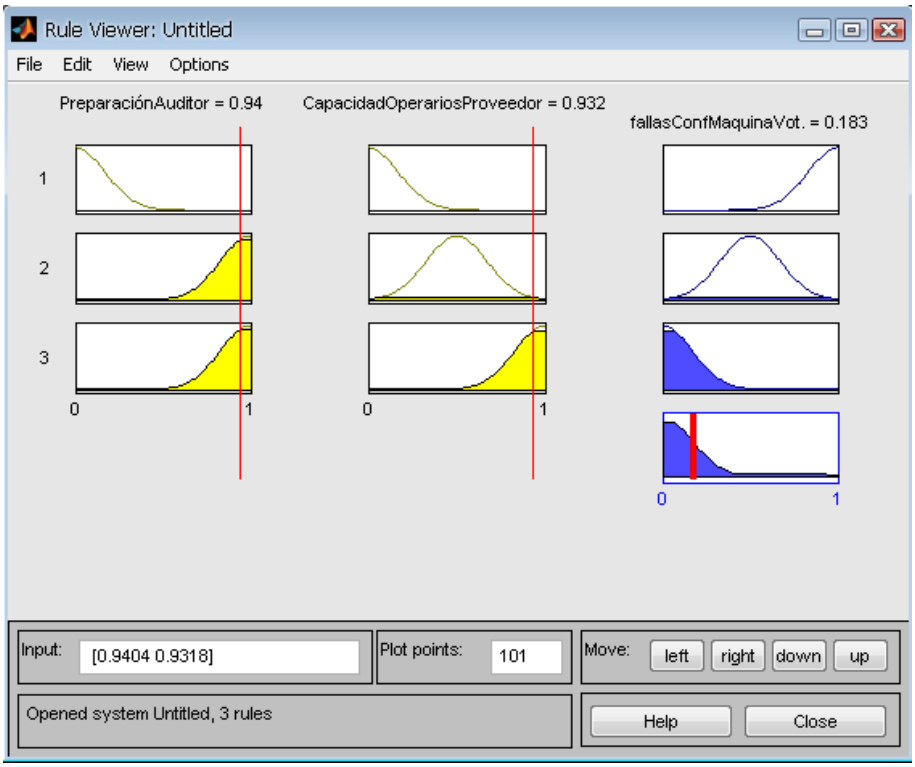


Figura B.42: Entradas y salidas del sistema

PrepAuditor	CapacidadOpPr	FallasConFMaq	
0.95	0.832	0.299	0.701
0.876	0.55	0.499	0.501
0.619	0.495	0.5	0.5
0.142	0.268	0.819	0.181

Tabla B.20: evento 27

En el proceso de congelamiento de máquinas de votación, estas son auditadas para verificar que cumplan con los requisitos establecidos y certificar que están listas para la votación. Uno de estos requisitos principales es que la base de datos que registra los votos en cada máquina, se encuentre vacía, es decir, no tenga ningún voto registrado. Para verificar esto, los auditores se valen de las evidencias que emite cada máquina. Si la máquina no se encuentra en ceros, el proveedor deberá reconfigurarla para que sea apta para el proceso. En conclusión, en la

medida en que el auditor conozca el proceso y detecte las máquinas que pueden tener errores de configuración y que los operarios (proveedor) configuren adecuadamente las máquinas, las fallas serán menos probables.

Evento 28 **: El proveedor no posee información suficiente acerca del proceso.**

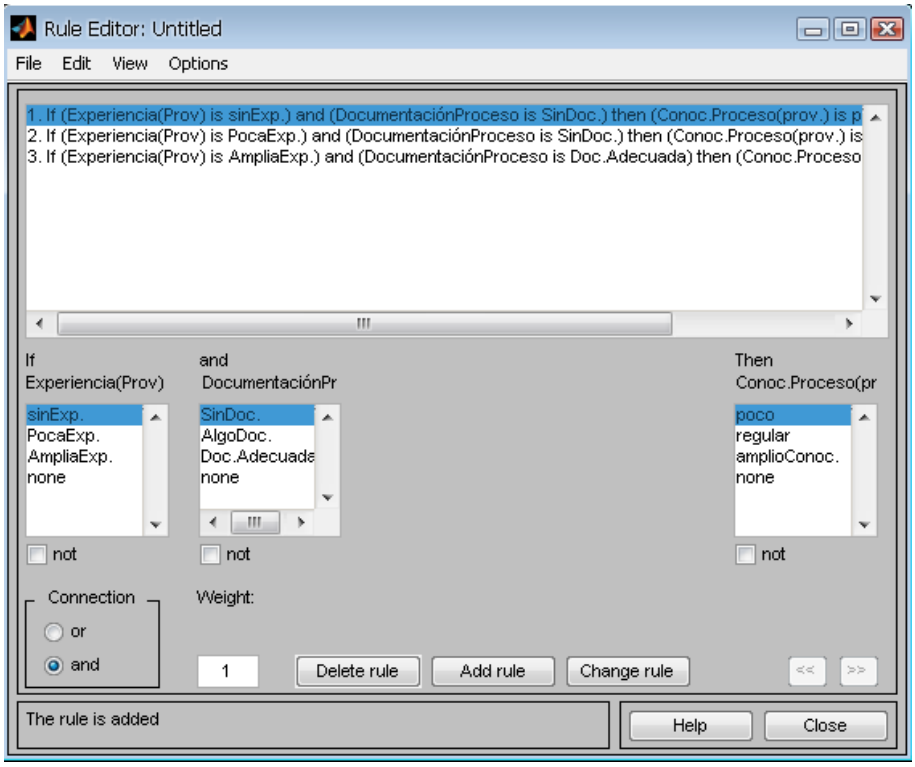


Figura B.43: Reglas para evento 28

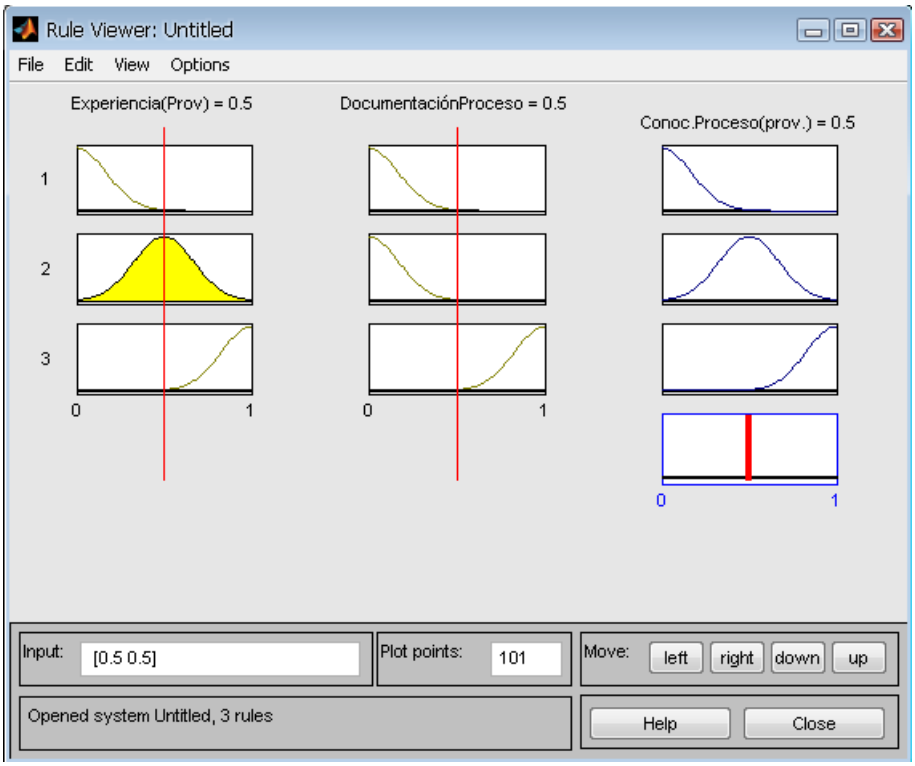


Figura B.44: Entradas y salidas del sistema

Exp.Provee	DocProceso	Conoc.Proceso(prov)	
0.95	0.832	0.848	0.152
0.876	0.55	0.678	0.322
0.619	0.495	0.5	0.5
0.142	0.268	0.35	0.65

Tabla B.21: evento 28

El conocimiento del proceso por parte de los proveedores depende principalmente de su experiencia en este tipo de actividades y de la disponibilidad de documentación del proceso a ejecutar.

