UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

EVALUACIÓN DE VULNERABILIDADES EN SISTEMAS DE VOTACIÓN ELECTRÓNICA DESDE UNA PERSPECTIVA DE CIBERSEGURIDAD: CASO DE ESTUDIO EN ECUADOR

AUTOR

Molina Noboa, Jorge Farouk

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR

Moreira Zambrano, César Armando

Santa Elena, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.

COORDINADORA DEL PROGRAMA

Firmado electrónicamente por:
CESAR ARMANDO MOREIRA ZAMBRANO

Ing. César Moreira Zambrano, Ph. D.

TUTOR

Firmado electrónicamente por:
ANA EVA CHACON LUNA

Ing. Ana Chacón Luna, Ph. D.

DOCENTE ESPECIALISTA

Firmado electrónicamente por:
OSCAR OMAR APOLINARIO ARZUBE

Lic. Oscar Apolinario Arzube, Ph. D.

DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, MSc.

SECRETARIO GENERAL

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Molina Noboa Jorge Farouk, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Firmado electrónicamente por:
CESAR ARMANDO
MOREIRA ZAMBRANO

Ing. César Armando Moreira Zambrano, Ph. D.

Santa Elena, 11 de octubre de 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Molina Noboa Jorge Farouk**

DECLARO QUE:

El trabajo de Titulación, **EVALUACIÓN DE VULNERABILIDADES EN SISTEMAS DE VOTACIÓN ELECTRÓNICA DESDE UNA PERSPECTIVA DE CIBERSEGURIDAD: CASO DE ESTUDIO EN ECUADOR** previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 11 de octubre de 2024

EL AUTOR

Firmado electrónicamente por:
JORGE FAROUK MOLINA NOBOA

Jorge Farouk Molina Noboa

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS DE LA INGENIERÍA
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **EVALUACIÓN DE VULNERABILIDADES EN SISTEMAS DE VOTACIÓN ELECTRÓNICA DESDE UNA PERSPECTIVA DE CIBERSEGURIDAD: CASO DE ESTUDIO EN ECUADOR**, presentado por el estudiante, Jorge Farouk Molina Noboa fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 6%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

CERTIFICADO DE ANÁLISIS
magister

FINAL V001

6%
Textos sospechosos

2% Similitudes
0% similitudes entre comillas
< 1% entre las fuentes mencionadas
4% Idiomas no reconocidos

Nombre del documento: FINAL V001.docx
ID del documento: e3c2d6fa42bad165e47bd488929a78ef06bbc2f8
Tamaño del documento original: 3,26 MB
Autores: []

Depositante: CÉSAR ARMANDO MOREIRA ZAMBRANO
Fecha de depósito: 9/10/2024
Tipo de carga: interface
fecha de fin de análisis: 9/10/2024

Número de palabras: 23.790
Número de caracteres: 168.201

TUTOR

Firmado electrónicamente por:
CESAR ARMANDO MOREIRA ZAMBRANO

Ing. César Armando Moreira Zambrano, Ph. D.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **Jorge Farouk Molina Noboa**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de mi trabajo de propuestas metodológicas y tecnológicas avanzadas con fines de difusión pública, además apruebo la reproducción de este trabajo de propuestas metodológicas y tecnológicas avanzadas dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 11 de octubre de 2024

EL AUTOR

Firmado electrónicamente por:
JORGE FAROUK MOLINA NOBOA

Jorge Farouk Molina Noboa

AGRADECIMIENTO

Primero, agradezco a **DIOS** por darme la fortaleza y sabiduría para alcanzar este logro. Su guía ha sido mi mayor apoyo en todo momento.

A la **Universidad Estatal Península de Santa Elena**, mi más sincero agradecimiento por permitirme realizar mis estudios de maestría en esta institución, y a los docentes, por su dedicación y valiosos conocimientos.

De manera especial, gracias a mi tutor, **Ing. César Moreira**, por su constante guía y apoyo. Su compromiso fue clave para la culminación de este trabajo.

A mis padres, **Tito Molina** y **Maritza Noboa**, y a toda mi familia, les expreso mi más profunda gratitud. Aunque mi padre ya no esté físicamente, su presencia sigue acompañándome. A mi madre y a todos mis seres queridos, gracias por su amor y apoyo incondicional.

A todos, mi más profundo agradecimiento.

Jorge Farouk, Molina Noboa

DEDICATORIA

A mis queridos padres y hermanos:

A ti, mamá, quien siempre has sido mi roca y mi apoyo incondicional en cada paso de mi camino. Tu amor y dedicación me han inspirado a esforzarme por ser la mejor versión de mí mismo.

A ti, papá, cuya memoria y enseñanzas continúan guiando mis pasos; siempre vivirás en mi corazón.

Y a mis hermanos, gracias por ser mis compañeros de vida y por compartir tantas risas y momentos inolvidables. Esta dedicación es un reflejo del amor y apoyo que siempre me han brindado. Agradezco profundamente tenerlos a mi lado en cada paso de este viaje.

Jorge Farouk, Molina Noboa

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Las instituciones electorales enfrentan el desafío de salvaguardar la integridad de los procesos democráticos. Esta investigación se enfoca en desarrollar mecanismos de detección de vulnerabilidades en sistemas de votación electrónica y en la creación de un plan integral de fortalecimiento de ciberseguridad. Para lograr este objetivo, se aplicó una metodología cuantitativa que incluye las fases de identificación de activos, identificación de amenazas, evaluación de vulnerabilidades y análisis de impacto. Se realizaron escaneos de vulnerabilidades en la aplicación web del CNE, lo que permitió identificar un total de 8,355 vulnerabilidades, clasificadas en niveles de riesgo alto, medio, bajo y muy bajo. La utilización de herramientas de detección facilitó un análisis exhaustivo del sistema, destacando la urgencia de implementar un plan de ciberseguridad robusto. Este plan debe integrar tecnologías innovadoras, *backups* inmutables y auditorías semestrales según la norma ISO 27001:2022, para garantizar la confianza ciudadana en el proceso electoral.

Palabras claves: Vulnerabilidades, Ciberseguridad, Evaluación de riesgos

ABSTRACT

Electoral institutions face the challenge of safeguarding the integrity of democratic processes. This research focuses on developing mechanisms for detecting vulnerabilities in electronic voting systems and creating a comprehensive cybersecurity strengthening plan. To achieve this objective, a quantitative methodology was applied that includes the phases of asset identification, threat identification, vulnerability assessment and impact analysis. Vulnerability scans were carried out in the CNE web application, which allowed the identification of a total of 8,355 vulnerabilities, classified into high, medium, low and very low risk levels. The use of detection tools facilitated a thorough analysis of the system, highlighting the urgency of implementing a robust cybersecurity plan. This plan must integrate innovative technologies, immutable *backups* and semi-annual audits according to the ISO 27001:2022 standard, to guarantee citizen confidence in the electoral process.

Keywords: Vulnerabilities, Cybersecurity, Risk Assessment

INTRODUCCIÓN

Con el advenimiento de la era digital, los avances tecnológicos han permeado diversos aspectos de la vida moderna, transformando la forma en que interactuamos, nos informamos y tomamos decisiones. En particular, el ámbito electoral ha sido testigo de una creciente incorporación de tecnología, con el propósito de optimizar los procesos electorales y fortalecer la integridad democrática. Estos avances han sido particularmente notables en América Latina, donde países como Ecuador han explorado el potencial del voto electrónico como medio para modernizar sus sistemas electorales (Francisco Gabriel et al., 2024).

Es evidente que las Tecnologías de la Información y la Comunicación (TIC) son fundamentales para la evolución de los procesos electorales. Autores como Haque y Carroll han destacado la importancia de las TIC en la mejora de la integridad electoral y en la eficiencia técnica de la administración electoral, respectivamente (Haque & Carroll, 2020). Además, con el creciente interés en los sistemas de votación electrónica, se han propuesto avances significativos, como el uso de blockchain para aumentar la seguridad y la privacidad del proceso electoral.

Blockchain, como innovación relativamente reciente, aporta muchas ventajas a los sistemas de información y se puede aplicar en una variedad de campos. Actualmente se están realizando investigaciones sobre la aplicación de soluciones basadas en blockchain en salud, logística, finanzas, y muchos otros (Berdik et al., 2021). Un tema cada vez más importante y popular en relación con blockchain y los sistemas de información es el voto electrónico (Xiao et al., 2020). Las cualidades únicas de esta tecnología, como la descentralización y la inmutabilidad, resultarán invaluables para garantizar que los votos realizados en el sistema sigan las mismas reglas que rigen las formas más tradicionales de elecciones y votación.

Investigaciones recientes, como la de (Kaudare et al., 2020), destacan el potencial del blockchain, particularmente con Hyperledger, para fortalecer estos sistemas. Sin embargo, a pesar de sus beneficios en términos de transparencia e inmutabilidad, la implementación de blockchain enfrenta desafíos importantes, incluidos la complejidad técnica, los costos asociados y la necesidad de adaptar la normativa vigente.

Aunque países como Estados Unidos, Países Bajos, comenzaron a implementar el voto electrónico desde el 2004, y otros como Reino Unido y Alemania desde el 2009 (Risnanto et al., 2020). Otros países como Ecuador que han considerado proyectos piloto con diversas tecnologías provenientes de países como Argentina, Venezuela, México y Brasil (Toapanta et

al., 2020; Toapanta Toapanta et al., 2020) con iniciativas legislativas para instituir estas herramientas como un componente fundamental de la democracia representativa.

Para febrero de 2021, Ecuador ha iniciado tres planes piloto para su posterior aprobación (Zurita Meza & Ramírez Supe, 2021), con miras a evaluar su viabilidad y eficacia para una eventual implementación futura (Ortiz Osorio, 2021). Esta exploración refleja el reconocimiento de la importancia de la innovación tecnológica en el ámbito electoral, así como el compromiso de mejorar la eficiencia y la transparencia en los procesos electorales.

En este sentido, la evaluación de las vulnerabilidades en los sistemas de votación electrónica desde una perspectiva de ciberseguridad emerge como una tarea imperativa. Es fundamental comprender y abordar los posibles riesgos y desafíos asociados con la implementación de sistemas de votación electrónica, con el fin de salvaguardar la integridad y la confiabilidad de los procesos electorales en Ecuador. Por lo tanto, el presente trabajo se propone como objetivo realizar una evaluación exhaustiva de las vulnerabilidades presentes en los sistemas de votación electrónica utilizados en Ecuador, con el fin de fortalecer la seguridad y la confianza en el proceso electoral del país.

Planteamiento de la investigación (Fundamentación de la investigación)

La adopción de sistemas de votación electrónica representa una evolución significativa en la gestión de los procesos electorales en todo el mundo (Darmawan, 2021; Rosacker & Rosacker, 2020). Además de reducir el riesgo de fraude y error humano, estos sistemas buscan aumentar la eficiencia, accesibilidad y transparencia del proceso electoral, como sucede en Estonia, Suiza y Canadá países donde el voto electrónico ha crecido considerablemente (Essex & Goodman, 2020). Sin embargo, la seguridad sigue siendo un desafío importante. Los sistemas de votación electrónica deben garantizar la integridad y confidencialidad de los datos electorales para preservar la credibilidad de los resultados, considerando que incluso un rumor puede generar dudas sobre la fiabilidad de un sistema de votación electrónico (Pawlak & Poniszewska-Marańda, 2021).

En Latinoamérica, varios países han adoptado sistemas de votación electrónica, pero enfrentan desafíos significativos. En Venezuela, el sistema ha sido criticado por problemas de transparencia y confianza (Corrales, 2020). En Brasil, según (Morgan et al., 2020), la baja adherencia en la rendición de cuentas y la percepción de vulnerabilidades han llevado a la desconfianza en el sistema. Por otro lado, (Khutkyy & Laureda, 2023) señalan que, en Chile y

Colombia, aunque ambos países han implementado el voto electrónico con diferentes enfoques—Chile con un formato simple y limitado en alcance, y Colombia con una plataforma más avanzada y una mayor campaña de educación cívica—ambos enfrentan desafíos relacionados con la brecha digital, la transparencia y la confianza pública, que afectan la efectividad y la participación en el proceso de votación electrónica.

A nivel nacional, Ecuador ha considerado proyectos piloto con diversas tecnologías provenientes de países como Argentina, Venezuela, México y Brasil (Toapanta et al., 2020; Toapanta Toapanta et al., 2020) con iniciativas legislativas para instituir estas herramientas como un componente fundamental de la democracia representativa. El país enfrenta el desafío de garantizar la seguridad de los futuros sistemas de votación electrónica. Esto incluye la implementación de tecnologías de seguridad avanzadas, así como políticas y procedimientos para garantizar la protección de la información electoral.

A nivel operativo, se requiere un análisis detallado de cómo se gestionan y protegen los datos en el sistema de votación electrónica. Esto incluye identificar vulnerabilidades específicas en las bases de datos que almacenan datos electorales, en la infraestructura y los procedimientos que se utilizarán. Las pruebas de escaneo y penetración deben evaluar la capacidad de un sistema para proteger la información de ataques cibernéticos y accesos no autorizados. Es importante garantizar que los datos no puedan modificarse ni manipularse sin autorización y que el acceso a la información se controle y registre adecuadamente.

Finalmente, contar con un plan integral de ciberseguridad es fundamental para proteger los datos almacenados en las bases de datos del sistema de votación electrónica. El plan debe incluir medidas específicas para evitar la manipulación de datos, detectar y responder a incidentes de seguridad y garantizar que se mantenga la integridad de los datos desde su recopilación hasta su almacenamiento. Garantizar la protección de la información es fundamental para mantener la confianza en el proceso electoral y garantizar que los resultados reflejen fielmente la voluntad del electorado.

Justificación

La implementación del sistema de votación electrónica en Ecuador representa un gran paso adelante en la modernización electoral, pero también plantea serios desafíos en materia de ciberseguridad. Proteger los datos confidenciales, desde la identidad de los votantes hasta los resultados de las elecciones, es fundamental para mantener la integridad del proceso. Identificar

y mitigar las vulnerabilidades en estas tecnologías es fundamental para evitar el acceso no autorizado y la manipulación que podría comprometer la validez de los resultados y la confianza del público.

Esta investigación es fundamental para desarrollar mecanismos eficaces de detección de vulnerabilidades y desarrollar planes integrales de ciberseguridad. Al abordar estos problemas de manera proactiva, garantizamos que los sistemas de votación electrónica sean seguros, promovamos una transición exitosa a tecnología electoral avanzada y mantengamos la transparencia y la legitimidad del proceso electoral de Ecuador.

Formulación del problema de investigación

¿De qué manera fortalecer la seguridad informática en los sistemas de votación electrónica en Ecuador, que permita la detección de vulnerabilidades y garantizar la disponibilidad de los datos en el proceso electoral?

Objetivo General:

Generar mecanismos de detección de vulnerabilidades en sistemas de votación electrónica y creación de un plan de fortalecimiento de ciberseguridad.

Objetivos Específicos:

1. Establecer los elementos estructurales y estado actual de seguridad de la información, políticas, procedimientos y tecnologías de seguridad vigentes que permita identificar vulnerabilidades.
2. Realizar pruebas de escaneo de vulnerabilidades en los sistemas de votación electrónica en Ecuador.
3. Evaluar la criticidad y el impacto de las vulnerabilidades identificadas en los sistemas de votación electrónica en Ecuador, para priorizar las acciones de mitigación y fortalecer la seguridad de los procesos electorales.
4. Generar un plan de fortalecimiento de ciberseguridad que permita mantener la integridad desde la generación de los datos, hasta el almacenamiento de los mismos.

Planteamiento hipotético

Hipótesis:

El uso de un plan integral de ciberseguridad, que incluya la implementación de tecnologías avanzadas como blockchain y la realización de pruebas de vulnerabilidades periódicas, fortalece la seguridad en los sistemas de votación electrónica en Ecuador, reduciendo significativamente los riesgos de ciberataques y mejorando la confianza en los procesos electorales.

Justificación de la Hipótesis:

- Identificación de vulnerabilidades: La presencia de vulnerabilidades en los sistemas de votación, como las identificadas mediante herramientas de escaneo como Nessus y Nmap, sugiere la necesidad de un enfoque proactivo en la seguridad de estos sistemas.
- Uso de blockchain: Según estudios recientes mencionados en el documento, blockchain ha demostrado ser una herramienta clave para garantizar la transparencia y la seguridad en los sistemas de votación electrónica, pero aún enfrenta desafíos técnicos.
- Pruebas de vulnerabilidades y corrección: La implementación de un sistema de correlación de eventos y auditorías semestrales reforzaría la capacidad del sistema para resistir ciberataques, asegurando la integridad de los datos durante las elecciones.

Este planteamiento hipotético serviría como base para comprobar si la implementación de estas medidas realmente mitiga los riesgos y fortalece la seguridad electoral.

CAPÍTULO 1. MARCO TEÓRICO REFERENCIAL

1.1. Estado del arte

1.1.1. Seguridad de la información

Basado en la norma ISO/IEC 27032:2012 la Seguridad de la Información, por su parte, se define como la "preservación de la confidencialidad, integridad y disponibilidad de la información". El principal objetivo de la Seguridad de la Información es garantizar la continuidad de los procesos de negocio con el menor daño y limitar los impactos negativos de los incidentes (Taherdoost, 2022).

La mayoría de las definiciones de seguridad de la información se centran en la confidencialidad, la integridad y la disponibilidad (también conocido como el "Triángulo Dorado de la Seguridad" o triángulo de la CIA). Por ejemplo, Matt Bishop afirma que "la seguridad informática se basa en la confidencialidad, la integridad y la disponibilidad" (Yin et al., 2020). Según (Wendy & Gunawan, 2019), cada sigla se define de la siguiente manera:

- **Confidencialidad (C)** significa que los datos y la información representados por datos deben protegerse de tal manera que su uso se limite únicamente a personas autorizadas.
- **Integridad (I)** significa proteger a los usuarios de modificaciones no autorizadas de información. Garantía de que los datos no serán alterados sin la debida autorización.
- **Disponibilidad (A)** significa proteger a los usuarios del uso no autorizado de la denegación.

En el informe *Global Cibersecutiry Index* de la ITU (*International Communication Union*), Ecuador ocupa el puesto 9 en Estados Unidos y el 65 a nivel mundial en términos de ciberseguridad. El gasto comercial global en soluciones de ciberseguridad crecerá un 33% en los próximos 4 años, lo que significa que alcanzará un total de 134.000 millones de dólares al año en 2022 (Morales et al., 2020).

Políticas y procedimientos

En el mundo moderno, la información es un bien valioso. Por lo tanto, los organismos profesionales deberían priorizar las políticas relacionadas con la seguridad de los sistemas de información (ISS) (Bansal et al., 2021; Liu et al., 2020; Silic & Lowry, 2020). El 59% de las empresas de EE. UU. y el Reino Unido informaron problemas de seguridad en 2019. Una Política de Seguridad de la Información (ISP) es un documento oficial que documenta los

procesos que trabajan hacia los objetivos de la organización para garantizar la seguridad de información valiosa y datos técnicos (Alraja et al., 2023).

Según (Afifi, 2020) las políticas de seguridad deben diseñarse y revisarse para que sean claras, concisas, completas y accesibles para todos los usuarios y grupos. Una vez diseñados y revisados, los documentos de política deben pasar por un proceso de revisión exhaustivo, de lo contrario, no tiene sentido desarrollar una política de este tipo; Esto puede parecer normal, pero la única forma de tener una infraestructura de red segura es mediante un monitoreo de seguridad efectivo. En este punto, hay que aclarar quiénes son las partes interesadas, individuos o grupos responsables de redactar la política y entidades responsables de la implementación continua de la política.

Internet es uno de los medios más utilizados para cometer delitos informáticos debido a su capacidad de conectar e interactuar con personas a nivel global, lo que facilita que los infractores se oculten sin dejar evidencia. (Gonzáles et al., 2019) argumentan que el Estado ecuatoriano debe priorizar la formación de recursos humanos y la adopción de tecnologías adecuadas para implementar políticas públicas efectivas contra los crímenes informáticos. Esto también requerirá un sistema de monitoreo y evaluación constante de dichas políticas para asegurar su eficiencia, como señalan (Ramos Torres et al., 2021).

Tecnologías de seguridad de la información

Las tecnologías de seguridad de la información son esenciales para salvaguardar datos y sistemas informáticos contra amenazas como el acceso no autorizado, la manipulación y la destrucción. Estas tecnologías garantizan la integridad, confidencialidad y disponibilidad de la información, protegiendo así los recursos críticos de posibles ataques y vulnerabilidades (Narváez Guerrón, 2024).

Existe una variedad de herramientas de seguridad perimetral que pueden ayudar a mantener segura su red, como *firewalls*, *honeypots*, *iptables* y más. De esta forma, es posible asegurar la confidencialidad e integridad de los datos, analizar criptosistemas, manejar diversos aspectos de los certificados digitales y analizar diferentes usos del cifrado de datos, como SSH, IPSec, VPN-SSL, etc. Estos métodos y técnicas evitan que la seguridad de la información se vea comprometida (Morales et al., 2020).

1.1.2. Sistemas de información

Vulnerabilidades de los sistemas de información

Las vulnerabilidades surgen debido a errores o fallos en el diseño del sistema. En un sentido más amplio, también pueden ser consecuencia de las limitaciones inherentes de la tecnología. Estas limitaciones reflejan que, por principio, ningún sistema puede ser completamente seguro. La seguridad absoluta es una meta inalcanzable, lo que subraya la necesidad constante de identificar, evaluar y mitigar riesgos potenciales en cualquier sistema tecnológico (Arévalo-Cordovilla et al., 2020).

Los sistemas de votación electrónica se están introduciendo o probando en varios países para proporcionar procedimientos de votación más eficientes. Sin embargo, la seguridad de las elecciones electrónicas se ha cuestionado seriamente. La seguridad que puede brindar un sistema de votación electrónica es el uso de sistemas de información y esquemas criptográficos con el fin de reducir costos y errores humanos, y aumentar la velocidad de procesamiento, sin descuidar la seguridad del proceso (Zurita Meza & Ramírez Supe, 2021).

1.1.3. El sistema electoral

La democracia se basa en la elección de autoridades mediante el voto universal, directo y secreto. En algunos casos, el voto es obligatorio para contrarrestar una débil cultura de participación electoral, mientras que, en países con mayor involucramiento y acceso a la información sobre el proceso y los candidatos, el voto es voluntario y se ejerce de manera más activa (Pabón Vásquez, 2021).

La historia electoral ecuatoriana está marcada por extensas y casi constantes reformas, la Tabla 1 muestra la evolución del sistema electoral legislativo desde 1831 hasta el 2002 de elecciones de listas cerradas con la asignación de escaños Webster y votos a estaños por partido (Hecimovich, 2022). También muestra varios métodos de adjudicación de escaños como *D´Hondt* o *Webster* que dividen el total de votos de cada lista para la serie de divisores continuos (Andrea et al., 2021).

Tabla 1.

Resumen de sistemas electorales para el parlamento ecuatoriano (1831-2021)

Elecciones	Tipo	Niveles	Cámaras	Votos	Votos a Estaños	Asignación de escaños
1831-1857	Elecciones indirectas	1	2	N/A	Por candidato	Pluralidad
1863-1924	Voto en bloque por individuos	1	2	M	Por candidato	Pluralidad
1930-1943	Voto limitado	2	2	1≤v≤7	Por candidato	Pluralidad
1948-1970	RP listas cerradas, desbloqueadas	2	2	1	Por partido	Hare
1979-1996	RP listas cerradas, bloqueadas		1			
1998	Voto en bloque por individuos	2			Por candidato	Pluralidad
2002	RP listas libres	1	1	M	Por partido	D'Hondt
2006	RP listas libres					Imperiali
2009	RP listas libres					
2013	RP listas libres	2				D'Hondt provincial, Webster nacional
2017	RP listas libres					
2021	Listas cerradas	2	1	1	Por partido	Webster

Nota: RP=representación proporcional; M=magnitud de distrito; v=votos.

Fuente: (Hecimovich, 2022)

1.1.4. Voto Electrónico

El voto online nunca se había enfrentado a una situación tan favorable como hoy. En tiempos de pandemia, la votación en línea se está convirtiendo cada vez más en la solución más lógica para todo tipo de elecciones. A nivel nacional y local, la velocidad de la innovación en los acuerdos especiales de votación no tiene precedentes. Los organismos de gestión electoral de todo el mundo están reflexionando sobre cómo adaptarse a la nueva normalidad y cómo abordar

algunos de los riesgos asociados con la organización de elecciones durante la pandemia (Castellanos Santamaría et al., 2021).

Voto electrónico en las elecciones nacionales

El voto electrónico es atractivo para las elecciones nacionales en muchos países porque tiene el potencial de eliminar muchos de los problemas asociados con las elecciones tradicionales en papel. Ofrece, entre otras, las siguientes ventajas (Daramola & Thebus, 2020):

- Facilidad para votar con una gran inversión en material electoral en papel y la logística de transportarlo de un lugar a otro;
- Rapidez del proceso de votación y recuento automático de votos y cotejo de resultados;
- Eliminación de errores humanos y sesgos en el registro y la compilación de votos válidos;
- Hasta cierto punto también puede proteger la privacidad de los votantes y la confidencialidad de sus opciones de voto.

