FORTALECIENDO LA DEMOCRACIA: DESAFÍOS Y SOLUCIONES EN LA SEGURIDAD DE LOS SISTEMAS DE VOTACIÓN ELECTRÓNICOS

Strengthening Democracy: Challenges and Solutions in Electronic Voting System Security

José David Falco González[1]
Juan Esteban Vargas Piñeros[2]

[1]10009-0006-9482-9179. Universidad Libre de Colombia, Bogotá, Colombia,
josed-falcog@unilibre.edu.co
[2]20009-0002-0478-1257. Universidad Libre de Colombia, Bogotá, Colombia,
juane-vargasp@unilibre.edu.co

Fecha de recepción: 05/05/2024

RESUMEN

La evolución tecnológica ha permitido mejorar varios aspectos de la vida cotidiana, esto ha permitido que el sufragio mediado por sistemas electrónicos emerja como una solución tecnológica más para beneficiar a la comunidad mejorando la eficiencia y accesibilidad al proceso de votación. Sin embargo, en la era actual de riesgo inminente de brechas de datos y ataques cibernéticos es algo que no es ajeno, en teoría, a todos los dispositivos eléctricos, todo sistema es inseguro por tanto se podrá vulnerar si se investiga lo suficiente y se cuenta con los recursos necesarios.

Así pues, con esta máxima en mente, se presenta un análisis detallado sobre una implementación segura de un sistemas de votación electrónica, en el que se destaca su seguridad basado en la fusión entre herramientas diseñadas, principalmente, con enfoques seguros como blockchain, la criptografía y la autenticación todas ellas implementadas para proteger la integridad de los datos electorales, así como estrategias de protección física para prevenir la manipulación del hardware, así como cualquier interferencia de comunicaciones, y los centros de datos involucrados en el proceso electoral. La integración de estas soluciones técnicas y físicas propone un enfoque integral para enfrentar los desafíos de seguridad en la votación electrónica. Por tanto, no solo hace frente a las inquietudes actuales sobre la integridad electoral y el cambio, sino que ofrece una visión hacia la transformación digital.

Palabras clave: Blockchain, democracia, seguridad, votación electrónica.

ABSTRACT

Technological evolution has improved several aspects of daily life, this has allowed the suffrage mediated by electronic systems to emerge as another technological solution to benefit the community by improving the efficiency and accessibility of the voting process. However, in the current era of imminent risk of data breaches and cyber attacks is something that is not alien, in theory, to all electrical devices, every system is insecure and therefore can be breached if it is sufficiently investigated and has the necessary resources. Thus, with this maxim in mind, a detailed analysis of a secure implementation of an electronic voting system is presented, highlighting its security based on the fusion between tools designed, mainly, with secure approaches such as blockchain, cryptography and authentication all implemented to protect the integrity of the electoral data, as well as physical protection strategies to prevent hardware manipulation, as well as any communication interference, and the data centers involved in the electoral process. The integration of these technical and physical solutions proposes a comprehensive approach to meet the security challenges in electronic voting. Therefore, it not only addresses current concerns about electoral integrity and change, but also offers a vision towards digital transformation.

Keywords: Blockchain, democracy, electronic voting, security.

1. INTRODUCCIÓN

La democracia moderna se basa en la participación ciudadana a través del voto, gracias a este los ciudadanos de una nación pueden elegir a las personas que los representarán en los altos cargos del estado [1]. La tecnología ha logrado permear a través de muchas actividades cotidianas, ya no es raro encontrar un dispositivo portable en la muñeca que evalúe la condición de salud de cada persona en segundos, así como tampoco se encuentra extraño ver vehículos que se conducen, prácticamente, sin intervención humana [2].

Así que, ¿Por qué la tecnología no encontraría un camino hacia formas de democracia, la decisión manifiesta de la ciudadanía, como los procesos electorales? En este escrito se contextualizará al lector sobre la implementación de un sistema de votación electrónica a modo de mejorar la eficiencia y la accesibilidad, así como la seguridad y la confianza de los procesos electorales que se llevan a cabo con regularidad en Colombia y que han causado controversia en muchas ocasiones., También se presenta un análisis sobre una propuesta de los investigadores para la puesta en marcha de cualquier implementación de sistemas similares. Como plantean las conclusiones de [3] la concepción de estos sistemas ha estado acompañada por preocupaciones sobre su seguridad y su fiabilidad es por eso que también se abordan los desafíos latentes en un sistema que precisa reemplazar al modelo tradicional y así mismo en ese artículo se presentó una propuesta enlazada con tecnologías blockchain.

Se realiza una revisión sobre pautas imprescindibles de seguridad que se aplican a cabalidad en sistemas que requieren de la máxima seguridad como cabría esperar en un sistema de elección popular. Las que

ISSN 2322-8415 / Año 2024 / No. 24 - Vol. 14 / Páginas 9-23 Universidad Libre - Facultad de Ingeniería

se abordan se enumeran a continuación: Inseguridad por naturaleza, seguridad en profundidad, seguridad por oscuridad, diseño seguro, hardening de comunicaciones, criptografía de datos en reposo y en tránsito, utilización de controles de seguridad, evaluación constante de tácticas, técnicas y procedimientos, blockchain, aseguramiento de confidencialidad, integridad y disponibilidad, minimización de la superficie de ataque y fallo seguro. Aunado a esto el lector podrá contar con algunas recomendaciones para el robustecimiento de la infraestructura y dispositivos físicos en zonas desmilitarizadas, todos estos conceptos reflejan los principios de la seguridad según la OWASP, un proyecto de código abierto proveniente de una organización internacional sin ánimo de lucro que se enfoca en la seguridad de las aplicaciones que hacen uso o se comunican por medio de internet [4].