Evento 30 **: El operario no conoce el funcionamiento adecuado de la máquina de votación.**
Evento 36: **Desconocimiento de las tecnologías de votación(elector).**

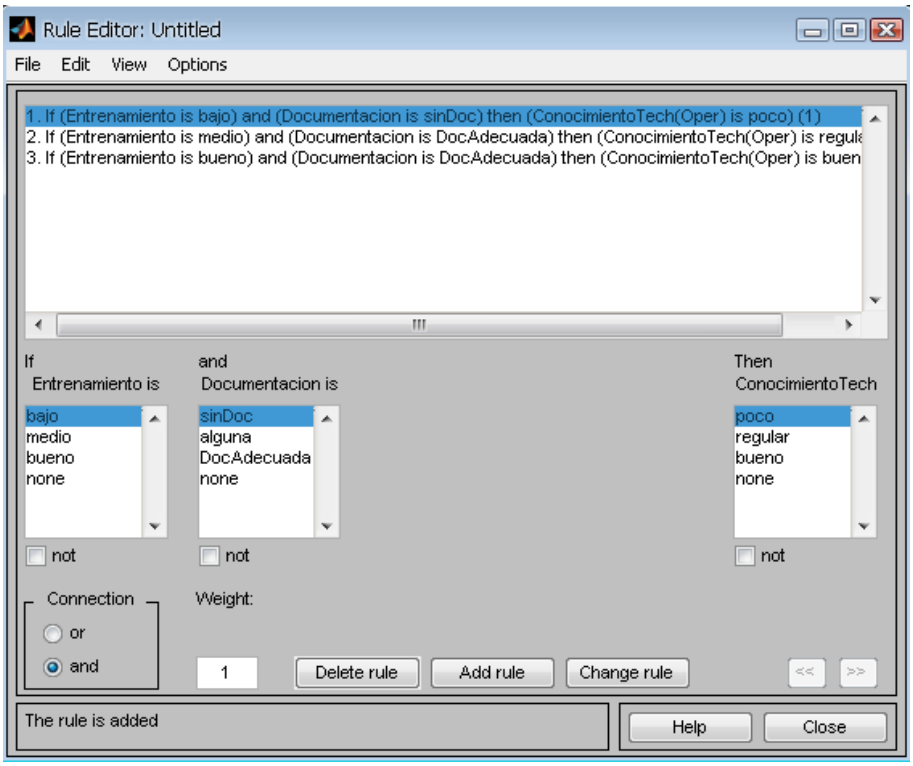


Figura B.45: Reglas para eventos 30, 36

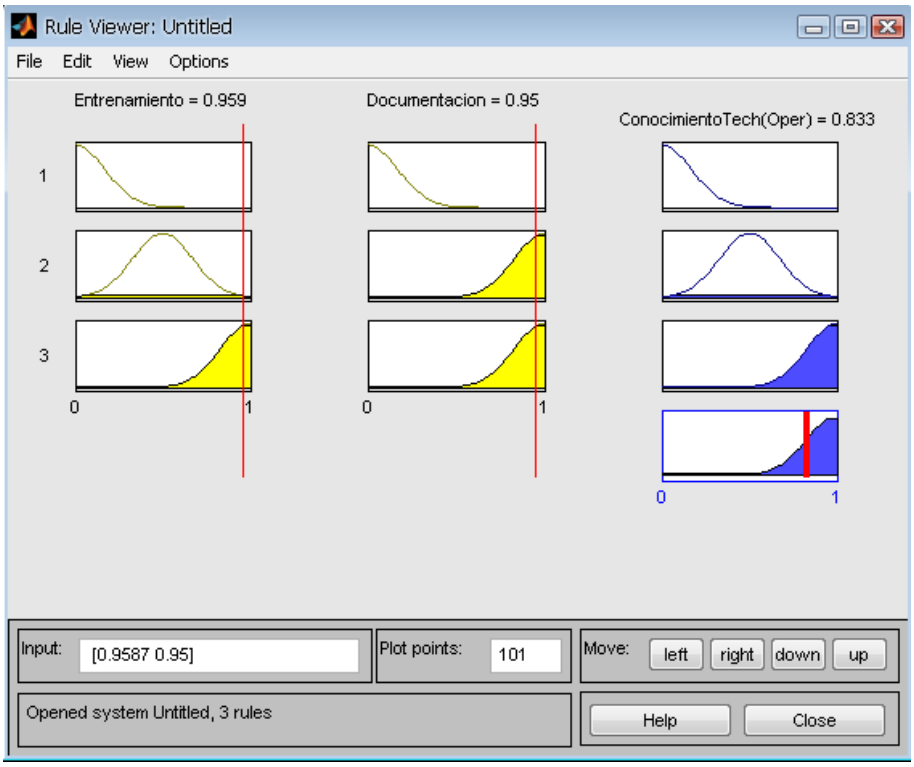


Figura B.46: Entradas y salidas del sistema

Entrenamiento	Documentación	ConocimientoTech(oper)	
0.95	0.832	0.804	0.196
0.876	0.55	0.51	0.49
0.619	0.495	0.5	0.5
0.142	0.268	0.178	0.822

Tabla B.22: eventos 30,36

Los factores que contribuyen al buen conocimiento acerca de la operación de las máquinas, tanto por operarios como por electores, son el entrenamiento en su uso y la documentación disponible.

Evento 31 **: Poca presencia de auditores.**

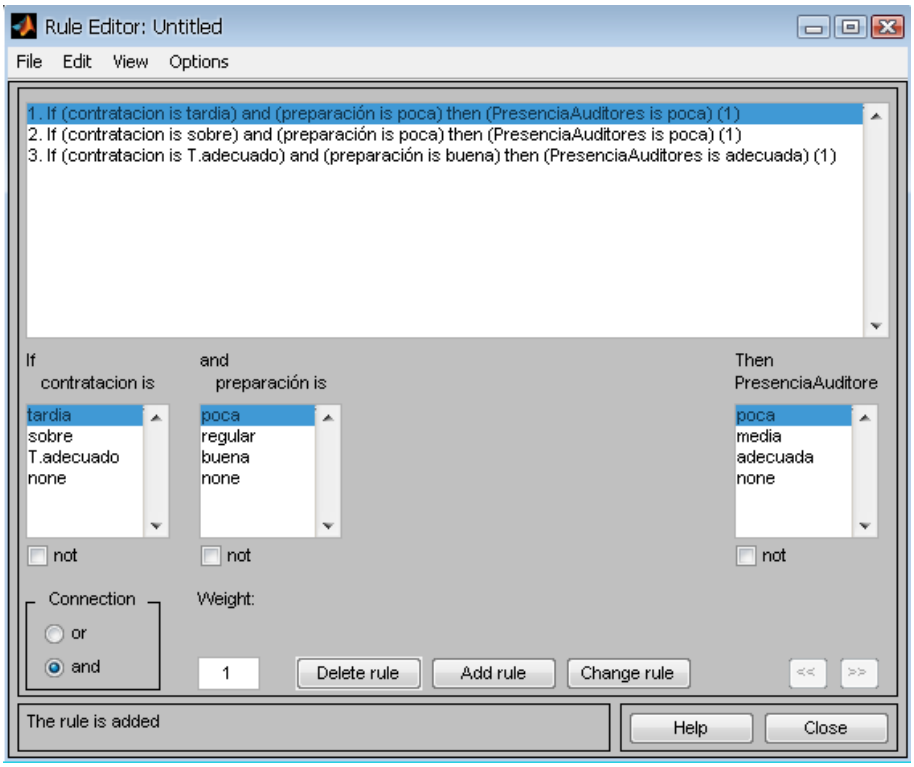


Figura B.47: Reglas para evento 31

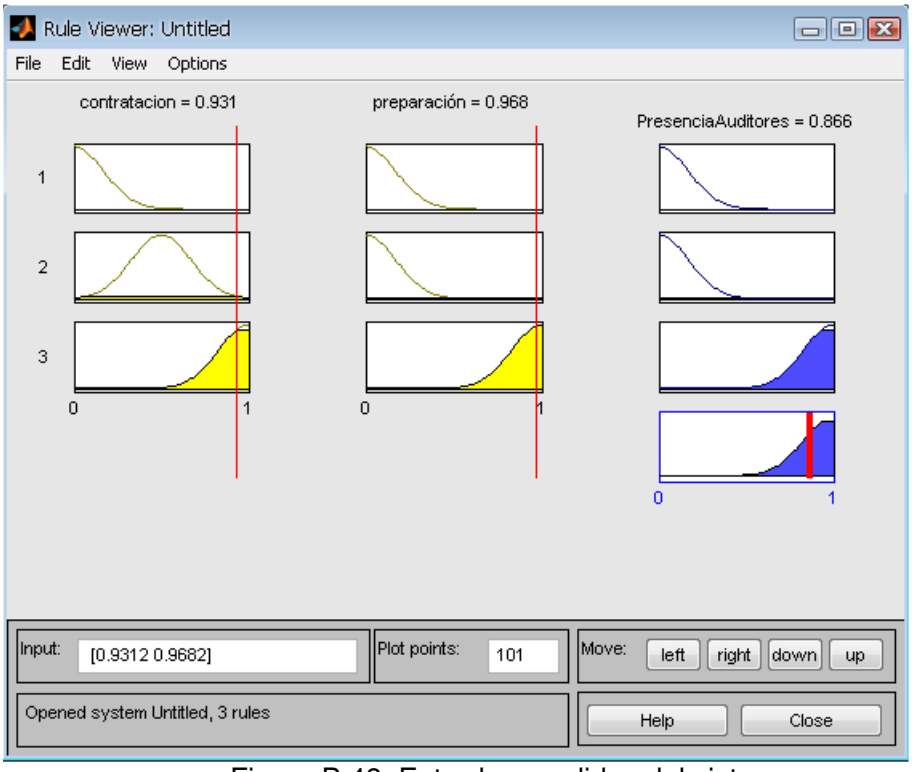


Figura B.48: Entradas y salidas del sistema

Contratación	PreparacionAuditor	PresenciaAuditores	
0.95	0.832	0.849	0.151
0.876	0.55	0.679	0.321
0.619	0.495	0.48	0.52
0.142	0.268	0.181	0.819