Vulnerabilidades del voto electrónico

La explotación de dispositivos consiste en manipular negativamente el hardware, software o equipo de una computadora para que un atacante pueda acceder a información sensible o alterar el funcionamiento del sistema. Esta vulnerabilidad otorga a un adversario un control extraordinario sobre un sistema digital, permitiendo ataques que pueden ser tanto escalables como indetectables. Una vez que los atacantes logran explotar estos sistemas, obtienen control total sobre los dispositivos de votación y su interacción con los votantes. Estos programas maliciosos pueden impedir que los votantes emitan su voto, engañarlos sobre algún aspecto del proceso electoral, exponer sus decisiones de manera pública o incluso degradar la experiencia de votación para desalentarlos a participar (Park et al., 2021).

La explotación a menudo pasa desapercibida para los usuarios, y puede llevarse a cabo de manera tan sutil que incluso un examen forense del dispositivo podría no detectar la presencia del programa malicioso. Un ejemplo especialmente sofisticado es *ShadowWalker*, donde (Palutke et al., 2020) comentan que reside únicamente en la memoria, que oculta la memoria interrumpiendo el proceso de traducción del sistema operativo Windows y proporciona a los escáneres de memoria una vista de la memoria manipulada, haciendo imposible su detección incluso por los niveles más privilegiados del sistema operativo. Este tipo de programa malicioso es extremadamente difícil de identificar y puede eliminarse del sistema sin dejar rastro alguno.

Tipos de equipos de votación electrónica

El sistema de voto electrónico puede utilizarse en diversas aplicaciones, (Panja & Roy, 2021; Umar et al., 2022) detallan algunos tipos de votación electrónica que se plasman la

Tabla 2. El sistema de voto electrónico ofrece unos resultados electorales más precisos, una tabulación más rápida de los resultados, minimiza los errores humanos, es más cómodo para las personas discapacitadas y permite el recuento automático de los resultados electorales (Carreño-Vélez et al., 2021; Kho et al., 2022).

Tabla 2.

Tipos de equipos de votación electrónica

Tipo de votación electrónica	Características	Sistemas de votación
Sistemas de votación por tarjetas perforadas	Con un sistema de votación con tarjeta perforada, una papeleta es una o más tarjetas que el elector perfora (utilizando el equipo de perforación proporcionado) junto al candidato de su elección. Una vez perforada, el votante puede colocar la boleta en una urna o conectarla a un dispositivo de conteo electrónico en el lugar de votación.	- Votomatic - Datavote
Sistemas de escaneado óptico	Estos sistemas cuentan las papeletas marcadas mediante un escáner óptico que las lee y registra los votos.	- Sistemas Marksense - EBM - Bolígrafo digital: estos sistemas utilizan papeletas en papel digital
Máquinas de votación DRE	Con una máquina DRE, la votación puede realizarse el día de las elecciones o puede utilizarse como dispositivo de votación anticipada en los colegios electorales. Es fácilmente comprensible: el votante sólo tiene que pulsar un botón junto a su candidato u opción favorita. O las máquinas DRE tienen una pantalla táctil que muestra la papeleta. Tras las elecciones o el referéndum, la máquina	- La empresa NEDAP suministró sus propias máquinas DRE desde 1989 - Las máquinas de votación DRE empezaron a utilizarse

	DRE produce una tabulación de los datos de la votación almacenados en un componente de memoria extraíble y/o como copia impresa. El sistema también puede permitir la transmisión de papeletas individuales o totales de votos a una ubicación central. El resultado puede entonces consolidarse en un lugar central.	- masivamente en 1996 en Brasil - También se utilizaron a gran escala en Estados Unidos tras la experiencia de Florida 2000

Nota: EBM = *Electronic Ballot Markers* (Marcadores electrónicos de papeletas), DRE = *Direct Recording Electronic* (Grabación electrónica directa)

Fuente: (Umar et al., 2022)

1.1.5. Voto en el Ecuador

En Ecuador, el ejercicio del voto se considera un derecho político fundamental de cada ciudadano, respaldado por las disposiciones constitucionales que aseguran esta libertad y establecen medidas punitivas para aquellos que violen estos principios. Es importante resaltar que, en el contexto ecuatoriano, el voto no solo se percibe como un derecho, sino también como una responsabilidad cívica, ya que cada individuo tiene el deber de participar en la toma de decisiones gubernamentales (Ruiz Romero, 2022).

A pesar de la posibilidad de utilizar métodos físicos o digitales para la votación, el proceso electoral en Ecuador sigue adherido al modelo tradicional. Los resultados se contabilizan, digitalizan, almacenan y presentan en tiempo real a través del sitio web del Consejo Nacional Electoral (CNE), tanto para elecciones presidenciales como para la selección de gobernantes seccionales (Toapanta et al., 2019).

Voto electrónico en el Ecuador

Ecuador experimentó por primera vez el voto electrónico en 2004, a través de un programa piloto con el 2,29% de las juntas receptoras de votos (JRV) en Guayas, Pichincha, Azuay, Imbabura y Manabí. Los proyectos más recientes surgieron en 2014 en Santo Domingo y Azuay; 300.000 personas en 1.000 JRV y 600.000 personas en 2.000 JRV. Además, fue utilizado en una zona rural de Pichincha (Meza Pérez et al., 2021).

1.1.6. Estudios recientes sobre el voto electrónico

La literatura reciente sobre el voto electrónico explora temas cruciales como la privacidad, el secreto del voto y la integridad del proceso. A continuación, se presentará una revisión de los estudios más recientes en estos aspectos, destacando sus hallazgos y contribuciones al campo.

SecureBallot: A secure open source e-Voting system

(Agate et al., 2021) indica en este estudio los desafíos críticos de la votación electrónica, incluyendo la privacidad, el secreto, el anonimato, la integridad, la unicidad y la autenticidad de los votos. Se propone el sistema SecureBallot, que separa las fases de identificación del votante y de votación mediante tecnologías de seguridad avanzadas y probadas, junto con un protocolo seguro basado en técnicas criptográficas de última generación. El procesamiento de datos se realizó con la herramienta automática Casper/FDR, que evaluó propiedades como el secreto, la privacidad de los paquetes de votación y la autenticación mutua. Las conclusiones muestran la eficacia de SecureBallot tanto teórica como práctica, tras su implementación en elecciones universitarias en la Universidad de Palermo durante seis meses, con análisis de comentarios de usuarios a través de cuestionarios. El código fuente del sistema está disponible públicamente para su revisión por expertos en seguridad.

Secure Internet Voting Protocol (SIVP): A secure option for electoral processes

(Satizábal et al., 2022) presentan el protocolo de votación electrónica SIVP, diseñado para garantizar elecciones libres de fraude. El protocolo utiliza firmas ciegas y criptografía de clave pública, y consta de seis fases: anuncio, registro, autenticación, votación, recuento y verificación. Se compara la carga computacional del SIVP con otros protocolos, destacándose por sus nueve características de seguridad. Aunque el número de operaciones criptográficas es alto, se propone el uso de criptografía de curva elíptica (ECC) para optimizar su coste.

Tecnologias Blockchain Voting: Publicly Verifiable Online Voting Protocol Without Trusted Tallying

(Yang et al., 2020) presentan un protocolo de votación en línea basado en blockchain que permite la verificación pública sin una autoridad de recuento confiable. Utiliza cifrado ElGamal con propiedad homomórfica para mantener la confidencialidad de los votos, almacenados en una blockchain inmutable. Aunque el protocolo facilita la verificación, autoconteo, y permite asignar diferentes puntuaciones a candidatos, no aborda la ausencia de recepción ni la resistencia a la coerción, y su seguridad necesita más validación en futuros estudios.

Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract.

(Alvi et al., 2020) presentan un sistema de votación electrónica basado en blockchain que busca mejorar la seguridad y transparencia electoral. El sistema, dividido en cinco fases (gestión de datos, registro de votantes, registro de candidatos, emisión del voto mediante contrato inteligente y recuento de votos), permite la participación remota y el conteo instantáneo de votos al cierre de la jornada electoral. El estudio destaca cómo el uso de técnicas de cifrado avanzadas refuerza la seguridad del sistema y su eficacia en el proceso electoral.

1.2. Políticas y Normativas de Seguridad

Internet es uno de los medios más utilizados para cometer delitos informáticos debido a su capacidad de conectar e interactuar con personas a nivel global, lo que facilita que los infractores se oculten sin dejar evidencia. Gonzáles et al. (2019) argumentan que el Estado ecuatoriano debe priorizar la formación de recursos humanos y la adopción de tecnologías adecuadas para implementar políticas públicas efectivas contra los crímenes informáticos. Esto también requerirá un sistema de monitoreo y evaluación constante de dichas políticas para asegurar su eficiencia, como señalan Ramos Torres et al. (2021).

En esta sección, se explorarán las políticas y normativas clave que guían la seguridad de la información en las organizaciones. Se examinarán los marcos regulatorios y las directrices que establecen estándares de protección, así como su impacto en la gestión de riesgos y el cumplimiento normativo.

Ley Orgánica de Protección de Datos Personales (LOPD)

De acuerdo con (Morán, 2023), la protección de datos personales es un derecho inherente consagrado en la Constitución Política del Estado y varios tratados internacionales en materia de derechos humanos. La protección sirve no sólo para garantizar la privacidad, sino también para asegurar el cumplimiento de las normas relativas a los casos internacionales de administración y procesamiento de información personal.

(Parrales Alarcón et al., 2024) señalan que “La Ley Orgánica de Protección de Datos de Carácter Personal” (LOPD) regula el tratamiento de datos personales para la protección de la intimidad y la vida privada de las personas. Establece principios básicos de: consentimiento, finalidad, proporcionalidad, calidad, seguridad y confidencialidad de los datos. Define las obligaciones de los responsables y encargados del tratamiento de datos y los derechos de los titulares, tales como acceso, rectificación, cancelación y oposición. También establece

procedimientos y sanciones por violación, fortaleciendo así la seguridad de la información dentro del Ecuador. Todo ello garantiza un tratamiento ético y seguro de los datos personales en consonancia con los estándares internacionales.

Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL)

ARCOTEL es una entidad gubernamental del Ecuador encargada de administrar, regular y controlar tanto las telecomunicaciones como el espectro radioeléctrico y su manejo. Además, se ocupa de los aspectos técnicos relacionados con la gestión de los medios de comunicación social que utilizan frecuencias del espectro radioeléctrico o que requieren la instalación y operación de redes (*Ley Orgánica de Telecomunicaciones*, 2015).

El seguimiento exhaustivo de diversos aspectos, como el número de usuarios en los diferentes proveedores de servicios de Internet que emplean distintas tecnologías, forma parte de las funciones de ARCOTEL (Alvarado et al., 2023). Esta entidad dicta el cumplimiento de los planes de seguridad de contingencia en relación con los servicios ofrecidos, aunque no establece mecanismos específicos para asegurar la implementación de estas normativas. Por ello, las empresas proveedoras de servicios de Internet tienen la flexibilidad de configurar o utilizar sistemas de seguridad según sus propios criterios y pueden establecer métodos de seguridad en conjunto con los usuarios o empresas que reciben el servicio, adaptándose a las necesidades particulares de cada caso (Pincay Romero, 2021).

Código Orgánico Integral Penal (COIP)

El COIP de Ecuador reconoce a Internet como un medio crucial para delitos informáticos, ya que facilita la conectividad global y permite a los infractores ocultarse. (Gonzáles et al., 2019) argumentan que el Estado ecuatoriano debe priorizar la formación de recursos humanos y la adopción de tecnologías para implementar políticas públicas efectivas contra estos delitos. Además, (Ramos Torres et al., 2021) destacan la necesidad de un sistema de monitoreo y evaluación constante para garantizar la eficiencia de estas políticas (Aparicio-Izurieta, 2022).

En Ecuador, las leyes vigentes condenan estos delitos con penas de prisión, y están claramente especificados en el COIP. Estas leyes buscan garantizar la seguridad y justicia, abordando una amplia gama de delitos que afectan la integridad y los derechos de las personas. Los delitos incluidos en el COIP son:

En Ecuador, la legislación actual tipifica estos delitos con pena privativa de libertad, y están expresamente señalados en el COIP. Estas leyes tienen como objetivo garantizar la seguridad y

la justicia, con una variedad de delitos contra la integridad y los derechos de las personas. Algunos de esos delitos, que tienen una incidencia considerable en la seguridad de la información, se describen en la Tabla 3 (*Código Orgánico Integral Penal – COIP*, 2014).

Tabla 3.

Delitos informáticos COIP de los sistemas de información

Delito	Sanción	Artículo del COIP
Revelación ilegal de base de datos	PPL de 1 a 3 años	Art. 229
Interceptación ilegal de datos	PPL de 3 a 5 años	Art. 230
Ataque a la integridad de sistemas informáticos	PPL de 3 a 5 años más agravantes	Art. 232
Delitos contra la información pública reservada legalmente	PPL de 5 a 7 años más agravantes	Art. 233
Transferencia electrónica de activo patrimonial	PPL de 3 a 5 años	Art. 231
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	PPL de 3 a 5 años	Art. 234

Nota: PPL = Pena privativa de libertad.

Fuente: (*Código Orgánico Integral Penal – COIP*, 2014).

Familia ISO/IEC 27000

La familia ISO/IEC 27000, también conocida como serie 27000 o familia SGSI (Sistema de Gestión de Seguridad de la Información), es un grupo de normas de seguridad de la información desarrolladas conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). Estas organizaciones son las principales responsables de emitir normas internacionales y de tecnología electrónica, respectivamente.

Esta familia de normas establece requisitos y directrices para que las empresas puedan implementar medidas de seguridad de la información de manera organizada. Para mantenerse al día con los cambios en el entorno de seguridad, estas normas se revisan de manera sistemática, ya sea cuando surge la necesidad o automáticamente después de un cierto período tras su publicación, dependiendo del tipo de norma (De la Rosa Martín, 2021).

El documento principal que ofrece una visión general de toda la familia es la norma ISO/IEC 27000. En él se detalla el propósito y el alcance de cada norma, además de incluir una lista de términos y definiciones fundamentales. Este documento describe, en particular, el concepto clave de Sistema de Gestión de la Seguridad de la Información, que se abordará en la siguiente subsección. Según la ISO/IEC 27000 (ISO, 2018), las normas de esta familia se pueden agrupar en cuatro macroáreas temáticas, que incluyen el vocabulario, las normas de requisitos, las guías de aplicación y los requisitos específicos para diferentes industrias (Morello, 2022). Las normas principales asociadas a cada categoría se ilustran en la Figura 1.

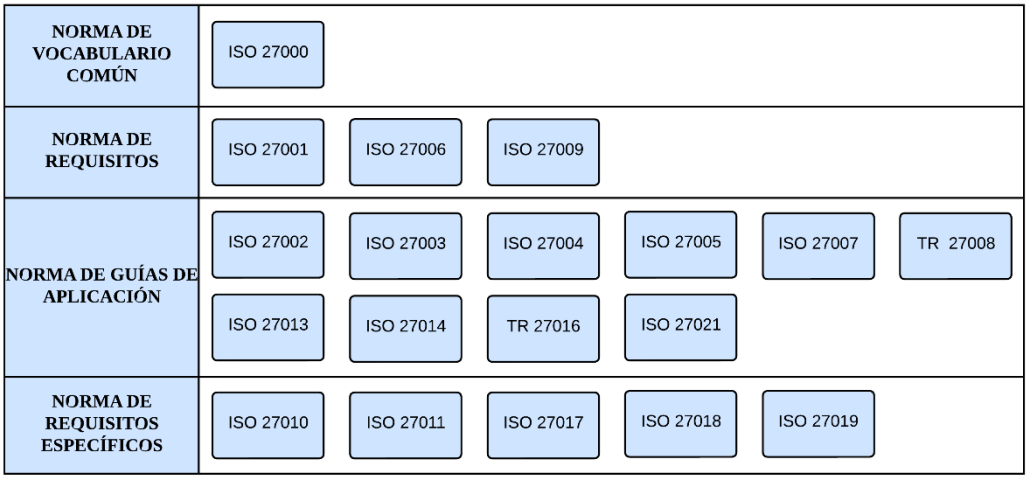

Figura 1. Relaciones de la familia de normas SGSI.

Fuente: Elaboración propia.

ISO/IEC 27001

La norma ISO 27001 es un SGSI que intenta identificar, evaluar y contrarrestar las amenazas a la seguridad de la información en tiempo real. Proporciona recomendaciones para que las organizaciones moldeen su estrategia de seguridad de la información con un enfoque que se ajuste a sus necesidades (Kitsios et al., 2023; Malatji, 2023).

Establecida y publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) en 2005, a medida que BS 7799 evolucionó hasta convertirse en ella, ISO 27001 es una norma que describe los requisitos para construir, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) dentro de cualquier organización. Estos requisitos serán de naturaleza

genérica y relevantes para todas las organizaciones, ya sean grandes o pequeñas, y cualquiera que sea su modelo de negocio (ISO/IEC 27001:2013) (Culot et al., 2021).

ISO/IEC 27002

La norma ISO/IEC 27002, también conocida simplemente como 27002, es un conjunto de controles de seguridad de la información reconocidos como buenas prácticas. Ofrece orientación sobre cómo implementar cada uno de estos controles, detallando su propósito y las directrices a seguir. Las organizaciones suelen utilizar este documento para establecer medidas de protección efectivas que les permitan cumplir con los objetivos de la norma ISO/IEC 27001 o para gestionar riesgos. Además, puede ser consultado durante auditorías para realizar un análisis más exhaustivo de lo que debe aplicarse. Sin embargo, al ser una guía, la norma 27002 no es certificable (Morello, 2022).

En relación con la estructura de la norma 27002, el número de controles y su organización han experimentado cambios a lo largo del tiempo. En revisiones anteriores, estos cambios no han resultado en mejoras significativas. Aunque se suprimieron o añadieron controles, no se actualizaron de manera efectiva, y su organización dentro del documento ha sido compleja y fragmentada, lo que ha reducido su uso en comparación con el Anexo A de la norma 27001, que es más sencillo. Por esta razón, la revisión más reciente se centró en superar estas limitaciones. En la Tabla 4, se muestra la evolución de los números de controles a través de los años.

Tabla 4.

Evolución del número de controles de ISO/IEC 27002 a lo largo del tiempo

Año	2000	2005	2013	2022
N° Controles	129	133	114	93

Fuente: (Morello, 2022).

NIST Cybersecurity Framework (CSF)

Fue publicado en febrero de 2014 en respuesta al decreto ejecutivo presidencial 13636 de 2013, "Mejorando la Ciberseguridad de Infraestructuras Críticas", que solicitaba a los propietarios y operadores de infraestructuras críticas reforzar las defensas y la resiliencia cibernéticas. Posteriormente, el decreto ejecutivo presidencial 13800 de 2017, "Orden Ejecutiva Presidencial sobre el Fortalecimiento de la Ciberseguridad de las Redes Federales y las Infraestructuras

Críticas", ordenó que todas las infraestructuras críticas cumplieran con el CSF (Kwon et al., 2020).

Este marco proporciona una amplia gama de mecanismos de defensa mediante más de 100 controles de ciberseguridad organizados en cinco dominios: Identificar, Proteger, Detectar, Responder y Recuperar, cada uno subdividido en categorías más específicas. Los dominios y categorías del CSF se actualizan anualmente para abordar las nuevas amenazas cibernéticas que emergen (Gordon et al., 2020).

Reglamento General de Protección de Datos

El reglamento general de protección de datos o en su traducción al inglés *General Data Protection Regulation* (GDPR) es la normativa más importante respecto a protección de datos y privacidad en estos años. Aunque es una ley de la Unión Europea, se aplica a cualquier organización que recopile o procese datos de ciudadanos de la UE, sin importar dónde esté ubicada. La naturaleza global del comercio y el flujo de personas hizo que empresas de todo el mundo ajustaran sus prácticas para cumplir con el GDPR en lo que respecta a la gestión de la información de identificación personal (PII) de sus empleados y clientes (Zaeem & Barber, 2020).

El reglamento entró en vigor el 25 de mayo de 2018 y muchas empresas que operan en la UE o procesan datos de sus ciudadanos han actualizado sus políticas de privacidad para cumplir con el GDPR (Marcén, 2021). Además, el GDPR impulsa el progreso global en la regulación de la privacidad para satisfacer las demandas de los consumidores respecto a sus derechos sobre los datos (Zaeem & Barber, 2020).

El GDPR tiene como objetivos principales otorgar a los individuos el control sobre sus datos personales y unificar las normativas dentro de la UE para simplificar los negocios. Sus principios fundamentales son:

- Legalidad, equidad y transparencia
- Limitación de la finalidad
- Minimización de datos
- Exactitud
- Limitación del almacenamiento
- Integridad y confidencialidad (seguridad)
- Rendición de cuentas

1.3. Tecnología Blockchain

Blockchain es una forma de libro mayor distribuido en el que los participantes pueden almacenar e intercambiar información directamente entre sí sin conocimiento previo ni confianza mutua. Blockchain aplica este concepto agregando registros en bloques de datos firmados criptográficamente para evitar la manipulación de datos. El enfoque habitual es crear un hash del registro anterior e insertarlo en el encabezado del siguiente bloque de datos. Por lo tanto, cada bloque depende del bloque anterior, y cualquier intento de modificar un registro en la cadena modificará el hash de los bloques posteriores de la cadena. Para que los participantes identifiquen una cadena válida de registros y garanticen la integridad de los datos, los participantes en una cadena de bloques deben acordar un protocolo de consenso (El Madhoun et al., 2021).

1.3.1. Implementaciones utilizadas con blockchain

Las diferentes aplicaciones de voto electrónico basadas en blockchain comparten un proceso general similar, que abarca desde el registro del votante hasta el anuncio de los resultados. En esta sección, después de una breve explicación del funcionamiento general del voto electrónico con tecnología blockchain, (Benabdallah et al., 2022) presentan algunas características técnicas de distintas implementaciones. Además, se detalla por fases el procesamiento del voto electrónico con blockchain, como se muestra en la Figura 2.

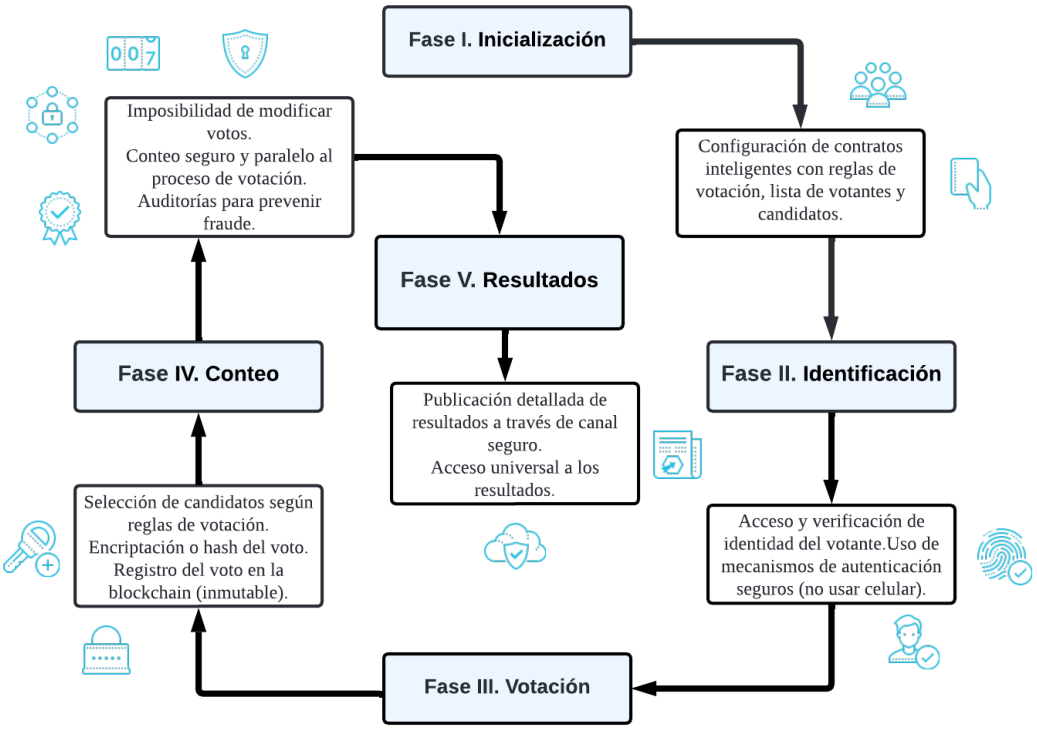

Figura 2. Fases de procesamiento del voto electrónico con Blockchain.

Fuente: Elaboración propia.

Características técnicas del voto electrónico con Blockchain

El protocolo de consenso — conjunto de normas y procedimientos establecidos en una red Blockchain (Guru et al., 2023) — es una característica importante de la solución. Los artículos (Al-Madani et al., 2020; Pramulia & Anggorojati, 2020; Zhang et al., 2019) proponen soluciones blockchain de *Ethereum* que admiten contratos inteligentes. Estos contratos inteligentes actúan como un libro de contabilidad público para registrar y contar votos. Garantizan la privacidad y pueden admitir métodos de cifrado personalizados. Sin embargo, los contratos inteligentes en Ethereum tienen problemas de escalabilidad que pueden resolverse implementándolos en una red menos descentralizada. Los autores (Afraz et al., 2023; Bellini et al., 2020; Soud et al., 2020) propusieron soluciones utilizando contratos inteligentes en *Hyperledger Fabric* que pueden ejecutar hasta 100.000 transacciones por segundo. Por otro lado, (McCorry et al., 2021) propone el uso de Bitcoin como implementación blockchain para el voto electrónico. Bitcoin es una conocida criptomoneda de código abierto basada en blockchain.