Además, se revisan algunos aspectos fundamentales de la seguridad física del sistema que servirán a la hora de la puesta en marcha del sistema como tal, el entorno físico que deberían tener estos puestos de votación en el futuro para que los procesos electorales se puedan llevar con total confianza. Por último, se explora cómo la tecnología blockchain puede ofrecer soluciones innovadoras para abordar estas preocupaciones y fortalecer la credibilidad en el proceso electoral del país como se analiza en [5], y como se concluye blockchain podría ofrecer soluciones para mejorar la privacidad del voto, además los votantes podrían verificar de manera segura y anónima que su voto se ha registrado, dado que esta es una tecnología basada en el diseño seguro, se pueden usar sus lineamientos de seguridad para proteger y validar cada voto que se registre, aunado al uso de Smart Contracts podría ayudar en tareas automatizadas cuando se cumple con una cierta condición, como el propio escrutinio de votos, en donde actualmente yace una profunda incertidumbre y desconfianza hacia el mismo.

2. METODOLOGÍA

Para abordar la compleja naturaleza de la seguridad en los sistemas de votación electrónica, se emplea una metodología cualitativa que permita una comprensión profunda y detallada de las percepciones, prácticas y desafíos relacionados con este tema crucial. La metodología aplicada aquí se basa en una variedad de técnicas cualitativas, incluyendo análisis de documentos y revisión de la literatura pertinente [6].

Se lleva a cabo un exhaustivo análisis de documentos relacionados con la seguridad en los sistemas de votación electrónica. Esto incluye informes técnicos, documentos de políticas gubernamentales, artículos académicos y otras fuentes relevantes. Este análisis documental permitió identificar tendencias, patrones y lagunas en la investigación existente sobre este tema, así como proporcionar una base sólida para el desarrollo de recomendaciones y conclusiones.

Finalmente, se realiza una revisión exhaustiva de la literatura pertinente sobre seguridad en sistemas de votación electrónica. Esto implica la identificación y análisis crítico de estudios previos, investigaciones académicas y otros recursos relevantes que aborden la seguridad de los sistemas de votación electrónica desde una perspectiva cualitativa. Esta revisión de la literatura servirá para contextualizar y enriquecer los hallazgos de la investigación, así como para identificar áreas de investigación adicionales que puedan ser exploradas en estudios futuros.

En conjunto, estas técnicas cualitativas proporcionan una comprensión integral y mul-

tidimensional de la seguridad en los sistemas de votación electrónica, permitiendo identificar los desafíos clave, evaluar las mejores prácticas y desarrollar recomendaciones informadas para mejorar la seguridad y la integridad de los procesos electorales en la era digital.

3. DESARROLLO

3.1. Seguridad de Software en Sistemas de Votación Electrónica

La seguridad en los sistemas de votación electrónica es crucial a la hora de siquiera pensar en reemplazar el modelo tradicional de papeletas y urnas. Dado el contexto actual de evolución tecnológica y la aún más preocupante escalada de tecnificación de tácticas y procedimientos que los atacantes usan para vulnerar un sistema se obliga a evaluar con detenimiento las pautas de seguridad de un dispositivo de sufragio como se explora en [7] en el que se prueba el artículo frente a si es posible mitigar la situación de fraude electoral presente en Latinoamérica mediante el uso de sistemas de votación electrónica basados en blockchain. Así pues, el artículo [7] escrito en 2020 se proponía a revisar alternativas de mecanismos de sufragio electrónico y, así como establecer los pros y los contras de las tecnologías blockchain.

En el mismo se concluye que la mejor alternativa sería una implementación total de un sistema con blockchain, sin embargo, la seguridad se queda corta si solo se limita a asegurar el proceso y no la infraestructura. Por consiguiente, la actual sinergia entre la política y la tecnología demanda un enfoque completo y adaptable para resguardar la integridad y la confianza en los procesos electorales. Frente al constante progreso y diversificación de las amenazas como se presenta en [3] por una estudiante de la UNAD de Colombia se concluye como el voto electrónico por medio de “Urnas Electrónicas de Reconocimiento de Marcas” como la mejor alternativa para proteger el secreto del voto, aunque se pone en entredicho la seguridad del programa de lecturas de marcas también destaca el hecho de un sistema de votación implementado con tecnologías blockchain aunado a la presencia de verificación biométrica con dispositivos destinados para este fin.