Tabla B.23: evento 31

La contratación de los auditores y su preparación para el proceso son variables que pueden influir en la presencia de los mismos durante el proceso. Si la contratación se realiza a tiempo y los auditores contratados realizan una buena preparación para auditar el proceso, su presencia será permanente y acertada. De lo contrario, si los auditores no son contratados a tiempo y no conocen el proceso, puede que no se presenten por temor a no poder cumplir bien su tarea.

Evento 32: **Poca presencia de veedores.**

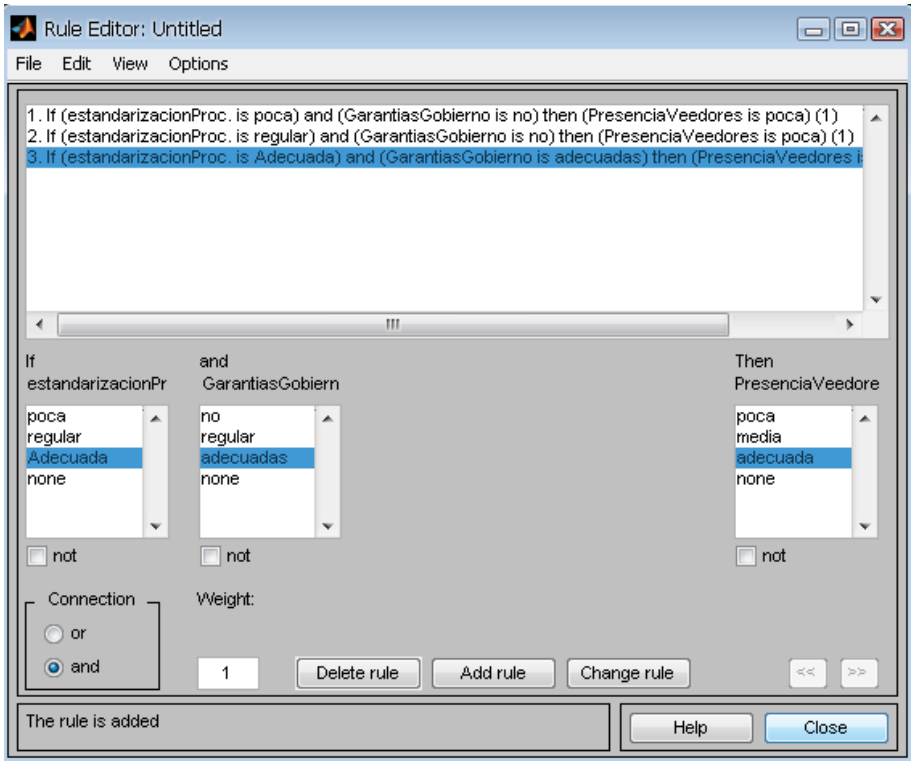


Figura B.49: Reglas para evento 32

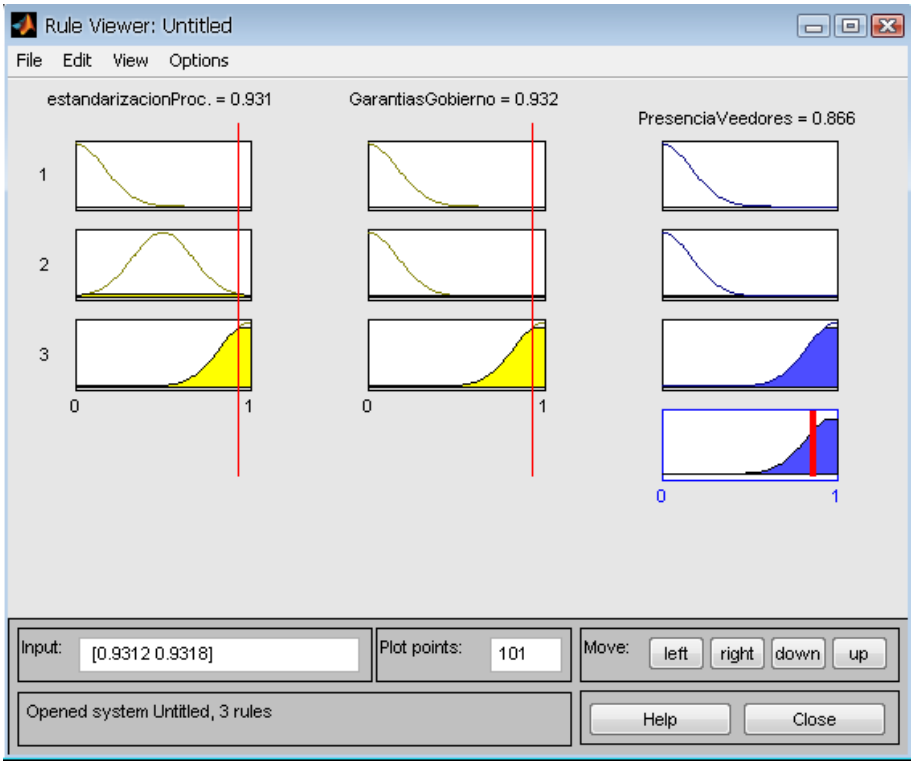


Figura B.50: Entradas y salidas del sistema

estandarizacionProc	GarantíasGob	PresenciaVeedores	
0.95	0.832	0.849	0.151
0.876	0.55	0.679	0.321
0.619	0.495	0.48	0.52
0.142	0.268	0.181	0.819

Tabla B.24: evento 32

Los veedores del proceso electoral juegan un papel muy importante ya que garantizan la transparencia de las votaciones, permitiendo conformidad de todas las partes. Los factores que pueden influir en la presencia de los

veedores son la estandarización de procesos y las garantías que brinde el gobierno y la organización electoral para que los veedores puedan cumplir su función. Si los procesos no han sido estandarizados, es decir, no son conocidos por todas las partes, o el gobierno no brinda las condiciones necesarias para la actividad de los veedores, estos no podrán hacer parte del proceso.

Evento 33 **: Información de votación no cifrada o cifrado débil.**
Evento 34 **: Passwords de usuario débiles.**
Evento 35 **: No hay segregación de funciones.**
Evento 48 **: Brecha de seguridad en el software de votación.**
Evento 49 **: Código malicioso bloquea la máquina de votación.**
Evento 50 **: Máquina no realiza copia periódica de seguridad de la información de votación.**