El uso de la tecnología blockchain no elimina por completo la presencia de una autoridad central que gestiona la votación. Además, las cadenas de bloques públicas tendrían dificultades para gestionar las elecciones nacionales debido a problemas de escalabilidad. Muchas soluciones ofrecen cadenas de bloques parcialmente centralizadas.

1.3.2. Evaluación y Gestión de Seguridad de la Información con Blockchain

Según (Dankan Gowda et al., 2023), Blockchain ofrece "una solución robusta a través de su libro mayor distribuido para el intercambio seguro de datos sin necesidad de confianza mutua entre entidades". Esta tecnología se está integrando en varias aplicaciones debido a sus capacidades para superar las brechas en la protección de datos y mejorar la identificación de vulnerabilidades en redes complejas. Su capacidad para proporcionar una base sólida para la seguridad puede mejorar la protección de datos y, en consecuencia, abordar los desafíos relacionados con la gestión de redes distribuidas.

1.3.3. Amenazas para la seguridad en Blockchain

A medida que la tecnología blockchain se utiliza cada vez más en diversas áreas de aplicación, el número de intentos de ataque blockchain también ha aumentado considerablemente, lo que lleva a muchos esfuerzos sobre qué ataques son específicos y deben identificarse y mitigarse. Por ejemplo, hay algunos trabajos como el de (Wu et al., 2020), que consideran las debilidades del algoritmo de consenso PoW, las inconsistencias de datos debido a bifurcaciones y la gestión de escalabilidad como algunas de las razones por las que >50% de ataques podrían ocurrir en sistemas basados en blockchain. Pero hasta donde sabemos, se ha prestado poca atención a cómo los ataques de maleabilidad afectarían a los sistemas basados en blockchain, especialmente la votación electrónica desde la perspectiva de blockchain.

El impacto de un ataque a un sistema de votación electrónica de este tipo probablemente sea grande, particularmente debido a la posible interrupción del proceso de votación que podría resultar de un ataque de falsificación de transacciones. En la Tabla 5 se muestra una clasificación de las amenazas a la seguridad de los sistemas basados en blockchain, que clasifica los siguientes ataques conocidos que pueden dañar las redes blockchain. Las tres clases incluyen los ataques basados en el diseño del software (Ajayi & Saadawi, 2021; Zhang et al., 2019), los ataques a redes P2P (Aggarwal & Kumar, 2021; Alangot et al., 2021; Báez Cheza, 2021; Iqbal & Matulevicius, 2021; Wani et al., 2021) y los ataques mineros (Chen et al., 2020; Chicarino et al., 2020; Khan et al., 2021; Li et al., 2020; Nicolas et al., 2021).

Tabla 5.

Amenazas para la seguridad de los sistemas basados en blockchain.

Categoría		Ataques	
Ataques basados en el diseño del software	Consisten en manipular el estado de la cadena de bloques al aprovechar vulnerabilidades en el software.	Estado del software y su estructura de datos incoherentes	
		Maleabilidad de las transacciones	Doble gasto con eclipse
			Doble gasto con confirmaciones
Ataques a redes P2P	En este tipo de ataque, los nodos maliciosos pueden insertar sus direcciones en la lista de nodos confiables del vecino, lo que permite al atacante aislar al nodo objetivo.	Sybil	Ocurre cuando un atacante asume múltiples identidades simultáneamente
		DDos	Agota la capacidad de la red, lo que provoca la denegación de servicio a los mineros legítimos
		Eclipse	Se centra en bloquear nodos específicos,
		Doble gasto	Permiten a los atacantes crear la ilusión de que un activo o token se presenta y reutiliza
Ataques mineros	Ocurren cuando los mineros manipulan el proceso de minería para beneficiarse a sí mismos, decidiendo qué transacciones aceptar o rechazar.	Doble gasto	Manipulación
			Fuerza bruta
			Finney
		Minería egoísta	
		Retención de bloque	
		Secuestro de tiempo	

Fuente: Elaboración propia.

1.3.4. Riesgos de los sistemas de votación electrónica basados en Blockchain

Aunque la tecnología blockchain ofrece prometedoras soluciones para la emisión y seguridad de votos, presenta varias vulnerabilidades que pueden comprometer su eficacia. Aspectos cruciales como la seguridad de los puntos finales, los desafíos de escalabilidad, la dificultad de mantener el anonimato mientras se verifica la elegibilidad, y los riesgos de compra de votos se detallan en la Tabla 6, basándonos en la información proporcionada por (Abuidris et al., 2019).

Comprender estas debilidades es esencial para evaluar el verdadero potencial y las limitaciones de la blockchain en el ámbito electoral.

Tabla 6.

Las vulnerabilidades de los sistemas de voto electrónico basados en blockchain.

Vulnerabilidad	Impacto
Escalabilidad	Capacidad de estos sistemas para manejar un creciente número de transacciones, usuarios, y datos de manera eficiente sin degradar su rendimiento, seguridad, o funcionalidad. Aunque Blockchain es inherentemente escalable, la experiencia ha demostrado que puede volverse considerablemente lento como ocurrió cuando Bitcoin alcanzó un valor de casi 20.000 dólares en diciembre de 2017 (Patel et al., 2022).
Anonimato y verificación	El sistema evita inherentemente que un votante vote dos veces gracias a que blockchain evita *double spending*. La blockchain sirve de registro donde publicar las pruebas que aseguran que el proceso ha funcionado correctamente.
Seguridad de los puntos finales	Estos puntos, como las máquinas que usan los votantes para interactuar con la blockchain, son susceptibles a problemas de seguridad que pueden comprometer las credenciales necesarias para acceder al sistema.
Compra de votos (coacción)	La blockchain podría facilitar la compra de votos al eliminar la confidencialidad del voto. Aunque la encriptación protege la información, el sistema puede permitir a los compradores verificar cómo votó una persona. Esto podría aumentar la posibilidad de coacción, especialmente si las identidades de los votantes están vinculadas a sistemas donde se pueden recibir sobornos, poniendo en riesgo la integridad del proceso democrático.

Fuente: Elaboración propia.

1.4. Tecnologías de Seguridad en Sistemas de Votación Electrónica

La Tabla 7 indica las diferentes herramientas para necesarias para aplicar defensa en profundidad para proteger los sistemas de votos electrónicos.

Tabla 7.

Tipos de firewall y su aplicación en los sistemas de votación electrónica.

Tipo de Firewall	Descripción	Aplicación en Sistemas de Votación Electrónica
Firewall Perimetral	Controla el tráfico de entrada y salida entre la red interna y el exterior.	Protege el acceso a los servidores de votación desde el exterior para evitar accesos no autorizados.
Firewall Interno	Segmenta la red interna en diferentes zonas de seguridad.	Aísla componentes críticos de la infraestructura de votación, como servidores y bases de datos, para limitar el impacto de posibles brechas de seguridad.
Firewall de Capa de Aplicación	Filtra el tráfico en la capa de aplicación para proteger aplicaciones específicas.	Protege aplicaciones de votación contra ataques específicos, como inyecciones SQL y *cross-site scripting* (XSS).
Firewall de Próxima Generación (NGFW)	Combina funcionalidades de firewall tradicionales con capacidades avanzadas como prevención de intrusiones y filtrado de contenido.	Ofrece una protección integral para sistemas de votación, identificando y mitigando amenazas avanzadas y proporcionando visibilidad detallada del tráfico.
Firewall de Estado	Monitorea el estado de las conexiones y asegura que el tráfico sea parte de una sesión establecida.	Garantiza que solo el tráfico legítimo y esperado pueda acceder a los sistemas de votación, reduciendo el riesgo de ataques de suplantación.
Firewall Basado en Host	Se instala en cada dispositivo individual para controlar el tráfico de red.	Protege cada componente del sistema de votación, como estaciones de trabajo y servidores, de ataques específicos dirigidos a esos dispositivos.

Nota: SQL = *Structured Query Language* (Lenguaje de consulta estructurada).

Fuente: Elaboración propia.

1.5. NIST SP 800-30

La publicación especial 800-30 del Instituto Nacional de Normas y Tecnología (NIST) ofrece pautas prácticas para la evaluación de riesgos en sistemas de información tanto organizacionales como gubernamentales. Estas pautas complementan las de la Publicación Especial 800-39, con un enfoque claro y sencillo que facilita su aplicación (Putra & Soewito, 2023).

El proceso incluye la identificación de fuentes y eventos de amenazas, la detección de vulnerabilidades, el análisis de probabilidades y tendencias, el estudio de impactos, y finalmente, la determinación del nivel de riesgo (Blank & Gallagher, 2012; Putro et al., 2021).

1.6. Herramientas de escaneo de vulnerabilidades

Nmap

Nmap son las siglas de Network Mapper. Es una herramienta de código abierto para la línea de comandos, principalmente para Linux, que se creó para realizar auditorías de ciberseguridad, gestión de actualizaciones de servicios y monitoreo de host. Nmap puede ejecutar diferentes tipos de escaneos, como escaneos de ping, escaneos de un solo host o escaneos ocultos. Además, permite que los tiempos de escaneo se exporten a archivos XML, lo que lo convierte en un analizador de paquetes ideal y establece un alto estándar de velocidad y facilidad de uso (Asmat, 2023; Eshetu et al., 2024).

Nessus

Tras haber superado los dos millones de descargas en todo el mundo, Nessus demuestra ser uno de los escáneres de vulnerabilidades más utilizados. Ofrece una cobertura amplia y detallada, capaz de analizar más de 59.000 vulnerabilidades (CVEs), lo que lo convierte en una herramienta fundamental para la identificación y gestión de riesgos de seguridad en cualquier entorno (Pandey & Chaudhary, 2023).

OpenVas

Open Vulnerability Assessment System (OpenVAS), uno de los escáneres de vulnerabilidades más avanzados, fue desarrollado por Greenbone Networks y mantenido para brindar una solución completa para la detección de vulnerabilidades. Incluye numerosas comprobaciones automatizadas y tiene una interfaz web intuitiva que permite una configuración y ejecución de escaneos fácil y rápida, aunque el usuario puede personalizarlo en gran medida (Muharrom & Saktiansyah, 2023).

Nexpose

Nexpose, herramienta de escaneo que detecta puertos abiertos, servicios y aplicaciones en ejecución. Mediante el uso de las aplicaciones y los servicios, intenta detectar vulnerabilidades existentes en una red (Chhillar & Shrivastava, 2021).

Qualys Guard

Qualys ofrece soluciones de gestión de vulnerabilidades en la nube que permiten a las empresas identificar, evaluar y priorizar los riesgos de seguridad asociados a sus operaciones comerciales. Garantiza la visibilidad de todos los activos locales y en la nube para detectar amenazas en tiempo real y evalúa automáticamente la gravedad de las vulnerabilidades para ahorrar tiempo a los equipos de seguridad al centrar sus esfuerzos en los riesgos críticos. Integrada con otras aplicaciones de seguridad y con informes automatizados, facilita enormemente el cumplimiento de los requisitos normativos y mejora la ciberseguridad general. Esta solución escalable y rentable optimiza la respuesta a incidentes sin infraestructura adicional (Srivastava & Singh, 2024).

Nikto

Nikto puede escanear varios servidores web a la vez y, por lo tanto, es flexible y rápido para que los profesionales de la seguridad evalúen el estado de sus aplicaciones web. Puede identificar más de 6700 archivos y scripts CGI potencialmente peligrosos, vulnerabilidades específicas de versiones en más de 270 servidores y software bastante desactualizado en los 1250 servidores, lo que permite a los administradores anticiparse a posibles brechas de seguridad. Esto puede brindar una oportunidad anticipada para fortalecer las defensas antes de que sean explotadas por los atacantes (Toto & Sánchez, 2021).

Acunetix

Acunetix, el pionero en análisis de seguridad web desde 2005, ha experimentado constantes mejoras a lo largo del tiempo. Es una herramienta avanzada y personalizada desarrollada por expertos en pruebas de ciberseguridad. Esta especialización ha permitido ofrecer una opción realista y más eficiente en comparación con la mayoría de las herramientas propietarias. *Acunetix Vulnerability Scanner* es una solución integral para la detección de vulnerabilidades en aplicaciones web, que puede usarse de forma autónoma o como parte de un sistema más amplio. Incluye detección y gestión de vulnerabilidades conocidas, además de diversas funciones complementarias con herramientas de desarrollo de software económicas (Sheikh & Kumar Singh, 2023).

CAPÍTULO 2. METODOLOGÍA

2.1. Contexto de la investigación

El proyecto se realizó en Ecuador, país ubicado en América del Sur sobre la línea ecuatorial (ver Figura 3). La ejecución abarcó un período de 3 meses y 2 semanas, iniciando en la tercera semana de julio y concluyendo en octubre de 2024. Durante este tiempo, se llevaron a cabo diversas actividades enfocadas en cumplir los objetivos establecidos, ajustándose al cronograma previamente definido.

Figura 3. Ubicación del Ecuador.

Fuente: Google Maps

2.2. Diseño y alcance de la investigación

La propuesta inicia con una evaluación detallada de la criticidad y el impacto de las vulnerabilidades detectadas en los sistemas de votación electrónica en Ecuador. Este análisis se centró en la aplicación web del Consejo Nacional Electoral (CNE), permitiendo una comprensión profunda de las debilidades y sus posibles repercusiones en la seguridad electoral.

La investigación se define como aplicada, se enfoca en identificar y evaluar las vulnerabilidades presentes en los sistemas de votación electrónica sin manipular o intervenir directamente en estos sistemas. En lugar de alterar el entorno para observar sus efectos, el análisis se realiza sobre el estado actual de los sistemas. Además, el alcance de la investigación es descriptivo, ya que su objetivo principal es proporcionar una descripción detallada de las vulnerabilidades identificadas y evaluar su impacto en la seguridad de los sistemas de votación en Ecuador. Esto

permite un entendimiento profundo del estado de la seguridad sin intentar establecer relaciones causales o probar nuevas hipótesis.

2.3. Tipo y métodos de investigación

Esta propuesta utilizará el enfoque cuantitativo mediante encuestas dirigidas a expertos en ciberseguridad. Este enfoque permitirá obtener datos objetivos y estructurados sobre la percepción de los especialistas en relación con las vulnerabilidades y medidas de seguridad en sistemas de votación electrónica. Al ser encuestados profesionales en el área, los resultados proporcionarán una base sólida para el análisis estadístico y facilitarán la identificación de tendencias y patrones relevantes para la investigación.

2.4. Población y muestra

La población es el Consejo Nacional Electoral (CNE) y la muestra tomada será representativa en los funcionaros del departamento del centro de datos.

2.5. Técnicas e instrumentos de recolección de datos

Para la recolección de datos en este estudio, se utilizó exclusivamente la **encuesta** como técnica, diseñada con preguntas cerradas que ofrecieron opciones predefinidas y escalas de medición, lo que permitió obtener información estructurada y cuantificable. El cuestionario, compuesto por 8 preguntas técnicas, fue dirigido a la población ecuatoriana y se distribuyó a través de *Google Forms*, garantizando así una mayor accesibilidad y cobertura en la recolección de datos.

2.6. Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información.

La Tabla 8 presenta a los tres expertos en ciberseguridad que participarán en la evaluación de las preguntas de la encuesta. Estos profesionales han sido seleccionados por su experiencia y conocimiento en el campo, asegurando que las preguntas sean relevantes, precisas y adecuadas para obtener datos significativos sobre la ciberseguridad en sistemas de votación electrónica.

Tabla 8.

Evaluadores de la Encuesta: Expertos en Ciberseguridad

Nombre del experto	Institución	Observación	Confiabilidad (1-10)
Ing. Edisson Quintuña Padilla, **M.Sc.**	Universidad Estatal Península de Santa Elena	- Se recomienda organizar las preguntas de manera que vayan de aspectos generales a temas más específicos por lo que sugiere un nuevo orden. - En las preguntas con respuestas escaladas, se ha añadido el término al que se refiere cada pregunta, esto con el fin de mantener consistencia con otras preguntas que usan este tipo de escala. - La última pregunta ha sido reformulada, proporcionando una descripción más detallada de cada opción.	8
Ing. Gabriel Eduardo Morejón López, **M.Sc.**	Universidad Técnica de Manabí	Abordar el uso de blockchain y los estándares que se están formando alrededor; tener en cuenta la situación política inestable que suele atravesar nuestro País.	9
Ing. Juan Carlos Enrique Ortega Acosta, **M.Sc.**	Universidad Técnica Estatal de Quevedo	Tener claro cuáles son las vulnerabilidades en el proceso de voto electrónico para de ahí sacar las preguntas, las primeras preguntas como que hacen referencia al sistema tradicional de votos. O tal vez, cambiar el objetivo de la encuesta a evaluación del sistema tradicional de votos.	9

Fuente: Elaboración propia

2.7. Metodología de desarrollo

La metodología cuantitativa en la Evaluación de Riesgos utiliza técnicas matemáticas y estadísticas para medir y gestionar riesgos de manera precisa. Basada en datos numéricos y modelos predictivos, permite identificar, evaluar y priorizar riesgos con objetividad. La Figura 4 ilustra las fases de esta metodología, desde la identificación de los activos hasta el análisis de impacto, proporcionando un enfoque riguroso y sistemático para la gestión de riesgos.

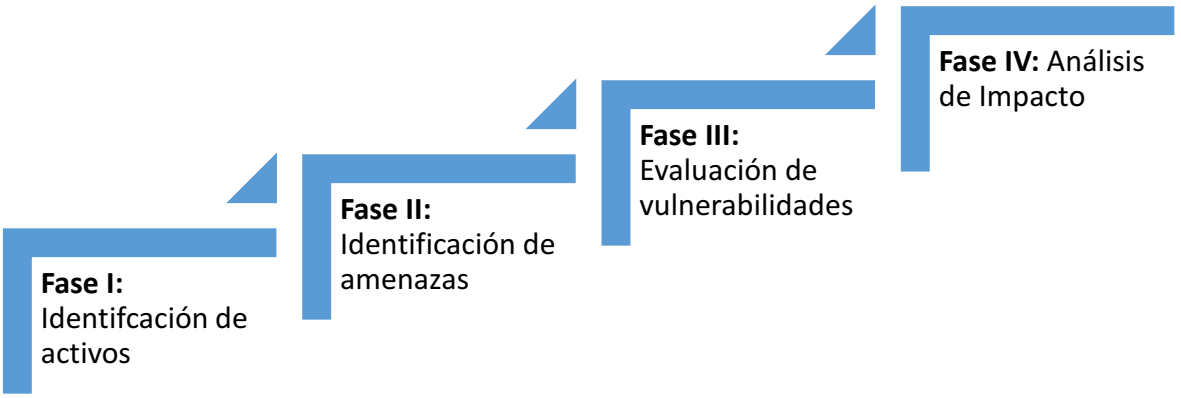

Figura 4. Fases de la metodología Risk Assessment

Fuente: Elaboración propia

2.7.1. Fase I: Identificación de Activos

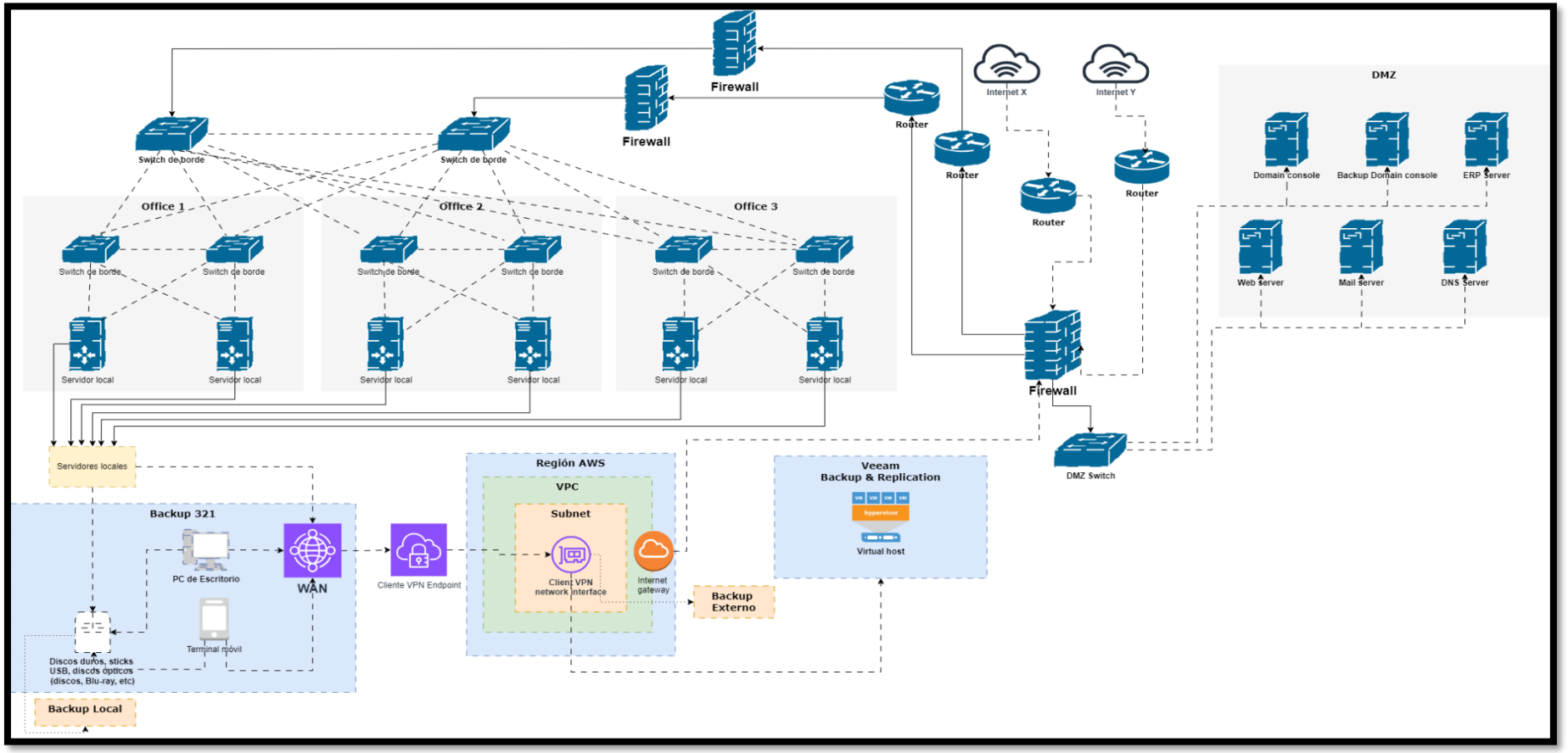

Figura 5. Arquitectura de red simulada del CNE

Fuente: Elaboración propia

La Tabla 9 presenta los principales componentes y sus características dentro de una arquitectura de red simulada del CNE, basada en la configuración ilustrada en la Figura 5. Esta infraestructura refleja un enfoque redundante y seguro, asegurando la continuidad de las operaciones críticas en el entorno electoral.

Tabla 9.

Componentes y Características Básicas de la Infraestructura de Red simulada del CNE

Componente	**Características básicas**
Enlaces de Internet	Conexiones de alta velocidad, redundantes para asegurar disponibilidad y balanceo de carga.
Firewalls	Dispositivos de seguridad que monitorean y controlan el tráfico de red. Incluyen inspección profunda de paquetes y gestión de VPN. Redundantes para alta disponibilidad.
Switches de borde	Switches gestionables con soporte para VLAN, redundancia a nivel de conexión (LACP/Spanning Tree), y priorización de tráfico.
Servidores	Equipos físicos o virtuales con alta capacidad de procesamiento y almacenamiento. Incluyen redundancia y soporte para virtualización.
AWS (Amazon Web Services)	Servicios de nube que proporcionan almacenamiento escalable, respaldo remoto, y opciones de recuperación ante desastres.
Sistema de *backup* local	Equipos NAS o discos duros externos utilizados para almacenamiento de copias de seguridad rápidas.
Sistema de *backup* externo	Servicios de almacenamiento remoto, en la nube o en sitios físicos fuera del lugar de operación principal.
Esquema de *backup* 3-2-1	Estrategia que asegura la redundancia de datos mediante la creación de múltiples copias, almacenadas local y remotamente.
Vin Backup	Software de *backup* que permite realizar copias automatizadas, con soporte para virtualización y respaldo incremental.

Fuente: Elaboración propia

2.7.2. Fase II: Identificación de Amenazas

Se llevará a cabo un análisis de seguridad enfocado en la detección de puertos abiertos en el servidor asociado a la aplicación web **https://app01.cne.gob.ec/**, con dirección IP: **45.223.23.130**. Este análisis tiene como objetivo identificar posibles puntos de entrada que podrían ser aprovechados por actores malintencionados para comprometer la seguridad del

sistema. Las herramientas utilizadas para realizar los análisis de escaneo de vulnerabilidades se encuentran en la tabla Tabla 10.

Tabla 10.