Este mismo artículo perseguía un objetivo aún más ambicioso, el de determinar si un sistema de votación electrónico satisface las exigencias de transparencia electoral en Colombia, donde finalmente resulta que el voto electrónico presenta tanto beneficios como dificultades. Entre los beneficios se encuentran principalmente una reducción al impacto ambiental comparado con el actual modelo de sufragio, no obstante, se debate los altos costos de la implementación de un sistema inteligente, así como su confianza y fiabilidad. Es por esto que resulta esencial desplegar una amplia gama de estrategias y tecnologías diseñadas para abordar los distintos vectores de ataque y resguardar la infraestructura electoral en todas sus dimensiones, a continuación, se detallan consideraciones generales para un sistema de votación electrónico.

3.1.1. No existe la seguridad absoluta

Como máxima presente en todo el artículo y a la evaluación de seguridad de cualquier sistema, cabe anotar lo que menciona [8]. Uno de los principios más importantes en la seguridad de la información es que ninguna aplicación, sistema o componente tiene una garantía de ser 100% seguro contra ataques. A pesar de que se pueda percibir como un punto de partida pesimista, a partir de aquí se construyen todos los contro-

ISSN 2322-8415 / Año 2024 / No. 24 - Vol. 14 / Páginas 9-23 Universidad Libre - Facultad de Ingeniería

les, mecanismos y formas de seguridad con los que actualmente se construyen las redes sociales, la mensajería instantánea, la computación en la nube, los dispositivos móviles, incluso las soluciones antivirus. Lastimosamente los recursos con que cuentan los atacantes son virtualmente infinitos en cuanto a tiempo, se podrían dedicar años y años de exploración sobre un sistema y encontrar alguna vulnerabilidad de día cero, vulnerabilidad la cual los proveedores desconocen. Esto sin contar la motivación y recursos económicos de los propios atacantes o de sus patrocinadores, como en el caso del hacktivismo.

Además, la ingeniería inversa podría ser usada como puerta de entrada a cualquier sistema. Como se concluye en uno de los documentos más afamados de la OWASP [4], el objetivo de la seguridad de software no es hacer un sistema completamente impenetrable, sino hacerlo lo suficientemente difícil de vulnerar para que cualquier atacante se desmotive y busque algo más que atacar, sin embargo, en el evento de comprometerse cualquier sistema, se busca entonces reducir su botín al mínimo para los agentes de amenaza, es por esto que a continuación se revisan algunos conceptos entregados por la misma OWASP.

3.1.2. Seguridad en profundidad

Es un enfoque estratégico de seguridad también conocido como defensa en capas, usado también para maniobras militares como se menciona en [19]. Se basa en establecer una defensa de múltiples capas para que, si alguna línea de defensa es atravesada, el enemigo, en nuestro caso un ciberatacante, tenga que lidiar con las demás capas dispuestas para frenarlo. Estas capas deben presentarse desde la red externa hasta los datos propios del sistema. Haciendo que para un atacante sea extremadamente difícil acceder hasta los datos que es realmente el botín de un sistema de votación electrónico. Sin embargo, de nuevo como se menciona en el libro ya citado, no importa cuántas capas coloquemos nuestro sistema no quedará aislado ante cualquier ataque motivado. Esta defensa no es mágica, el objetivo es establecer una red de defensa que nos de tiempo a percibir y reaccionar al ataque y remediar todos los daños causados para asegurar la continuidad del proceso de sufragio.

La siguiente figura muestra un esquema general de la seguridad en profundidad, el centro sería el punto de entrada a nuestro sistema, la red externa y nuestros datos estarían en el perímetro asegurados por múltiples controles de seguridad dispuestos en los sitios ubicados en la imagen.

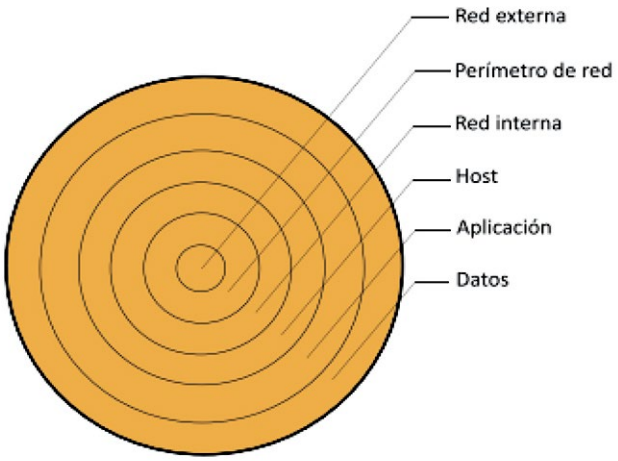

Figura 1.
Seguridad en profundidad, tomada de [19].

3.1.3. Seguridad por oscuridad

Este principio de seguridad no debería ser utilizado por ningún motivo por la siguiente razón, utiliza el ocultamiento para garantizar la seguridad. Algo sucedido en 2016 tie-

ne ahora relevancia al momento de analizar este tema relacionado con la votación electrónica. Se mencionó en una plenaria de comisiones del tribunal electoral de la provincia de salta, Argentina, que su sistema de votación electrónica debería permanecer cerrado, ya que, por ejemplo, al momento de realizarse una auditoría por los fiscales informáticos de la universidad de Salta al sistema de boleta única electrónica, si un CD, que contiene el sistema operativo de la máquina de votación, cayera en manos de alguien que quisiera hacerle daño al sistema o a la misma democracia de la provincia, este podría cambiar el software y alterar las votaciones.