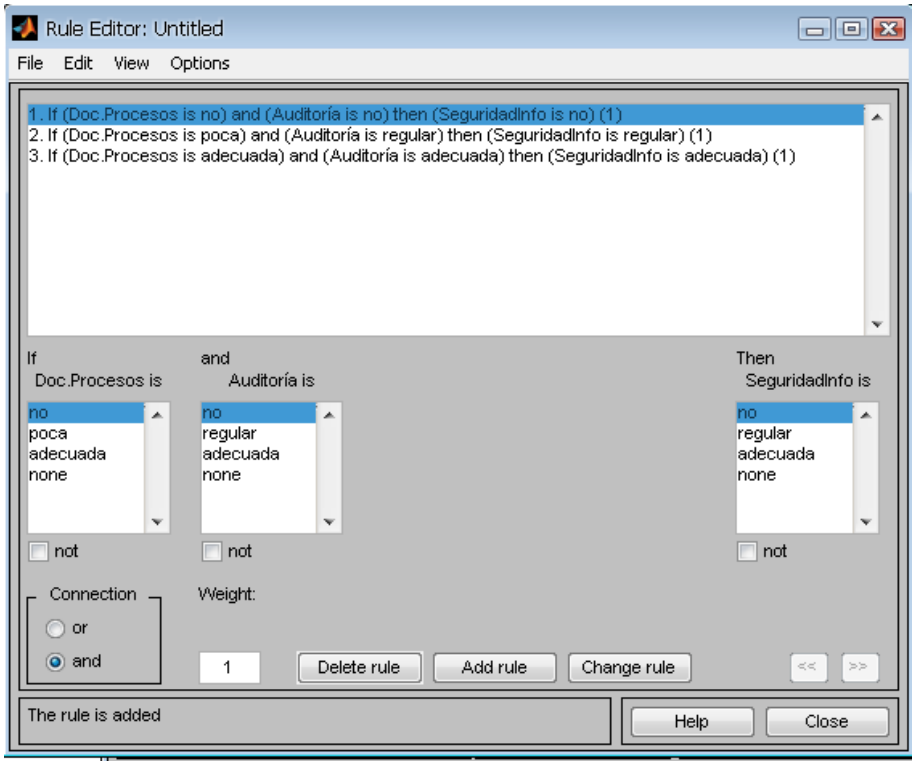


Figura B.51: Reglas para eventos 33,34,35,48,49,50,56

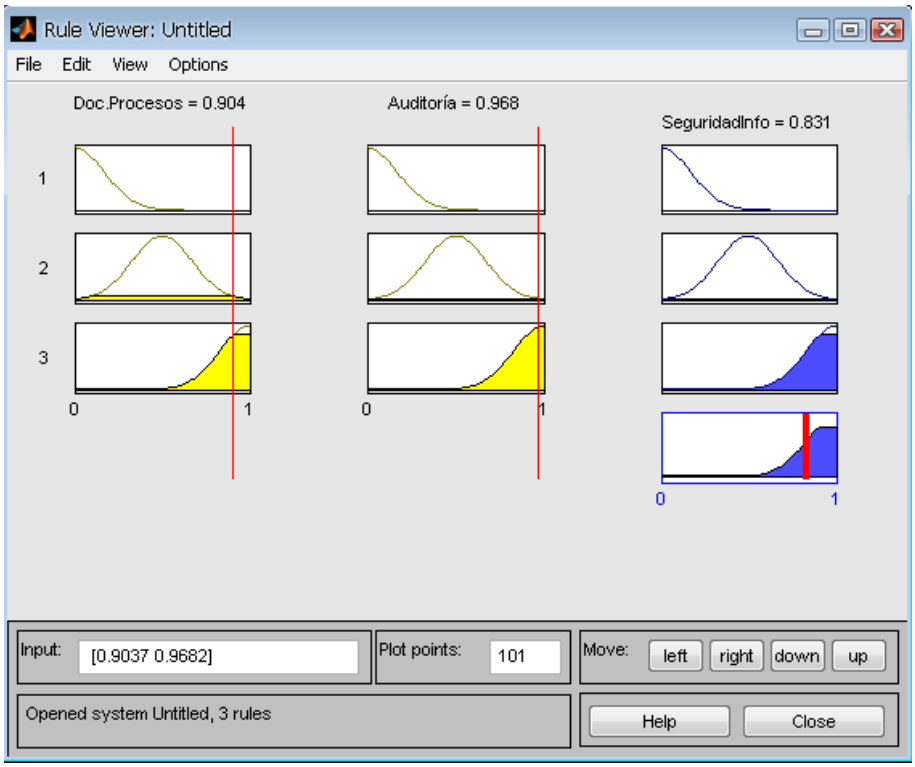


Figura B.52: Entradas y salidas del sistema

DocProcesos	Auditoría	SeguridadInfoVot	
0.95	0.832	0.804	0.196
0.876	0.55	0.502	0.498
0.573	0.905	0.511	0.489
0.142	0.268	0.349	0.651

Tabla B.25: eventos 33, 34, 35, 48, 49, 50,56

Los eventos iniciales representados en este sistema hacen parte de los tópicos que los auditores deben revisar en cumplimiento de su función. Si el auditor revisa adecuadamente estos temas de seguridad y además los procesos están documentados, se puede garantizar que habrá gran probabilidad de brindar seguridad al proceso de votación.

Evento 37 : **Desconfianza en las políticas del gobierno.**

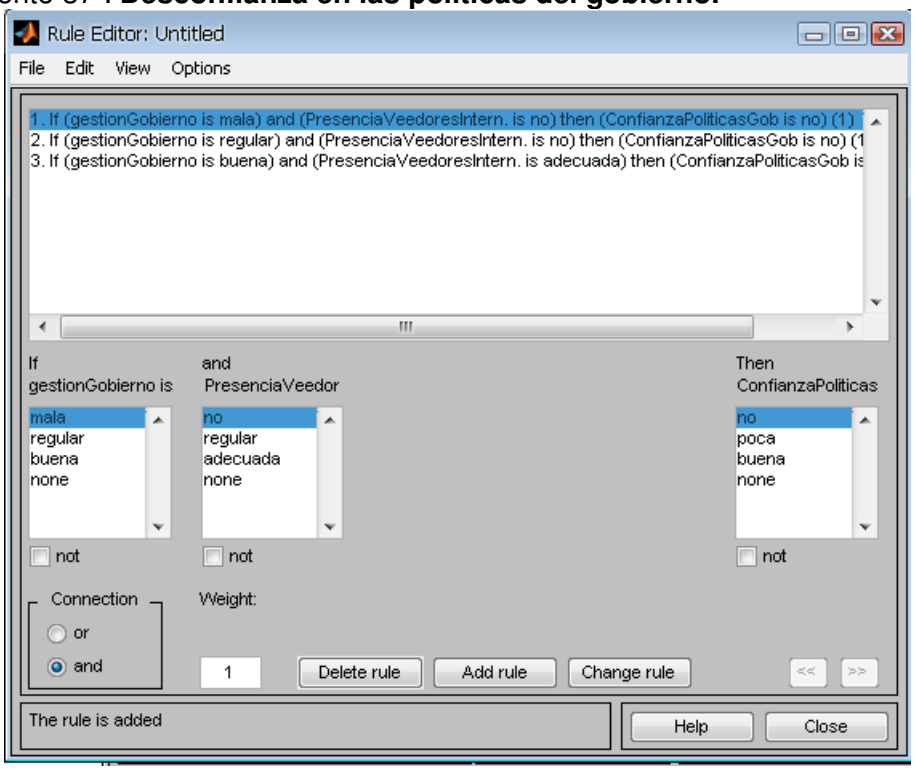


Figura B.53: Reglas para evento 37

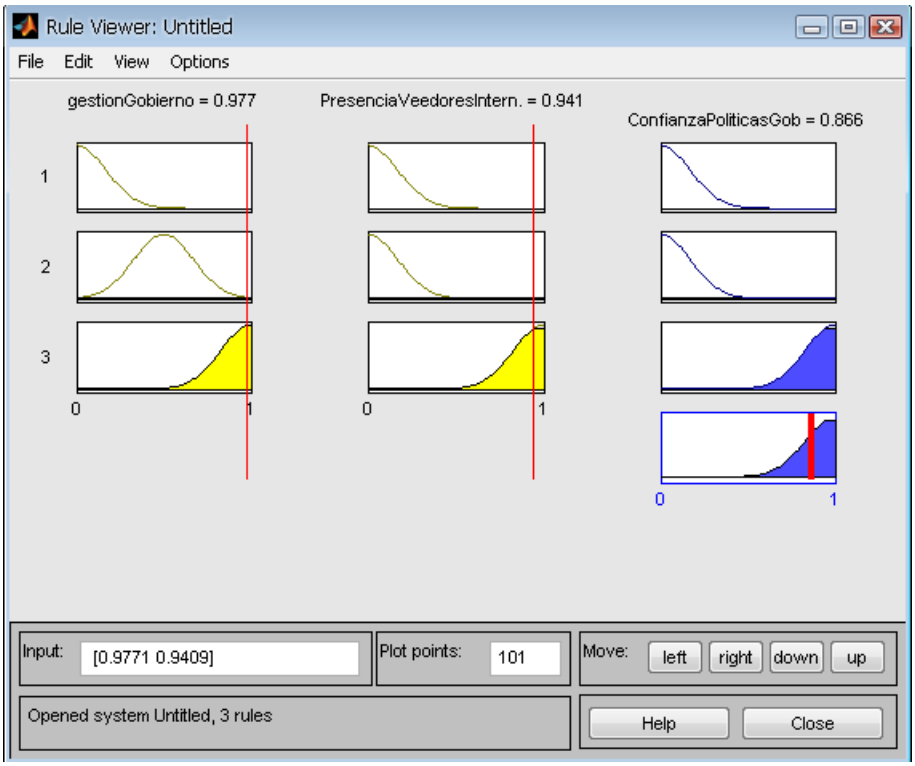


Figura B.54: Entradas y salidas del sistema

GestionGobierno	VeedoresInternacionales	ConfianzaGobierno	
0.95	0.832	0.849	0.151
0.876	0.55	0.679	0.321
0.619	0.495	0.48	0.52
0.142	0.268	0.181	0.819

Tabla B.26: evento 37

Entre los muchos factores que influyen en el grado de confianza de la ciudadanía en la gestión del gobierno y por ende la confianza en el proceso electoral, se encuentran la gestión que este haya desarrollado y las garantías que brinde a veedores nacionales e internacionales para su presencia en el proceso electoral.