Herramientas de Escaneo

Herramienta	Función
Nmap	Para identificar servicios y puertos abiertos que puedan estar expuestos en el servidor.
Nessus	Herramienta de escaneo de vulnerabilidades que detecta fallas de seguridad en sistemas y redes, ayudando a identificar y corregir posibles puntos de ataque

Fuente: Elaboración propia

La Tabla 11 presenta un análisis exhaustivo de los puertos abiertos con mayor riesgo, identificados en los escaneos realizados con Nessus y Nmap. Cada puerto se evalúa según su uso común, la razón de su vulnerabilidad, su probabilidad, el impacto potencial en caso de ser explotado, y el nivel de riesgo asignado. Esta información es clave para priorizar acciones correctivas, ya que permite identificar rápidamente los puertos más expuestos y con mayor potencial de causar daños en la infraestructura. La tabla sirve como una herramienta crucial para guiar las decisiones en la fase de mitigación de amenazas y refuerzo de la ciberseguridad del sistema.

Tabla 11.

Identificación de puertos abiertos con riesgo alto en los análisis de Nessus y Nmap

Puerto	Uso Común	Razón	Probabilidad	Impacto	Nivel de riesgo
11	Systat	Información del sistema expuesta.	Alto	Importante	Alto
21	FTP (Transferencia de archivos)	Datos sin cifrar, vulnerable a ataques de sniffing y MitM.	Alto	Importante	Alto
48	UUCP (Protocolo Unix de Copiado de Archivos)	Obsoleto, susceptible a ataques de red.	Alto	Importante	Alto

53	DNS	Vulnerable a envenenamiento de caché y ataques de redirección.	Alto	Importante	Alto
65	TACACS (Autenticación en redes)	Cifrado débil, susceptible a ataques.	Alto	Moderada	Alto
66	Oracle SQL*Net	Vulnerable a ataques DoS y desbordamiento de búfer.	Alto	Moderada	Alto
80	HTTP (Web no cifrada)	Tráfico sin cifrar, susceptible a ataques MitM.	Alto	Importante	Alto
88	Kerberos (Autenticación)	Vulnerable a ataques de repetición.	Alto	Importante	Alto
118	Autenticación remota	Autenticación débil, susceptible a ataques remotos.	Alto	Moderada	Alto
135	Microsoft RPC	Ejecución remota de código, ataques de red.	Alto	Importante	Alto
139	NetBIOS	Permite acceso no autorizado a recursos compartidos.	Alto	Importante	Alto
389	LDAP (Directorio sin cifrado)	Vulnerable a inyección y ataques DoS.	Alto	Importante	Alto
443	HTTPS (Web cifrada)	SSL/TLS mal configurado, ataques de downgrade.	Alto	Importante	Alto
444	Apache JServ Protocol (AJP)	Vulnerabilidad en control remoto de servidores.	Alto	Importante	Alto
465	SMTPS (Correo seguro)	Vulnerabilidades de SSL/TLS mal configuradas.	Alto	Importante	Alto
500	IKE (VPN, IPSec)	Vulnerable a ataques de fuerza bruta en configuraciones VPN.	Alto	Importante	Alto
543	Kerberos (Autenticación)	Autenticación débil.	Alto	Importante	Alto
554	RTSP (Streaming)	Expuesto a ataques DoS y de explotación.	Alto	Importante	Alto
555	Control remoto	Control remoto no autenticado.	Alto	Importante	Alto

587	SMTP (Correo con autenticación)	Susceptible a relé de correos no deseados y ataques de spam.	Alto	Importante	Alto
631	CUPS (Impresión en red)	Vulnerable a ataques DoS y ejecución remota.	Alto	Importante	Alto
636	LDAP (Seguridad mejorada)	SSL/TLS mal configurado.	Alto	Importante	Alto
783	SpamAssassin (Anti-spam)	Desbordamiento de búfer.	Alto	Importante	Alto
990	FTPS (Transferencia de archivos segura)	Vulnerable a problemas de cifrado.	Alto	Importante	Alto
993	IMAPS (Correo seguro)	SSL/TLS mal configurado, ataques MitM.	Alto	Importante	Alto
995	POP3S (Correo seguro)	Vulnerable a ataques de downgrade y cifrado débil.	Alto	Importante	Alto
1080	SOCKS Proxy	Proxy abierto, abuso para tráfico malicioso.	Alto	Importante	Alto
1111	Depuración remota	Sin autenticación, acceso remoto a debug.	Alto	Importante	Alto
1186	Oracle Database	Vulnerable a desbordamientos de búfer.	Alto	Importante	Alto
1194	OpenVPN	Susceptible a configuraciones inseguras.	Alto	Importante	Alto
1352	Lotus Notes	Ejecución remota de código y ataques DoS.	Alto	Importante	Alto
1433	Microsoft SQL Server	Inyecciones SQL y acceso remoto.	Alto	Importante	Alto
1494	Citrix	Vulnerable a ataques no autorizados.	Alto	Importante	Alto
1521	Oracle Database	Autenticación débil, ataques de red.	Alto	Importante	Alto
1701	L2TP/IPsec (VPN)	Vulnerable a ataques de fuerza bruta.	Alto	Importante	Alto
2000	Cisco SCCP	Susceptible a control remoto no autorizado.	Alto	Importante	Alto

2375	Docker (Sin autenticación)	Control remoto no autenticado, ejecución de comandos maliciosos.	Alto	Moderada	Alto
2376	Docker (Con TLS)	Mal configurado, susceptible a ataques de red.	Alto	Moderada	Alto
2377	Docker Swarm	Expuesto a ataques de explotación de red.	Alto	Moderada	Alto
2379	etcd	Sin autenticación, datos expuestos.	Alto	Importante	Alto
2380	etcd Clúster	Sin autenticación, control remoto abierto.	Alto	Importante	Alto
13218	Honeywell HC900	Vulnerable a control remoto no autenticado.	Alto	Importante	Alto
13223	Sistemas industriales	Autenticación débil, susceptible a ataques remotos.	Alto	Importante	Alto
13224	Honeywell	Control remoto no autorizado, explotable.	Alto	Importante	Alto
13701	Edgeport	Acceso no autorizado, vulnerabilidad en autenticación.	Alto	Importante	Alto
13702	Edgeport	Falta de cifrado, expuesto a ataques críticos.	Alto	Importante	Alto
13705	Edgeport	Acceso a comandos remotos sin autorización.	Alto	Importante	Alto
13706	Edgeport	Vulnerabilidad de autenticación débil.	Alto	Importante	Alto
13708	Edgeport	Exposición de datos sensibles.	Alto	Importante	Alto
13709	Edgeport	Comandos remotos ejecutados sin autorización.	Alto	Importante	Alto
13710	Edgeport	Vulnerable a acceso remoto.	Alto	Importante	Alto
13711	Edgeport	Sin autenticación, servicios abiertos.	Alto	Importante	Alto
13712	Edgeport	Riesgo de control remoto sin restricciones.	Alto	Importante	Alto
13713	Edgeport	Comandos ejecutados remotamente sin autorización.	Alto	Importante	Alto

13714	Edgeport	Acceso a comandos privilegiados sin control.	Alto	Importante	Alto
13715	Edgeport	Vulnerabilidad a ataques externos.	Alto	Importante	Alto
13716	Edgeport	Riesgo elevado de explotación remota.	Alto	Importante	Alto
13717	Edgeport	Sin protección adecuada contra ataques remotos.	Alto	Importante	Alto
13718	Edgeport	Control remoto no autorizado.	Alto	Importante	Alto
13720	Edgeport	Autenticación insuficiente.	Alto	Importante	Alto
13721	Edgeport	Servicios expuestos sin autenticación.	Alto	Importante	Alto
13722	Edgeport	Vulnerabilidad en control remoto de dispositivos.	Alto	Importante	Alto
13782	Servicios industriales	Sin cifrado, expuestos a abuso.	Alto	Importante	Alto
13783	Servicios industriales	Control remoto sin autenticación.	Alto	Importante	Alto
13785	Servicios industriales	Explotación de comandos remotos sin seguridad.	Alto	Importante	Alto
13786	Servicios industriales	Vulnerabilidad crítica en autenticación y control remoto.	Alto	Importante	Alto
14141	Honeywell	Autenticación débil, susceptible a ataques.	Alto	Importante	Alto
14142	Honeywell	Falta de cifrado, expuesto a abuso.	Alto	Importante	Alto
14143	Honeywell	Vulnerabilidades críticas en control externo.	Alto	Importante	Alto
14145	Honeywell	Riesgo de explotación remota no autenticada.	Alto	Importante	Alto
14250	Honeywell	Control remoto con autenticación débil.	Alto	Importante	Alto
14414	Honeywell	Autenticación deficiente.	Alto	Importante	Alto
15151	Servicios industriales	Control remoto no autorizado.	Alto	Importante	Alto
15555	Servicios industriales	Acceso remoto con credenciales débiles.	Alto	Importante	Alto

16080	HTTP alternativo	Tráfico no cifrado, susceptible a ataques MitM.	Alto	Importante	Alto
28080	Apache Tomcat	Configuración débil, accesible a ataques externos.	Alto	Importante	Alto
30001	Palo Alto Networks	Control no autenticado, explotación remota.	Alto	Importante	Alto
30002	Palo Alto Networks	Vulnerabilidad en control de red.	Alto	Importante	Alto
38000	Hipos (sistemas de gestión)	Vulnerable a inyecciones SQL.	Alto	Importante	Alto
48000	Apache Traffic Server	Configuración insegura, accesible a ataques.	Alto	Importante	Alto
48001	Apache	Vulnerabilidad en autenticación, accesible a ataques.	Alto	Importante	Alto
48002	Servicios internos	Expuesto a ataques de control remoto.	Alto	Importante	Alto
50000	SAP RFC	Ejecución remota de código y explotación de red.	Alto	Importante	Alto

Fuente: Elaboración propia

2.7.3. Fase III: Evaluación de Vulnerabilidades

Matriz de riesgo

Las matrices de riesgo se presentan en forma visual y numérica, proporcionando una clara representación de los datos. La matriz en formato textual se encuentra en la Tabla 12, mientras que la misma matriz en formato numérico se presenta en Tabla 13. Ambas matrices están basadas en la evaluación de Probabilidad por Impacto, lo que permite un análisis detallado de los niveles de riesgo asociados a cada puerto. Estas matrices facilitan la comprensión de los riesgos y ayudan a priorizar las acciones de mitigación según la probabilidad de ocurrencia y el impacto potencial de las vulnerabilidades identificadas.

Tabla 12.

Matriz de riesgo en formato textual.

	IMPACTO			
PROBABILIDAD	Minima	Menor	Moderada	Importante
Alto	Bajo	Medio	Alto	Alto
Medio	Bajo	Medio	Medio	Alto
Bajo	Muy bajo	Bajo	Medio	Medio
Muy bajo	Muy bajo	Muy bajo	Bajo	Bajo

Fuente: Elaboración propia

Tabla 13.

Matriz de riesgo en formato numérico.

		IMPACTO			
PROBABILIDAD		Mínima	Menor	Moderada	Importante
		1	2	3	4
Alto	4	4	8	12	16
Medio	3	3	6	9	12
Bajo	2	2	4	6	8
Muy Bajo	1	1	2	3	4

Fuente: Elaboración propia

Análisis realizado por Nessus

La Tabla 14 muestra el conteo y el porcentaje de puertos abiertos clasificados según su nivel de riesgo. En total, se identificaron 1024 puertos abiertos. De estos, el 87,21% (893 puertos) se categoriza con un riesgo bajo, el 10,25% (105 puertos) con un riesgo medio, y el 2,54% (26 puertos) con un riesgo alto. Este desglose indica que la mayoría de los puertos abiertos son bajos, aunque también hay puertos con niveles de riesgo medio y alto que deben abordarse, mostrando que el entorno evaluado es relativamente seguro, pero con un número significativo de vulnerabilidades.

Tabla 14.

Clasificación de puertos abiertos por riesgos del análisis realizado con Nessus

RIESGO	Cantidad	Porcentaje
Muy Bajo	0	0,00%
Bajo	893	87,21%
Medio	105	10,25%
Alto	26	2,54%
	1024	100,00%

Fuente: Elaboración propia

La Figura 6 presenta un gráfico detallado que ilustra los porcentajes de riesgo asociados a los puertos abiertos en el sistema. Este gráfico facilita la visualización de la magnitud del riesgo al que está expuesto el sistema debido a la presencia de estos puertos, permitiendo una comprensión más clara y rápida de las áreas que requieren atención y medidas de mitigación. Gracias a esta representación gráfica, es posible identificar de manera más efectiva los puertos que representan un mayor peligro y priorizar las acciones correctivas en función del nivel de riesgo mostrado.

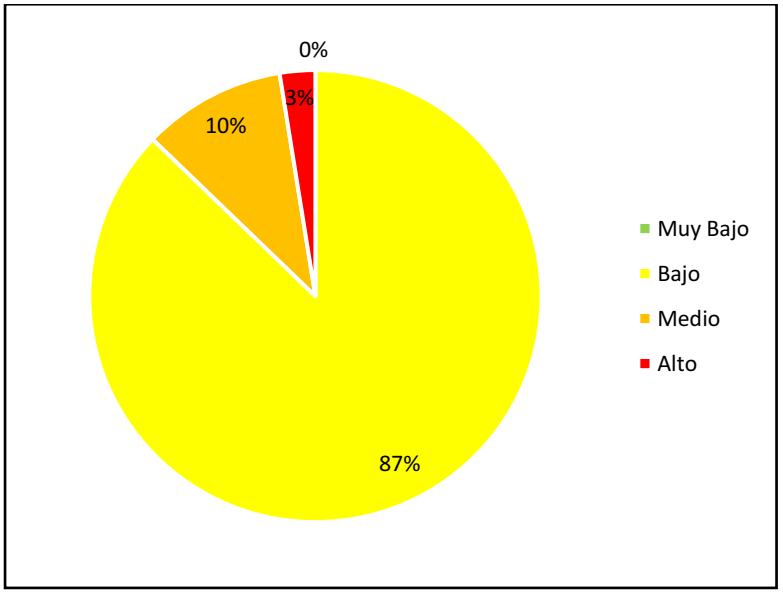

Figura 6. Porcentajes de clasificación según el nivel de riesgo del análisis realizado con Nessus.

Fuente: Elaboración propia.

Análisis realizado por Nmap

La Tabla 15 muestra los resultados del análisis de puertos TCP abiertos. Según los datos, el 76,30% (6375 puertos) se clasifican como de "Muy Bajo" riesgo, lo que sugiere una baja probabilidad de explotación. Un 17,45% (1458 puertos) están en la categoría de "Bajo" riesgo, mientras que el 5,34% (446 puertos) se consideran de "Medio" riesgo. Finalmente, el 0,91% (76 puertos) se encuentran en la categoría de "Alto" riesgo, indicando que estos puertos son los más vulnerables y necesitan una atención especial para mitigar posibles amenazas.

Tabla 15.

Clasificación de puertos abiertos por riesgos del análisis realizado con Nmap.

RIESGO	Cantidad	Porcentaje
Muy Bajo	6375	76,30%
Bajo	1458	17,45%
Medio	446	5,34%
Alto	76	0,91%
	8355	100,00%

Fuente: Elaboración propia

En total, se analizaron 8355 puertos, lo que proporciona una visión general del perfil de seguridad de la red evaluada. La Figura 7 presenta un gráfico que ilustra los porcentajes de riesgo asociados a los puertos abiertos, proporcionando una visualización clara y accesible de los niveles de riesgo identificados en el análisis, que sugiere la necesidad de una gestión continua para asegurar que estas pequeñas vulnerabilidades no se conviertan en problemas mayores. Este gráfico facilita la comprensión del perfil de seguridad, destacando la distribución de los puertos en las diferentes categorías de riesgo.

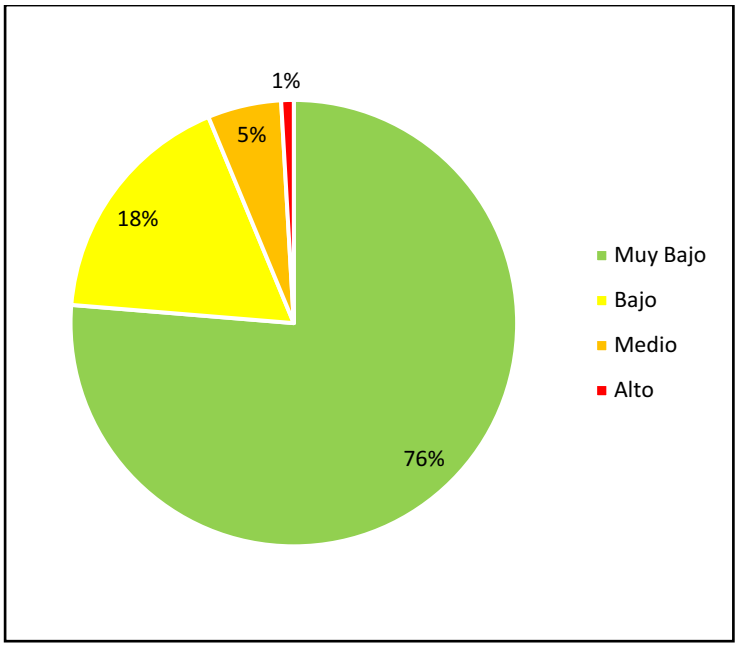

Figura 7. Porcentajes de clasificación según el nivel de riesgo del análisis realizado con Nmap.

Fuente: Elaboración propia.

2.7.4. Fase IV: Análisis de Impacto

Análisis/evaluación y tratamiento de riesgos

El Consejo Nacional Electoral (CNE) de Ecuador enfrenta riesgos cibernéticos que pueden afectar la integridad de los sistemas de votación electrónica. Estas vulnerabilidades podrían ser explotadas, comprometiendo la seguridad y fiabilidad de los procesos electorales. Es esencial que el CNE realice una evaluación exhaustiva de estas vulnerabilidades desde una perspectiva de ciberseguridad para proteger los sistemas y asegurar la confianza en las elecciones.

Tabla 16.

Evaluación de Riesgos – Probabilidades

Tabla de probabilidad			
Nivel	**Tipo**	**Descripción**	**Frecuencia**
1	Muy bajo	El evento puede ocurrir en algún momento.	Al menos una vez en los últimos 5 años.
2	Bajo	El evento podría ocurrir en algún momento.	Al menos una vez en los últimos 2 años.
3	Medio	El evento probablemente ocurra en la mayoría de las circunstancias.	Al menos una vez en el último año.
4	Alto	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una vez al año.

Tabla 17.

Evaluación de Riesgos - Impactos

Tabla de impacto		
Nivel	**Tipo**	**Descripción**
1	Mínima	Si llegara a presentarse, tendría consecuencias o efecto mínimo sobre la entidad.
2	Menor	Si llegara a presentarse, tendría bajo impacto o efecto mínimos sobre la entidad.
3	Moderada	Si llegara a presentarse, tendría medianas consecuencias o efecto sobre la entidad.
4	Importante	Si llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.

Fórmula para calcular la criticidad: **CRITICIDAD = PROBABILIDAD * IMPACTO.**

Tabla 18.

Criticidad de Riesgos – Cuantitativa – Formato Numérico

Probabilidad	Impacto			
	Mínima (1)	Menor (2)	Moderada (3)	Importante (4)
Alto (4)	4	8	12	16
Medio (3)	3	6	9	12
Bajo (2)	2	4	6	8
Muy bajo (1)	1	2	3	4

Tabla 19.

Rangos de criticidad

Criticidad	Muy baja	Baja	Media	Alta
Rango	2 – 1	4-3	9-8-6	16-12

Tabla 20.

Criticidad de Riesgos – Cuantitativa - Formato Textual

Probabilidad	Impacto			
	Mínima (1)	Menor (2)	Moderada (3)	Importante (4)
Alto (4)	B	M	A	A
Medio (3)	B	M	M	A
Bajo (2)	MB	B	M	M
Muy bajo (1)	MB	MB	B	B

Tabla 21.

Tratamiento de Riesgos

MB: Zona de Riesgo Muy baja	Asumir el riesgo
B: Zona de Riesgo Baja	Asumir el riesgo, Reducir el Riesgo
M: Zona de Riesgo Moderada	Reducir el riesgo, Compartir o Transferir
A: Zona de Riesgo Alta	Reducir el riesgo, Evitar, Compartir o Transferir

El tratamiento de los riesgos

El tratamiento de los riesgos es tomar decisiones frente a los diferentes riesgos existentes de acuerdo con la estrategia de la institución. Se deben seleccionar controles para reducir, aceptar/retener, evitar o transferir los riesgos y se debe definir un plan para el tratamiento del riesgo. Existen cuatro opciones disponibles para el tratamiento del riesgo:

Evitar el riesgo

Esta opción de tratamiento busca eliminar la probabilidad de ocurrencia o el impacto del riesgo.

Tomar las medidas necesarias para prevenir la materialización del riesgo.

Reducir riesgos

Se implementa cuando el riesgo se puede tratar internamente y puede llevarse a un nivel aceptable.

Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección).

Transferir todo o parte del riesgo

Requiere hacer un traslado a terceros u otras organizaciones parte del impacto negativo de una amenaza, como contratos a riesgo compartido.

Al transferir el riesgo a un tercero le damos la responsabilidad para su administración, pero no significa que eliminamos el riesgo.

Asumir el riesgo

Luego de que el riesgo ha sido reducido o transferido, puede quedar un riesgo residual que se mantiene; en este caso, el encargado del proceso acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Tabla 22.

Matriz Análisis, Evaluación y Tratamiento de Riesgos

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
REDES Y TELECOMUNICACIONES	**Hardware, Redes y Telecomunicaciones**	Rack, Switch, Router, Transiver	Personal no autorizado con acceso a equipos	**Usuarios:** • Usuarios que practican actos ilegales • Desastres causados por personas • Uso no autorizado del equipo **Fallos de programación:** • Accesos no autorizados **Robo o hurto:** • Hurto de equipos de cómputo • Asalto a un empleado	**Personal:** • Trabajo no supervisado de personal externo o de limpieza • Configuración inadecuada de equipos **Lugar:** • Uso inadecuado de los controles de acceso al edificio • Ausencia de protección en puertas y ventanas • Ausencia de procedimiento de registro/retiro de usuarios	**2**	**3**	**6**	Servicio de internet interrumpido	Asumir el riesgo y Reducir el riesgo	5.1.1 9.1.1 9.1.2 9.2.1 11.1.2
		Switch, Router y Access Point	Falta de equipos robustos para acceso a redes inalámbricas simultáneos	**Usuarios:** • Falta de gestión en recursos de red • Consumo excesivo del ancho de banda **Fallos de equipos o electrónicos**:	**Hardware:** • Ausencia de esquemas de reemplazo periódico • Pérdida de funcionalidad del equipo • Depreciación de la vida útil del equipo	**3**	**3**	**9**	Pérdida de funcionalidad del equipo e intermitencia en el servicio de internet	Reducir el riesgo, Compartir o Transferir	6.1.3 13.1.3

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
				• Fallas del equipo • Daños físicos en los equipos • Equipo inadecuado para las operaciones	**Personal:** • Ausencia de políticas de uso aceptable						
	Redes y Telecomunicaciones	Equipos de redes y telecomunicaciones	Daños a equipos por inconvenientes eléctricos	**Usuarios:** • Desastres causados por personas **Siniestros:** • Pérdida o fallas de suministros básicos **Fallos de equipos o electrónicos**: • Daños físicos en los equipos	**Hardware**: • Susceptibilidad a las variaciones de temperatura **Lugar:** • Conexiones eléctricas inadecuadas y ausencia de backup para problemas de energía • Red eléctrica inestable	**4**	**3**	**12**	Desconfiguración de equipos de redes y telecomunicaciones	Reducir el riesgo, Evitar, Compartir o Transferir	11.1.4 11.2.2 11.2.4
		Equipos de redes y telecomunicaciones	Fallas en la conectividad por falta de segmentación del ancho de banda para usuario final	**Usuarios:** • Consumo excesivo del ancho de banda • Usuarios internos que practican actos ilegales	**Hardware**: • Pérdida de funcionalidad del equipo • Ausencia de esquemas de reemplazo periódico **Red:** • Topología de red inadecuada	**4**	**3**	**12**	Inestabilidad en la conectividad	Reducir el riesgo, Compartir o Transferir	5.1.1 12.4.1 13.1.1 13.1.2 13.1.3
	Instalaciones	Edificio donde reposan los equipos de redes y	Fácil acceso y poca seguridad en lugares donde se encuentran equipos de red	**Robo o hurto:** • Hurto de equipos de cómputo **Usuarios:**	**Lugar:** • Lugares inadecuados para instalación de equipos	**4**	**4**	**16**	Sustracción, desconexión y daños en los equipos	Reducir el riesgo, Evitar, Comparti	11.1.1 11.1.2 11.1.3