O lo que es lo mismo, toda la seguridad de las votaciones de la provincia en aquel entonces se basaba en un CD que puede y debe ser de fácil manipulación para la auditoría del sistema. Sin duda, este no debería ser de lejos el eslabón más débil de la cadena, se deben aplicar principios de seguridad de software más sofisticados como los que veremos a continuación, de modo tal que, si el código fuente del sistema es filtrado, este sufra el menor daño posible.

3.1.4. Diseño seguro

El diseño seguro recoge todas las técnicas usadas para estructurar la creación e implementación de un sistema informático teniendo como eje central la seguridad. Así pues, como recomienda [20] se debe utilizar el principio del privilegio mínimo, validación y sanitización de entradas y protocolos de comunicación y transmisión seguros.

El principio del privilegio mínimo establece que los permisos otorgados a un usuario del sistema deben ser mínimos para que pueda realizar sus tareas normales. Este principio limita el daño que puede ser ocasionado por una confusión de roles y privilegios, para el caso del sistema de votación, el votante debe poder ser autenticado en el sistema y emitir su voto una única vez. Para los administradores del sistema se deben brindar roles específicos para las tareas que estos desarrollen, ya que también debe haber una separación de deberes como establece [4]. La validación y sanitización de datos es el proceso por el que los datos entrantes en el sistema se validan y se limpian en caso de que contengan información no pertinente para el sistema, para el caso del sistema de votación se debe validar que el votante es una persona habilitada para ello y que el voto apunta directamente a un candidato habilitado igualmente.

Del lado del sistema, se debe firmar con una suma de verificación el firmware y el software que ejecuta la máquina con el fin de evitar implantaciones de software ilegítimo en caso de que sea vulnerada la seguridad. Se deben utilizar protocolos de comunicación y transmisión cifrada que no estén obsoletos para garantizar la integridad de los datos en tránsito. Como protocolo de comunicación se propone TLS/SSL por su facilidad de implementación y teniendo en cuenta que permite cifrar la información transmitida en las arquitecturas cliente-servidor.

3.1.5. Tácticas de reforzamiento de seguridad

A continuación, se detallan algunas medidas de hardening de sistemas que no está de más tomar y que pueden evitar algún error tonto [9]. Este procedimiento se basa en robustecer los sistemas minimizando su superficie de ataque, a continuación, se detallan algunas recomendaciones generales, independientes de la infraestructura en que se despliegue:

ISSN 2322-8415 / Año 2024 / No. 24 - Vol. 14 / Páginas 9-23 Universidad Libre - Facultad de Ingeniería

Tabla 1.
Medidas de seguridad que se deben implementar en la arquitectura de un sistema de votación electrónico.

Medidas de seguridad	Descripción
Cambiar contraseñas por defecto	Actualizar todas las contraseñas predeterminadas a contraseñas robustas.
Desinstalación de software innecesario	Eliminar programas que no son necesarios para la operación del sistema.
Revisión y revocación de cuentas de usuario inactivas	Revisar periódicamente y eliminar cuentas de usuarios que no participan directamente en el proceso de sufragio
Deshabilitar servicios no necesarios	Desactivar servicios y funciones que no son esenciales para el funcionamiento del sistema de votación.
Cerrar puertos no necesarios	Cerrar puertos en el sistema que no afectan el funcionamiento de la aplicación, para prevenir accesos no autorizados.
Instalación de dispositivos de seguridad en red	Implementar firewalls NGFW, IDS e IPS para proteger la red de amenazas externas e internas.
Revisión periódica de actualizaciones y parches	Verificar e instalar actualizaciones y parches ofrecidos por los proveedores para mantener el sistema actualizado y seguro.

3.1.6. Criptografía

La criptografía, como cimiento esencial de la seguridad de la información, desempeña un rol primordial en asegurar la confidencialidad e integridad de los datos electorales [7]. Además, como se desarrolló en el prototipo funcional probado en la universidad Distrital Francisco José de Caldas de [5] todos los votos deben ser pasados a funciones de hash criptográfico con algoritmos de complejidad mínima como SHA256, y luego compartirse a la cadena de bloques mediante AES ya que como se menciona en [10], es un protocolo de cifrado simétrico óptimo para grandes conjuntos de datos, las recomendaciones de AES con la distinción de sus labores se presentan a continuación:

AES

- Cifrado de votos: AES es una opción eficiente para el cifrado de votos electrónicos durante la transmisión y almacenamiento, garantizando que solo los destinatarios autorizados puedan acceder al contenido de los votos.

- Protección de datos sensibles: AES puede utilizarse para cifrar datos sensibles relacionados con la identidad de los votantes o el proceso electoral, protegiéndolos contra accesos no autorizados y ataques de ingeniería social.

- Seguridad en la transmisión de resultados: AES puede ser utilizado para cifrar los resultados de las elecciones durante la transmisión desde los dispositivos de votación hasta el centro de recuento, garantizando la confidencialidad e integridad de los datos.