Evento 39 : **Circuito de votación no demarcado correctamente.**
Evento 40 : **Poca presencia de encargados de vigilar que los votantes ingresen a la máquina de votación adecuadamente.**
Evento 41 : **Insuficiente cantidad de personal de seguridad.**

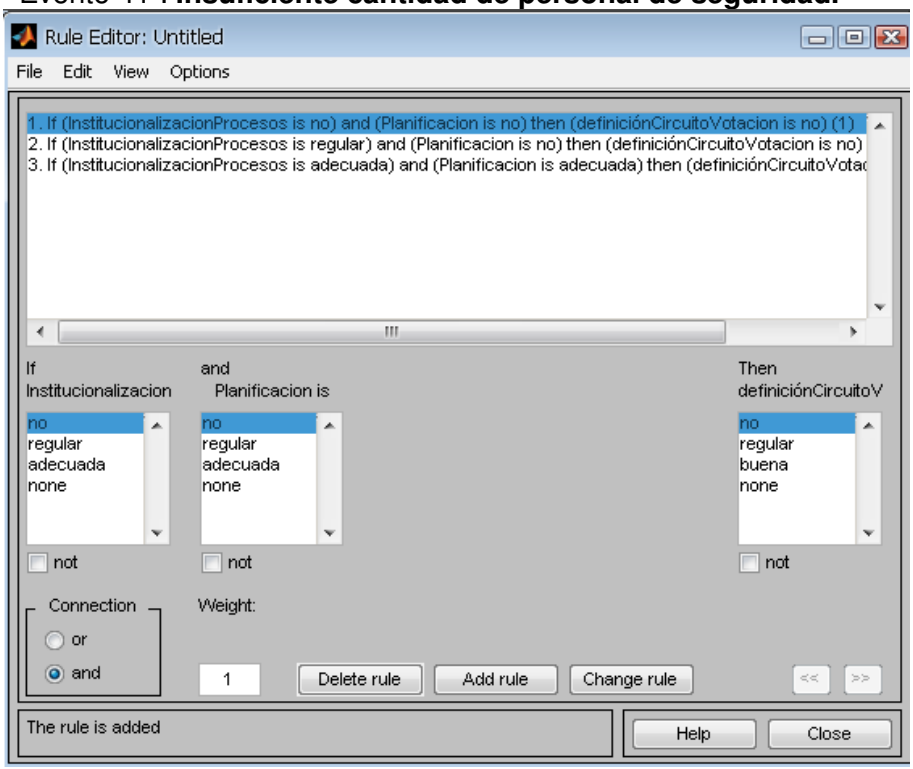


Figura B.55: Reglas para eventos 39,40,41

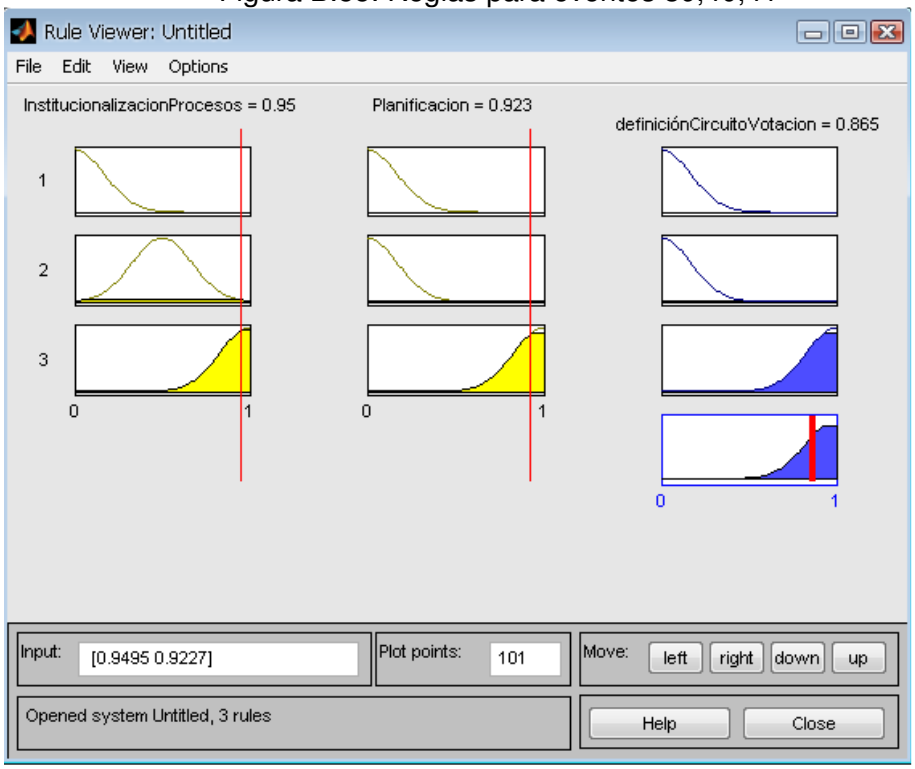


Figura B.56: Entradas y salidas del sistema

InstitucionalizacionProce.	Planificacion	DefiniciónCircuitoVotacion	
0.95	0.832	0.849	0.151
0.876	0.55	0.679	0.221
0.619	0.495	0.48	0.52
0.142	0.268	0.181	0.819

Tabla B.27: eventos 39,40,41

Los eventos 39,40 y 41 se pueden presentar generalmente por la falta de institucionalización de los procesos que componen la votación electrónica y por la falta de planificación adecuada de la jornada electoral. Si se lleva a cabo un buen plan de institucionalización de procesos, jornadas de capacitación y un plan de gestión del proceso electoral, la probabilidad de ocurrencia de estos eventos será casi nula.

Evento 55 : **Cédula falsa**

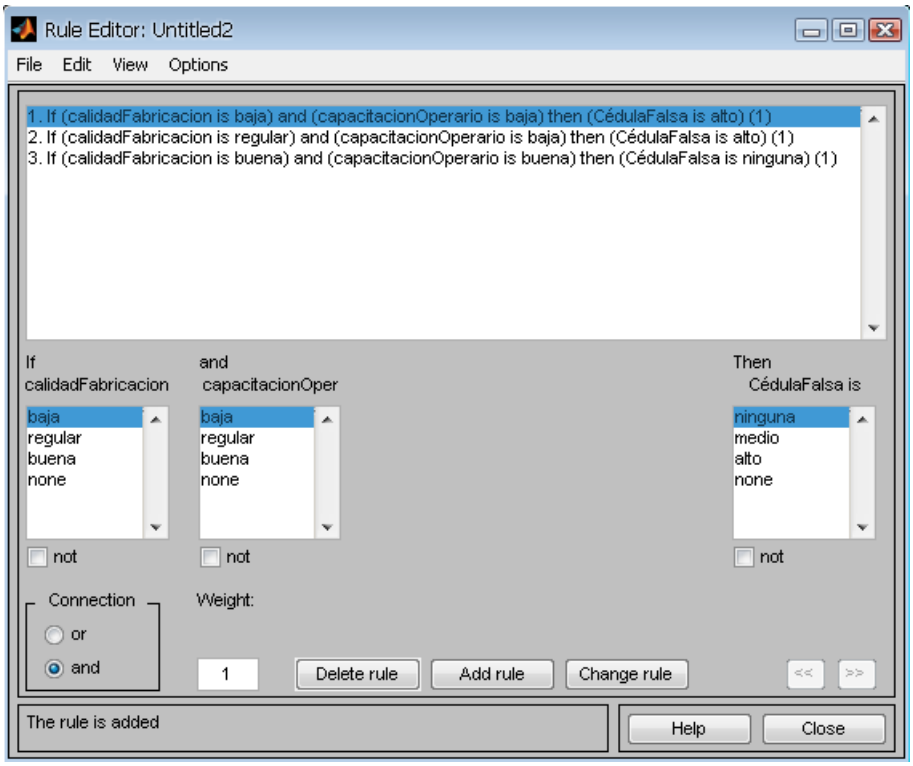


Figura B.57: Reglas para evento 55

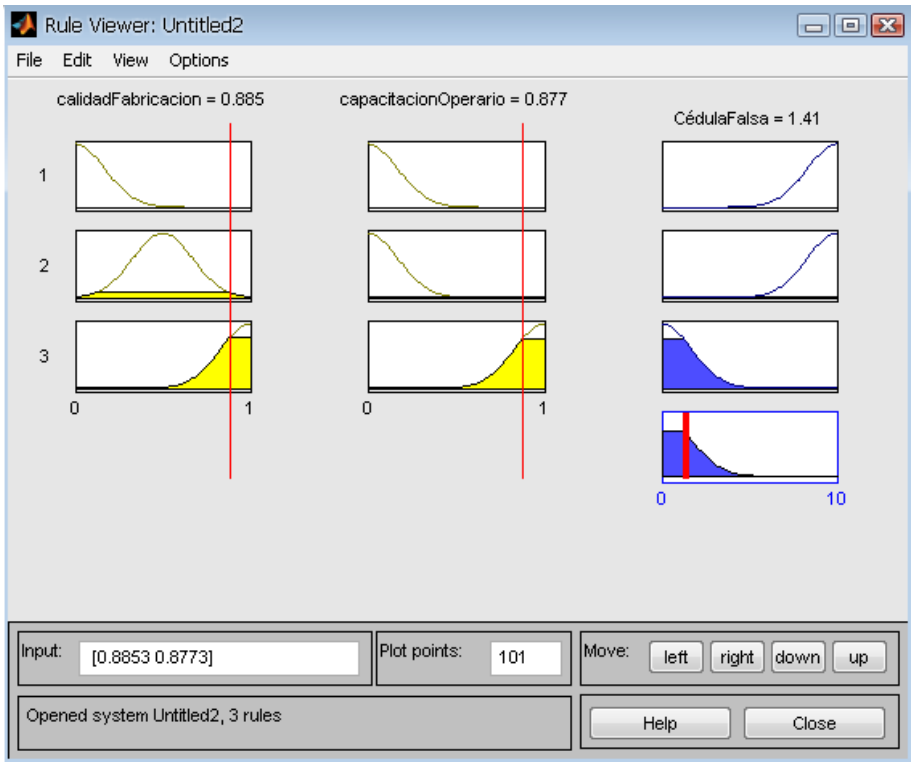


Figura B.58: Entradas y salidas del sistema

Calidad	CapacitacionOper	CédulaFalsaEnProceso	
0.95	0.832	0.151	0.849
0.876	0.55	0.321	0.679
0.619	0.495	0.52	0.48
0.142	0.268	0.819	0.181

Tabla B.30: evento 55

La recedulación que se está llevando a cabo en estos momentos en el país está encaminada a la disminución de la falsificación de los documentos de identidad. Para esto se implementaron estrategias de seguridad y calidad para hacer mas difícil la tarea de falsificación. Además de lo anterior, los jurados de mesa y específicamente los encargados de la autenticación de los electores deben conocer detalladamente las características de la cédula, de tal forma que sean capaces de identificar a simple vista, cuando una cédula no es legítima. Si el operario no detecta la cédula falsa, se espera que el dispositivo de autenticación lo haga. En conclusión, si hay buena calidad y seguridad en la fabricación de las cédulas y además existe capacitación a los funcionarios, se podrá evitar el ingreso de votantes con documento falso.

Evento 56 : **Intrusión en la red de datos**

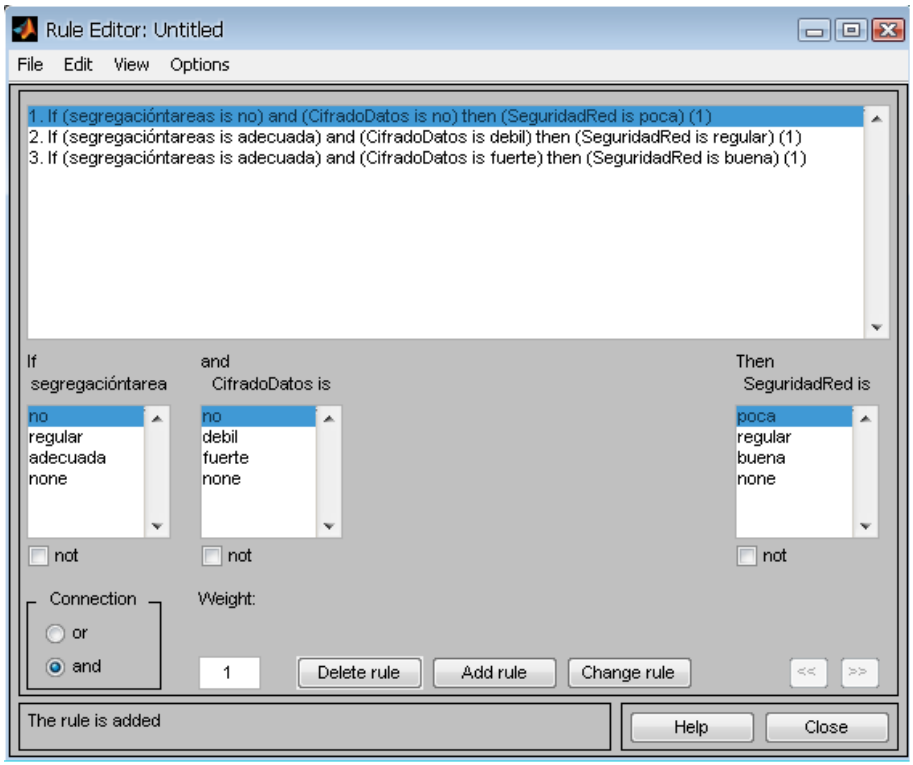


Figura B.59: Reglas para evento 56

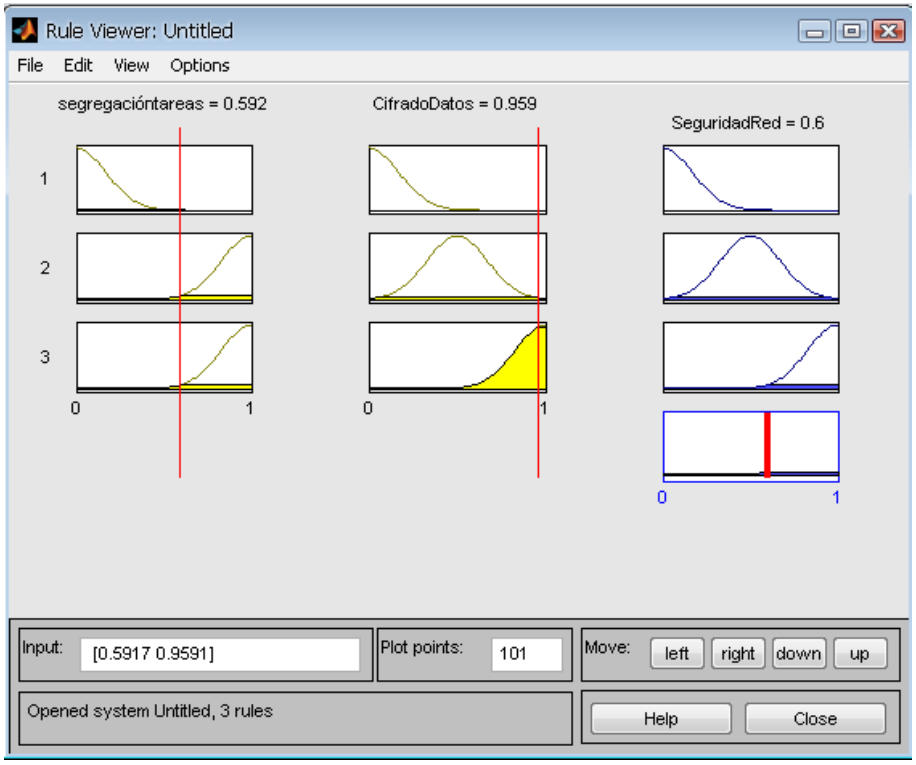


Figura B.60: Entradas y salidas del sistema

Segregaciontareas	CifradoDatos	Seguridadred	
0.95	0.832	0.701	0.299
0.876	0.55	0.501	0.499
0.619	0.495	0.5	0.5
0.142	0.268	0.181	0.819

Tabla B.31: evento 56

El evento 56 se relaciona principalmente con la seguridad de las redes de telecomunicaciones. Una intrusión se considera al evento en el que un ente no autorizado ingresa a la red a través de métodos fraudulentos, para sabotear, robar o modificar la información existente. La seguridad comprende muchos aspectos, pero se consideró que la adecuada segregación de tareas dentro del proceso y el cifrado fuerte de datos inciden de manera directa en la ocurrencia de este evento.

ANEXO C: AMENAZAS IDENTIFICADAS PARA LA PRUEBA PILOTO DE VOTO ELECTRÓNICO Y MATRIZ DE RIESGOS

AMENAZA 1: MANIPULACION NO AUTORIZADA DEL CÓDIGO DE LA TERMINAL DE VOTACIÓN.

En la etapa de programación de las terminales de votación, se puede presentar el caso que un operario o programador, de forma accidental o intencional manipule el código para que realice cualquiera de las siguientes actividades:

- Guardar un voto diferente al mostrado al elector en la pantalla. Esta actividad la puede hacer de forma aleatoria o frecuente.
- Modificar los votos guardados o el número total de votos.
- Hacer que la máquina se vuelva inoperable y quede fuera de servicio.
- Contar votos que no provienen de electores legítimos.
- Consolidar total de votos antes de la autorización para esta actividad.
- Modificar las evidencias de auditoría de la máquina.
- Identificar los votos emitidos por ciertos electores, con o sin su complicidad.
- Causar el registro incorrecto de votos, ya sea de forma aleatoria o siguiendo algún tipo de lógica para beneficiar o perjudicar a algún candidato.
- Cambiar la programación del tarjetón.

Controles preventivos:

- Creación de políticas y procedimientos para asegurar que el control de la programación de las máquinas no recaiga sobre una sola persona. Para que el control sea efectivo, las personas encargadas (dos o más) de la programación deben ser capaces de entender el proceso y detectar fallas. Si las personas solo se encargan de observar o vigilar pero no entienden el proceso, el control pierde efectividad. Por lo tanto, todas las personas

deben estar igualmente capacitadas e informadas de la actividad que realizan.

- También se deben hacer pruebas al código fuente (pruebas abiertas y pruebas paralelas).

Control detectivo: Un control detectivo es que la máquina de votación emita certificado de votación y permita un escrutinio posterior. Como su nombre lo dice, al ser un control de este tipo, indica que la amenaza se materializó y se deben tomar acciones correctivas.

AMENAZA 2: IMPLANTACIÓN DE VIRUS EN LOS SERVIDORES DE CONSOLIDACIÓN.

Código malicioso de diferentes tipos puede ser introducido en los servidores de consolidación antes y durante el proceso. Por ejemplo, troyanos, pueden ser implantados en los servidores de consolidación de alguna de estas dos formas:

- En lazo cerrado o código autocontenido que no requiere entradas adicionales para ejecutar sus tareas.

- En lazo abierto, el cual crea un canal de comunicación que puede ser usado luego para aceptar entradas adicionales (comandos, scripts) para alterar el sistema operativo, las aplicaciones o aceptar algún otro código malicioso. El lazo abierto es también conocido como 'puerta trasera' y es creado frecuentemente por miembros del equipo de programación para ingresar al sistema en un futuro.

Un virus puede ser colocado en el código fuente del servidor de tal forma que sea muy improbable su detección. El virus puede ser diseñado para activarse en momentos específicos y desactivarse cuando pueda ser detectado, como por ejemplo en las pruebas al sistema. Una vez lanzado el ataque, virus podría modificar la base de datos del servidor de forma directa o interceptar la comunicación entre la memoria y la base de datos y alterar los totales de votación. También podría realizar acciones de 'limpieza' en el servidor, como por ejemplo, alterar los registros de auditoria, registros de tiempo, registros de operaciones, para encubrir sus propias actividades. También podría reescribir la tarjeta de memoria. Por eso es necesario establecer varios mecanismos de registro oficial de votos, además del uso de las memorias.

Controles preventivos: Se pueden implementar los siguientes controles con miras a evitar la materialización de esta amenaza.

- Realizar simulaciones del funcionamiento de los servidores de consolidación y realizar rigurosos análisis estadísticos.

- Redundancia en servidores de consolidación, preferiblemente en sitios diferentes para comparar resultados.

- Utilizar herramientas tradicionales de seguridad en el servidor y políticas de acceso.

- Monitorear el funcionamiento del servidor a través de software de administración para conocer el estado del mismo en cualquier instante.

- Inhabilitar todos los canales de comunicación del servidor, remover adaptadores de red y cualquier conexión externa con las máquinas de votación, hasta el momento que se vaya a realizar la transmisión de los datos.

AMENAZA 3: COMPRA DE VOTOS A TRAVÉS DE CADENAS DE VOTACIÓN.

Esta amenaza es aplicable a los sistemas de votación que todavía emplean tarjetones para realizar la elección, como por ejemplo los de lectura óptica. La persona interesada en realizar esta actividad la puede iniciar, robando un tarjetón válido, antes de las elecciones o falsificándolo. El día de la elección, marca el tarjetón con el candidato de su preferencia, y compra el voto a cualquier elector que esté dispuesto a venderlo. El perpetrador, da el tarjetón marcado al elector y este se dirige al sitio de votación. En la caseta donde el elector está solo, marcando el tarjetón, este lo cambia por el previamente marcado y lo deposita en la urna. Cuando sale del sitio de votación, entrega el tarjetón en blanco al perpretador y recibe su pago. Así sucesivamente se pueden comprar los votos.

Controles preventivos:

- **Seguridad en la distribución de los tarjetones:** Los tarjetones impresos deben ser estrictamente contados, con el requisito que los sobrantes, al final de la jornada sean destruidos. Deben asignarse observadores en todas las etapas por las que pasan los tarjetones para evitar irregularidades. Instantes antes de iniciar la votación, los jurados deben verificar que el número de tarjetones recibidos concuerda con los programados para esa mesa de votación.
- **Prevenir la falsificación de los tarjetones:** Uso de papeles y tintas especiales para evitar la falsificación.
- **Marcar los tarjetones con seriales únicos:** Cuando el elector se identifica para votar ,el número del tarjetón debe ser grabado. Cuando el votante retorna el tarjetón para introducirlo en la urna, el número debe ser chequeado para verificar que sea el mismo tarjetón. Para proteger la privacidad del votante, el voto debe introducirse en un sobre que permite visualizar solo el número de serie. Cuando el voto vaya a ser emitido, este número debe ser retirado del tarjetón para evitar cualquier asociación del voto con su emisor.

AMENAZA 4: FALLAS EN LA CALIBRACIÓN DEL ESCANER ÓPTICO

Los sistemas de lectura óptica de votos, poseen un umbral de sensado, esto quiere decir que las marcas en los tarjetones que son más oscuras que el umbral del escáner son consideradas como votos. Las que sean menos oscuras que el valor umbral, no serán contadas como votos. Este valor umbral es variable.

El sensor del escáner puede ser calibrado de tal forma que solo acepte marcas bastante oscuras o que acepte hasta la marca más débil. Calibrar el escáner significa establecer umbrales de detección de las marcas de los tarjetones de votación de tal forma que los votos sean contados de acuerdo a lo que establece la ley. Idealmente, todos los escaners utilizados para una votación deben aplicar el mismo estándar que es comparable a una o varias personas examinando los tarjetones de votación para determinar si la marca realizada en él es un voto o no. Los extremos en la calibración de los escaners son perjudiciales. Si se coloca un umbral muy sensible al escáner, este contará puntos, manchas y hasta motas de polvo como votos efectivos. Por otro lado si el umbral del escáner es poco sensible, entonces dejará de contar votos válidos.

La amenaza que genera la mala calibración o la calibración deliberada de un escáner es que los resultados de las votaciones no reflejarán la realidad de la intención de voto y creará confusión. En este tipo de evento es más difícil manipular votos cambiándolos de un candidato a otro, porque el escáner no es inteligente, pero si generará votos o presentará errores donde no los hay.

Controles preventivos:

Realizar pruebas a los escáneres en los siguientes escenarios:

Escanear varios tarjetones marcados correctamente, esto es para verificar que el dispositivo cuenta de manera correcta. Luego escanear varios tarjetones que se hayan marcado con otro tipo de lapicero diferente al obligatorio y que sea de uso común entre la gente. Finalmente, incluir tarjetones que estén a medio marcar, con marcas muy pequeñas y que puedan generar dudas en la intención de voto. Este último escenario se realiza para conocer el estado de calibración del escáner ya que lo que más interesa es que tan bien el sistema captura la intención de voto de los electores y no que tan bien cuenta los tarjetones que han sido correctamente marcados.

AMENAZA 5: CALIBRACIÓN DE LA PANTALLA TACTIL.

La amenaza que introduce la pantalla táctil se debe a su naturaleza y diseño. Las pantallas tactiles están conformadas además por otra pantalla que despliega la información, esto quiere decir que el usuario final al utilizar una pantalla táctil o touch screen realmente no entra en contacto con la pantalla sensible al tacto sino que sobre esta hay otra pantalla protectora que despliega la información y es la que realmente hace contacto con el usuario. Como resultado de esto, no hay una relación desde fábrica, entre las coordenadas de un punto de la pantalla que despliega los datos y las coordenadas de la pantalla táctil, ya que son dos dispositivos diferentes. Por esto, el software que hace de interfaz entre touch screen y la pantalla, debe reconocer cuales puntos en el sensor de la pantalla tactil, recaen sobre que puntos en la pantalla que despliega los datos. La sincronización de las coordenadas de estas dos pantallas se conoce como calibración del touch-screen o pantalla tactil. Para calibrar la pantalla táctil de la máquina, generalmente se le pide a la persona que toque al menos tres puntos de la pantalla, estos puntos frecuentemente son dos esquinas opuestas y uno central. Si durante la etapa de calibración se tocan deliberadamente otros puntos que no se han indicado, la pantalla quedará mal calibrada.

Controles preventivos:

- Utilizar las interfaces votante-máquina que brindan la posibilidad de tocar en cualquier parte del nombre del candidato en vez de tocar un punto específico para que la opción sea tenida en cuenta, porque son menos sensibles a las fallas en la calibración.

- También es importante que el votante pueda verificar la opción que escogió y devolverse si no es la adecuada, esto permitiría dar a conocer a los jurados de mesa la situación (las terminales de votación empleadas en la prueba piloto de voto electrónico presentaban esta opción).

AMENAZA 6: ERRORES HUMANOS: JURADOS DE MESA

Entre los errores más comunes que pueden ser cometidos por los roles encargados de la administración de las mesas de votación (jurados) están: Mala administración de los tarjetones (provisionales y sobrantes), fallas al dar instrucciones a los votantes que requieran tal información, admisión de electores que no están autorizados a votar en la mesa (esto se puede dar de manera intencional o no intencional) y manipulación de comprobantes de voto.

Todos estos errores se pueden presentar por la deliberada asignación de jurados, solo basándose en competencias y por la no homogeneidad en el entrenamiento a los mismos, algunos reciben entrenamiento oficial de parte del ente organizador de las elecciones y otros no. Otra gran razón es la asignación de jurados a sitios de votación muy cercanos a su vivienda y entorno, esto crea la situación en la cual votantes que no han tenido la oportunidad de una buena educación electoral debido a su locación geográfica (lugares remotos) tendrán que lidiar con jurados con la misma poca educación del votante, que no podrán solucionar las dudas que surjan en el momento de la votación.

Controles preventivos:

- La capacitación a los jurados debe ser un proceso estandarizado y diseñado de tal forma que esté compuesto por materiales instruccionales, manuales y demás ayudas pedagógicas que permitan el buen entendimiento de las funciones de los jurados.

- Se deben examinar periódicamente las competencias de los jurados, de tal forma que estos sean escogidos no solo porque residen cerca al sitio de votación o por simpatía sino por sus habilidades y competencias.

AMENAZA 7: ASISTENCIA AL VOTANTE.

Este evento puede presentarse cuando el elector requiere de la ayuda de alguna persona para realizar su votación. Esta situación puede ser aprovechada por personas que deseen manipular o presionar al votante para que escoja una opción determinada.

Controles preventivos:

- La ayuda a los votantes se debe realizar solo en los casos donde es absolutamente necesario, es decir, que el votante demuestre que realmente es incapaz de ejercer su voto (Adultos mayores, personas con algún tipo de discapacidad física, etc.) y necesite la asistencia de otra persona.

- 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). Si un jurado o asistente de mesa brinda ayuda al votante, la debe realizar en presencia de los veedores de los partidos políticos participantes.

- Desarrollar sistemas de votación con ayudas a discapacitados y que sean de manejo intuitivo.

Controles Detectivos

- Documentar cada instancia del proceso de ayuda a un votante, desde el momento que la solicita hasta que ejerce su voto.

- Observar y Registrar la frecuencia con la que los votantes solicitan ayuda para establecer patrones que permitan realizar auditorias y detectar comportamientos inusuales que indiquen irregularidades.

AMENAZA 8: ATAQUE A TRAVÉS DEL PUERTO LECTOR DE LA TARJETA INTELIGENTE.

Este tipo de ataque se puede realizar a través de la creación de una interfaz basada en un software residente en otra máquina. El ataque se realizaría de la siguiente forma: La máquina de votación sería accesada a través del puerto lector de la tarjeta. El objetivo principal sería el controlador de este puerto que normalmente no es revisado debido a que casi siempre es comprado a otro proveedor y este no permite su manipulación o modificación. El atacante solamente coloca el dispositivo en el lector de tarjeta, el cual puede comunicarse con un computador externo a través de una conexión inalámbrica, haciendo mucho más difícil su detección, y descargar todo tipo de código malicioso que pueda modificar los registros de la máquina y cambiar su comportamiento.

El impacto de este ataque depende del momento en que se realice. Si el ataque toma lugar en la etapa de programación de las máquinas, será bastante alto debido a que se pueden manipular mayor cantidad de máquinas. SI el ataque se realiza en

el momento de la votación, solo afectará la máquina o máquinas a las que el atacante tenga acceso.

Controles Preventivos:

- Eliminar el uso de tarjetas inteligentes.

- Asegurar que el sistema operativo y el controlador de la tarjeta inteligente sean lo suficientemente robustos como para evitar cualquier ataque. Esto incluye la remoción de cualquier restricción en el software adquirido externamente (COTS) y realizar pruebas de penetración y ataques a través del puerto lector de las tarjetas inteligentes.

AMENAZA 9: ATAQUE WI-FI

El ataque se puede realizar en las máquinas de votación con capacidades de conexión inalámbrica. Algunas máquinas pueden tener capacidades Wi-Fi sin que los vendedores lo sepan.

El ataque puede realizarse con complicidad de una persona con acceso a la programación de las máquinas (ataque interno) o solo por una persona externa que pueda acceder a la máquina a través de la tecnología inalámbrica. En el primer caso (ataque con complicidad interna), el atacante puede tener la habilidad de modificar el software de las máquinas y programarla para que acepte comandos en determinados periodos de tiempo activando el enlace inalámbrico. En este momento el atacante ingresa a la máquina haciendo posible obtener datos de votación, modificar la programación de los tarjetones, reprogramar la máquina o cambiar la lógica de conteo de los votos. En este caso también la o las personas interesadas en atacar el sistema pueden utilizar intencionalmente, un sistema de cifrado de

datos bastante débil, de tal forma que sea fácil violar la seguridad y acceder al sistema. Entonces, deben existir dos roles en este tipo de ataque, que pueden ser ejecutados por dos personas diferentes o inclusive una sola persona. Un rol sería el de la persona con acceso a la programación de las máquinas quien introduce la vulnerabilidad y el otro rol que realiza el ataque.

En el caso en que el atacante no cuente con la ayuda de alguna persona con accesos a la programación de las máquinas antes del día de las elecciones, su objetivo será ingresar al sistema a través de la conexión Wi-Fi para modificar los votos o hacer que la máquina falle. En este caso es un poco más difícil que sea ejecutado el ataque, porque dependerá de las habilidades del atacante.

Controles preventivos:

- Revisión del código fuente con el fin de buscar vulnerabilidades en el uso inapropiado de las capacidades Wi-Fi de las máquinas. Encontrar estas vulnerabilidades es más complejo cuando se han introducido de manera intencional.

- A pesar que las capacidades Wi-Fi en una máquina de votación puede ser bastante útil para efectos de programación y distribución del software a las demás máquinas es preferible que el hardware de las máquinas de votación no contenga ninguna capacidad de conexión inalámbrica. Esto cada vez es más difícil de controlar debido a la forma de adquisición de los productos electrónicos (COTS)

AMENAZA 10: SUPLANTACIÓN DE VOTANTES A TRAVES DE LA FALSIFICACIÓN DE DOCUMENTOS DE IDENTIFICACIÓN.

La suplantación generalmente se realiza con personas ya fallecidas, de las cuales se utiliza su número de identificación falsificando su documento y otra persona toma su puesto para emitir el voto. Esta amenaza no es exclusiva de un proceso electrónico electoral, también se presenta en los procesos electorales actuales del país.

Precisamente se esta realizando en estos momentos el proceso de modernización tecnológica PMT, el cual contempla el cambio de cédulas que permitan tener una base de datos centralizada de electores donde se pueda controlar y consultar en cualquier momento la habilidad de una persona para votar. También se evitará en mayor número las falsificaciones del documento de identidad, lo que permite el camuflaje de delincuentes y otros delitos importantes.

Controles preventivos:

- Utilizar papeles, tintas especiales y demás herramientas tecnológicas para la fabricación de documentos de identificación que eviten su falsificación.
- Implementar bases de datos actualizadas y centralizadas, de electores habilitados para ejercer su voto, que puedan ser consultadas en la etapa de inscripción de cédulas y en el momento que el elector se identifique en la mesa de jurados de votación el día de las elecciones.

RIESGOS DEL PROCESO

Los riesgos asociados al proceso electrónico electoral son pocos teniendo en cuenta que están asociados al objetivo principal del voto electrónico. En este orden de ideas se establecen 4 grandes riesgos del proceso. Los riesgos fueron identificados teniendo en cuenta las características que debe tener el proceso electoral (figura 4):

- Manipulación de votos.
- Manipulación al votante.
- Interrupción o demora del proceso.
- Manipulación de resultados.

ANEXO D: MODELO DE CONFIABILIDAD