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
		telecomunicaciones		• Usuarios internos que practican actos ilegales	• Ausencia de procedimiento de registro/retiro de usuarios • Ausencia de mecanismos de monitoreo de video vigilancia					r o Transferir	
		Lugares no aclimatados para equipos de redes telecomunicaciones	Lugares expuestos a temperaturas altas	**Siniestros:** ●Desastres por amenazas físicas ●Pérdida o fallas de suministros básicos **Catástrofes naturales:** ●Desastres naturales	**Hardware**: ●Susceptibilidad a las variaciones de temperatura **Lugar:** ●Climatización inadecuada • Red eléctrica inestable	**2**	**2**	**4**	Calentamiento excesivo y/o quema los equipos y sus componentes	Asumir el riesgo	11.1.4
	Datos o Información	Seguridad de datos en la red	Hackeo o acceso de intrusos	**Usuarios:** ●Usuarios que practican actos ilegales ●Uso de contraseñas débiles **Programas maliciosos:** ●Códigos maliciosos, ●Spyware **Intrusos:** ●Acceso a la red, Espionaje remoto ●Ataques contra el sistema	**Software:** ●Ausencia de mecanismos de identificación y autenticación de usuarios **Red:** • Tráfico sensible sin protección • Ausencia de pruebas de envío o recepción de mensajes • Falta de seguridad de firmware	**3**	**2**	**6**	Pérdida de información o bloqueo de acceso a equipos	Asumir el riesgo y Reducir el riesgo	9.1.2 9.2.2 9.2.4 9.4.1
	Personal	Administrador de equipos de	Fallas en el monitoreo y	**Usuarios:**	**Red:**	**3**	**3**	**9**	Inestabilidad en el servicio,	Reducir el riesgo,	6.1.2

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
		redes y telecomunicaciones	soporte técnico, poco personal encargado de administrar el acceso	● Error en el uso o abuso de derechos ● Falta de gestión en recursos de red **Fallos de programación:** ● Monitoreo del tráfico de la red	● Falta de herramientas de monitoreo **Personal**: • Ausencia del personal • Segregación de Actividades				incumplimiento en el soporte técnico	Compartir o Transferir	9.1.2 13.1.1 13.1.2 13.1.3
	Servicios	Seguridad a la conectividad	Personal no autorizado con acceso a la administración de los equipos de red	**Usuarios:** ● Uso no autorizado del equipo ● Error por desconocimiento u omisión **Intrusos:** ● Acceso a la red ● Acceso a los archivos de contraseñas	**Red:** ● Configuración inadecuada de equipos **Software:** ● Ausencia de terminación de sesión ● Asignación errada de los derechos de acceso **Personal:** ● Concienciación en seguridad de la información	**1**	**3**	**3**	Inestabilidad en todo el sistema de red	Asumir el riesgo	9.1.1 9.1.2 9.2.1 9.2.2 9.2.3 9.2.5 9.2.6 9.4.2 10.1.2
		Equipos de redes y telecomunicaciones	Falta de recursos económicos para adquirir equipos	**Usuarios:** ● Falta de gestión en recursos de red ● Error por desconocimiento u omisión	**Hardware:** ● Ausencia de esquemas de reemplazo periódico ● Pérdida de funcionalidad del equipo ● Depreciación de la vida útil de equipos	**4**	**4**	**16**	Falta de conectividad al Internet	Reducir el riesgo, Evitar, Compartir o Transferir	5.1.1 6.1.3

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE EQUIPOS DE CÓMPUTO	**Aplicaciones**	Antivirus sin licencia o licencia caducada	Equipos de cómputo con poca o nula seguridad	**Usuarios:** ● Instalación de hardware y software no autorizado **Programas maliciosos:** ● Virus informático ● Activadores no oficiales ● Crackeo de software **Intrusos:** ● Espionaje remoto	**Software:** ● Software ilegal **Red:** ● Falta de herramientas de monitoreo	**3**	**3**	**9**	Puertas traseras abiertas que vulneran el sistema fácilmente y permiten infección de información	Reducir el riesgo, Compartir o Transferir	11.2.4 12.2.1
	Hardware	Equipos de cómputo	Descargas y variaciones eléctricas que producen desperfectos en los equipos	**Siniestros:** ● Pérdida o fallas de suministros básicos	**Lugar:** ● Conexiones eléctricas inadecuadas y backup para problemas de energía ● Red eléctrica inestable	**4**	**3**	**12**	Daños en el sistema operativo y en dispositivos o periféricos	Reducir el riesgo, Evitar, Compartir o Transferir	11.1.3 11.1.4
		Equipos de cómputo, dispositivos y periféricos	Daños de equipos y pérdida de información por parte de los usuarios	**Usuarios:** ● Instalación de hardware y software no autorizado ● Usuarios internos que practican actos ilegales ● Desastres causados por personas ● Ingeniería social **Siniestros:**	**Hardware:** ● Mantenimiento insuficiente ● Copia no controlada ● **Personal:** ● Ausencia del personal ● Entrenamiento insuficiente	**4**	**3**	**12**	Entorpece las actividades y pérdida de información	Reducir el riesgo, Evitar, Compartir o Transferir	7.2.2 8.1.3 9.4.1 11.2.1

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
				●Desastres por amenazas físicas **Robo o hurto:** ●Hurto de equipos de cómputo	●Concienciación en seguridad de la información ●Ausencia de políticas de uso aceptable						
		Equipos de cómputo, dispositivos y periféricos	Fallas en hardware por falta de mantenimiento preventivo físico	**Usuarios:** ●Instalación de hardware y software no autorizado ●Desastres causados por personas ●Error por desconocimiento u omisión **Siniestros:** ●Desastres por amenazas físicas **Fallos de equipos o electrónicos**: ●Fallas del equipo ●Daños físicos en los equipos ●Equipo inadecuado para las operaciones	**Hardware:** ●Susceptibilidad a las variaciones de temperatura ●Mantenimiento insuficiente **Personal:** ●Entrenamiento insuficiente ●Concienciación en seguridad de la información ●Ausencia de políticas de uso aceptable ●Configuración inadecuada de equipos **Lugar:** ●Climatización inadecuada	**4**	**3**	**12**	Daños en los equipos de cómputo, dispositivos o periféricos y pérdida de información	Reducir el riesgo, Compartir o Transferir	11.1.3 11.1.5 11.2.4
		Impresoras compartidas en red	Compromiso de la información y acciones no autorizadas, por seguridad reducida en configuración de	**Usuarios:** ●Usuarios internos que practican actos ilegales ●Uso de contraseñas débiles ●Uso no autorizado del equipo	**Software:** ●Ausencia de terminación de sesión ●Software ilegal **Red:** ●Falta de herramientas de monitoreo	**1**	**2**	**2**	Infección con archivos maliciosos y compromiso de la información por acceso de	Asumir el riesgo	7.2.2 9.2.4 9.3.1

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
			uso compartido de archivos e impresoras	**Programas maliciosos:** ●Códigos maliciosos ●Virus informático **Fallos de programación:** ●Información comprometida ●Accesos no autorizados **Intrusos:** ●Modificación de la información ●Acceso a la Red	**Personal:** ●Concienciación en seguridad de la información				personas no autorizadas		
		Equipos de cómputo e impresoras	Traslado de equipos de un área a otra, sin precauciones de seguridad ante robos, accidentes o siniestros	**Usuarios:** ●Desastres causados por personas ●Uso de contraseñas débiles **Siniestros:** ●Desastres por amenazas físicas **Robo o hurto:** ●Hurto de equipos de cómputo ●Asalto a un empleado ●Robo de información	**Personal:** ●Falta de conciencia en seguridad de la información	**3**	**4**	**12**	Daños por caídas de los equipos al trasladarlos a otras áreas, pérdida o robo de equipos de cómputo e información	Reducir el riesgo	6.2.1 7.2.2 11.1.4 11.2.1 11.2.5 11.2.6
	Datos o Información	Información institucional	Pérdida de información por mal uso o	**Usuarios:**	**Hardware:** ●Almacenamiento sin protección	**3**	**2**	**6**	Acceso a equipos por parte de	Asumir el riesgo y	7.2.2 8.1.3

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
			configuración inadecuada de contraseñas de los usuarios	●Usuarios internos que practican actos ilegales ●Uso de contraseñas débiles **Programas maliciosos:** ●Rasonware **Fallos de programación:** ●Accesos no autorizados **Intrusos:** ●Robo o suplantación de identidad **Robo o hurto:** ●Hurto de equipos de cómputo	**Software:** ●Ausencia de terminación de sesión ●Contraseñas sin encriptación **Personal:** ●Entrenamiento insuficiente ●Concienciación en seguridad de la información ●Ausencia de políticas de uso aceptable				personas no autorizadas	Reducir el riesgo	9.1.1 9.4.1 9.4.2 9.4.3
	Software	Sistema operativo y aplicaciones	Fallas en software y aplicaciones	**Usuarios:** ●Instalación de hardware y software no autorizado ●Error por desconocimiento u omisión ●Ausencia o falta de copias de seguridad **Programas maliciosos:** ●Virus informático ●Activadores no oficiales	**Hardware:** ●Mantenimiento insuficiente **Software:** ●Software nuevo o inmaduro ●Software ilegal **Personal:** ●Entrenamiento insuficiente ●Concienciación en seguridad de la información	**4**	**4**	**16**	Daños en el sistema operativo y pérdida de información	Reducir el riesgo, Evitar, Compartir o Transferir	11.2.4

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
				●Crackeo de software **Fallos de programación:** ●Errores en los sistemas operativos ●Aplicaciones desactualizadas **Fallos de equipo o electrónicos:** ●Fallos del equipo	●Ausencia de políticas de uso aceptable ●Configuración inadecuada de equipos						
	Servicios, Datos e Información	Datos e Información	Pérdida de información por falta de procedimientos efectivos para recuperación de información	**Usuarios:** ●Uso no autorizado del equipo ●Error por desconocimiento u omisión ●Ausencia o falta de copias de seguridad **Fallos de programación:** ●Información comprometida **Robo o hurto:** ●Hurto de equipos de cómputo	**Hardware:** ●Almacenamiento sin protección ●Copia no controlada ●Pérdida de funcionalidad del equipo ●Depreciación de la vida útil de equipos **Personal:** ●Entrenamiento insuficiente ●Formación no es acorde a su puesto de trabajo	**2**	**4**	**8**	Daño de disco duro, pérdida de información y respaldos históricos	Asumir el riesgo y Reducir el riesgo	5.1.1 12.3.1
	Personal	Software y aplicaciones	Instalación de programas por parte de los usuarios, sin la autorización de la UT	**Usuarios:** ●Instalación de hardware y software no autorizado ●Usuarios internos que practican actos ilegales	**Hardware:** ●Mantenimiento insuficiente **Software:** ●Ausencia o insuficiencia de pruebas de software	**4**	**4**	**16**	Acceso de intrusos e infección con archivos maliciosos	Reducir y Evitar el riesgo	5.1.1 6.1.1 7.2.2 9.4.4 12.6.2

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
				Programas maliciosos: ● Activadores no oficiales ● Crackeo de software	● Software ilegal **Red:** ● Falta de herramientas de monitoreo **Personal:** ● Concienciación en seguridad						
DESARROLLO DE SOFTWARE Y NUEVAS TECNOLOGÍAS	**Servicios y Personal**	Correo electrónico institucional	Acceso de los usuarios a correos de dudosa procedencia	**Intrusos:** ● Ataques contra el sistema ● Robo o suplantación de identidad	**Personal:** ● Falta de conciencia en seguridad de la información	**3**	**4**	**12**	Pérdida de información, infección y/o bloqueo de acceso a equipos	Asumir el riesgo y Reducir el riesgo	6.1.1 10.1.2 12.2.1 13.2.1
	Información y Datos	Base de datos institucional	Acceso no autorizado a las bases de datos	**Intrusos:** ● Acceso a los archivos de contraseña **Usuario:** ● Usuarios internos que practican actos ilegales	**Personal:** ● Ausencia de políticas de uso aceptable **Software:** ● Ausencia de terminación de sesión ● Ausencia de registros de auditoría	**3**	**4**	**12**	Integridad de los datos comprometida (reportería o certificaciones)	Asumir el riesgo y Reducir el riesgo	5.1.1 6.1.1 7.2.2 9.2.2 9.2.3 9.2.4 9.2.6 9.4.1 9.4.2

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
	Aplicaciones	Aplicaciones institucionales	Software en producción sin pruebas	**Fallos de programación:** ● Fallas en el diseño de software **Usuario:** ● Error en el uso o abuso de derechos	**Software:** ● Ausencia o insuficiencia de pruebas de software ● Software nuevo o inmaduro **Personal:** ● Entrenamiento insuficiente ● Falta de concienciación en seguridad	**3**	**1**	**3**	Inconsistencias al entregar el sistema y fallas de este al estar en ejecución	Asumir el riesgo	12.1.4 12.5.1 12.6.2 14.2.1 14.2.2 14.2.6 14.2.8 14.2.9 14.3.1
		Aplicaciones institucionales	Código fuente de aplicaciones no sincronizado	**Usuario:** ● Desastres causados por personas **Fallos de programación:** ● Incumplimiento en el mantenimiento del sistema de información	**Personal:** ● Configuración inadecuada de equipos ● Entrenamiento insuficiente **Lugar:** ● Ausencia de control de los activos que se encuentran dentro y fuera de las instalaciones	**2**	**2**	**4**	Confusiones en la sincronización y respaldos del código fuente	Asumir el riesgo	9.4.4 9.4.5 12.7.1 14.2.1 14.2.2 14.2.6
		Equipos de cómputo	Aplicaciones para desarrollo de software sin soporte y licencias	**Usuarios:** ● Error en el uso o abuso de derechos **Fallos de programación:** ● Aplicaciones desactualizadas	**Software:** ● Software ilegal	**3**	**2**	**6**	Funcionalidad disminuida de aplicaciones e infecciones por activadores	Asumir el riesgo y Reducir el riesgo	11.2.4 14.2.1 14.2.5

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
	Soporte de información	Base de datos institucional	Respaldos no automatizados de las bases de datos	**Fallos de programación:** ● Monitoreo de cambios **Siniestros:** ● Fallas de suministros básicos **Fallos del equipo o electrónico**: ● Fallos del equipo	**Hardware:** ● Almacenamiento sin protección **Software:** ● Ausencia de documentación **Red:** ● Punto único de falla **Personal:** ● Entrenamiento insuficiente	**2**	**2**	**4**	Pérdida de información relevante y pérdida de la continuidad del negocio.	Asumir el riesgo	5.1.1 6.1.1 12.1.1 12.1.2 12.3.1 12.6.1 17.1.1
	Hardware	Equipos de cómputo	Equipos de desarrollo no adecuado	**Fallas de equipo o electrónico:** ● Fallas de equipo ● Equipo no adecuado para operaciones	**Hardware:** ● Pérdida de funcionalidad del equipo ● Depreciación de vida útil del equipo	**3**	**4**	**12**	Retardo en la producción de software y soporte de aplicaciones	Reducir y compartir o transferir el riesgo	8 11.2.4 12.6.1 14.1.1
	Servicio	Aplicaciones institucionales	Soporte técnico de aplicaciones sin seguimiento	**Usuarios:** ● Instalación de hardware y software no autorizado ● Desastres causados por personas ● Error por desconocimiento u omisión ● Ausencia o falta de copias de seguridad **Fallos de programación:**	**Hardware:** ● Almacenamiento sin protección ● Copia no controlada **Software:** ● Ausencia o insuficiencia de pruebas de software ● Ausencia de documentación ● Software nuevo o inmaduro	**3**	**3**	**9**	Inhabilitación de aplicaciones sin soporte, servicios de aplicaciones detenidos	Reducir y compartir o transferir el riesgo	5.1.1 8.1.1 9.2.3 9.4.4 9.4.5 11.2.4 12.1.1 12.4.3

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
				● Fallas en el diseño del software ● Incumplimiento en el mantenimiento del sistema de información	**Personal:** ● Entrenamiento insuficiente ● Segregación de actividades ● Formación no es acorde a su puesto de trabajo						14.1.1 14.2.1 14.2.2 14.2.5 16.1.4 16.1.5
	Personal	Aplicaciones institucionales	Usuarios sin actualizar credenciales periódicamente	**Usuarios:** ● Uso de contraseñas débiles ● Error por desconocimiento u omisión	**Software:** ● Interfaz de usuario compleja **Personal:** ● Falta de concienciación en seguridad	**4**	**2**	**8**	Alteración de datos en roles específicos y confidencialidad expuesta a otros usuarios	Reducir y compartir o transferir el riesgo	6.1.1 7.2.2 8.1.3 9.1.1 9.2.5 9.4.2 9.4.3
		Equipo de trabajo	Falta de personal de desarrollo	**Usuarios:** ● Desastres causados por personas ● Error el uso o abuso de derechos ● Error por desconocimiento u omisión	**Software:** ● Ausencia o insuficiencia de pruebas de software **Personal:** ● Ausencia de personal ● Formación no es acorde a su puesto de trabajo	**4**	**2**	**8**	Sistemas sin actualizar y vulnerables, rendimiento en aplicaciones muy bajo	Asumir el riesgo y Reducir el riesgo	7.1.2 7.2.1 7.2.3 8

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
		Aplicaciones y/o sitios institucionales	Información errónea cargada a sitios o aplicaciones institucionales	**Usuarios:** ● Desastres causados por personas ● Error por desconocimiento u omisión **Fallos de programación:** ● Fallas en el diseño del software ● Accesos no autorizados ● Monitoreo de cambios **Intrusos:** ● Corrupción de datos ● Modificación de la información	**Software:** ● Ausencia de terminación de sesión ● Asignación errada de los derechos de acceso ● Interfaz de usuario compleja ● Software nuevo o inmaduro **Personal:** ● Ausencia de personal ● Entrenamiento insuficiente	**4**	**3**	**12**	Desinformación por canales oficiales, atenta contra la reputación de la empresa	Reducir y compartir o transferir el riesgo	5.1.1 6.1.1 14.2.2 14.2.4 17.1.3
DATA CENTER	**Hardware, Redes y Telecomunicaciones, Personal, Instalación**	Equipos y acceso a aplicaciones y bases de datos	Acceso no controlado al centro de datos	**Usuarios:** ● Instalación de hardware y software no autorizado ● Usuarios internos q practican actos ilegales ● Desastres causados por personas ● Error en el uso o abuso de derechos **Siniestros:** ● Desastres por amenazas físicas.	**Hardware:** ● Ausencia de esquemas de reemplazo periódico ● Pérdida de funcionalidad del equipo ● Depreciación de la vida útil de equipos **Red:** ● Tráfico sensible sin protección **Personal:**	**4**	**4**	**16**	Pérdida absoluta de información crítica y equipos del CNE	Reducir el riesgo, Evitar, Compartir o Transferir	8.1.1 11.1.2 11.1.3 11.2.1 11.2.5 11.2.6

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
				Catástrofes Naturales: ● Desastres Naturales ● Penetración en el sistema **Fallas de equipo o electrónico:** ● Fallas del equipo ● Daños físicos en los equipos ● Equipo inadecuado para las operaciones	● Ausencia de políticas de uso aceptable ● Entrenamiento insuficiente ● Trabajo no supervisado de personal externo o de limpieza **Lugar:** ● Uso inadecuado de los controles de acceso al edificio						
	Hardware, Soporte de Información, Servicios, Aplicaciones	Servidores	Manipulación indebida de los equipos físicos	**Usuario:** ● Uso no autorizado del equipo **Programas maliciosos:** ● Virus informáticos ● Activadores no oficiales ● Spyware **Fallos de programación:** ● Aplicaciones desactualizadas **Intrusos:** ● Corrupción de datos ● Acceso a los archivos de contraseña ● Acceso a la red **Fallos de equipo o electrónicos:** ● Daños físicos en los equipos	**Hardware:** ● Mantenimiento insuficiente ● Pérdida de funcionalidad del equipo ● Depreciación de la vida útil de los equipos **Software:** ● Ausencia de registros de auditoría **Red:** ● Conexión deficiente de cableado ● Líneas de comunicación sin protección **Personal:** ● Concienciación en seguridad de la información ● Trabajo no supervisado de personal externo o de limpieza	**3**	**2**	**6**	Acceso no consentido a los siste32mas informáticos	Asumir el riesgo y Reducir el riesgo	8.1.1 8.1.3 8.1.4 8.2.3 11.1.2 11.1.3 11.1.4 11.2.1 11.2.2 11.2.3 11.2.7 11.2.8 11.2.9

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
				Robo o hurto: ● Robo de información							13.1.2 15.1.1 16.1.2
	Hardware y Redes de Telecomunicaciones, Servicios	Data Center	Fallas energéticas	**Siniestros:** ● Desastres por amenazas físicas ● Pérdidas o fallas de suministros básicos **Catástrofes naturales:** ● Desastres naturales **Fallos de equipo o electrónicos:** ● Fallas del equipo ● Daños físicos en los equipos	**Hardware:** ● Pérdida de funcionalidad del equipo **Lugar:** ● Conexiones eléctricas inadecuadas y backup para problemas de energía ● Red eléctrica inestable	**4**	**4**	**16**	Daños críticos en los componentes hardware de los servidores	Reducir el riesgo, Evitar, Compartir o Transferir	11.1.4 11.1.5
	Aplicaciones y Servicios	Sistemas operativos e información general de la institución	Sistemas de respaldo no inmutado ante Ransonware	**Usuario:** ● Piratería ● Falsificación ● Fraude informático **Programas maliciosos:** ● Ransonware **Fallos de programación:** ● Errores en los sistemas operativos ● Información comprometida **Intrusos:** ● Espionaje remoto ● Corrupción de datos ● Ataques contra el sistema	**Hardware:** ● Almacenamiento sin protección ● Copia no controlada ● Pérdida de funcionalidad del equipo **Software:** ● Ausencia de registros de auditoría ● Software ilegal **Red:** ● Falta de herramientas de monitoreo **Personal:** ● Concienciación en seguridad de la información ● Entrenamiento insuficiente	**4**	**4**	**16**	Pérdida completa de los sistemas de backup por ataque de Ransonware	Reducir el riesgo, Evitar, Compartir o Transferir	12.3.1 12.4.1 12.4.2 12.6.1 12.6.2 12.7.1 16.1.1 16.1.5 16.1.6 16.1.7

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
				●Chantaje ●Acceso a la red **Robo o hurto:** ●Hurto de documentos ●Robo de información							
	Hardware, Servicios y Redes de Telecomunicaciones	Servidores	Inhibición de los servidores por procesamiento	**Usuario:** ●Error por desconocimiento u omisión ●Instalación de hardware y software no autorizado **Programas maliciosos:** ●Códigos maliciosos **Intrusos:** ●Invasión ●Espionaje remoto **Fallas de equipo o electrónicos:** ●Fallas del equipo ●Equipo inadecuado para las operaciones	**Hardware:** ●Mantenimiento insuficiente ●Pérdida de la funcionalidad del equipo **Red:** ●Punto único de falla **Personal:** ●Configuración inadecuada de equipos **Lugar:** ●Climatización inadecuada	**1**	**3**	**3**	Servicios colapsados por falla de equipo	Asumir el riesgo	8.1.3 8.2.3 11.1.4 11.2.4
	Datos o información, Servicios, y	Sistemas operativos, aplicaciones y bases de datos	Ataques hacia las aplicaciones	**Usuarios:** ●Piratería ●Ingeniería social	**Hardware:** ●Almacenamiento sin protección **Software:** ●Contraseñas sin encriptación	**4**	**4**	**16**	Información comprometida de la institución, Servicios	Reducir el riesgo, Evitar, Comparti	9.1.2 9.4.5 10.1.2

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
	Aplicaciones			●Uso no autorizado del equipo **Programas maliciosos:** ●Spyware ●Código malicioso ●Ransonware **Intrusos:** ●Corrupción de datos ●Invasión ●Ataques contra el sistema ●Robo o suplantación de identidad **Robo o hurto:** ●Robo de información	**Red:** ●Tráfico sensible sin protección **Personal:** ●Concienciación en seguridad de la información ●Configuración inadecuada de equipos ●Entrenamiento insuficiente				institucionales no disponibles	r o Transferir	11.1.3 11.1.4 12.2.1 12.6.2 12.7.1 13.1.2 13.1.3 14.1.2 14.2.5 16.1.3 16.1.4 16.1.5
	Hardware, Datos o información, Aplicaciones	Instancias virtuales y servidores físicos y storage de almacenamiento masivo	Servidores no actualizados	**Fallos de programación.:** ●Aplicaciones desactualizadas **Intrusos:** ●Ataques contra el sistema	**Hardware:** ●Mantenimiento insuficiente ●Depreciación de la vida útil de los equipos **Software:** ●Ausencia de registros de auditoria **Red:** ●Líneas de comunicación sin protección	4	4	16	Pérdida completa de los sistemas de backup por ataque de Ransonware	Reducir el riesgo, Evitar, Compartir o Transferir	8.1.3 8.2.3 8.3.1 8.3.2 9.4.4 11.2.1 11.2.2 11.2.4

ANÁLISIS/EVALUACIÓN Y TRATAMIENTO DE RIESGOS											
Área	**Tipo de Activo**	**Descripción del Activo**	**Tipo de Riesgo**	**Amenazas**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Criticidad**	**Tipo de Impacto**	**Medida de Respuesta**	**Control/es**
					Personal: ● Entrenamiento insuficiente ● Configuración inadecuada de equipos						12.4.4 16.1.1
	Servicios, Datos o información	Sistemas operativos y servicios en producción	Defectuosa gestión de proceso de licenciamiento	**Usuarios:** ● Instalación de hardware y software no autorizado **Programas maliciosos:** ● Códigos maliciosos ● Virus informático **Fallos de programación:** ● Fallas en el diseño de software **Intrusos:** ● Invasión ● Corrupción de datos	**Hardware:** ● Mantenimiento insuficiente **Software:** ● Ausencia o insuficiencia de pruebas de software **Personal:** ● Ausencia de políticas de uso aceptable	**4**	**4**	**16**	Reinicio y apagado de los sistemas	Reducir el riesgo, Evitar, Compartir o Transferir	8 8.1.3 11.2.4 12.1.1 12.2.1 14.2.5 16.1.1

2.8. Plan de fortalecimiento de ciberseguridad para el centro de datos del CNE.

Este plan tiene como finalidad establecer un marco estratégico para mejorar la ciberseguridad en el centro de datos del CNE, tomando en cuenta la arquitectura de red simulada. Se enfoca en medidas que aseguren la protección integral de los sistemas electorales, garantizando la integridad, confidencialidad y disponibilidad de los datos en un entorno en constante evolución de ciberamenazas por lo cual se propone seguir este protocolo para evitar *Common Vomiting Environment* (CVE) y *Common Vulnerability Scoring System* (CVESS), adicional seguir las mejores prácticas recomendadas en la norma ISO/IEC 27001.