Este algoritmo de cifrado se puede usar para asegurar tanto la información en tránsito como la almacenada, reduciendo así la

superficie de ataque y blindando los datos críticos contra accesos no autorizados de modo que, de producirse una intrusión en el sistema, el atacante no pueda leer la información directamente, sino que tendría que valerse de una clave altamente compleja para descifrar el mensaje [5] y [10]. Además, la criptografía simétrica facilitaría una comunicación segura entre los distintos componentes del sistema.

3.1.7. Controles de seguridad

En la norma internacional ISO 27001 se mencionan decenas de controles de seguridad que pueden ser aplicados según el caso, estos se agrupan en 4 grupos de controles como se muestra a continuación:

Figura II.
Grupos de controles de seguridad, tomada de innevo.com.

Para nuestro caso en concreto se propone usar:

- **Políticas de seguridad de la información:** En forma de documentos que especifiquen el alcance de la seguridad y los compromisos con la seguridad de los votantes.
- **Organización de la seguridad de la información:** Determina al personal de seguridad sus labores y sus responsabilidades.
- **Gestión de activos:** Se debe tener un registro de todos los activos de la infraestructura.
- **Controles de acceso:** La parte administrativa del sistema debe contar con una lista blanca de acceso que solo permita acceder a direcciones ip de confianza en la intranet.
- Criptografía: Cómo ya se comentó.
- Seguridad de las comunicaciones: Para asegurar los datos en tránsito.
- Gestión de incidentes: Se debe preparar, detectar y analizar, contener, erradicar, y recuperarse tras el evento como recomiendo el marco NIST.

3.1.8. Confidencialidad, integridad y disponibilidad

Además de las estrategias tecnológicas planteadas hasta el momento, es crucial mantener los principios de la triada CID (confidencialidad, integridad y disponibilidad) como pilar fundamental para el sistema de votación electrónica [21].

Confidencialidad: Implica garantizar la identidad de toda la ciudadanía que se dispone a votar y asimismo sus votos se mantengan privados y seguros frente a accesos no autorizados. Para este caso se usarían controles de seguridad y la criptografía, aunado a blockchain, todo esto para asegurar que los votos se registran en la cadena y se puede acceder a ella de manera anónima.

Integridad: Resulta de registrar y contar los votos de manera precisa, sin modificaciones alguna, para esto las sumas de verificación deben comprobarse en cada bloque nuevo añadido a la cadena blockchain. De

ISSN 2322-8415 / Año 2024 / No. 24 - Vol. 14 / Páginas 9-23 Universidad Libre - Facultad de Ingeniería

esta manera se preserva la exactitud de los resultados electorales.

Disponibilidad: Consiste en garantizar que los sistemas de votación estén accesibles y operativos cuando se necesiten, sin interrupciones que puedan afectar la participación electoral o el escrutinio de los votos. La arquitectura descentralizada de blockchain contribuye a prever puntos únicos de fallo, lo que reduce el riesgo de caída del sistema.

Figura III.
Triada de la seguridad de la información, tomado de [21].

3.1.9. Infraestructura segura

Asimismo, el empleo de dispositivos de seguridad de red como los sistemas de prevención de intrusiones (IPS) y sistemas de detección de intrusiones (IDS) [14] juega un rol crucial en la salvaguarda de la infraestructura electoral contra las amenazas cibernéticas. Estas soluciones no solo monitorizan y analizan el tráfico de red en busca de actividades sospechosas, sino que también son capaces de actuar proactivamente bloqueando y evitando el paso de posibles paquetes de amenaza.

Así, también, como se desarrolla en [11] un artículo de revisión redactado en 2020 por un estudiante de la universidad de San Marcos, sobre la información como activo más valioso de las organizaciones, se propone analizar todas las nuevas amenazas a las que se enfrenta el mundo al momento en que a internet se le suman cada día más y más usuarios, en este artículo también se discute sobre la protección de datos almacenados y de sistemas de red ya que estos canales podrían percibir intermitencias malintencionadas y por consiguiente verse envueltos en

La evaluación continua de TTPs como se observa en [12] provee de información valiosa sobre las últimas tácticas, técnicas y procedimientos utilizadas por actores maliciosos en el ámbito de la ciberseguridad. Este artículo destaca como esencial para una defensa activa contra amenazas digitales, escrito en 2022, resalta la importancia de la postura de seguridad que en este contexto es aplicable debido a la sensibilidad de los datos, además orienta a las tácticas de defensa y respuesta enmarcadas en un libro de estrategias diseñado especialmente para este sistema. Sin embargo, para el alcance de esta revisión no se contempla un playbook dado su complejidad y objetividad dependiendo del contexto de aplicación.

Dado que cada vez es más frecuente que los agentes de amenaza usen varios ataques en simultáneo y combinen trozos de código de las pruebas de concepto de las vulnerabilidades conocidas, el estar a la vanguardia de las novedades en el campo de la seguridad sería fundamental para actualizar el sistema a tiempo y evitar riesgos. Este enfoque proactivo permite identificar y abordar posibles vulnerabilidades en el sistema antes de que puedan ser explotadas por adversarios, contribuyen-

do así a fortalecer la integridad y confiabilidad de los procesos electorales en un entorno digital cada vez más complejo y desafiante. Juntos, los elementos mencionados en este numeral forman una solución integral que mejora la capacidad, en nuestro caso, del Concejo Nacional Electoral, para prevenir, detectar y responder a incidentes cibernéticos ocasionados contra el sistema electrónico de votación de manera efectiva.

3.2. Seguridad Física en Sistemas de Votación Electrónica

La protección integral de los sistemas de votación electrónica es un tema de suma importancia en el contexto de la democracia moderna, donde la intersección entre la tecnología y los procesos electorales exige un enfoque meticuloso y completo para garantizar la confiabilidad y la integridad de los resultados [14]. En un mundo cada vez más digitalizado, la seguridad de los sistemas se ha convertido en una preocupación fundamental, dada la creciente sofisticación y diversificación de las amenazas a las que están expuestos, como se estudia también en [5].

Para comprender adecuadamente la importancia de la seguridad en los sistemas de votación electrónica, es crucial analizar en detalle los diferentes aspectos que intervienen en su protección integral. Entre estos aspectos, destacan la seguridad física del hardware, la gestión de la cadena de custodia y la protección de los centros de datos sin olvidar los desastres naturales, que, a pesar de no ser causados deliberadamente por un agente malicioso, se deben planes de recuperación contra estos eventos. Cada uno de estos elementos desempeña un papel fundamental en la salvaguarda de la integridad y la confiabilidad de los procesos electorales.

En primer lugar, la seguridad del hardware es un aspecto crucial para garantizar la integridad de los sistemas de votación electrónica. Los dispositivos de sufragio, como las máquinas de votación y los sistemas informáticos utilizados para tabular los resultados, son los componentes fundamentales de cualquier sistema electoral electrónico. Por lo tanto, proteger estos dispositivos contra manipulaciones físicas y accesos no autorizados es de vital importancia para garantizar la confiabilidad de los resultados.

Para lograr esto, se deben emplear una serie de medidas de seguridad física diseñadas para proteger el hardware contra cualquier intento de manipulación o interferencia [15]. Entre estas medidas se incluyen el uso de sellos de seguridad de alta resistencia que evidencian cualquier intento de manipulación, carcasas robustas diseñadas para resistir ataques físicos y sistemas de detección de intrusiones que alertan ante cualquier actividad sospechosa.

Además, elementos que se incluyen en el sistema contribuyen para este aspecto de la seguridad activa, el escáner de retina, lector de huellas dactilares y lectores de barras pueden ser usados en esta etapa para evitar el acceso no autorizado al sistema interno de votación. Junto con esto es indispensable una vigilancia permanente al sistema para asegurar que un usuario no está haciendo un mal uso del sistema. Estas salvaguardas no solo protegen el hardware en sí, sino que también garantizan la integridad del sistema electoral en su conjunto, manteniendo la confianza pública en la legitimidad de los resultados.

Además de la seguridad física del hardware, la gestión de la cadena de custodia como se menciona en el artículo [16] es otro aspecto crucial en la protección de los sistemas de votación electrónica. Se refiere al proceso

ISSN 2322-8415 / Año 2024 / No. 24 - Vol. 14 / Páginas 9-23 Universidad Libre - Facultad de Ingeniería

de supervisar y verificar cada etapa del ciclo de vida de los equipos de votación electrónica, desde su fabricación hasta su despliegue en el día de las elecciones. Este proceso meticuloso asegura que los dispositivos se mantengan seguros y libres de manipulaciones indebidas en todo momento, lo que proporciona una capa adicional de seguridad y confianza en el proceso electoral.

La gestión de la cadena de custodia implica el establecimiento de procedimientos claros y transparentes para el manejo y transporte de los equipos de votación, así como la implementación de controles estrictos para garantizar que no se produzcan alteraciones o manipulaciones durante su almacenamiento y uso. Además, se lleva a cabo un seguimiento detallado de cada dispositivo, registrando todas las actividades relacionadas con su manejo y asegurando su integridad en todo momento.

Finalmente, la protección de los centros de datos que almacenan y procesan los datos electorales es otro aspecto crítico en la seguridad de los sistemas de votación electrónica. Estos centros de datos albergan información sensible y confidencial, incluyendo los resultados de las elecciones y los datos de los votantes, por lo que es fundamental protegerlos contra amenazas físicas y cibernéticas.

Dado que la configuración de varios centros de datos puede implicar una alta complejidad en cuanto a la configuración de los mismos de modo que cada uno sea seguro, se recomienda montar una infraestructura en la nube, que integre protocolos seguros de comunicación entre cliente y servidor, listas blancas de control de acceso y firewalls que rechacen toda comunicación que no provenga de un punto de confianza, como podría ser un sistema de sufragio, u otros centros de datos.

3.3. Uso de blockchain

La tecnología blockchain ha irrumpido en numerosos campos, transformando la forma en que realizamos transacciones y almacenamos datos [17]. Sin embargo, uno de los ámbitos donde su potencial es más prometedor es en los procesos electorales. En un mundo donde la confianza en los sistemas electorales tradicionales se ve socavada por preocupaciones sobre la seguridad y la transparencia, blockchain ofrece una solución revolucionaria que podría redefinir la democracia moderna.

3.3.1. Seguridad Inquebrantable

Una de las características más destacadas de blockchain es su seguridad inquebrantable [18]. Al utilizar criptografía avanzada y un diseño descentralizado, blockchain crea un registro inmutable de cada transacción o acción realizada en la red. En el contexto de los procesos electorales, esto significa que cada voto registrado en la blockchain es prácticamente imposible de alterar o manipular. Un conjunto de votos se convierte en un bloque en la cadena, vinculado de manera criptográfica a los bloques anteriores, lo que garantiza su integridad y autenticidad.

3.3.2. Transparencia Absoluta

Otra ventaja significativa de blockchain es su transparencia absoluta. A diferencia de los sistemas electorales tradicionales, donde los procesos de conteo y tabulación pueden ser opacos y susceptibles a manipulación, blockchain permite una visibilidad completa de todas las transacciones [17]. Además, como se menciona en [5] luego de poner en funcionamiento el sistema propuesto por un estudiante de la universidad Distrital, se consiguió añadir a la cadena de bloques con éxito el voto de cada sufragan-

te. Además, también se revela su factibilidad económica al comparar como iguales el actual modelo de votación en Colombia versus uno implementado en la nube. Además, con el prototipo propuesto cada estudiante pudo verificar la validez de su voto y rastrear su viaje a lo largo de la cadena de bloques. Esta transparencia fomenta la confianza en el proceso electoral al eliminar cualquier sospecha de fraude o irregularidad.

3.3.3. Eliminación de Intermediarios

La naturaleza descentralizada de blockchain también elimina la necesidad de intermediarios en el proceso electoral. En los sistemas tradicionales, los organismos electorales y los funcionarios gubernamentales actúan como intermediarios entre los votantes y el resultado final de las elecciones.

Sin embargo, con blockchain, los contratos inteligentes pueden automatizar gran parte de este proceso, garantizando una ejecución imparcial y transparente de las reglas electorales preestablecidas. Esto reduce significativamente el riesgo de corrupción y manipulación por parte de terceros.

3.3.4. Accesibilidad y Participación

Además de mejorar la seguridad y la transparencia, blockchain también puede aumentar la accesibilidad y la participación en los procesos electorales. Con la introducción de sistemas de votación electrónica basados en blockchain, los ciudadanos pueden emitir sus votos de manera segura y conveniente desde cualquier lugar del mundo con acceso a internet.

Esto elimina las barreras geográficas y logísticas que a menudo dificultan la participación en las elecciones, especialmente para aquellos que residen en áreas remotas o tienen dificultades para movilizarse.

A continuación, se presenta un diagrama que ejemplifica la estructura del sistema de votación concebida por los autores. Este se encuentra dividido en cuatro capas:

Capa	Descripción
Presentación	Proporcionar una interfaz intuitiva para los votantes, permitiendo la autenticación y la emisión del vot. Hace empleo de dispositivos de reconocimiento biométrico, y de la interacción del votante.
Lógica	Gestiona la autenticación y autorización de los votos emitidos por la capa de presentación, implementa protocolos de comunicación segura haciendo uso de la capa de seguridad, verifica identidad con métodos biométricos. Asegura el voto emitido con cifrados de alta complejidad.
Datos	Gestiona el almacenamiento y procesamiento de datos electorales, protegidos con medidas físicas y controles lógicos que presta la capa de seguridad.
Seguridad	Componente crítico del sistema que se encarga de garantizar la confidencialidad, integridad y disponibilidad.

ISSN 2322-8415 / Año 2024 / No. 24 - Vol. 14 / Páginas 9-23 Universidad Libre - Facultad de Ingeniería

Figura IV.
Diagrama de arquitectura sistema electrónico de votación, elaboración propia.

4. CONCLUSIONES

La implementación de blockchain como eje central del sistema de votación ha sido validada por múltiples investigaciones y prototipos que se han incluido en esta investigación. Proporciona una solución robusta para garantizar la integridad de los votos y así mismo, reforzar la confianza de la ciudadanía en el sistema electoral. Se repasaron varios aspectos a tener en cuenta para blindar el proceso de sufragio, entre ellos la autenticación y cifrado de datos en reposo y tránsito con algoritmos de complejidad alta para garantizar la confidencialidad y privacidad de los votantes tanto como la fiabilidad en el sistema. Se propone la integración de firewalls de siguiente generación (NGFW) capaces de detectar patrones de ataque conocidos y bloquear las conexiones maliciosas, sin embargo, teniendo en mente el principio de la seguridad en profundidad también se introduce dispositivos IDS/IPS y ACL entre los nodos de red para poder tener un control total del tráfico que por esta transita.

Además del uso de técnicas de diseño seguro que reforzará el software de la aplicación desde su interior, protegiendo sus entradas, validando sus procesos y generando salidas correctas. Por último, el apego al cumplimiento de una norma internacional como la ISO 27001, proporciona un marco estructurado e integral para la protección de información sensible, aunado al mejoramiento de la gestión de riesgos e incidentes de ciberseguridad.

Este documento presenta un avance en la revisión y evaluación de los sistemas de votación electrónica en Colombia, centrándose mayoritariamente en la seguridad. Aunque proporciona una visión detallada y actualizada sobre el estado del arte de un posible sistema seguro de votación electrónica, los resultados y recomendaciones aquí expuestos no constituyen una solución definitiva.

La tecnología y las amenazas a esta avanzan a pasos agigantados día tras día, por ello este documento puede servir de base para futuras consideraciones en la implementación de un sistema electrónico de sufragio.

ISSN 2322-8415 / Año 2024 / No. 24 - Vol. 14 / Páginas 9-23 Universidad Libre - Facultad de Ingeniería

REFERENCIAS BIBLIOGRÁFICAS

[1] *L. García,* «El derecho al voto. Una aproximación para su entendimiento y adecuada aplicación,» Vida Científica Boletín Científico de la Escuela Preparatoria No. 4, vol. 12, nº 23, pp. 39-42, 2024.

[2] *M. Colombo,* «La revolución 4.0: los nuevos paradigmas a los 55 años de la sanción de la Ley de Seguros,» El Derecho, 2022.

[3] *E. Henao,* «Análisis Sobre La Implementación Del Voto Electrónico En Colombia,» 2020. [En línea]. Available: https://repository.unad.edu.co/bitstream/handle/10596/35935/mphenaoe.pdf?sequence=1&isAllowed=y.

[4] *OWASP,* «Principles of Security,» 2024. [En línea]. Available: https://owasp.org/www-project-developer-guide/draft/foundations/security_principles/.

[5] *S. Cruz,* «Prototipo de un sistema para el control y seguridad del voto electrónico en el sistema de elección democrático en Colombia utilizando Blockchain,» 2020. [En línea]. Available: https://repository.udistrital.edu.co/bitstream/handle/11349/25078/CruzTarquinoSaulFernando2020.pdf.

[6] *S. Hernandez,* Metodología de la investigación, Mc Graw Hill, 2014.

[7] *J. Fernández y A. Santa,* «ESTADO DEL ARTE DEL VOTO ELECTRÓNICO BASADO EN TECNOLOGÍA,» 2020. [En línea]. Available: https://repositorio.utp.edu.co/server/api/core/bitstreams/34262c64-a74b-4293-8f72-8d1b5913ca61/content.

[8] *O. Baran bo,* Dirección, Hackers - Ningún sistema es seguro. [Película]. Alemania: Wiedemann & Berg Film Production, 2014.

[9] *KeepCoding,* «¿Qué es el Hardening en Ciberseguridad?,» 2023. [En línea]. Available: https://keepcoding.io/blog/que-es-el-hardening-en-ciberseguridad/#Configuraciones_necesarias_para_protegerse_de_posibles_ataques_fisicos_o_de_hardware_de_la_maquina. [Último acceso: 25 Marzo 2024].

[10] *R. Sood,* «A Literature Review on RSA, DES and AES Encryption Algorithms,» Emerging Trends in Engineering and Management, pp. 57-63, 2023.

[11] *M. Giraldo, A. Arias, L. Giraldo y D. Arango,* «PRINCIPALES TENDENCIAS INVESTIGATIVAS EN SEGURIDAD DE REDES INFORMÁTICAS A PARTIR DEL ESTUDIO BIBLIOMÉTRICO,» EVOLUCIÓN Y TENDENCIAS INVESTIGATIVAS, pp. 52-62, 2020.

[12] *J. Couretas,* «Cyber Policy, Doctrine, and Tactics, Techniques, and Procedures (TTPs): An Introduction to Cyber Analysis and Targeting,» Cham: Springer International Publishing, pp. 13-36, 2022.

[13] *A. Postigo,* Seguridad Informática, Madrid: Ediciones Paraninfo, 2020.

[14] *M. C.,* Seguridad física y lógica en redes, 2020. [En línea]. Available: https://repositorio.usam.ac.cr/xmlui/handle/11506/2080. [Último acceso: 29 03 2024].

[15] *J. Costas,* Seguridad Informática, Madrid: RA-MA, 2014.

[16] *S. Gallardo,* Cadena de suministro, Revista Sistemas, vol. 164, pp. 42-52, 2022.

[17] *D. Tapscott,* La revolución Blockchain, Barcelona: Ediciones Deusto, 2017.

[18] *J. Lecuit,* «La seguridad y privacidad del blockchain, más allá de la tecnología y las criptomonedas,» Real Instituto El Cano, Madrid, 2019.

[19] *E. Briceño,* Seguridad de la información, Alicante: 3Ciencia, 2021.

[20] *Linkedin,* «7 Pasos para Implementar Diseño Seguro de Aplicaciones,» 20 Septiembre 2023. [En línea]. Available: https://es.linkedin.com/pulse/7-pasos-para-implementar-patrones-de-dise%C3%B1o-seguros. [Último acceso: 1 Agosto 2024]

[21] *J. L,* «Linkedin,» 21 Noviembre 2022. [En línea]. Available: https://es.linkedin.com/pulse/triada-cid-base-de-la-seguridad-informaci%C3%B3n-jonathan-l%C3%B3pez-acevedo. [Último acceso: 1 Agosto 2024].