2.8.1. ISO 27001:2022

Las auditorías de seguridad son fundamentales para garantizar el cumplimiento de las mejores prácticas y normas internacionales, como la ISO 27001:2022, que establece un marco de referencia para la gestión de la seguridad de la información. Este plan propone la realización de auditorías semestrales basados en la cláusula **División de 9.2 en 9.2.1 General / 9.2.2 Programa de auditoría** para evaluar la efectividad del sistema de gestión de seguridad implementado en el CNE. Estas auditorías deberán ser exhaustivas, abarcando todos los aspectos críticos, con especial atención en la identificación y mitigación de vulnerabilidades relacionadas con los puertos abiertos detectados en la fase de **Identificación de Amenazas**, documentados en la Tabla 11.

2.8.2. Implementación de *backups* inmutables

La arquitectura de red presentada en la Figura 5 de la fase de **Identificación de Activos** no incluye actualmente un sistema que garantice la inmutabilidad de los datos. Es esencial introducir un sistema de *backups* inmutables que garantice que la información almacenada no pueda ser modificada o eliminada, incluso en el caso de un ataque, como *ransomware*, que busque secuestrar o destruir los datos críticos del CNE.

Estos *backups* inmutables deben estar completamente aislados de la red operativa principal, utilizando almacenamiento en medios desconectados o en sistemas diseñados específicamente para resistir modificaciones no autorizadas. La inmutabilidad asegura que los datos se mantengan íntegros y recuperables en su estado original, incluso en el peor escenario de un ataque masivo.

Además, la arquitectura de red del CNE debe ser mejorada para incluir mecanismos que permitan una separación clara entre los sistemas operativos principales y los sistemas de almacenamiento de *backups*. Esta separación física y lógica reducirá el riesgo de que un mismo ataque pueda comprometer tanto los sistemas principales como las copias de seguridad.

El rediseño de la arquitectura debe contemplar también la implementación de medidas de aislamiento de los entornos de *backup*, así como la introducción de sistemas de replicación en tiempo real a centros de datos remotos y seguros. Estos centros de datos adicionales proporcionarán redundancia geográfica y garantizarán la disponibilidad de los datos críticos en cualquier momento.

En resumen, el fortalecimiento de la arquitectura de red del CNE junto con la implementación de sistemas de *backups* inmutables garantizará que los datos puedan ser restaurados en caso de ataque, asegurando la integridad y disponibilidad de la información, elementos clave para la operación continua y segura de los sistemas electorales.

2.8.3. Implementación de tecnología blockchain

La tecnología blockchain ofrece una solución innovadora para mejorar la seguridad y la integridad de los datos en los sistemas electorales. Al implementar un sistema basado en blockchain, se establece un registro inmutable y distribuido que garantiza que cualquier intento de alterar los datos sea registrado y fácilmente detectable. Esto proporciona una capa adicional de confianza, ya que cada bloque de información está criptográficamente vinculado al anterior, formando una cadena que no puede ser modificada sin afectar toda la estructura.

La integración de blockchain en los procesos del CNE no solo asegura la integridad de los datos, sino que también proporciona un mecanismo de auditoría constante y verificable en tiempo real. Esto es especialmente valioso en el contexto electoral, donde la transparencia y la confianza son fundamentales para la legitimidad del proceso.

Además, el uso de blockchain puede facilitar la trazabilidad, permitiendo que cada transacción relacionada con el proceso electoral quede registrada de forma segura y accesible para auditorías futuras. Esta capacidad de rastreo y verificación en tiempo real fortalecerá la confianza pública en los sistemas de votación electrónica y ayudará a prevenir fraudes.

En conclusión, la implementación de tecnología blockchain en los sistemas electorales del CNE no solo mejorará la seguridad, sino que también reforzará la transparencia y la confianza en los procesos, elementos esenciales para la integridad electoral

2.8.4. Arquitectura simulada del CNE con un sistema inmutable de *backup*, sistema de correlación de eventos y SOC.

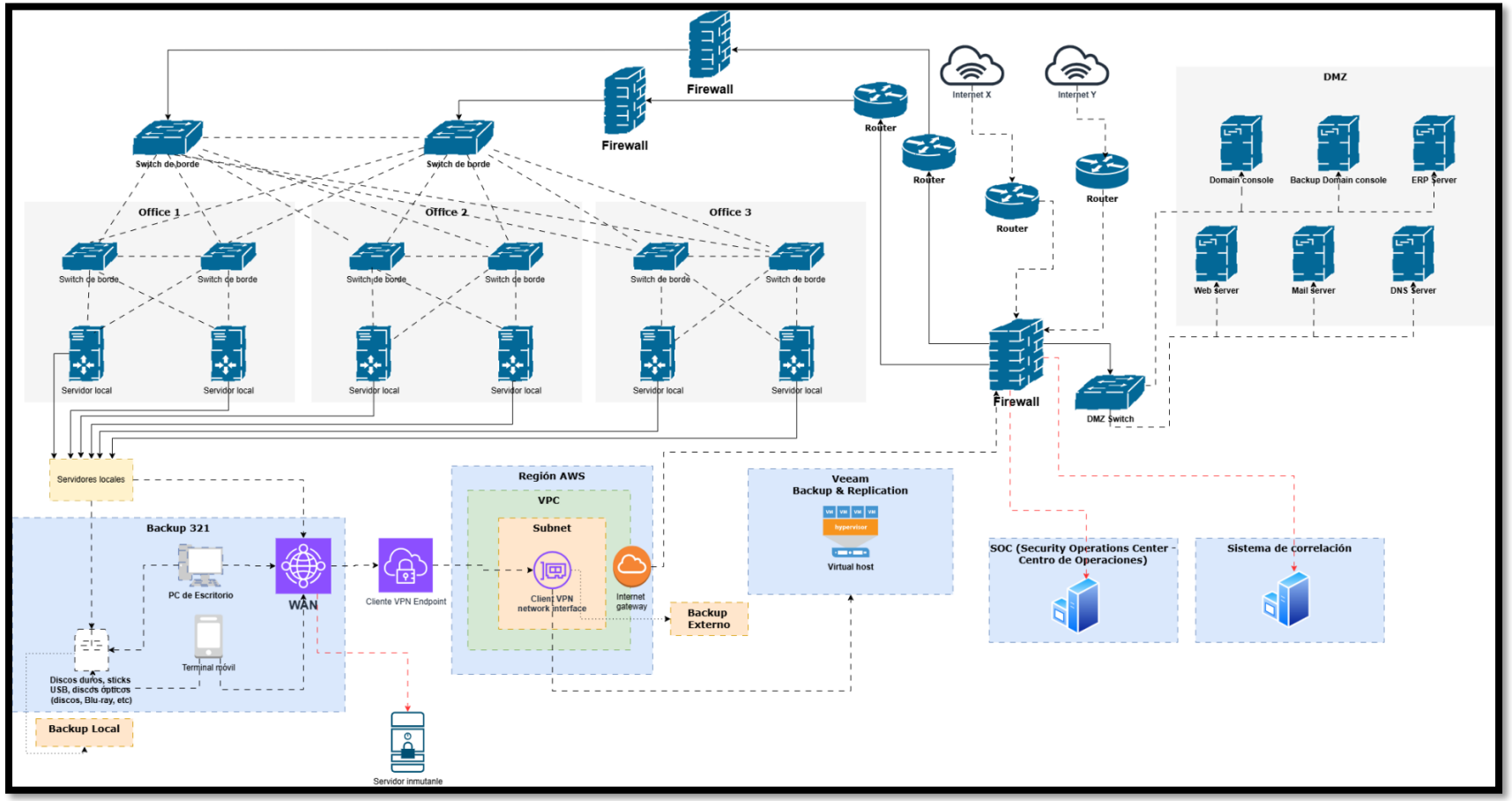

Figura 8. Arquitectura de red simulada del CNE con un sistema de correlación de eventos, servidor inmutable y SOC.

Fuente: Elaboración propia

2.8.5. Sistema de correlación de eventos

Con la implementación de un Sistema de Gestión de Información y Eventos de Seguridad (SIEM), se fortalece la seguridad de la organización al permitir la detección de comportamientos inusuales y paquetes sospechosos de manera proactiva, dentro de los cuales se van a generar un plan de contingencia para la continuidad del negocio. Esto permite identificar patrones sospechosos y responder de manera efectiva a incidentes de ciberseguridad, mejorando así la visibilidad de la seguridad, acelerando la detección de amenazas y optimizando la respuesta ante incidentes, lo que resulta en una defensa más robusta y proactiva para proteger nuestra información y nuestros recursos (González-Granadillo et al., 2021).

2.8.6. Centro de Operaciones de Seguridad (SOC)

Implementar un SOC mejorará significativamente la detección de amenazas y la respuesta rápida a incidentes, optimizando además la gestión de riesgos mediante informes detallados que permitirán ajustar políticas de seguridad y tomar decisiones informadas. También facilitará el cumplimiento de normativas y estándares, evitando sanciones y problemas en auditorías. Al integrar inteligencia de amenazas en tiempo real, permitirá anticiparse a nuevos ataques y adaptar las defensas de manera proactiva, garantizando una protección más robusta y eficaz para la infraestructura crítica (Kinyua & Awuah, 2021; Vielberth et al., 2020).

2.8.7. Sistema Inmutable de Backup

Con un sistema de *backup* inmutable, los ataques de *ransomware* no podrán encriptar los *backups*, dado que son de solo lectura y no de escritura. Esto permitirá mantener la integridad, la seguridad, la confiabilidad y la disponibilidad de la información, lo que a su vez facilitará un tiempo de respuesta y continuidad del negocio en cuestión de minutos o segundos mientras se levantan los sistemas de *backup* en un centro de datos alterno. Esto no solo ayuda a minimizar el tiempo de inactividad y a evitar la pérdida de información valiosa, sino que también garantiza la continuidad del negocio (Malecki, 2021; Singhal, 2022).

CAPÍTULO 3. RESULTADOS Y DISCUSIÓN

En la Figura 9, se observa que el 76.92% de los encuestados tiene un conocimiento bajo sobre Blockchain, lo que indica una comprensión limitada del funcionamiento de esta tecnología. Un 11.54% posee un conocimiento básico, mientras que un 8.97% reporta no tener ningún conocimiento sobre el tema. Solo el 2.56% de los encuestados afirma tener un buen conocimiento y entender tanto su funcionamiento como sus aplicaciones. Estos resultados destacan una falta generalizada de comprensión sobre Blockchain entre los participantes.

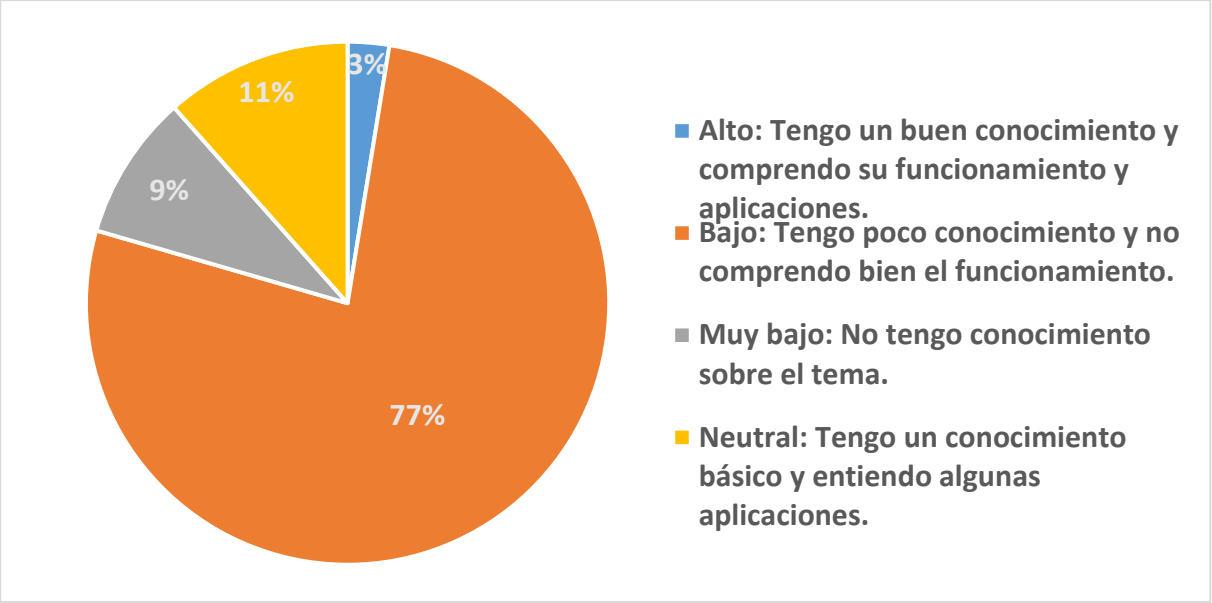

Figura 9. Nivel de conocimiento sobre Blockchain entre los encuestados.

Fuente: Elaboración propia

En la Figura 10, se evidencia que el 69.23% de los encuestados tiene un conocimiento bajo sobre los sistemas de votación electrónica, habiendo escuchado de ellos, pero sin saber cómo funcionan. Un 15.38% tiene un conocimiento básico y comprende su funcionamiento general, mientras que un 10.26% reporta no tener ningún conocimiento sobre estos sistemas. Solo el 5.13% de los encuestados afirma conocer bien los sistemas de votación electrónica y sus procesos. Estos resultados indican que existe una limitada comprensión detallada de los sistemas de votación electrónica entre los participantes.

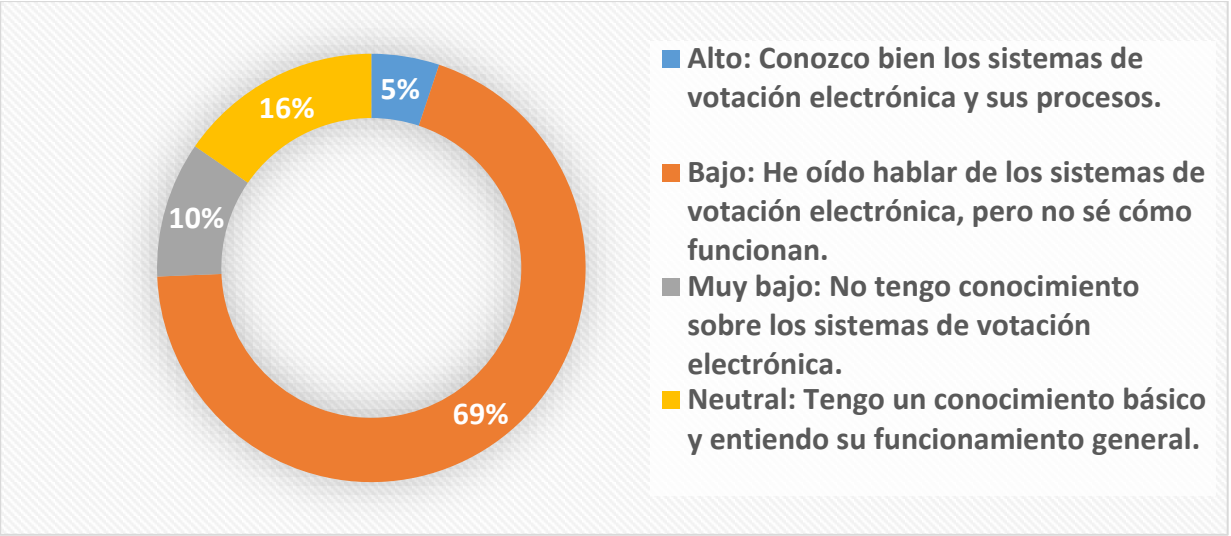

Figura 10. Distribución del nivel de conocimiento sobre los sistemas de votación electrónica

Fuente: Elaboración propia

En la Figura 11, se observa que la gran mayoría de los encuestados (80.77%) percibe el sistema electoral en Ecuador como poco transparente. Un 12.82% considera que es transparente, mientras que un 3.85% opina que el sistema es nada transparente. Solo el 2.56% de los participantes cree que el sistema electoral es muy transparente. Estos resultados reflejan una percepción generalizada de falta de transparencia en el sistema electoral ecuatoriano.

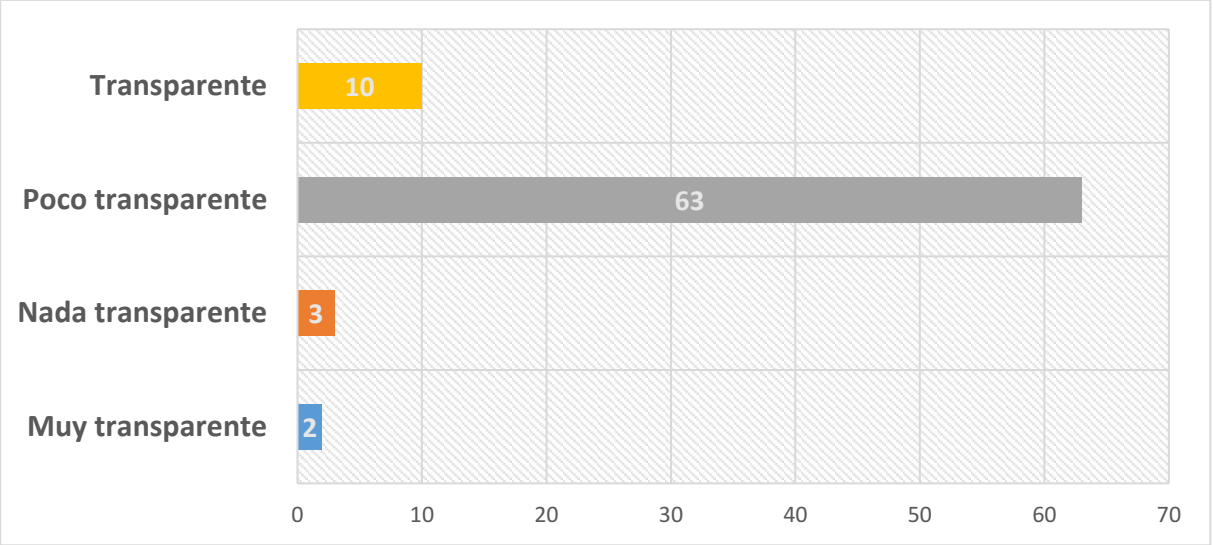

Figura 11. Percepción de la transparencia del sistema electoral en Ecuador.

Fuente: Elaboración propia

En la figura 12, se observa que la mayoría de los encuestados (69.23%) considera pertinente la implementación de un sistema de voto electrónico en Ecuador, mientras que un 26.92% lo califica como muy pertinente. Solo un 2.56% opina que no sería pertinente en absoluto, y un 2.56% más considera que sería poco pertinente. Estos resultados sugieren un apoyo considerable entre los participantes hacia la adopción de un sistema de voto electrónico en el país.

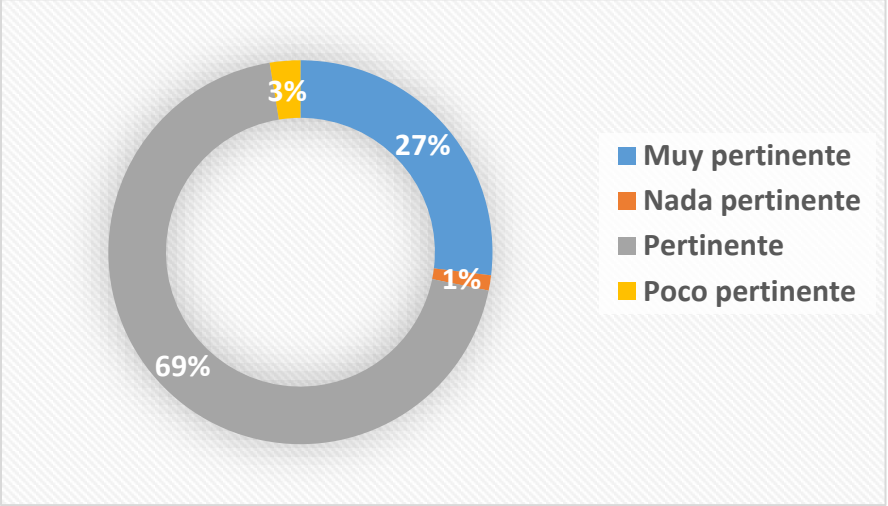

Figura 12. Opiniones sobre la pertinencia de implementar un sistema de voto electrónico en Ecuador.

Fuente: Elaboración propia

En la Figura 13, se muestra que la mayoría de los encuestados (71.79%) no está familiarizada con los mecanismos de seguridad utilizados en sistemas de votación electrónica, como el cifrado de datos y la autenticación de usuarios. Un 20.51% de los participantes indica que no sabe o no conoce estos mecanismos, mientras que solo el 20.51% afirma estar familiarizado con ellos. Estos resultados revelan una falta significativa de conocimiento sobre las medidas de seguridad en los sistemas de votación electrónica entre los encuestados.

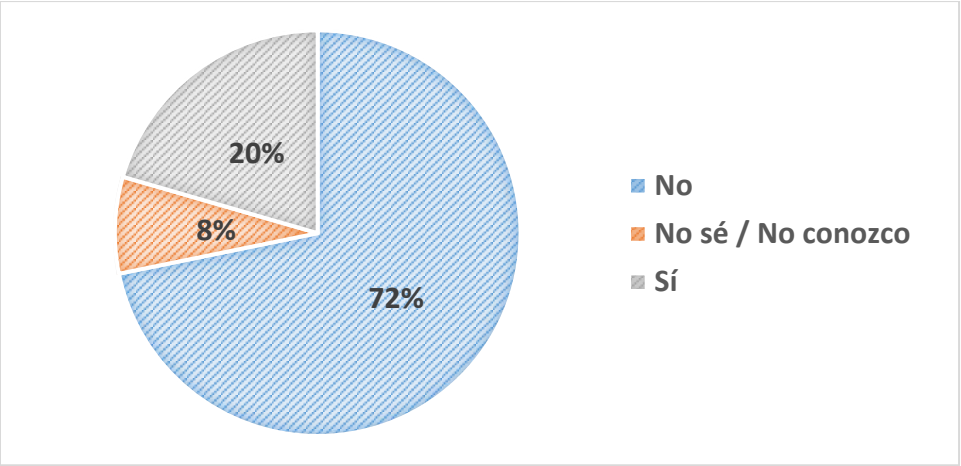

Figura 13. Familiaridad con los mecanismos de seguridad en sistemas de votación electrónica.

Fuente: Elaboración propia

Los resultados presentados en la figura 14 muestran que un 91.03% de los encuestados cree que la implementación de blockchain en el voto electrónico podría aumentar la seguridad del proceso electoral. Solo un 2.56% de los participantes se opone a esta idea, mientras que un 6.41% se muestra indeciso. Esta información sugiere un fuerte apoyo hacia el uso de la tecnología blockchain como una herramienta para mejorar la seguridad en los procesos electorales.

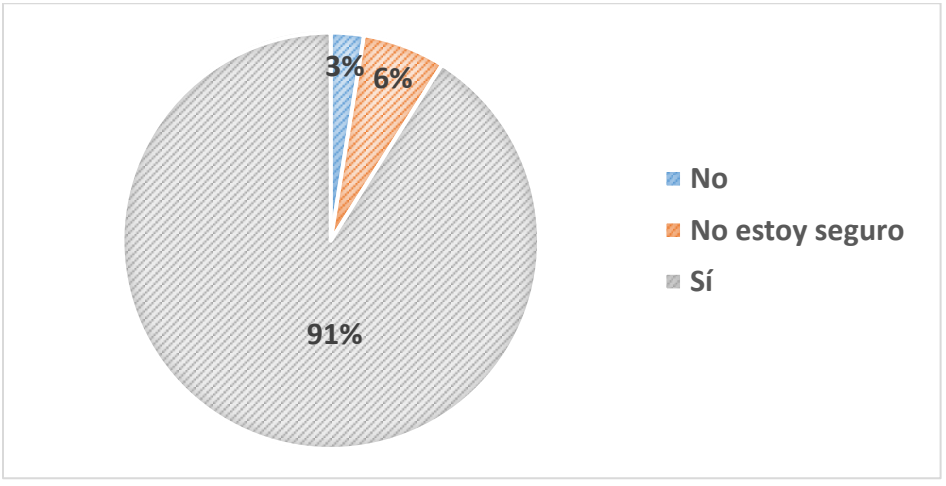

Figura 14. Percepción sobre el impacto de blockchain en la seguridad del voto electrónico.

Fuente: Elaboración propia

Los resultados de la figura 15 indican que una abrumadora mayoría de los encuestados (82.05%) está de acuerdo con la afirmación de que blockchain y los estándares emergentes, como ISO/TC 307 y W3C Verifiable Credentials, pueden mejorar la transparencia electoral en Ecuador, especialmente en el contexto de inestabilidad política. Además, un 10.26% se muestra neutral al respecto, mientras que un 10.26% afirma estar totalmente de acuerdo. Estos datos sugieren un fuerte respaldo hacia la utilización de estas tecnologías para fomentar la transparencia en el proceso electoral del país.

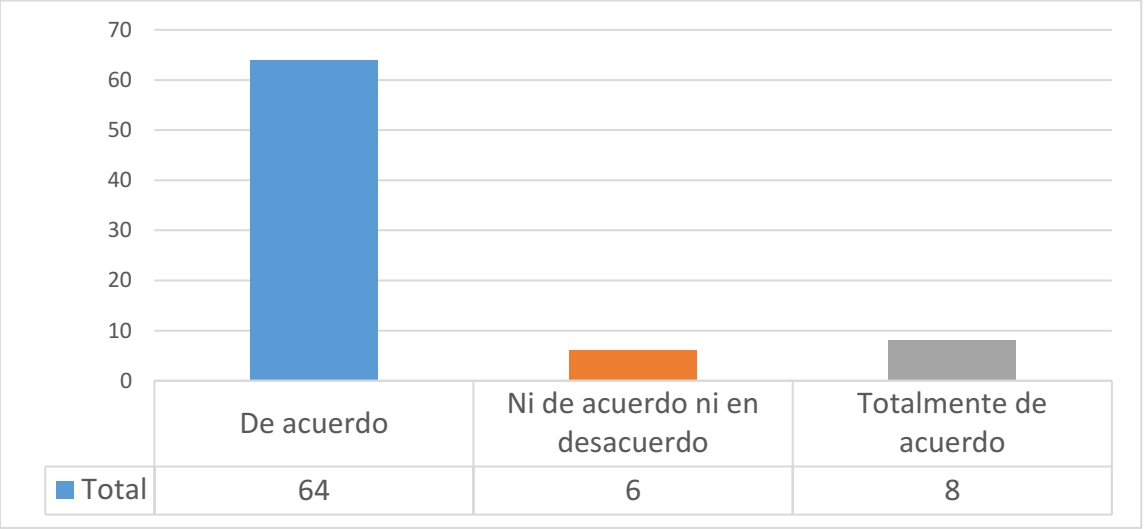

Figura 15. Aceptación de blockchain y estándares emergentes para aumentar la transparencia electoral en Ecuador.

Fuente: Elaboración propia

La Figura 16 presenta un panorama claro sobre las preocupaciones de seguridad en los sistemas de voto electrónico. Un notable 79.49% de los encuestados identifica los ataques que bloquean el acceso al sistema, como los ataques de denegación de servicio (DDoS), como la principal amenaza. En contraste, solo un 2.56% percibe la interceptación de comunicaciones para espiar o modificar datos como el riesgo más crítico. Asimismo, un 3.85% menciona la inyección de *malware*, mientras que un 14.10% se preocupa por la manipulación de los resultados del voto. Estos hallazgos subrayan una percepción dominante de vulnerabilidad frente a ataques que afectan la disponibilidad del sistema, lo que destaca la necesidad de fortalecer las medidas de seguridad para garantizar la integridad y la confianza en los procesos electorales.

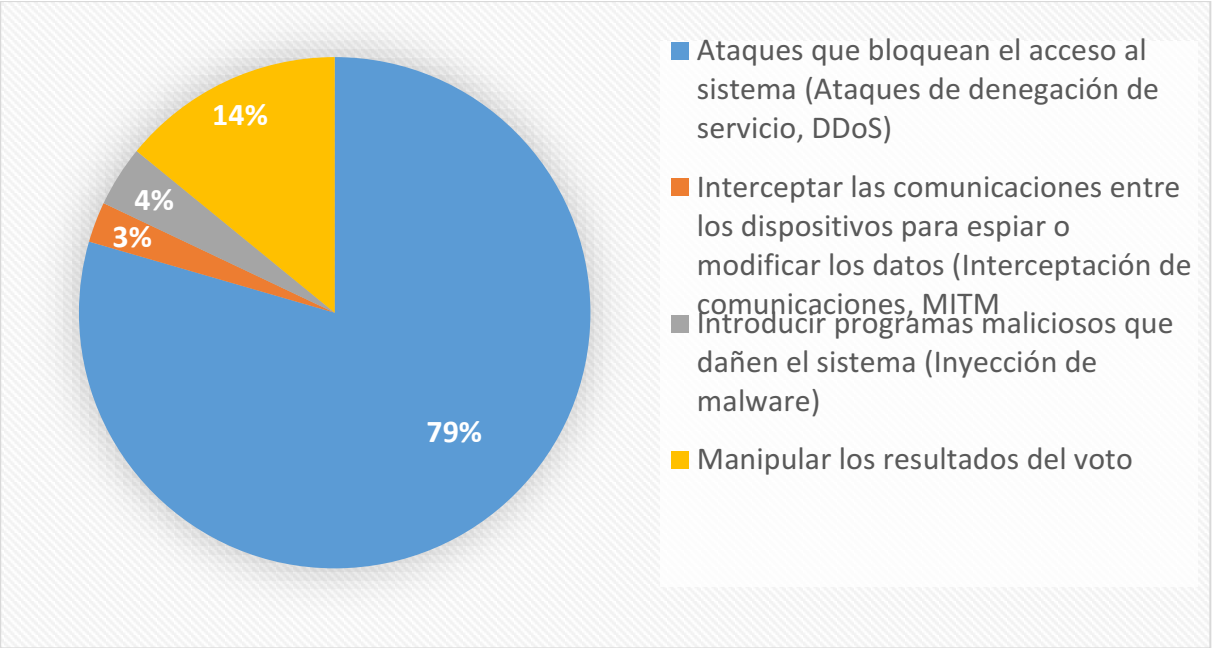

Figura 16. Percepciones sobre las amenazas de seguridad en sistemas de voto electrónico.

Fuente: Elaboración propia

Con la implementación del Sistema de Correlación de Eventos (SIEM), se prevé una mejora sustancial en la arquitectura de seguridad de la organización. Al consolidar la gestión de eventos de seguridad e integrar diversas fuentes de datos, como dispositivos de red, servidores y aplicaciones, se espera lograr una visibilidad completa y en tiempo real de las posibles amenazas. Esto facilitará una correlación más precisa de eventos y permitirá detectar anomalías de manera temprana, optimizando la capacidad para anticipar y mitigar incidentes. Además, los flujos automatizados de respuesta ante alertas agilizarán la toma de decisiones, reduciendo considerablemente los tiempos de reacción ante ataques, lo que hará la infraestructura más resiliente y eficiente, fortaleciendo la protección de los activos críticos y mejorando la postura de ciberseguridad en toda la organización.

Con la implementación de un SOC, se logrará anticipar desastres cibernéticos mediante la identificación proactiva de patrones de ataque, incluyendo la precedencia de incidentes, direcciones IP involucradas y su georreferenciación por país de origen y destino. Esto permitirá aplicar defensas en múltiples niveles, ajustando las medidas de seguridad según la amenaza específica y su contexto geográfico. Además, se facilitará la recolección de inteligencia de amenazas, optimizando la respuesta ante incidentes y mejorando la capacidad para mitigar ataques antes de que causen daños significativos.

El despliegue de un sistema inmutable de *backup* permitirá proteger de manera efectiva la integridad y disponibilidad de la información crítica. Se espera que los *backups* permanezcan inalterados frente a ataques, como el *ransomware*, garantizando su inmunidad frente a manipulaciones no autorizadas. Gracias a esto, los sistemas podrán restaurarse rápidamente a su estado original, minimizando el tiempo de inactividad y evitando la pérdida de datos. Esto fortalecerá la continuidad del negocio, mejorará la capacidad de respuesta ante incidentes de ciberseguridad y reforzará la confianza en la protección de los activos digitales de la organización.

Se espera que las auditorías semestrales, basadas en la norma ISO 27001:2022 en la cláusula 9.2.1 y 9.2.2, permitan minimizar significativamente las vulnerabilidades y brechas de inseguridad en el sistema de gestión de seguridad del CNE. A través de una revisión exhaustiva de los puertos abiertos y otras posibles áreas críticas documentadas en la fase de Identificación de Amenazas de la metodología, estas auditorías identificarán los puntos débiles del sistema y propondrán medidas correctivas oportunas. Como resultado, se anticipa una mejora continua en la seguridad, reduciendo los riesgos de accesos no autorizados y fortaleciendo la resiliencia del sistema ante posibles amenazas.

Discusión

Según (Al Barghuthi et al., 2019), *Blockchain* es una tecnología que facilita la trazabilidad en los procesos electorales basados en sistemas de voto electrónico, incrementando no solo la transparencia, sino también aportando un nivel adicional de seguridad. La capacidad de rastrear cada voto y vincularlo a un registro inmutable refuerza la confianza en la integridad del proceso. Esto en concordancia con (Vladucu et al., 2023) quien señala que *blockchain* ha sido implementada en países desarrollados como Alemania, Rusia, Estonia y Suiza, precisamente por su capacidad de almacenar los votos de manera inmutable. Esto ha reducido significativamente la amenaza de manipulación de votos y ha salvaguardado la legitimidad de las elecciones, demostrando que la tecnología no solo optimiza el proceso de conteo, sino que también asegura que los resultados sean confiables y verificables.

Por otra parte, según (Farooq et al., 2022), el voto electrónico respaldado por *blockchain* es esencial para proporcionar máxima transparencia y confiabilidad, factores críticos para construir una relación de confianza entre los votantes y las autoridades locales. Sin embargo, como advierte (Park et al., 2021), los sistemas de votación electrónica no están exentos de

vulnerabilidades. Los riesgos de ciberseguridad asociados al voto electrónico, como ataques de denegación de servicio y manipulación de resultados, generan inquietudes sobre la seguridad de estos sistemas. Esto subraya la necesidad de mecanismos de monitoreo y protección más robustos. Como señalan (Cucurull et al., 2020; González-Granadillo et al., 2021), la integración de sistemas SIEM fortalece aún más la seguridad en los sistemas de voto electrónico al correlacionar eventos y proporcionar alertas automáticas sobre posibles incidentes de seguridad. Estos sistemas mejoran la capacidad de las autoridades para reaccionar rápidamente ante amenazas emergentes. Finalmente, (Scarfone et al., 2008), en su publicación de la guía técnica para la evaluación y pruebas de seguridad de la información (NIST SP 800-115), subrayan la importancia de realizar pruebas y auditorías informáticas basadas en principios que también son reflejados en la norma ISO 27001:2022 para identificar y corregir brechas de seguridad (Sabillon et al., 2024). Estas auditorías regulares son especialmente cruciales en los sistemas de voto electrónico, ya que permiten mantener un control constante sobre la infraestructura de seguridad, minimizando la posibilidad de ataques y asegurando el cumplimiento de los estándares internacionales de seguridad de la información. Como menciona (Zambrano Cedeño & Zambrano Moreira, 2023), la implementación de sistemas de *backup* inmutables asegura la integridad y disponibilidad de la información crítica, protegiéndola incluso en casos de ataques como el *ransomware*, garantizando así la continuidad operativa y la protección de los datos electorales.

CONCLUSIONES

- Estableciendo los elementos estructurales del estado actual de la seguridad de la información, se logró identificar las vulnerabilidades en los sistemas de votación electrónica en Ecuador. A través del análisis de políticas, procedimientos y tecnologías vigentes, se establece una base sólida para implementar medidas de seguridad efectivas, como el uso de tecnologías innovadoras que fortalezcan la integridad y transparencia del proceso electoral. Esto permite avanzar hacia un sistema de votación más seguro y confiable, garantizando que cada ciudadano pueda ejercer su derecho al voto con confianza en la protección de su voluntad.
- La utilización de herramientas de detección de vulnerabilidades como Nmap y Nessus, permitió realizar un análisis exhaustivo de la aplicación web del CNE. Estos mecanismos facilitaron la identificación de amenazas, como puertos abiertos, que podrían ser explotados por actores maliciosos. Con esta estrategia de detección, se busca fortalecer la ciberseguridad de la aplicación, proporcionando una base sólida para implementar medidas correctivas y mejorar la protección ante posibles ataques.
- Con el escaneo de vulnerabilidades se encontraron un total de 8,355 vulnerabilidades, las cuales fueron clasificadas mediante una matriz de riesgo en niveles de riesgo alto, medio, bajo y muy bajo, estando todas ellas propensas a un ataque cibernético. Este análisis ha revelado la significativa exposición de los sistemas, subrayando la importancia de priorizar las acciones de mitigación, especialmente en aquellas vulnerabilidades que presentan un mayor nivel de criticidad.
- La implementación del plan de fortalecimiento de ciberseguridad para el centro de datos del CNE permitió mejorar significativamente la protección de los sistemas electorales. A través de la introducción de *backups* inmutables y tecnología blockchain, se garantizó la integridad de los datos y la trazabilidad de los procesos. Además, las auditorías semestrales basadas en la norma ISO 27001:2022 y el rediseño de la arquitectura de red ayudaron a minimizar riesgos, detectar brechas de seguridad y reforzar la resiliencia frente a ciberamenazas, asegurando la continuidad y confianza.

RECOMENDACIONES

- Realizar análisis de vulnerabilidades y mantener un monitoreo constante de las redes del centro de datos del CNE es fundamental para mejorar la seguridad. Asimismo, se sugiere establecer protocolos de seguridad que permitan un control más efectivo sobre la información y los sistemas informáticos en los servidores de la organización.
- Invertir en herramientas avanzadas de detección de vulnerabilidades y tecnologías de seguridad informática en el centro de datos. La ciberseguridad debe ser considerada como un proceso de mejora continua, donde las soluciones y protocolos se ajusten a las amenazas emergentes y a los cambios en el entorno digital. Esta inversión permitirá mantener un nivel de protección adecuado y asegurar la integridad de la información frente a posibles ataques.
- Realizar monitoreos constantes de los sistemas informáticos en producción dentro de los servidores, con el fin de minimizar los riesgos de vulnerabilidades. Este enfoque permitirá identificar de manera proactiva las amenazas y priorizar las acciones de mitigación, especialmente en aquellas vulnerabilidades clasificadas como de alto riesgo. Al implementar un programa de pruebas regulares, como las de caja negra y caja blanca, se podrá reforzar la seguridad y reducir la exposición a ataques cibernéticos.
- Implementar los sistemas de correlación de eventos y establecer un SOC en el centro de datos para mejorar la capacidad de detección y respuesta ante incidentes de seguridad. Esta iniciativa permitirá una monitorización continua de las amenazas, asegurando una gestión más efectiva de la ciberseguridad y una protección robusta de los sistemas.

REFERENCIAS

Abuidris, Y., Hassan, A., Hadabi, A., & Elfadul, I. (2019). Risks and Opportunities of Blockchain Based on E-Voting Systems. *2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing*, 365–368. https://doi.org/10.1109/ICCWAMTIP47768.2019.9067529

Afifi, M. A. M. (2020). Assessing information security vulnerabilities and threats to implementing security mechanism and security policy audit. *Journal of Computer Science*, *16*(3), 321–329. https://doi.org/10.3844/JCSSP.2020.321.329

Afraz, N., Wilhelmi, F., Ahmadi, H., & Ruffini, M. (2023). Blockchain and Smart Contracts for Telecommunications: Requirements vs. Cost Analysis. *IEEE Access*, *11*, 95653–95666. https://doi.org/10.1109/ACCESS.2023.3309423

Agate, V., De Paola, A., Ferraro, P., Lo Re, G., & Morana, M. (2021). SecureBallot: A secure open source e-Voting system. *Journal of Network and Computer Applications*, *191*, 103165. https://doi.org/10.1016/J.JNCA.2021.103165

Aggarwal, S., & Kumar, N. (2021). Attacks on blockchain. *Advances in Computers*, *121*, 399–410. https://doi.org/10.1016/BS.ADCOM.2020.08.020

Ajayi, O., & Saadawi, T. (2021). Detecting Insider Attacks in Blockchain Networks. *2021 International Symposium on Networks, Computers and Communications (ISNCC)*. https://doi.org/10.1109/ISNCC52172.2021.9615799

Al Barghuthi, N. B., Hamdan, I., Al Suwaidi, S., Lootah, A., Al Amoudi, B., Al Shamsi, O., & Al Aryani, S. (2019). An Analytical View on Political Voting System using Blockchain Technology-UAE Case Study. *2019 Sixth HCT Information Technology Trends (ITT)*, 132–137. https://doi.org/10.1109/ITT48889.2019.9075074

Alangot, B., Reijsbergen, D., Venugopalan, S., Szalachowski, P., & Yeo, K. S. (2021). Decentralized and Lightweight Approach to Detect Eclipse Attacks on Proof of Work Blockchains. *IEEE Transactions on Network and Service Management*, *18*(2), 1659–1672. https://doi.org/10.1109/TNSM.2021.3069502

Al-Madani, A. M., Gaikwad, A. T., Mahale, V., & Ahmed, Z. A. T. (2020). Decentralized E-voting system based on Smart Contract by using Blockchain Technology. *2020 International Conference on Smart Innovations in Design, Environment, Management,*

Planning and Computing (ICSIDEMPC), 176–180. https://doi.org/10.1109/ICSIDEMPC49020.2020.9299581

Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers & Security*, *129*, 103208. https://doi.org/10.1016/J.COSE.2023.103208

Alvarado, J. G., Alvarado, A. D., & Cuaical, L. A. (2023). Application of regression methods to statistical data recorded by the Telecommunications Regulation and Control Agency in Ecuador. *Remittances Review*, *8*(4), 2669–2677. https://doi.org/10.33182/rr.v8i4.185

Alvi, S. T., Uddin, M. N., & Islam, L. (2020). Digital voting: A blockchain-based E-voting system using biohash and smart contract. *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 228–233. https://doi.org/10.1109/ICSSIT48917.2020.9214250

Andrea, K., Sherdek, G., Manuel, S., & Cevallos, C. (2021). Sistema electoral ecuatoriano, ¿concentrador o proporcional?: una aproximación crítica a las reformas del 2019-2020. *Estado & Comunes*, *1*(12), 17–36. https://doi.org/10.37228/ESTADO_COMUNES.V1.N12.2021.208

Aparicio-Izurieta, V. V. (2022). Computer crimes in Ecuador according to the COIP: documentary analysis. *Sapienza: International Journal of Interdisciplinary Studies*, *3*(1), 1057–1063. https://doi.org/10.51798/SIJIS.V3I1.284

Arévalo-Cordovilla, F. E., Ordoñez-Sigcho, I. B., Peñaherrera-Larenas, M. F., & Suárez-Matamoros, V. J. (2020). Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de información. *Dominio de Las Ciencias*, *6*(2), 835–846. https://doi.org/10.23857/DC.V6I2.1197

Asmat, H. (2023). Network Security Monitors: Tools, Incident Detection and Response. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.4505734

Báez Cheza, J. E. (2021). *Metodología de detección y mitigación de ataques DDOS en entornos SDN basado en la norma ISO/IEC 27001 para mejorar la seguridad en el plano de control* [Tesis de maestría, UNIVERSIDAD TÉCNICA DEL NORTE]. https://repositorio.utn.edu.ec/handle/123456789/11483

Bansal, G., Muzatko, S., & Shin, S. Il. (2021). Information system security policy noncompliance: the role of situation-specific ethical orientation. *Information Technology and People*, *34*(1), 250–296. https://doi.org/10.1108/ITP-03-2019-0109/FULL/XML

Bellini, E., Ceravolo, P., Bellini, A., & Damiani, E. (2020). Designing process-centric blockchain-based architectures: A case study in e-voting as a service. *Lecture Notes in Business Information Processing*, *379 LNBIP*, 1–23. https://doi.org/10.1007/978-3-030-46633-6_1/FIGURES/8

Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review. *IEEE Access*, *10*, 70746–70759. https://doi.org/10.1109/ACCESS.2022.3187688

Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A Survey on Blockchain for Information Systems Management and Security. *Information Processing & Management*, *58*(1), 102397. https://doi.org/10.1016/J.IPM.2020.102397

Blank, R. M., & Gallagher, P. D. (2012). NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments. *United States: National Institute of Standard & Technology*. https://doi.org/10.6028/NIST.SP.800-30R1

Carreño-Vélez, Y. M., Moreno-Arvelo, P. M., & Atencio-González, R. E. (2021). El voto electrónico alternativa para el proceso electoral ecuatoriano en tiempos de pandemia. *CIENCIAMATRIA*, *7*(1), 394–406. https://doi.org/10.35381/CM.V7I1.542

Castellanos Santamaría, A. S., Dandoy, R., Umpierrez de Reguero, S., Castellanos Santamaría, A. S., Dandoy, R., & Umpierrez de Reguero, S. (2021). Between a Rock and a Hard Place: Ecuador During The COVID-19 Pandemic. *Revista de Ciencia Política (Santiago)*, *41*(2), 321–351. https://doi.org/10.4067/S0718-090X2021005000117

Chen, Y., Chen, H., Han, M., Liu, B., Chen, Q., & Ren, T. (2020). A Novel Computing Power Allocation Algorithm for Blockchain System in Multiple Mining Pools under Withholding Attack. *IEEE Access*, *8*, 155630–155644. https://doi.org/10.1109/ACCESS.2020.3017716

Chhillar, K., & Shrivastava, S. (2021). University Computer Network Vulnerability Management using Nmap and Nexpose. *International Journal of Advanced Trends in Computer Science and Engineering*, *10*(6), 3084–3090. https://doi.org/10.30534/ijatcse/2021/021062021

Chicarino, V., Albuquerque, C., Jesus, E., & Rocha, A. (2020). On the detection of selfish mining and stalker attacks in blockchain networks. *Annals of Telecommunications*, *75*(3–4), 143–152. https://doi.org/10.1007/S12243-019-00746-2/METRICS

Código Orgánico Integral Penal – COIP. (2014). Registro Oficial Suplemento 180 de 10-feb.-2014. Última modificación: 17-feb.-2021. Recuperado de: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Corrales, J. (2020). Democratic backsliding through electoral irregularities: The case of Venezuela. *European Review of Latin American and Caribbean Studies*, *109*, 41–65. https://doi.org/10.32992/ERLACS.10598

Cucurull, J., Tselios, C., Rueda, C., Folch, N., Copty, F., Igbaria, R., Athanatos, M., Krithinakis, A., Ioannidis, S., Ruiz, J. F., & Barrientos, P. (2020). Integration of an online voting solution with the SMESEC security framework. *2020 IEEE International Systems Conference (SysCon)*. https://doi.org/10.1109/SYSCON47679.2020.9275838

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal*, *33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202/FULL/PDF

Dankan Gowda, V., Kawale, S. R., Prasad, K. D. V., Anil Kumar, N., Reddy, N. S., & Ashreetha, B. (2023). Technologies for Comprehensive Information Security in the IoT. *2023 International Conference for Advancement in Technology (ICONAT)*. https://doi.org/10.1109/ICONAT57137.2023.10080332

Daramola, O., & Thebus, D. (2020). Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-Voting for National Elections. *Informatics 2020*, *7*(2), 16. https://doi.org/10.3390/INFORMATICS7020016

Darmawan, I. (2021). E-voting adoption in many countries: A literature review. *Asian Journal of Comparative Politics*, *6*(4), 482–504. https://doi.org/10.1177/20578911211040584

De la Rosa Martín, T. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001. *Revista Universidad y Sociedad*, *13*(5), 495–506. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500495&lng=es&nrm=iso&tlng=es

El Madhoun, N., Hatin, J., & Bertin, E. (2021). A decision tree for building IT applications: What to choose: blockchain or classical systems? *Annales of Telecommunications*, *76*(3–4), 131–144. https://doi.org/10.1007/S12243-020-00814-Y/METRICS

Eshetu, A. Y., Mohammed, E. A., & Salau, A. O. (2024). Cybersecurity vulnerabilities and solutions in Ethiopian university websites. *Journal of Big Data*, *11*(1), 1–35. https://doi.org/10.1186/S40537-024-00980-Z/TABLES/4

Essex, A., & Goodman, N. (2020). Protecting Electoral Integrity in the Digital Age: Developing E-Voting Regulations in Canada. *Election Law Journal: Rules, Politics, and Policy*, *19*(2), 162–179. https://doi.org/10.1089/ELJ.2019.0568

Farooq, M. S., Iftikhar, U., & Khelifi, A. (2022). A Framework to Make Voting System Transparent Using Blockchain Technology. *IEEE Access*, *10*, 59959–59969. https://doi.org/10.1109/ACCESS.2022.3180168

Francisco Gabriel, V.-R., Gema Eliseth, B.-C., & de la Judicatura Ecuador, C. (2024). Gestión electoral y políticas públicas. *Revista Científica Arbitrada de Investigación En Comunicación, Marketing y Empresa REICOMUNICAR. ISSN 2737-6354.*, *7*(13 Ed. esp.), 2–10. https://doi.org/10.46296/RC.V7I13EDESPJUN.0250

Gonzáles, J., Hidalgo, C., Arce, J., & Ordoñes, P. (2019). Análisis y revisión sobre delitos informáticos en el Ecuador. *Revista Conference Proceedings*, *3*(1). http://repositorio.utmachala.edu.ec/handle/48000/18031

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, *21*(14), 4759. https://doi.org/10.3390/S21144759

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/CYBSEC/TYAA005

Guru, A., Mohanta, B. K., Mohapatra, H., Al-Turjman, F., Altrjman, C., & Yadav, A. (2023). A Survey on Consensus Protocols and Attacks on Blockchain Technology. *Applied Sciences*, *13*(4), 2604. https://doi.org/10.3390/APP13042604

Haque, Z., & Carroll, D. (2020). Assessing the Impact of Information and Communication Technologies on Electoral Integrity. *Https://Home.Liebertpub.Com/Elj*, *19*(2), 127–148. https://doi.org/10.1089/ELJ.2019.0558

Hecimovich, J. P. (2022). Coaliciones reformistas y tipo de régimen: una teoría del cambio electoral aplicada al Ecuador. *Revista Ecuatoriana de Ciencia Política*, *1*(1), 81–100. https://doi.org/10.59352/RECP.V1I1.26

Iqbal, M., & Matulevicius, R. (2021). Exploring Sybil and Double-Spending Risks in Blockchain Systems. *IEEE Access*, *9*, 76153–76177. https://doi.org/10.1109/ACCESS.2021.3081998

ISO. (2018). *ISO/IEC 27000 - Information technology — Security techniques — Information security management systems — Overview and vocabulary*. https://www.iso.org/standard/73906.html

Kaudare, A., Hazra, M., Shelar, A., & Sabnis, M. (2020). Implementing electronic voting system with blockchain technology. *2020 International Conference for Emerging Technology (INCET)*. https://doi.org/10.1109/INCET49848.2020.9154116

Khan, K. M., Arshad, J., & Khan, M. M. (2021). Empirical analysis of transaction malleability within blockchain-based e-Voting. *Computers & Security*, *100*, 102081. https://doi.org/10.1016/J.COSE.2020.102081

Kho, Y. X., Heng, S. H., & Chin, J. J. (2022). A Review of Cryptographic Electronic Voting. *Symmetry 2022*, *14*(5), 858. https://doi.org/10.3390/SYM14050858

Khutkyy, D., & Laureda, E. A. (2023). Internet Voting for Policy Proposals: Amplifying Open Government in Chile and Colombia. *JeDEM - EJournal of EDemocracy and Open Government*, *15*(1), 48–72. https://doi.org/10.29379/jedem.v15i1.791

Kinyua, J., & Awuah, L. (2021). AI/ML in Security Orchestration, Automation and Response: Future Research Directions. *Intelligent Automation & Soft Computing*, *28*(2), 527–545. https://doi.org/10.32604/IASC.2021.016240

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability*, *15*(7), 5828. https://doi.org/10.3390/SU15075828

Kwon, R., Ashley, T., Castleberry, J., McKenzie, P., & Gupta Gourisetti, S. N. (2020). Cyber threat dictionary using MITRE ATTCK matrix and NIST cybersecurity framework mapping. *2020 Resilience Week (RWS)*, 106–112. https://doi.org/10.1109/RWS50334.2020.9241271

Ley Orgánica de Telecomunicaciones. (2015). Registro Oficial Suplemento 439 de 18-feb.-2015. Recuperado de: https://www.arcotel.gob.ec/wp-content/uploads/2017/06/002_ley-organica-de-telecomunicaciones-LOT.pdf

Li, T., Chen, Y., Wang, Y., Wang, Y., Zhao, M., Zhu, H., Tian, Y., Yu, X., & Yang, Y. (2020). Rational Protocols and Attacks in Blockchain System. *Security and Communication Networks*, *2020*(1), 8839047. https://doi.org/10.1155/2020/8839047

Liu, C., Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management*, *54*, 102152. https://doi.org/10.1016/J.IJINFOMGT.2020.102152

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. *2023 International Conference On Cyber Management And Engineering (CyMaEn)*, 117–122. https://doi.org/10.1109/CYMAEN57228.2023.10051114

Malecki, F. (2021). Optimising storage processes to reduce the risk of ransomware. *Network Security*, *2020*(5), 6–8. https://doi.org/10.1016/S1353-4858(20)30055-6

Marcén, A. G. (2021). El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea. *CUADERNOS DE DERECHO TRANSNACIONAL*, *13*(2), 209–232. https://doi.org/10.20318/CDT.2021.6256

McCorry, P., Mehrnezhad, M., Toreini, E., Shahandashti, S. F., & Hao, F. (2021). On Secure E-Voting over Blockchain. *Digital Threats: Research and Practice*, *2*(4). https://doi.org/10.1145/3461461/ASSET/80AD40D2-4640-4DFF-9AD9-2C5CA4A31432/ASSETS/GRAPHIC/DTRAP0204-33-T03.JPG

Meza Pérez, E. J., Méndez Garcés, E. F., Meza Pérez, D. A., Meza Pérez, E. J., Méndez Garcés, E. F., & Meza Pérez, D. A. (2021). El voto electrónico en el Ecuador; perspectivas desde crecientes avances tecnológicos. *Revista Universidad y Sociedad*, *13*(3), 525–535.

http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000300525&lng=es&nrm=iso&tlng=es

Morales, F., Toapanta, S., & Toasa, R. M. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. *Revista Ibérica de Sistemas e Tecnologias de Informação*.

Morán, I. (2023). La Ley de protección de datos y su incidencia en los derechos digitales en Ecuador en el año 2022. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, *7*(48), 57–66. https://doi.org/10.29018/ISSN.2588-1000VOL7ISS48.2023PP57-66

Morello, M. L. (2022). *Towards standardization of audit procedures for the new version of ISO/IEC 27002* [Tesis de máster]. Politecnico di Torino.

Morgan, D., Saldanha, F., & Barbosa Da Silva, M. (2020). Transparency and accountability of government algorithms: the case of the Brazilian electronic voting system. *Cadernos EBAPE.BR*, *18*(spe), 697–712. https://doi.org/10.1590/1679-395120190023X

Muharrom, M., & Saktiansyah, A. (2023). Analysis of Vulnerability Assessment Technique Implementation on Network Using OpenVas. *International Journal of Engineering and Computer Science Applications (IJECSA)*, *2*(2), 53–62. https://doi.org/10.30812/IJECSA.V2I2.3297

Narváez Guerrón, J. P. (2024). *Análisis de la seguridad informática basado en la norma ISO/IEC 27002:2022 y NIST 800-61 para el área de operaciones y servicios del Gobierno Provincial de Imbabura* [Tesis de maestría, UNIVERSIDAD TÉCNICA DEL NORTE]. https://repositorio.utn.edu.ec/handle/123456789/15944

Nicolas, K., Wang, Y., Giakos, G. C., Wei, B., & Shen, H. (2021). Blockchain System Defensive Overview for Double-Spend and Selfish Mining Attacks: A Systematic Approach. *IEEE Access*, *9*, 3838–3857. https://doi.org/10.1109/ACCESS.2020.3047365

Ortiz Osorio, M. E. (2021). *DISEÑO DE UNA HERRAMIENTA TECNOLÓGICA PARA MEJORAR EL VOTO ELECTRÓNICO EN LAS ELECCIONES ESTUDIANTILES DE LA FEDERACIÓN DE ESTUDIANTES DE UNA INSTITUCION DE EDUCACION SUPERIOR* [ESCUELA SUPERIOR POLITECNICA DEL LITORAL]. http://www.dspace.espol.edu.ec/handle/123456789/50892

Palutke, R., Block, F., Reichenberger, P., & Stripeika, D. (2020). Hiding Process Memory Via Anti-Forensic Techniques. *Forensic Science International: Digital Investigation*, *33*, 301012. https://doi.org/10.1016/J.FSIDI.2020.301012

Pandey, S., & Chaudhary, A. (2023). Vulnerability Scanning. *Authorea Preprints*. https://doi.org/10.36227/TECHRXIV.20317194.V1

Panja, S., & Roy, B. (2021). A secure end-to-end verifiable e-voting system using blockchain and cloud server. *Journal of Information Security and Applications*, *59*, 102815. https://doi.org/10.1016/J.JISA.2021.102815

Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going from bad to worse: from Internet voting to blockchain voting. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/CYBSEC/TYAA025

Parrales Alarcón, F., Silva Lapo, R., Jiménez Silva, P., & Wong Cruz, S. (2024). La protección constitucional del derecho a la privacidad en la era digital. *Sinergia Académica*, *7*(Especial 3), 602–615. https://doi.org/10.51736/SA.V7IESPECIAL

Patel, N. P., Parekh, R., Thakkar, N., Gupta, R., Tanwar, S., Sharma, G., Davidson, I. E., & Sharma, R. (2022). Fusion in Cryptocurrency Price Prediction: A Decade Survey on Recent Advancements, Architecture, and Potential Future Directions. *IEEE Access*, *10*, 34511–34538. https://doi.org/10.1109/ACCESS.2022.3163023

Pawlak, M., & Poniszewska-Marańda, A. (2021). Trends in blockchain-based electronic voting systems. *Information Processing & Management*, *58*(4), 102595. https://doi.org/10.1016/J.IPM.2021.102595

Pincay Romero, K. G. (2021). Características de la conectividad a internet en el cantón Pasaje. *Revista Universidad y Sociedad*, *13*(3), 150–160. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000300150&lng=es&nrm=iso&tlng=pt

Pramulia, D., & Anggorojati, B. (2020). Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask. *2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*, 18–23. https://doi.org/10.1109/ICIMCIS51567.2020.9354310

Putra, A. P., & Soewito, B. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector. *IJACSA) International Journal of Advanced Computer Science and Applications*, *14*(4), 1–9. www.ijacsa.thesai.org

Putro, A. A., Ambarwati, A., Setiawan, E., Rahman, J. A., & 51 Surabaya, H. N. (2021). Analisa Manajemen Risiko E-Learning Edlink Menggunakan Metode NIST SP 800-30 Revisi 1. *Jurnal Teknologi Dan Informasi*, *11*(2), 125–136. https://doi.org/10.34010/JATI.V11I2.5314

Ramos Torres, C., Vieira, D., & Jacobovski, R. (2021). Estrutura institucional na avaliação e monitoramento de políticas públicas: uma análise nos países do MERCOSUL. *Revista Brasileira de Administração Científica*, *12*(2), 232–245. https://doi.org/10.6008/CBPC2179-684X.2021.002.0019

Risnanto, S., Bin, Y., Rahim, A., & Suryana Herman, N. (2020). E-VOTING READINESS MAPPING FOR GENERAL ELECTION IMPLEMENTATION. *Journal of Theoretical and Applied Information Technology*, *31*, 20. https://www.jatit.org/volumes/Vol98No20/16Vol98No20.pdf

Rosacker, K. M., & Rosacker, R. E. (2020). Voting is a right: a decade of societal, technological and experiential progress towards the goal of remote-access voting. *Transforming Government: People, Process and Policy*, *14*(5), 701–712. https://doi.org/10.1108/TG-03-2020-0053/FULL/XML

Ruiz Romero, R. R. (2022). *El constreñimiento al sufragante como delito contra los derechos de participación en el Código Orgánico Integral Penal* [Posgrado / Maestría en Derecho Mención Derecho Procesal / Tesis Maestría en Derecho Mención Derecho Procesal, Universidad Laica Vicente Rocafuerte de Guayaquil]. http://repositorio.ulvr.edu.ec/handle/44000/5170

Sabillon, R., Bermejo, J. R., Cano, J., Higuera, J. B., & Sicilia, J. A. (2024). Assessing the Effectiveness of Cyber Domain Controls When Conducting Cybersecurity Audits: Insights from Higher Education Institutions in Canada. *Electronics*, *13*(16), 3257. https://doi.org/10.3390/ELECTRONICS13163257

Satizábal, C., Páez, R., & Forné, J. (2022). Secure Internet Voting Protocol (SIVP): A secure option for electoral processes. *Journal of King Saud University - Computer and Information Sciences*, *34*(6), 3647–3660. https://doi.org/10.1016/J.JKSUCI.2020.12.016

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment. *Nist Special Publication*, *800*, 1–80. https://doi.org/10.6028/NIST.SP.800-115

Sheikh, S., & Kumar Singh, U. (2023). An Investigation of Vulnerabilities Discovery and Assessment in Educational Institutions. *ICONIC RESEARCH AND ENGINEERING JOURNALS*, *6*(7), 143–150.

Silic, M., & Lowry, P. B. (2020). Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. *Journal of Management Information Systems*, *37*(1), 129–161. https://doi.org/10.1080/07421222.2019.1705512

Singhal, M. K. (2022). Protecting customer databases to shield business data against ransomware attacks and effective disaster recovery in a hybrid production environment. *ICIMMI '22: Proceedings of the 4th International Conference on Information Management & Machine Intelligence*. https://doi.org/10.1145/3590837.3590927

Soud, M., Helgason, S., Hjalmtysson, G., & Hamdaqa, M. (2020). TrustVote: On Elections We Trust with Distributed Ledgers and Smart Contracts. *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 176–183. https://doi.org/10.1109/BRAINS49436.2020.9223306

Srivastava, K., & Singh, P. (2024). Cybersecurity: An In-Depth Analytical Review. *Journal of Management and Service Science (JMSS)*, *4*(1), 1–13. https://doi.org/10.54060/A2ZJOURNALS.JMSS.49

Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, *215*, 483–487. https://doi.org/10.1016/J.PROCS.2022.12.050

Toapanta, S. M. T., Piguave, J. E. A., & Gallegos, L. E. M. (2020). Analysis of Adequate Bandwidths to Guarantee an Electoral Process in Ecuador. *Smart Innovation, Systems and Technologies*, *165*, 255–265. https://doi.org/10.1007/978-981-15-0077-0_26

Toapanta, S. M. T., Sañicela, S. X. R., Valencia, D. W. B., & Gallegos, L. E. M. (2019). Analysis of information security for a voting process for sectional governments in

Ecuador. *Advances in Science, Technology and Engineering Systems*, *4*(5), 352–359. https://doi.org/10.25046/AJ040546

Toapanta Toapanta, S. M., Huilcapi Subia, D. F., Cepeda Aveiga, M. A., & Mafla Gallegos, L. E. (2020). Ensuring the Blind Signature for the Electoral System in a Distributed Environment. *Proceedings of 2020 IEEE International Conference on Power, Intelligent Computing and Systems, ICPICS 2020*, 211–215. https://doi.org/10.1109/ICPICS50287.2020.9202348

Toto, R., & Sánchez, C. (2021). Análisis y Proceso de Hardening de Servidor Virtual Web, Facultad de Ingeniería (IngeTic). In *Revista PGI. Investigación, Ciencia y Tecnología en Informática* (Vol. 8, pp. 189–192). https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/82

Umar, H. S., Atte, J., & Haruna, S. (2022). ELECTRONIC VOTING AS AN INSTRUMENT FOR FREE, FAIR AND CREDIBLE ELECTIONS IN NIGERIAN POLITICAL SYSTEM: ISSUES AND CHALLENGES. *European Journal of Political Science Studies*, *5*(2). https://doi.org/10.46827/EJPSS.V5I2.1215

Vielberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, *8*, 227756–227779. https://doi.org/10.1109/ACCESS.2020.3045514

Vladucu, M. V., Dong, Z., Medina, J., & Rojas-Cessa, R. (2023). E-Voting Meets Blockchain: A Survey. *IEEE Access*, *11*, 23293–23308. https://doi.org/10.1109/ACCESS.2023.3253682

Wani, S., Imthiyas, M., Almohamedh, H., Alhamed, K. M., Almotairi, S., & Gulzar, Y. (2021). Distributed Denial of Service (DDoS) Mitigation Using Blockchain—A Comprehensive Insight. *Symmetry 2021*, *13*(2), 227. https://doi.org/10.3390/SYM13020227

Wendy, & Gunawan, W. (2019). Measuring Information Security and Cybersecurity on Private Cloud Computing. *Journal of Theoretical and Applied Information Technology*, *15*(1). www.jatit.org

Wu, Y., Song, P., & Wang, F. (2020). Hybrid Consensus Algorithm Optimization: A Mathematical Method Based on POS and PBFT and Its Application in Blockchain.

Mathematical Problems in Engineering, *2020*(1), 7270624. https://doi.org/10.1155/2020/7270624

Xiao, S., Wang, X. A., Wang, W., & Wang, H. (2020). Survey on Blockchain-Based Electronic Voting. *Advances in Intelligent Systems and Computing*, *1035*, 559–567. https://doi.org/10.1007/978-3-030-29035-1_54

Yang, X., Yi, X., Nepal, S., Kelarev, A., & Han, F. (2020). Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities. *Future Generation Computer Systems*, *112*, 859–874. https://doi.org/10.1016/J.FUTURE.2020.06.051

Yin, L., Fang, B., Guo, Y., Sun, Z., & Tian, Z. (2020). Hierarchically defining Internet of Things security: From CIA to CACA. *International Journal of Distributed Sensor Networks*, *16*(1). https://doi.org/10.1177/1550147719899374/ASSET/IMAGES/LARGE/10.1177_1550147719899374-FIG5.JPEG

Zaeem, R. N., & Barber, K. S. (2020). The Effect of the GDPR on Privacy Policies. *ACM Transactions on Management Information Systems (TMIS)*, *12*(1). https://doi.org/10.1145/3389685

Zambrano Cedeño, R. J., & Zambrano Moreira, A. C. (2023). Sistemas inmutables de backup ante ataques de ransomware hacia una infraestructura TI. *Código Científico Revista de Investigación*, *4*(1), 600–612. https://doi.org/10.55813/GAEA/CCRI/V4/N1/133

Zhang, Y., Li, Y., Fang, L., Chen, P., & Dong, X. (2019). Privacy-protected Electronic Voting System Based on Blockchin and Trusted Execution Environment. *2019 IEEE 5th International Conference on Computer and Communications (ICCC)*, 1252–1257. https://doi.org/10.1109/ICCC47050.2019.9064387

Zurita Meza, E. de las M., & Ramírez Supe, D. S. (2021). Vulnerabilidades y seguridades en el voto electrónico: una revisión. *REVISTA ODIGOS*, *2*(1), 55–67. https://doi.org/10.35290/RO.V2N1.2021.405

ANEXOS

Anexo 1. Encuesta técnica realizada en Google Forms

1. ¿Está familiarizado con los protocolos de seguridad utilizados en sistemas de votación electrónica (cifrado de datos, autenticación de usuarios)? ¿Cuál es su nivel de conocimiento sobre Blockchain?

   - ☐ Muy alto: Tengo un conocimiento profundo, incluyendo desarrollo y aplicaciones avanzadas.
   - ☐ Alto: Tengo un buen conocimiento y comprendo su funcionamiento y aplicaciones.
   - ☐ Neutral: Tengo un conocimiento básico y entiendo algunas aplicaciones.
   - ☐ Bajo: Tengo poco conocimiento y no comprendo bien el funcionamiento.
   - ☐ Muy bajo: No tengo conocimiento sobre el tema.

2. ¿Cuál es su nivel de conocimiento sobre los sistemas de votación electrónica?

   - ☐ Muy alto: Tengo un conocimiento profundo sobre los sistemas de votación electrónica, incluyendo sus características técnicas y desafíos de seguridad.
   - ☐ Alto: Conozco bien los sistemas de votación electrónica y sus procesos.
   - ☐ Neutral: Tengo un conocimiento básico y entiendo su funcionamiento general.
   - ☐ Bajo: He oído hablar de los sistemas de votación electrónica, pero no sé cómo funcionan.
   - ☐ Muy bajo: No tengo conocimiento sobre los sistemas de votación electrónica.

3. ¿Considera que el sistema electoral en Ecuador es transparente?

   - ☐ Muy transparente
   - ☐ Transparente
   - ☐ Poco transparente
   - ☐ Nada transparente

4. ¿Cree que sería pertinente implementar un sistema de voto electrónico en Ecuador?

   - ☐ Muy pertinente
   - ☐ Pertinente
   - ☐ Poco pertinente

- ☐ Nada pertinente

5. ¿Está familiarizado con los mecanismos de seguridad utilizados en sistemas de votación electrónica (cifrado de datos, autenticación de usuarios)?

   - ☐ Sí
   - ☐ No
   - ☐ No sé / No conozco

6. ¿Cree que la implementación de blockchain en el voto electrónico podría aumentar la seguridad del proceso electoral?

   - ☐ Sí
   - ☐ No
   - ☐ No estoy seguro

7. ¿Qué tan de acuerdo está usted con la afirmación de que blockchain y los estándares emergentes (como ISO/TC 307 y W3C Verifiable Credentials) pueden mejorar la transparencia electoral en Ecuador, considerando la inestabilidad política?

   - ☐ Totalmente de acuerdo
   - ☐ De acuerdo
   - ☐ Ni de acuerdo ni en desacuerdo
   - ☐ En desacuerdo
   - ☐ Totalmente en desacuerdo

8. ¿Qué tipo de ataque o problema de seguridad cree que es más probable en un sistema de voto electrónico?

   - ☐ Ataques que bloquean el acceso al sistema (Ataques de denegación de servicio, DDoS)
   - ☐ Interceptar las comunicaciones entre los dispositivos para espiar o modificar los datos (Interceptación de comunicaciones, MITM)
   - ☐ Manipular los resultados del voto
   - ☐ Introducir programas maliciosos que dañen el sistema (Inyección de malware

Anexo 2. Validación 1 del Instrumento: Encuesta – Datos del experto

UNIVERSIDAD ESTATAL "PENÍNSULA DE SANTA ELENA"

INSTITO DE POSTGRADO
MAESTRIA EN CIBERSEGURIDAD

HOJA DE REGISTRO PARA VALIDACIÓN DE EXPERTOS
Maestrante: JORGE FAROUK MOLINA NOBOA

Universidad Estatal Península de Santa Elena: jorge.molinanoboa2610@upse.edu.ec

DATOS DEL EXPERTO:

Nombre/Apellidos:	Edisson Pompilio Quintuña Padilla
Última titulación académica:	Magister en Seguridad Informática Aplicada
Institución de adscripción	Universidad Estatal Península de Santa Elena
Cargo:	Docente de módulo de maestría
Teléfono celular (no es obligatorio)	
Dirección de correo:	equintuna@upse.edu.ec

Instrumento

Formato de encuesta para expertos en ciberseguridad

Sobre el instrumento.

Para su validación se presenta el formato de encuesta para expertos en ciberseguridad, cuyo objetivo es "Evaluar la percepción de expertos en ciberseguridad sobre la transparencia electoral, la viabilidad del voto electrónico y los riesgos de seguridad, para desarrollar un plan de detección de vulnerabilidades y fortalecimiento de la ciberseguridad en sistemas electorales"

Tema:

Evaluación de vulnerabilidades en sistemas de votación electrónica desde una perspectiva de ciberseguridad: caso de estudio en Ecuador.

Sobre la validación:

A continuación, se presentan las tablas con la referencia numérica de los ítems o aspectos sobre los que se indaga a través del cuestionario.

Estimado especialista, por favor, se le solicita valore cada item de acuerdo con los siguientes criterios:

Anexo 3. Validación 1 del Instrumento: Encuesta – Proceso de evaluación

Indicadores	Criterios o aspectos para considerar
SUFICIENCIA	El instrumento está alineado con el objetivo de la investigación.
CLARIDAD	Las preguntas formuladas responden a la finalidad del estudio.
COHERENCIA	Las preguntas guardan coherencia con el objetivo de la investigación.
RELEVANCIA	La redacción de las preguntas es clara y está bien argumentada.

Para ello, coloque en la casilla una "X" correspondiente a un número del uno (1) hasta el cuatro (4) de acuerdo con la siguiente escala.

Expresión cual	Calificación
Alto Nivel	4
Moderado Nivel	3
Bajo Nivel	2
No cumple con el contenido	1

El instrumento consta de 5 preguntas, cada una diseñada con opciones de respuesta en formato de opción múltiple. Se solicita, además de la calificación de cada pregunta, que los participantes aporten observaciones que permitan mejorar la redacción y precisión del cuestionario, optimizando así su efectividad. A continuación, se presentan las 5 preguntas con sus respectivas opciones de respuesta.

Anexo 4. Validación 1 del Instrumento: Encuesta - Rúbrica

RÚBRICA: INSTRUMENTO DE ENCUESTA PARA EXPERTOS EN CIBERSEGRUDAD.																	
CRITERIOS		SUFICIENCIA				CLARIDAD				COHERENCIA				RELEVANCIA				OBSERVACIÓN
Nº	PREGUNTAS	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	
1	¿Considera que el sistema electoral en Ecuador es transparente?				X				X				X				X	
2	¿Cree que sería pertinente implementar un sistema de voto electrónico en Ecuador?				X				X				X				X	
3	¿Está familiarizado con los mecanismos de seguridad utilizados en sistemas de votación electrónica (cifrado de datos, autenticación de usuarios)?				X				X				X				X	
4	¿Cree que la implementación de blockchain en el voto electrónico podría aumentar la seguridad del proceso electoral?				X				X				X				X	
5	¿Qué tipo de ataque o problema de seguridad cree que es más probable en un sistema de voto electrónico?				X				X				X				X	

Anexo 5. Validación 1 del Instrumento: Encuesta – Sugerencias y recomendaciones

Sugerencias y recomendaciones:

_____
_____
_____
_____

Nombre/Apellidos: Edisson Pompilio Quintuña Padilla
Correo: e[redacted]se.edu.ec
Teléfono celular: