Universidad Internacional de La Rioja (UNIR)

ESIT

Máster universitario en Seguridad Informática

Nueva metodología de seguridad informática para procesos electorales (MSIPE) en Ecuador.

Trabajo Fin de Máster

Presentado por: Carlos Fabricio Espín Armijo

Director/a: Sergio Mauricio Martínez Monterrubio. PhD

Ciudad: Quito, Ecuador
Fecha: 23 de septiembre de 2020

Índice de Contenidos

Índice de Figuras

Índice de Tablas

Resumen

En el presente trabajo de investigación se busca implementar una Nueva Metodología de Seguridad Informática para Procesos Electorales (MSIPE) en Ecuador. La metodología MSIPE se asienta en los controles de seguridad determinados por el *(Center for Internet Security)* en adelante CIS y en los estándares de calidad ISO17582 alineados a procesos electorales, aprobados por la Organización de Estados Americanos en adelante OEA. Este trabajo realiza una metodología eficiente que permita el control de accesos al Sistema Informático de Resultados Electorales del organismo electoral de Ecuador. Ello contribuirá efectivamente la implementación con el aseguramiento de la “confidencialidad”, “integridad” y “disponibilidad” del sistema, asegurando la seguridad informática de las elecciones en Ecuador.

Palabras Clave: Metodología de seguridad informática para elecciones, Accesos a sistemas informáticos, Auditoría Informática.

Abstract

In the present research work, it seeks to implement a New Methodology of Information Security for Electoral Processes (MSIPE) in Ecuador. The MSIPE methodology is based on the security controls determined by the Center for Internet Security (CIS) and on the ISO17582 quality standards for electoral processes approved by the Organization of American States (OAS). This work carries out an efficient methodology that allows the control of access to the Computerized System of Electoral Results of the electoral agency of Ecuador. This will effectively contribute to the implementation by ensuring the "confidentiality", "integrity" and "availability" of the system, ensuring the computer security of elections in Ecuador.

Keywords: Computer security methodology for elections, Access to computer systems, Computer audit

Agradecimientos

Existe un largo camino recorrido desde la decisión de iniciar el máster hasta la presentación de este trabajo. Durante este tiempo personas cercanas a mí, me han apoyado en este camino por lo que este trabajo pertenece al sostén de todas esas personas que finalmente me permiten disfrutar el sacrificio realizado.

Primero quiero agradecer a Dios, por permitirnos la salud y vida en medio de esta crisis mundial por la pandemia que estamos atravesando.

Agradezco a mis queridos padres Carlos y Adela, y mis hermanos Daniel y Sarita quienes han sido mi refugio en momentos difíciles y me dan las ganas de seguir adelante.

Agradezco a mi amigo y consejero Fidel Ycaza por sus lecciones y apoyo en todos y cada uno de los pasos que he dado durante el proceso de formación de maestría y a mi sensei Fabián Benalcázar, quien por medio de la práctica del karate me ha transmitido las enseñanzas de las artes marciales, si uno cae debe levantarse con más ganas de seguir adelante sin importar las circunstancias hasta vencer las adversidades.

Y un agradecimiento especial al Dr. Sergio Mauricio Martínez como mi Director de TFM por su paciencia, constante apoyo y direccionamiento claves para el correcto desarrollo del presente trabajo.

Muchas Gracias a todos

Glosario de términos

SIGLA	DESCRIPCIÓN
FE	Función Electoral
CNE	Consejo Nacional Electoral
TCE	Tribunal Contencioso Electoral
DPE	Delegación Provincial Electoral
JPE	Junta Provincial Electoral
JEE	Junta Especial en el Exterior
JRV	Juntas Receptoras del Voto
MJRV	Miembros de Juntas Receptoras del Voto
PPL	Personas Privadas de Libertad
STPR	Sistema de Transmisión y Publicación de Resultados
SG	Secretaria General
CNTPE	Coordinación Nacional Técnica de Procesos Electorales
CNSIPTE	Coordinación Nacional de Seguridad Informática y Proyectos Tecnológicos Electorales
DNITCE	Dirección Nacional de Infraestructura Tecnológica y Comunicaciones Electorales
DNSIE	Dirección Nacional de Sistemas e Informática Electoral
DNSMIR	Dirección Nacional de Seguridad y Manejo integral de Riesgos
OSI	Oficial de Seguridad de la Información
TIC	Tecnologías de la Información y Comunicación
CRE	Constitución de la República del Ecuador
RO	Registro Oficial de Ecuador
BOE	Boletín Oficial del Estado España
LOE	Ley Orgánica Electoral y de Organizaciones Políticas de ña República del Ecuador, Código de la Democracia
COIP	Código Orgánico Integral Penal
ISO	Organización Internacional de Estandarización (International Standardization Organization)
CIS	Centro para la Seguridad de la Información (Center for Information Security)
ONU	Organización de Naciones Unidas
OEA	Organización de Estados Americanos
CAPEL	Centro de Asesoría y Promoción Electoral
INEC	Instituto Nacional de Estadísticas y Censos (Ecuador)
INE	Instituto Nacional de Estadística (España)
CGE	Contraloría General del Estado
SGC	Sistema de Gestión de Calidad
SGSI	Sistema de Gestión de Seguridad de la Información

Introducción

La toma de decisiones libres y voluntarias, así como la representatividad de un pueblo, ha sido adoptada como un sistema y una forma de organización política actualmente conocida por todos nosotros como Democracia. Si bien el término **Democracia,** fue acuñado desde antigua Grecia con la palabra **dēmokratía,** cuyos vocablos: **demos** significa pueblo; y **kratos** significa gobierno, establece que democracia es el **"gobierno del pueblo"**. Etimología que fue perfeccionada y definida en el discurso de (Lincoln, 1863) como **"el gobierno del pueblo, por el pueblo y para el pueblo"** (Centro de Asesoría y Promoción Electoral CAPEL, 2017, p. 249). Para ejercer la democracia es necesario establecer el derecho al sufragio como uno de los principios de los derechos humanos, el cual transcribo de la (Organizacion de las Naciones Unidas ONU, 1948) ***"Artículo 21.- 1. Toda persona tiene derecho a participar en el gobierno de su país, directamente o por medio de representantes libremente escogidos. 3. La voluntad del pueblo es la base de la autoridad del poder público; esta voluntad se expresará mediante elecciones auténticas que habrán de celebrarse periódicamente, por sufragio universal e igual y por voto secreto u otro procedimiento equivalente que garantice la libertad del voto".*** Los países que reconocen la Carta Universal de Derechos Humanos de las Naciones Unidas, adoptan en sus constituciones el sufragio bajo los principios del democráticos de elecciones libres, a fin de garantizar la transparencia, estabilidad y el progreso de los sistemas democráticos adoptados en cada estado soberano. Para la aplicación de este derecho, los organismos electorales de cada país deben transparentar las acciones que realicen, por lo que muchos se apoyan en las herramientas que ofrecen las Tecnologías de la Información y Comunicación TIC, en todas o en alguna etapa del proceso electoral. Estas tecnologías deben garantizar el principio de elecciones transparentes, que comprueben que la presentación de resultados es rápida y efectiva, evitando que entre los actores electorales se conciban dudas durante el procesamiento de las actas, cómputo y presentación de las mismas y la determinación de ganadores en la contienda electoral, en razón que la etapa de presentación de resultados es el punto de quiebre y la parte más importante de todo proceso electoral. Con lo expuesto, el presente trabajo busca la implementación de una nueva metodología de controles de accesos a sistemas de información que mitiguen falencias normativas y procedimentales que deben ser verificados en uno o varios sistemas del que principalmente debe prevalecer el sistema de escrutinios, de manera que permita generar confianza y seguridad, en cuanto a calidad y seguridad informática.

I. Motivación

En un proceso electoral, el escrutinio y presentación de resultados es la parte más importante de un proceso electoral, la rapidez y transparencia de esta etapa determinan la efectividad de los organismos electorales en los países que realizan las elecciones de manera periódica respetando los principios democráticos. En ocasiones, los diferentes actores electorales y han manifestado su desconfianza en los organismos públicos con la función y responsabilidad de la organización, dirección, vigilancia de procesos electivos de dignatarios transparentes y eficaces. El termino confianza que deben tener los actores electorales deriva de la satisfacción que tiene la ciudadanía hacia el organismo electoral de su país, la cual ha venido decayendo a lo largo del tiempo. Para esta investigación se ha elaborado la gráfica de la Figura 1, en donde se ven reflejados los informes presentados por la (Corporacion Latinobarometro, 2018) desde el año 1996 al 2018. La confianza en la democracia en el Ecuador refleja la desconfianza en las instituciones electorales, los procesos que organiza y los sistemas informáticos utilizados.

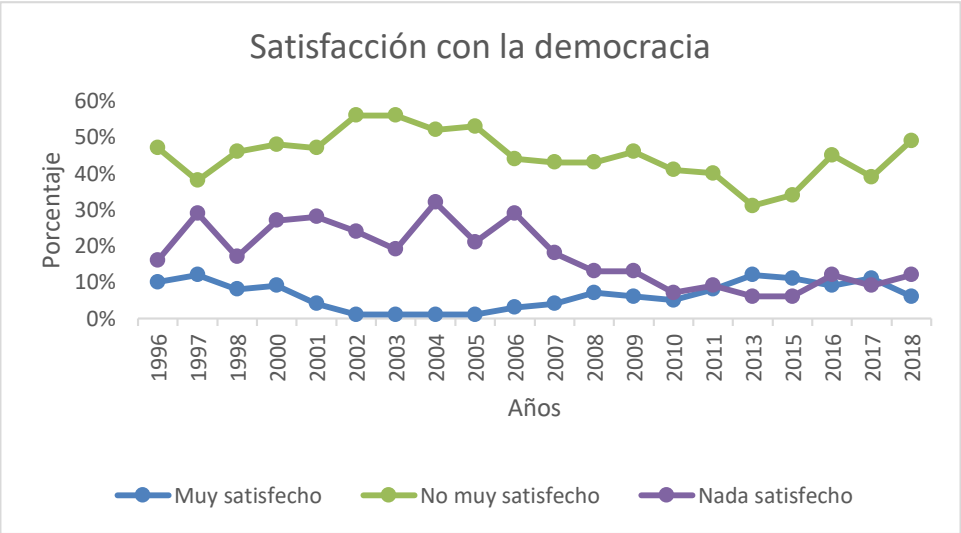


Figura 1: Satisfacción de la ciudadanía con la democracia en el Ecuador del año 1996 al 2018
Fuente: (Corporacion Latinobarometro, 2018)

Como podemos observar en la figura 1, el informe muestra que la confianza en la democracia tiene un promedio del 6% comparativamente bajo con respecto a la desconfianza que entre los criterios de no muy satisfecho y nada satisfecho tiene un promedio de 62% en los años de estudio de presentación de los informes. Así mismo, en la figura número 2 se analiza la confianza en el organismo electoral. Esta institución tenia por nombre hasta el 2009 como Tribunal Supremo Electoral. Con la aprobación de la nueva Constitución y publicación en el número 449 del (Registro Oficial Ecuador, 2008) de fecha 20 de octubre del año 2008, la institución paso a llamarse Consejo Nacional Electoral del Ecuador como se establece en la

(Constitución de la República del Ecuador, 2008), en su artículo 217, nombre que lleva hasta el día de hoy. La grafica muestra estudios aplicados durante los años 2006, 2007, 2010, 2015, 2016, 2017 y 2018 en la cual se representa el nivel de confianza con respecto al organismo electoral, el parámetro **"Mucha confianza"** refleja un promedio del 4%, el parámetro **"Algo de confianza"** refleja un promedio del 22%, el parámetro **"Poca confianza"** refleja un promedio del 40%, y el parámetro **"Ninguna confianza"** refleja un promedio del 31%, demostrando una gran serie de inconvenientes al momento de organizar procesos electorales.

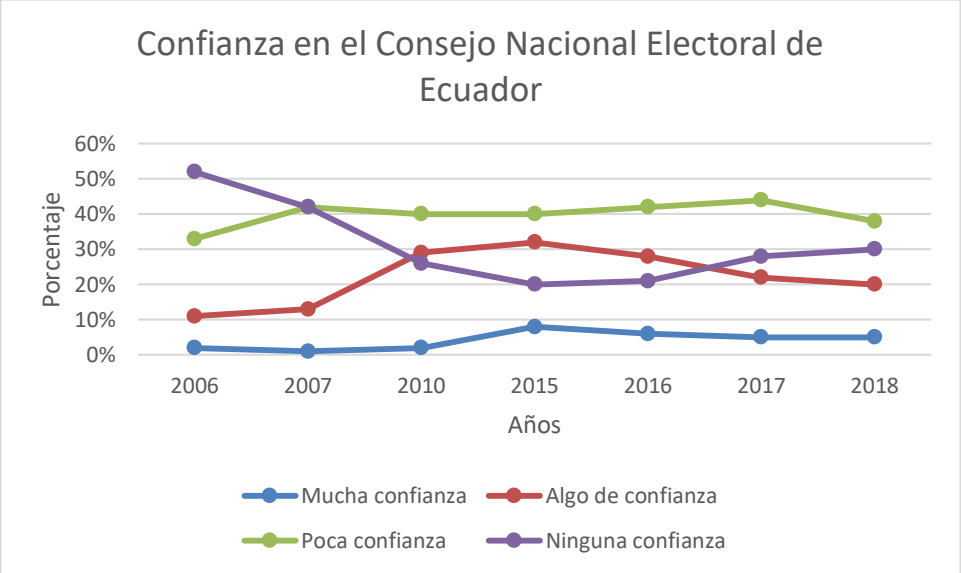


Figura 2: Confianza en el organismo electoral ecuatoriano
Fuente: (Corporacion Latinobarometro, 2018)

La información se ratifica en el año 2019 a través de un informe presentado por la empresa (Eureknow, 2009), empresa de análisis de mercados, quien publica un estudio referente al nivel de confianza del organismo electoral por parte de la ciudadanía, como se puede apreciar en la figura 3, se realiza un estudio sobre las instituciones públicas del Ecuador, en el cual la aceptación del Consejo Nacional Electoral es del 79% baja, 15% es regular y 6% es alta.

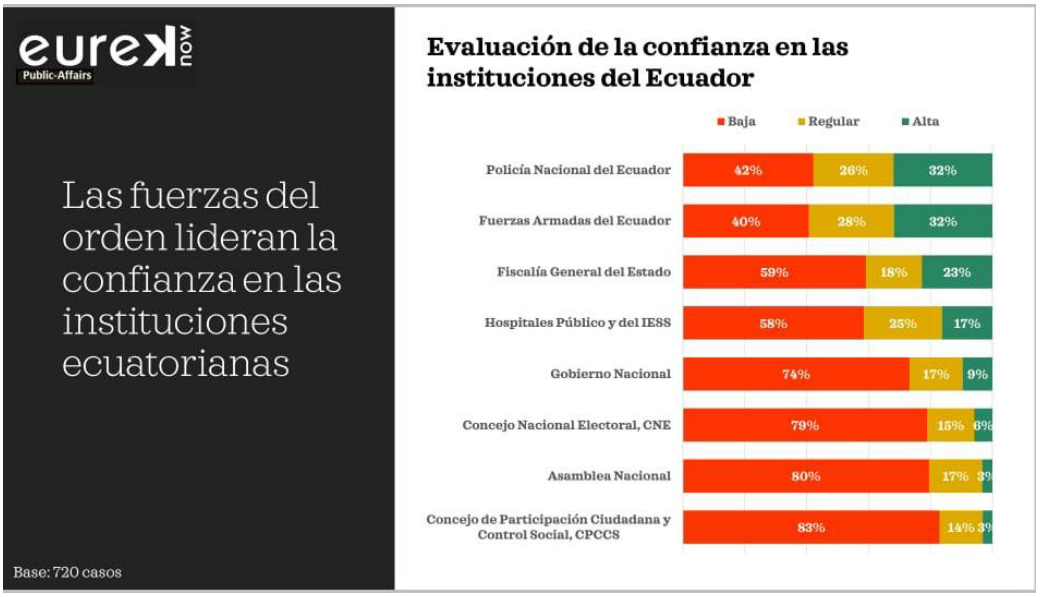


Figura 3: Evaluación de la confianza en las instituciones del Ecuador 2019
Fuente: (Eureknow, 2009)

Por su parte la empresa (CEDATOS, 2020), en el año 2020 presenta el análisis realizado a los ecuatorianos y ecuatorianas respecto al proceso electoral que debe organizar el CNE en el mes de febrero de 2021 en el que indica *"En una sola palabra, díganos: ¿Usted CONFÍA o NO CONFÍA en la gestión que realiza el Consejo Nacional Electoral para las elecciones del próximo año 2021?"*, los resultados de la figura 4 muestran los siguientes resultados: SI CONFÍA : 19%; NO CONFÍA: 81%.

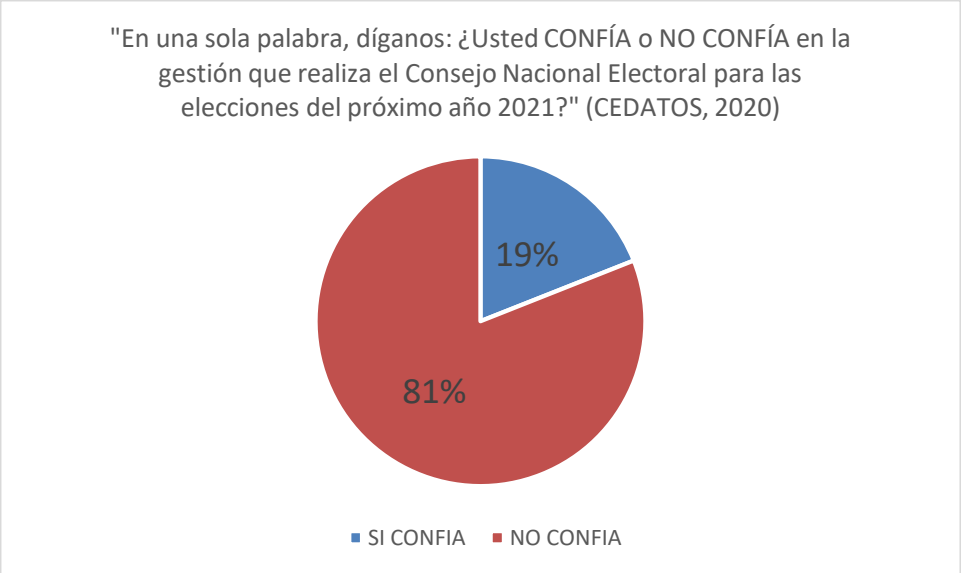


Figura 4: Confianza en el organismo electoral
Fuente: (CEDATOS, 2020)

En la misma encuesta de (CEDATOS, 2020) se pregunta *"Concretamente: ¿Usted CONFÍA o NO CONFÍA en la gestión de la Presidenta del Consejo Nacional Electoral, Diana Atamaint?"* ante lo cual los encuestados responden: SI CONFÍA, 15%; NO CONFÍA, 85% como se presenta en la información detallada de la figura 5.

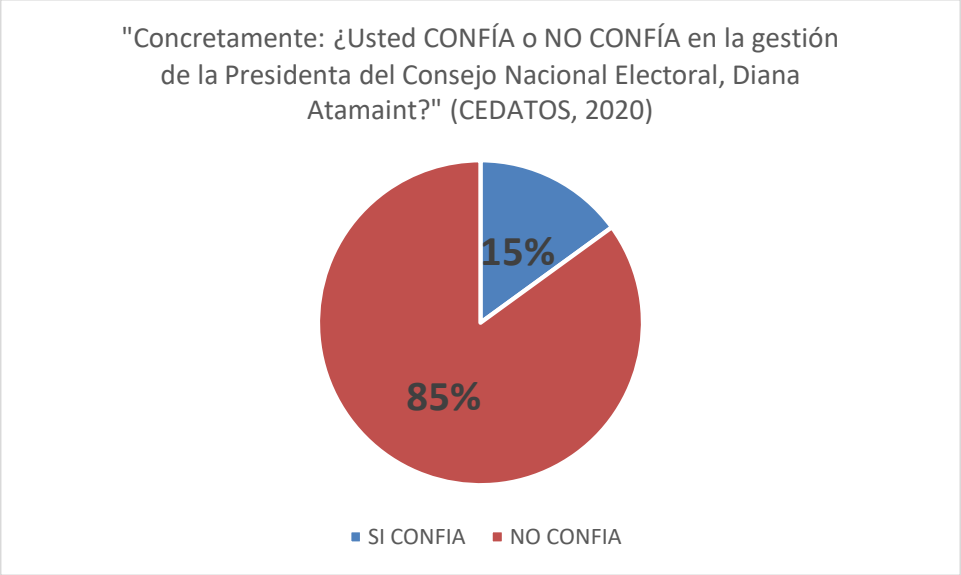


Figura 5: Confianza en la máxima autoridad del organismo electoral
Fuente: (CEDATOS, 2020)

Esta desconfianza hace que el cómputo de resultados con la implementación de las TIC, generen cuestionamientos en los actores electorales, quienes describiendo el principio de seguridad de seguridad de la información que **ningún sistema puede ofrecer una confiabilidad total de seguridad o "ningún sistema es seguro"** (Odar, 2014), concluyen que los sistemas creados para transmisión y publicación de resultado son fácilmente alterados, viciando así la transparencia del proceso electoral, ya que en alguna etapa de desarrollo o implementación del software, todo sistema puede verse comprometido. Estas variables hacen que el sistema informático se vea afectado, para lo cual el organismo electoral debe asegurar a los actores electorales una normativa o procedimiento enfocado en ciberseguridad o seguridad informática, en el que se establecen las normas claras de defensa de los sistemas; que concluyan en la confianza de la organización del proceso electoral.

I.I. Planteamiento del Problema

Entendiendo la realidad ecuatoriana en cuanto a la implementación de seguridad de la información planteamos la siguiente afirmación:

En Ecuador existe una deficiencia en la normativa legal relacionada con la seguridad informática y una desconfianza en los organismos electorales, ocasionando suspicacia respecto a vulnerabilidades en los sistemas informáticos utilizados para los procesos electorales.

En el campo de seguridad informática, el estado ecuatoriano en cuanto a normativa legal mantiene vigente el Código Orgánico Integral Penal (COIP) que juzga los comportamientos y acciones atípicas o antijurídicas que mediante el uso de las Tics se cometen en contra de la seguridad de la información. Además del COIP no existe norma jurídica que prevenga, mitigue o sancione las acciones realizadas por personas no autorizadas a los sistemas de información, por lo que es necesario que los organismos estatales o empresas privadas implementen metodologías o herramientas que garanticen la inviolabilidad de los sistemas informáticos implementados, como son los controles CIS o el anexo 1 de la norma ISO 27001. En ese campo un organismo electoral debe garantizar la transparencia de la información debe asegurarse mediante metodologías y herramientas que los resultados presentados son la decisión legitima del pueblo, evitando así la deslegitimación del proceso.

I.II. Estructura del trabajo

El presente trabajo busca la presentación de una metodología basado en el estudio de prácticas de seguridad informática y normas relacionadas que garanticen la calidad, que son aprobadas, implementadas y verificadas por las instituciones públicas y empresas privadas, que recoja los puntos relevantes que aporten en la transparencia de la información referente a los accesos de los sistemas informáticos que utiliza el organismo electoral del Ecuador y busque generar confianza en la sociedad en general. En un capítulo se describe el estado de arte de las metodologías y normas referentes a seguridad de la información como son los 20 controles CIS y el anexo 1 relacionado con los dominios y controles de la norma ISO 27001, así como las normas basadas en cuanto a la norma ISO 9001 relacionado con el Ciclo de Deming y la norma ISO/TS 17582 que se encuentra relacionada con la calidad en servicios electorales. Con la explicación realizada en el apartado relacionado con el estado del arte se procederá con la descripción de la metodología concebida en 4 etapas (Análisis, Planificación, Ejecución e Informe) que permite una retroalimentación para la realización del proceso de forma continua. Posteriormente se realizará la experimentación del trabajo a través accesos al sistema de escrutinio que implemento el organismo electoral del Ecuador vigentes a la fecha en concordancia con la implementación de la metodología detallada, para finalmente establecer las conclusiones y determinación de trabajos futuros a poder implementarse.

I.III. Hipótesis

Hipótesis Nula (H0)

Conociendo las mejores prácticas recomendadas y acogidas en las diferentes metodologías de calidad y de seguridad de la información que han implementado los diferentes organismos estatales o empresas privadas, podemos plantear que para generar confianza de la ciudadanía respecto a los organismos que tienen a cargo la organización de los procesos electorales podemos establecer como hipótesis nula que:

> Las Metodologías CIS e ISO 17582 son lo suficientemente seguras para los procesos electorales en cuanto al control de accesos autorizados que aseguren el ingreso sus sistemas.

Hipótesis Alternativa (HA)

Actualmente en el Ecuador no existe una cultura enfocada a la seguridad de la información, por lo que puede haber susceptibilidad referente a la implementación de las TIC en las etapas de escrutinio y presentación de resultados. Por lo tanto, se propone la siguiente hipótesis alternativa:

> La metodología de seguridad de la información para procesos electorales (MSIPE) es mejor para el control de accesos autorizados que las metodologías del Centro de Seguridad de la Información, *Center Information Security (CIS)* acrónimo en inglés y la Organización de Estandarización Internacional, *International Standarization Organization (ISO)* acrónimo en inglés, estándar ISO17582 en el Sistema Informático de Resultados Electorales.

Preguntas de investigación

1. ¿Puede una nueva metodología de seguridad informática mitigar el riesgo en procesos electorales que se realicen en el Ecuador?
2. ¿La nueva metodología de seguridad informática para procesos electorales (MSIPE) de Ecuador es mejor para a) garantizar el proceso de escrutinios y presentación de resultados de la norma ISO 17582, b) Mejorar los controles y sub controles en consideración con las mejores prácticas del *Center Information Security* (CIS) acrónimo en inglés de Centro de Seguridad de la Información?

I.IV. Objetivos

Objetivo General

Ofrecer una metodología de seguridad de la información que mitigue los riesgos de accesos no autorizados a través de su control en el sistema manejado en los procesos electorales que garantice la transparencia del sufragio durante el proceso electoral del Ecuador.

Objetivo Específico

1. Establecer la metodología de análisis de un proceso electoral mediante controles de acceso de la seguridad informática.
2. Evaluar la seguridad de la información del sistema utilizado en los escrutinios del organismo electoral de Ecuador.
3. Experimentar la metodología de seguridad informática aplicado al sistema informático aplicado en los procesos de escrutinios del organismo electoral de Ecuador y descripción de los resultados presentados.

Capítulo 1 - Estado del arte

Este capítulo realiza un análisis comparativo mediante indicadores del uso de las TIC en cuanto al nivel de utilización de estas tecnologías en las actividades diarias; la aceptación de una cultura de seguridad informática que mitigue los riesgos asociados al uso de las TIC; y, las acciones que toman los estados de Ecuador y España para que este uso no derive en acciones ilegales, así como son normadas con la descripción de los artículos descritos en los respectivos cuerpos legales una vez se realice el cometimiento de la infracción. Más adelante se realiza la descripción de las metodologías existentes como son los controles CIS de seguridad informática y una comparativa con el estándar ISO 27001 que son implementados por las empresas para mitigar los riesgos asociados con accesos no autorizados en empresas y sistemas o aplicaciones informáticas. De la misma manera se realiza una descripción de las normativas relacionadas con la calidad de los procesos como son ISO 9001 e ISO 17582 que determine los aspectos a ser considerados en la Metodología de seguridad informática para procesos electorales MSIPE. Finalmente se realiza la descripción de los tipos de acceso a sistemas informáticos y el sistema utilizado en el organismo ecuatoriano encargado de organizar, dirigir y vigilar el normal y correcto desarrollo de los procesos de elecciones que se realicen en el país.

1.1. Las Tecnologías de la Información y la Comunicación y aceptación de la Seguridad Informática en Ecuador

En la última década, el Ecuador ha registrado un aumento en el uso de las Tics, en todos los campos y eso se refleja en los estudios realizados y presentados en el portal web institucional del (Instituto Nacional de Estadísticas y Censos INEC - Ecuador, 2012 -2019), en la sucesiva figura 6 refleja el crecimiento en el acceso y uso de internet del 22.5% en el año 2012 al 45.5% en el año 2019, un crecimiento del 23% en 7 años, así como el uso de teléfonos inteligentes con conexión a internet del 6.2% en el año 2012 al 76.8% en el año 2019, reflejando un crecimiento del 70.6% en 7 años.

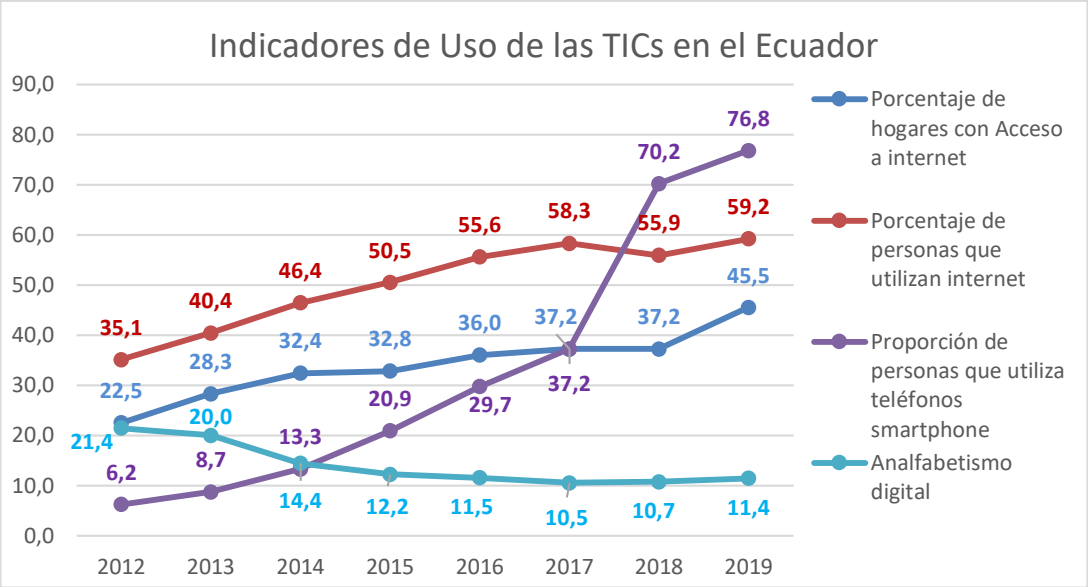


Figura 6: Equipamiento de las TIC en los hogares de Ecuador
Fuente: (Instituto Nacional de Estadísticas y Censos INEC - Ecuador, 2012 -2019)

Indicadores de Uso de las TIC en el Ecuador

	2012	2013	2014	2015	2016	2017	2018	2019
Porcentaje de hogares con Acceso a internet	22,5%	28,3%	32,4%	32,8%	36,0%	37,2%	37,2%	45,5%
Porcentaje de personas que utilizan internet	35,1%	40,4%	46,4%	50,5%	55,6%	58,3%	55,9%	59,2%
Proporción de personas que utiliza teléfonos Smartphone	6,2%	8,7%	13,3%	20,9%	29,7%	37,2%	70,2%	76,8%
Analfabetismo digital	21,4%	20,0%	14,4%	12,2%	11,5%	10,5%	10,7%	11,4%

Tabla 1: Aceptación e implementación de las TIC en el Ecuador
Fuente: (Instituto Nacional de Estadísticas y Censos INEC - Ecuador, 2012 -2019)

Este incremento se ve reflejado en las aplicaciones y beneficios que las organizaciones del estado y empresas privadas obtienen mediante el empleo de las TIC, los organismos encargados de organizar elecciones mediante el uso de estas herramientas, hoy en día existe gran cantidad de soluciones utilizadas en internet suplantando aquellas que se hacían de manera presencial como retirar dinero, inscripción o matriculación en centros educativos, clases presenciales, obtener un turno para atención médica, sin embargo ese crecimiento en el uso de las TIC no refleja con la cultura en seguridad de la información que debe tener el usuario con respecto a sus datos personales y a vulnerabilidades que están presentes en los sistemas de cómputo empleados.

Un informe publicado por la empresa (DELOITE, 2017), referente a un estudio en Seguridad de la Información en empresas ecuatorianas concluye en 4 puntos lo siguiente:

1. De las empresas analizadas en el año 2017, el 50% sufrió una brecha de seguridad y el 20% no pudo evaluar el impacto que causo la brecha ya que no cuentan con un procedimiento de gestión de incidentes.
2. El factor humano representa un punto de consideración importante referente a los riesgos y las vulnerabilidades que presentan los en cuanto a los ataques a sistemas informáticos, para lo cual es necesario la implementación de políticas de concienciación a los usuarios.
3. Las empresas no consideran los temas de seguridad informática un punto esencial, por lo que no se consideran el asignar presupuesto que salvaguarde los activos de información.
4. Las empresas en el Ecuador no cuentan con la experticia requerida para afrontar incidentes de seguridad

En cuanto a la cultura en seguridad informática que deben tener los ecuatorianos, existe muy poca experiencia o concienciación respecto a las seguridades que deben tener al momento de conectarse a internet o a la información que debe colocar en la misma creando excesiva confianza al momento de registro de información personal en infinidad de sitios web. Al existir inexperiencia a nivel estatal para la prevención y mitigación de problemas en seguridad es necesario realizar una revisión de la normativa legal y reglamentaria con el que cuenta el país a fin de realizar un análisis de las seguridades que deben existir en los sistemas informáticos relacionados con los procesos electorales, específicamente aquellos que realicen la presentación de resultados.

1.2. Análisis normativo con respecto de a las leyes aprobadas y vigentes respecto a Seguridad Informática en el territorio ecuatoriano.

Como ya se ha mencionado anteriormente, la seguridad informática es un tema no tomado muy en cuenta en el Ecuador, tanto a nivel ciudadano, empresarial o gobierno central, es así que el país sudamericano solo cuenta con una legislación que establece los procedimientos a ser aplicados en caso de cometimiento de un delito informático es decir solo para castigar el cometimiento del delito, mas no para la prevención del mismo, estas regulaciones son tomadas en consideración en el Código Orgánico Integral Penal. Adicionalmente como lo menciona el Reporte de Ciberseguridad 2020, publicado por el Observatorio de Ciberseguridad del (Banco Interamericano de Desarrollo, 2020), indica que el país no cuenta con una normativa concerniente a la resguardo de datos de carácter personal y asegure su privacidad, si bien esta información cuenta con protección a nivel constitucional en su artículo

66[1] en sus numerales 11 y 19 existe la protección en datos de carácter personal, sin embargo no se ha trabajado en una ley específica que establezca el procedimiento adecuado para la protección de este tipo de información.

1.2.1. Código Orgánico Integral Penal – COIP Ecuador

Este cuerpo normativo ecuatoriano fue publicado por el (Registro Oficial de Ecuador, 2017) posterior a la aprobación de la organismo de la Función Legislativa del Ecuador, establece los delitos y sanciones en las que se incurre por sus cometimientos, contiene un total de 730 artículos, incluyendo un total de 77 delitos no especificados en el Código Penal ecuatoriano derogado con la aprobación del COIP. Referente a delitos informáticos se encuentran tipificados 7 delitos, y delitos electorales el COIP tipifica 4. Los delitos informáticos contemplan los siguientes casos:

Clasificación del Delito Informático	Delito Informático	Descripción según COIP Ecuador	Promedio Sanciones
Delitos que atentan los principios de confidencialidad, integridad y disponibilidad de datos y sistemas informáticos	**Ingreso indebido.-** intrusión intencional e ilegal a un módulo o a todo el sistema informático.	**Art. 178.-** Violación a la intimidad	Privación de libertad de 1 a 3 años
		Art. 190.- Adjudicación fraudulenta de informaciones con la utilización de los diferentes medios electrónicos	Privación de libertad de 1 a 3 años
		Art. 229.- Revelación ilegal de información contenidas en bases de información (Data Base) DB	Privación de libertad de 1 a 3 años
		Art. 234.- Acceso no consentido no autorizado programas de computación o aplicaciones informáticas por vía telemática o de telecomunicaciones	Privación de libertad 3 a 5 años
	Interceptación ilícita.- apropiación intencionada e ilegítima de obtención de datos informáticos, transmisiones no públicas de información dirigidas a un sistema informático por medios técnicos, originadas en un programa o aplicación informática o efectuadas dentro del mismo	**Art. 178.-** Violación de intimidad	Privación de libertad de 1 a 3 años
		Art. 230, núm. 1.- apropiación ilegal e indebida de datos de carácter personal	Privación de libertad 3 a 5 años

[1] Art. 66, CRE: *"11. El derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica. (…)*
19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley."

Clasificación del Delito Informático	Delito Informático	Descripción según COIP Ecuador	Promedio Sanciones
	Ataques a la integridad de los datos.- acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.	**Art. 231.-** Transferencia de información mediante el uso de medios o dispositivos electrónicos	Privación de libertad 3 a 5 años
	Ataques a la integridad del sistema.- obstaculización grave, premeditada e ilegítima del normal funcionamiento de un programa o aplicación informática mediante el ingreso, transmisión, daño, borrado, deterioro, alteración, supresión o privación de datos informáticos	**Art. 232.-** Irrupción deliberada a la integridad de los programas de computación y aplicaciones informáticas	Privación de libertad 3 a 5 años
	Abuso de los dispositivos.- Desarrollo, venta y obtención de dispositivos adaptados con el fin de cometimiento de un delito informático, obtención de contraseñas o códigos de acceso que permitan en ingreso no autorizado a los sistemas, se sancionara la utilización, importación de estos dispositivos, así como distribución	**Art. 191.-** Reprogramación o modificación del software de fábrica o aplicaciones informáticas propias de equipos terminales móviles (Tablet, Smartphone)	Privación de libertad de 1 a 3 años
Delitos Informáticos	**Falsificación informática.-** Se sancionara actividades relacionadas con el Ingreso, modificación, borrado y eliminación intencional e indebida de datos almacenados en sistemas y aplicaciones informática, generando información falsificada con la intención de que sean tomados o utilizados a efectos legales como auténticos	**Art. 230, núm. 2-3-4 .-** Interceptación ilegal de datos	Privación de libertad 3 a 5 años
	Fraude informático. – Actividades ilegales que produzcan perjuicio personal a otros ciudadanos o usuarios del ciberespacio mediante el acceso, alteración, borrado o supresión de datos informáticos, así como la interferencia en el funcionamiento de un sistema informático	**Art. 178.-** Violación a la intimidad	Privación de libertad de 1 a 3 años
Delitos relacionados con el contenido	**Delitos relacionados con la pornografía infantil.** Producción, difusión, transmisión, adquisición, o posesión de material sexualmente explícito en el que	**Art. 173.-** Establecer contactos con personas menores de dieciocho años por medios electrónicos, buscando finalidades de explotación sexual	Privación de libertad 1 a 5 años

Clasificación del Delito Informático	Delito Informático	Descripción según COIP Ecuador	Promedio Sanciones
	se encuentren personas menores de 18 años en los que se utilicen sistemas informáticos	**Art. 174.-** Promoción y publicidad de servicios sexuales en la cual participen niñas, ni{os y jóvenes menores de los 18 años de edad mediante el uso de medios electrónicos, telemático e internet	Privación de libertad 7 a 10 años
Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	**Delitos relacionados con infracciones respecto al derecho de propiedad intelectual y afines**	No se especifica	No se especifica

Tabla 2: Descripción y análisis de los delitos relacionados con seguridad informática recopilados y tipificados en el COIP
Fuente: Propia en base a lo establecido en el COIP publicado en el **(Registro Oficial de Ecuador, 2017)** y Convenio sobre la Ciberdelincuencia publicado en el portal **(OEA, 2001)**

En lo que respecta a delitos electorales establece:

Delito	Descripción	Promedio Sanciones
Fraude electoral	1. Alteración de resultados de un proceso electoral, esto puede incluir alteración de bases de datos o sistemas de información	Reclusión 3 a 5 años

Tabla 3: Cuadro delitos electorales tipificados en el COIP publicado en el **(Registro Oficial de Ecuador, 2017)**
Fuente: Propia en base a los artículos del COIP

1.3. Las Tecnologías de la Información y la Comunicación y aceptación de la Seguridad Informática en España.

En el país ibérico el uso de las TIC es mucho más común que el caso ecuatoriano esto se muestra en la encuesta realizada, analizada y presentada por el (Instituto Nacional de Estadistica INE - España, 2012 - 2019) sobre la utilización de estas herramientas, el caso español visualiza que el 91,4% de los residencias españolas tiene conexión a internet, reflejando enormemente la diferencia respecto a Ecuador que cuenta con el 45.5% de acuerdo a lo determinado en tabla 1 presentado en el apartado 1.1 de este documento.

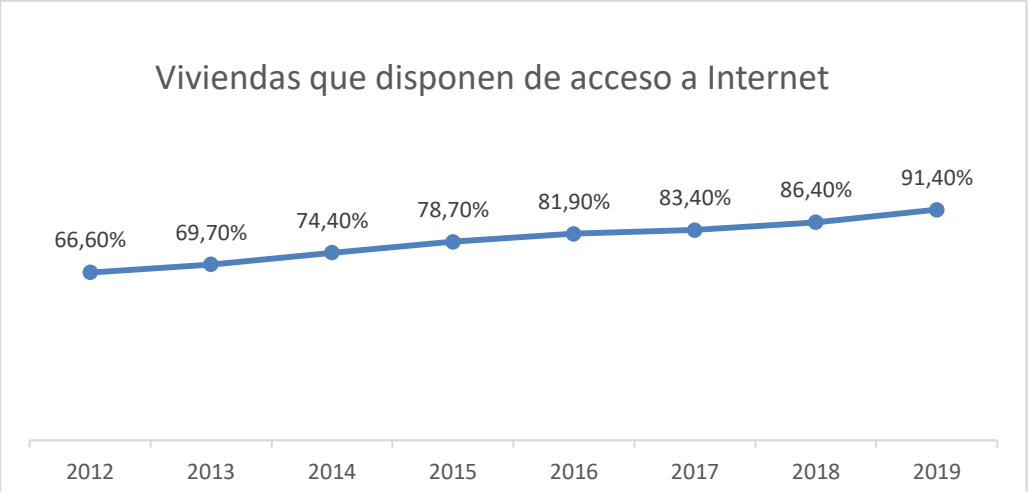


Figura 7: Equipamiento de las TIC en los hogares de España
Fuente: (Instituto Nacional de Estadistica INE - España, 2012 - 2019)

El incremento del uso del internet en el España refleja también el acrecentamiento en la concienciación sobre la seguridad que deben tener los usuarios el momento de navegar en internet, así como el número de ataques cibernéticos a los que el país debe preparase de forma constante. Un informe publicado por Google haciendo referencia al Panorama actual de la ciberseguridad en España en su apartado "Principales conclusiones sobre la ciberseguridad en España" (The Cocktail Analysis, 2019) concluye:

1. Existe un Incremento del número de ciberataques a nivel mundial en un 350% solo en un tiempo establecido entre los años 2018 y 2019.
2. La ciberseguridad es una disciplina que traspasa fronteras y requiere de una legislación transnacional, a fin de monitorear los ataques.
3. Las empresas están poco o nada protegidos por lo que en los próximos años se requiere la contratación de un número mayor de profesionales expertos en ciberseguridad.
4. La ciudadanía tiene conciencia en aplicación de normas de seguridad y eso refleja que el 75% de los encuestados afirma que es muy importante la ciberseguridad y 6 de cada 10 mantiene normas de protección.

1.4. Análisis normativo con respecto de a las leyes aprobadas y vigentes respecto a Seguridad Informática en el territorio español.

En España con respecto a la legislación que regula la ciberseguridad se encuentran las siguientes:

a. **Ley Orgánica 15/1999 aprobada el 13 de diciembre de 1999 relacionada con la Protección de Datos de Carácter Personal. –** Norma jurídica aprobada para

garantizar y salvaguardar la intimidad de los datos considerados de carácter personal de las ciudadanas y ciudadanos españoles, aplicando medidas de seguridad en los niveles alto, medio y bajo en relación a los archivos que cree cada institución con la información de carácter personal, para la creación de un archivo se debe contar con la aprobación de la Agencia de Protección de Datos.

b. **Ley 34/2002 aprobada el 11 de junio de 2002 relacionada con los servicios de la información y el comercio electrónico. –** Norma jurídica relacionada con los servicios relacionados con la contratación de bienes o servicios por medios electrónicos y/o telemáticos, en la cual se deba proporcionar información de carácter personal y toda contratación que derive por este medio tiene igual valor que el que se realice de manera presencial.

c. **Ley Orgánica 10/1995 aprobada el 23 de noviembre de 1995 relacionadas con los delitos informáticos tipificados en la Ley Orgánica Código Penal. -** sanciona los delitos cometidos mediante el uso de equipos o sistemas de información, si bien se adhieren al Convenio de sobre Ciberdelincuencia y se ratifican el 1 de octubre de 2010, la legislación española tipifica otros delitos que también los considera de importancia en la prevención de delitos informáticos.

Clasificación del Delito Informático	Delito Informático	Descripción según Código Penal Español	Promedio Sanciones
Delitos que atentan los principios de confidencialidad, integridad y disponibilidad de datos y sistemas informáticos	**Ingreso indebido.-** intrusión intencional e ilegal a un módulo o a todo el sistema informático.	**Art. 197.-** apropiación de información personal y difusión de la misma	Prisión de 1 a 5 años y multa de 12 a 24 meses
		Art. 197 bis.- 1 ingreso no consentido a programas y aplicaciones informáticas	Prisión 6 meses a 2 años
		Art. 199.- revelación de información confidencial o de carácter personal	Prisión 1 a 3 años y multa de 6 a 12 meses
		Art. 278. Apropiación de información de las empresas	Prisión de 2 a 5 años y multa de 12 a 24 meses
	Interceptación ilícita.- apropiación intencionada e ilegítima de obtención de datos informáticos, transmisiones no públicas de información dirigidas a un sistema informático por medios técnicos, originadas en un programa o aplicación informática o efectuadas dentro del mismo	**Art. 197 bis.- 2** intercepción de comunicaciones	Prisión 3 meses a 2 años o multa de 3 a 12 meses
		Art. 285 bis. Manejo de información inviolable y confidencial a la que tuviera acceso reservado personas que forman parte de los órganos de administración pública, y que son parte de la	Prisión de 6 meses a 4 años, multa de 12 a 24 meses e inhabilitación especial

Clasificación del Delito Informático	Delito Informático	Descripción según Código Penal Español	Promedio Sanciones
		gestión o supervisión de instituciones administren aquella información reservada	para el ejercicio de la profesión o actividad de 1 a 3 años
	Ataques a la integridad de los datos.- acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.	**Art. 285 bis.** Manejo de información inviolable y confidencial a la que tuviera acceso reservado personas que forman parte de los órganos de administración pública, y que son parte de la gestión o supervisión de instituciones administren aquella información reservada	Prisión de 6 meses a 4 años, multa de 12 a 24 meses
	Ataques a la integridad del sistema.- obstaculización grave, premeditada e ilegítima del normal funcionamiento de un programa o aplicación informática mediante el ingreso, transmisión, daño, borrado, deterioro, alteración, supresión o privación de datos informáticos	**Art. 199.-** revelación de información	Prisión uno a 3 años y multa de 6 a 12 meses
	Abuso de los dispositivos.- Desarrollo, venta y obtención de dispositivos adaptados con el fin de cometimiento de un delito informático, obtención de contraseñas o códigos de acceso que permitan en ingreso no autorizado a los sistemas, se sancionara la utilización, importación de estos dispositivos, así como distribución	**Art. 197 ter.-** adquisición o venta de dispositivos y/o contraseñas y medios de acceso a sistemas informáticos	Prisión 6 meses a 2 años o multa de 3 a 18 meses
		Art. 286.- alteración de equipos para cometimiento del delito	Prisión 6 meses a 2 años y multa de 6 a 24 meses
		Artículo 264 ter .facilitación de equipos o accesos para el cometimiento del delito	Prisión de 6 meses a 2 años o multa de 3 a 18 meses
Delitos Informáticos	**Falsificación informática.-** Se sancionara actividades relacionadas con el Ingreso, modificación, borrado y eliminación intencional e indebida de datos almacenados en sistemas y aplicaciones informática, generando información falsificada con la intención de que sean tomados o utilizados a efectos legales como auténticos	**Artículo 264.** Daño, alteración, borrado de información	Prisión de 6 meses a 3 años
		Artículo 264 bis. Quien entorpeciera o prohibiera el correcto funcionamiento de un programa o aplicación informática	Prisión de 6 meses a 3 años
	Fraude informático. – Actividades ilegales que produzcan perjuicio personal	**Art. 199.-** revelación de información	Prisión 1 a 3 años y multa

Clasificación del Delito Informático	Delito Informático	Descripción según Código Penal Español	Promedio Sanciones
	a otros ciudadanos o usuarios del ciberespacio mediante el acceso, alteración, borrado o supresión de datos informáticos, así como la interferencia en el funcionamiento de un sistema informático		de 6 a 12 meses
Delitos relacionados con el contenido	**Delitos relacionados con la pornografía infantil.** Producción, difusión, transmisión, adquisición, o posesión de material sexualmente explícito en el que se encuentren personas menores de 18 años en los que se utilicen sistemas informáticos	**Artículo 183 ter.** Uso de las tics para establecer contacto con personas menores de dieciséis años edad y se proponga concertar encuentros	Prisión 1 a 3 años y multa de 6 a 12 meses
		Artículo 189. Producción de material con contenido sexual en la que intervienen personas menores de edad	Prisión de 1 a 5 años
Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	**Delitos relacionados con infracciones respecto al derecho de propiedad intelectual y afines**	**Artículo 270.** Reproducción de material protegido por propiedad intelectual	Prisión de 6 meses a 4 años y multa de 12 a 24 meses

Tabla 4: Descripción y análisis de los delitos relacionados con seguridad informática recopilados y tipificados en la Ley Orgánica Código Penal español
Fuente: Elaboración propia en base a lo establecido en la Ley Orgánica Código Penal español publicada en el Boletín Oficial del Estado (Boletin Oficial del Estado, s.f.) y al Convenio sobre la Ciberdelincuencia publicado en el portal (OEA, 2001)

Como se ha podido identificar la legislación española con respecto a la legislación ecuatoriana regula de mejor manera los delitos informáticos identificados de acuerdo al Convenio de Ciberseguridad, por lo que es necesario que las organizaciones públicas y privadas en el Ecuador analicen herramientas, metodologías o las mejores prácticas que mitiguen los riesgos relacionados con la seguridad informática.

1.5. Controles de Seguridad

La seguridad de la información se crea para mantener los datos importantes de cualquier empresa, institución u organización almacenados de forma segura. La seguridad de la información debe brindar confiabilidad, disponibilidad y debe mantener la integridad de la información (Universitat de Barcelona, 2018). Para reducir la posibilidad de que los datos sean alterados o sustraídos se implementan métodos y controles. Existen dos tipos de controles, generales y de aplicaciones. Los controles generales establecen los lineamientos en el diseño y el uso de programas de computación, mientras que los controles de aplicación son específicos para cada aplicación y se restringe los permisos que la aplicación va a utilizar

(Ronquillo, 2014). La clasificación general de los controles en la seguridad de la información es:

a. **Controles Preventivos. -** Buscan reducción de ocurrencia de eventos que vulneren los sistemas informáticos

b. **Controles Correctivos. -** Una vez identificada la vulnerabilidad y esta ha sido explotada corrigen el error y se evalúa el riesgo

c. **Controles Disuasivos. -** Reducen la posibilidad de un ataque deliberado

1.6. Centro para la Seguridad de la Información (CIS) acrónimo ingles de *Center for Internet Security*

CIS es un organismo que identifica, desarrolla, valida, sostiene y promociona entre sus miembros, soluciones referentes a las mejores prácticas de defensa cibernética, y a la vez construye y lidera comunidades de instituciones y profesionales de TIC que consientan el desarrollo y la convivencia en ambientes de confianza en el ciberespacio. Este organismo que funciona desde el año 2000, establecida en la ciudad Nueva York en los Estados Unidos, no tiene interés económico por lo que sus documentos como *CIS Controls* y *CIS Benchmarks* pueden ser descargados de manera libre en su portal web. Los documentos son recopilaciones o recomendaciones de profesionales reconocidos por sus mejores prácticas en mitigación de riegos hacia los sistemas de seguridad para IT (tecnología de la información). Proveen directrices y estas son continuamente actualizadas por una comunidad global voluntaria de profesionales expertos en IT (Center for Internet Security, 2018). Los Controles CIS en conjunto agrupan sub controles específicos que detallan la forma de implantación y su medición respecto a los ataques cibernéticos que se presentan constantemente. Debido a ello estos controles evolucionan en su versión porque cuando se detecta nuevos ataques, lo que hace es el análisis de los mismos para generar las actualizaciones en los controles CIS para que puedan eliminar o mitigar riesgos relacionados con los ataques realizados en el ciberespacio (SANS, 2018).

1.6.1. Descripción de controles CIS V7.1.

Existen actualmente 20 controles CIS (Tripwire, 2018), se los describirá a continuación:

Controles Básicos:

1. **Control CIS 1: Custodiar un inventario y control de equipos informáticos (hardware). -** Realizar un control sobre los dispositivos que se encuentra en la red,

monitorearlos de forma continua para reducir los riesgos de un ataque. Usar DHCP para actualizar la lista de dispositivos conectados a la red.

2. **Control CIS 2: Custodiar un inventario y control de programas de computación (software). -** Utilizar software autorizado, es decir no utilizar software pirata, además de instalar una aplicación que permita hacer *" Whitelisting*" para garantizar que solo el software autorizado está siendo utilizado.
3. **Control CIS 3: Gestión de las vulnerabilidades de red. -** Realizar un análisis de red en intervalos regulares para buscar vulnerabilidades y corregirlas antes de que otras personas ajenas a la institución las descubra.
4. **Control CIS 4: Administración de los Privilegios Administrativos de los sistemas. -** Llevar un inventario detallado de las cuentas de administrador y cambiar las contraseñas por defecto.
5. **Control CIS 5: Establecimiento de configuraciones seguras para equipos informáticos (hardware) y programas de computación o aplicaciones móviles (software) instalados en terminales de conexión móvil (Tablet, Smartphone), equipos portátiles, equipos de escritorio y servidores instalados en la red. -** Utilizar un sistema de monitoreo integrado de archivos (FIM) el cual permite detectar si los datos han sido alterados de forma intencional o accidental.
6. **Control CIS 6: Administración y análisis respecto al mantenimiento, monitoreo y análisis de evidencias obtenidas mediante los registros de auditoría. -** Analizar los registros del sistema porque proporcionan información precisa de toda la actividad en la red.

Controles Fundacionales:

7. **Control CIS 7: Protecciones de correo electrónico y navegador web. -** Informar a las personas que tengan cuidado al abrir correos electrónicos de remitentes desconocidos, y al navegar por internet no abrir anuncios spam porque lo utilizan para realizar phishing y obtener datos para realizar un ataque cibernético.
8. **Control CIS 8: Defensas de malware. -** Verificar que las herramientas del antivirus no interfieran con el resto de herramientas de seguridad. Además, mantener registros precisos de las auditorías de línea de comandos y las consultas DNS.
9. **Control CIS 9: Administración y configuración correcta de puertos de red, protocolos y servicios levantados en la red. -** Realizar escaneo automático de puertos y activar los firewalls para proteger a las computadoras de posibles ataques.

10. **Control CIS 10: Capacidades de recuperación de datos. -** Realizar copias de seguridad de forma regular y automática para garantizar la recuperación de datos de manera correcta.
11. **Control CIS 11: Configuración segura para dispositivos de red, como cortafuegos, enrutadores y switch. –** Proteger mediante el establecimiento, la implementación y la gestión de los dispositivos conectados a la red a través de configuraciones que permita la autenticación segura y se implemente un cifrado de múltiples factores en todos los dispositivos que accedan a la red.
12. **Control CIS 12: Defensa de límites. -** Usar sensores IDS para la red y sistemas de prevención de intrusos.
13. **Control CIS 13: Protección de Datos. -** Realizar inventarios de la información confidencial y resguardarla con contraseñas y encriptar los datos.
14. **Control CIS 14: Acceso controlado basado en la necesidad de saber. -** Ejecutar encriptaciones de la información y deshabilitar la comunicación entre las estaciones de trabajo dentro de la red para limitar los posibles incidentes de seguridad.
15. **Control CIS 15: Control de acceso inalámbrico. -** Realizar un inventariar de los puntos de acceso de red inalámbricos.
16. **Control CIS 16: Control y monitoreo de la cuenta. -** Instalar un sistema que permita controlar los mecanismos de autenticación de las credenciales.

Controles Organizacionales:

17. **Control CIS 17: Formalizar un programa continuo de concientización e instrucción del personal de la organización en temas de seguridad informática. -** Realizar una capacitación continua en seguridad y riesgos asociados con la información como activo primordial de la organización a todos los empleados de la empresa.
18. **Control CIS 18: Procedimientos de pruebas de seguridad a programas informáticos (software) de la organización. -** Realizar evaluaciones de seguridad a través de procesos como análisis de seguridad estáticos y dinámicos para descubrir vulnerabilidades ocultas.
19. **Control CIS 19: Respuesta y manejo de incidentes de ciberseguridad. -** Implementar estrategias para planificar y evaluar los incidentes de seguridad cibernética.
20. **Control CIS 20: Pruebas de defensa contra ataques de penetración a los sistemas de la organización y ejercicios de hackeo ético conocidos como equipo rojo. -** Realizar pruebas de penetración en intervalos regulares para identificar

vulnerabilidades mediante simulaciones de equipos u organizaciones de cibercriminales que se encuentran en la red.

1.7. Estándar Internacional de Seguridad Informática basado en estándar ISO 27001:2013

Versión del año 2013 aprobada por la Organización Internacional de Estandarización ISO, acrónimo en inglés de *International Organization for Standarization*, aplicada en empresas que busquen una acreditación internacional en ejecución y administración de un Sistema de Gestión de Seguridad Informática SGSI, integra esta norma el conocido e implementado "Anexo A" que contiene la descripción de los controles a implementar (114 controles), agrupados en objetivos de control (35 objetivos) que forman parte de los dominios de la norma (14 dominios) analizados previo a su implementación, los dominios establecidos en secciones en el "Anexo A" que forman parte de la norma se describe a continuación:

1. **Sección A5: Determinar una política de seguridad informática. -** Establece requisitos relacionados con la creación, aprobación, implementación, evaluación y mejoramiento de políticas de seguridad que la organización requiera con respecto al cuidado de la información.
2. **Sección A6: Organización de la seguridad informática. -** Instaurar un grupo de criterios básicos que determinen el correcto funcionamiento de los actores, procesos, herramientas que intervienen en la organización.
3. **Sección A7: Requisitos relacionados con el antes, durante y finalización de la relación laboral con la organización. -** Establece criterios para la contratación, asignación de recursos, seguimiento y desvinculación del personal de la organización
4. **Sección A8**: **Gestión de activos. -** Establece criterios sobre responsabilidades, asignaciones, clasificación, manipulación y tratamiento de los activos de información de la organización.
5. **Sección A9: Control de acceso. -** Establece los requisitos para la administración de las credenciales de acceso a sistemas informáticos y aplicaciones que utiliza y mantiene la organización, a los que tienen acceso los usuarios.
6. **Sección A10: Métodos de Criptografía. -** Establece políticas de uso de medios criptográficos para la organización.
7. **Sección A11: Establecimiento de la seguridad física y entorno de trabajo. -** Establece criterios para entornos seguros y seguridad en los equipos informáticos de la organización.
8. **Sección A12: Seguridad en las operaciones que desarrolla TI. -** Asegura el correcto funcionamiento de los equipos

9. **Sección A13: Protección de la seguridad redes. –** gestiona de manera efectiva los servicios de red de comunicación e intercambio de comunicaciones de la organización en lo interno y externo
10. **Sección A14: Compra, desarrollo y mantenimiento de sistemas de la organización. -** Establece políticas seguras del software utilizado en la organización sea esta propia (desarrollada por la misma organización), o de terceros (adquirida a otras organizaciones).
11. **Sección A15: Relaciones con los proveedores. -** Implementa criterios para la seguridad en la entrega de la información a proveedores o personas que no tienen relación de trabajo directa con la organización, pero integran el proceso de desarrollo de productos y servicios con los que cuenta la organización.
12. **Sección A16: Administración de acontecimientos relacionados con la seguridad de la información. -** Controles de determinan el manejo oportuno y efectivo de incidentes de seguridad ocurridos en la organización.
13. **Sección A17: Aspectos que aseguren el mantenimiento de seguridad informática y permitan la correcta continuidad del negocio. -** Asegurar el correcto funcionamiento de la empresa ante cualquier fallo de seguridad.
14. **Sección A18: Cumplimiento. -** Asegurar la implementación correcta de las políticas de seguridad y de manera que garantice la madurez de implementación y evidente mejora continua.

1.8. Comparación de Controles entre CIS e ISO 27001

Como ya se ha explicado tanto CIS e ISO 27001 ponen en práctica controles que hacen factible la mitigación de riesgos de Seguridad de la Información, ante lo cual las organizaciones de acuerdo a su necesidad hacen posible la adaptación de cualquier modelo de acuerdo a su realidad, es así que varios sub controles establecidos en CIS se pueden verificar en los controles establecidos en ISO 27001, en la tabla 5 podemos apreciar un mapeo de controles proporcionado por (CIS, 2020).

CIS				ISO 27001	
Control		Sub control		Dominio	Control
1.	**1. Custodiar un inventario y control de equipos informáticos (hardware)**	**1.1**	Manejo de herramientas que permitan el descubrimiento de equipos informáticos conectados a la red	**A.8** Administración de los activos de hardware y software	**A.8.1.1** Levantamiento de un inventario de activos relacionados con el ciclo de vida de seguridad de información
		1.2	Manejo de herramientas que permitan el descubrimiento de	**A.8** Administración de los activos de	**A.8.1.1** Levantamiento de un inventario de

CIS				ISO 27001	
Control		Sub control		Dominio	Control
			equipos informáticos conectados a la red de forma pasiva	hardware y software	activos relacionados con el ciclo de vida de seguridad de información
		1.3	Manejo de logging para DHCP Logging que permita la actualización del inventario de equipos informáticos	**A.8** Administración de los activos de hardware y software	**A.8.1.1** Levantamiento de un inventario de activos relacionados con el ciclo de vida de seguridad de información
		1.4	Manejo de un inventario de equipos informáticos detallado	**A.8** Administración de los activos de hardware y software	**A.8.1.1** Levantamiento de un inventario de activos relacionados con el ciclo de vida de seguridad de información
		1.5	Gestionar el detalle de información respecto al catálogo o inventario de equipos informáticos	**A.8** Administración de los activos de hardware y software	**A.8.1.1** Levantamiento de un inventario de activos relacionados con el ciclo de vida de seguridad de información
		1.6	Gestionar el detalle de los equipos informáticos no autorizados en la red	**A.11** Establecimiento de la seguridad física y entorno de trabajo	**A.11.2.5** Control de los equipos respecto a la salida de la empresa
		1.7	Implementación de controles de acceso a nivel de puerto para evitar ingresos no autorizados	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
				A.9 Implementación de controles de los accesos de los usuarios	**A.9.1.2** Servicios que permitan el acceso a las redes y a los servicios asociados
		1.8	Utilizar certificados clientes que permitan la autenticación de los equipos informáticos hardware	**A.9** Implementación de controles de los accesos de los usuarios	**A.9.3.1** Aseguramiento de la no divulgación de la información secreta que permita la autenticación
				A.13 Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
2	**2. Custodiar un inventario y control de**	**2.1**	Mantener un inventario de programas de	**A.8** Administración de los activos de	**A.8.1.1** Levantamiento de un inventario de

CIS				ISO 27001	
Control		Sub control		Dominio	Control
	programas de computación (software)		computación (software) autorizado	hardware y software	activos relacionados con el ciclo de vida de seguridad de información
		2.2	Asegurarse que los programas de computación (software) cuenten con el soporte del fabricante	N/A	No se encuentra en la comparación
		2.3	Utilizar herramientas para el inventario de programas de computación (software)	N/A	No se encuentra en la comparación
		2.4	Rastrear información referente al inventario de los programas de computación (software)	**A.8** Administración de los activos de hardware y software	**A.8.1.1** Levantamiento de un inventario de activos relacionados con el ciclo de vida de seguridad de información
		2.5	Integrar un catálogo o inventarios de activos de equipos de computación (hardware) y programas de computación (software)	N/A	No se encuentra en la comparación
		2.6	Controlar los programas de computación (software) no aprobado	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.5.1** Instalación de los programas informáticos (software) operacional y aplicaciones
				A. 12 Seguridad en las operaciones que desarrolla TI	**A.12.6.2** Establecer políticas respecto a la prohibición de instalación de software por el usuario
		2.7	Implementar una lista blanca de uso de aplicaciones seguras	N/A	No se encuentra en la comparación
		2.8	Implementar lista blanca de uso de librerías	N/A	No se encuentra en la comparación
		2.9	Implementar lista blanca de uso de scripts	N/A	No se encuentra en la comparación
		2.10	Separar las aplicaciones que supongan un alto riesgo tanto a nivel físico como lógico	N/A	No se encuentra en la comparación

CIS				ISO 27001	
Control		Sub control		Dominio	Control
3	**3. Gestión de las vulnerabilidades de red**	**3.1**	Ejecutar herramientas de escaneo automatizados de vulnerabilidades	N/A	No se encuentra en la comparación
		3.2	Realizar análisis de vulnerabilidades autenticados	N/A	No se encuentra en la comparación
		3.3	Uso de cuentas específicas para escaneo de vulnerabilidades y auditorias de seguridad	N/A	No se encuentra en la comparación
		3.4	Manejo de herramientas que permitan la gestión automatizada de parches para los sistemas operativos	N/A	No se encuentra en la comparación
		3.5	Manejo de herramientas que realicen la gestión automatizada de parches de programas de computación (software)	N/A	No se encuentra en la comparación
		3.6	Comparar escaneos de vulnerabilidades consecutivos	N/A	No se encuentra en la comparación
		3.7	Utilizar un proceso de calificación de riesgo	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.6.1** Obtención de información de las vulnerabilidades relacionados con los sistemas
4	**4. Administración de los Privilegios Administrativos de los sistemas**	**4.1**	Mantener un inventario de cuentas administrativas	N/A	No se encuentra en la comparación
		4.2	Cambiar contraseñas por defecto	**A.9** Implementación de controles de los accesos de los usuarios	**A.9.4.3** Aplicar uso de credenciales que permitan la gestión efectivas de contraseñas
		4.3	Asegurar el uso de cuentas administrativas dedicadas	**A.9** Implementación de controles de los accesos de los usuarios	**A.9.4.3** Aplicar uso de credenciales que permitan la gestión efectivas de contraseñas
		4.4	Usar contraseñas únicas	**A.9** Implementación de controles de los accesos de los usuarios	**A.9.4.3** Aplicar uso de credenciales que permitan la gestión efectivas de contraseñas
		4.5	Usar autenticación multifactor para todo acceso administrativo	N/A	No se encuentra en la comparación
		4.6	Usar máquinas específicas que permitan la gestión de	N/A	No se encuentra en la comparación

CIS				ISO 27001	
Control		Sub control		Dominio	Control
			las tareas administrativas		
		4.7	Limitar el acceso a usuarios administrativos con herramientas de scripts	N/A	No se encuentra en la comparación
		4.8	Configuración de sistemas que registren y alerten los cambios de los miembros del grupo que tenga asignados privilegios administrativos	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.4.3** Registro, protección y revisión de las actividades realizadas por el administrador del sistema
		4.9	Manejo de los Registros y alertas sobre los inicios de sesión fallidos en cuentas administrativas	**A.9** Implementación de controles de los accesos de los usuarios	**A.9.4.2** Política para el control de acceso seguros de inicio de sesión a sistemas y aplicaciones
5	**5. Establecimiento de configuraciones seguras para equipos informáticos (hardware) y programas de computación o aplicaciones móviles (software) instalados en terminales de conexión móvil (Tablet, Smartphone), equipos portátiles, equipos de escritorio y servidores instalados en la red**	**5.1**	Establecer configuraciones seguras	**A.8** Administración de los activos de hardware y software	**A.8.1.3** Identificar, documentar e implementar los activos de hardware y software
				A.14 Compra, desarrollo y mantenimiento de sistemas de la organización	**A.14.2.5** Principios de ingeniería de sistemas seguros
		5.2	Mantener imágenes seguras	N/A	No se encuentra en la comparación
		5.3	Almacenar las imágenes maestras de forma segura	N/A	No se encuentra en la comparación
		5.4	Implementar herramientas de gestión de configuración de sistema	N/A	No se encuentra en la comparación
		5.5	Implementar sistemas de monitoreo automatizado de configuración	N/A	No se encuentra en la comparación
6	**6. Administración y análisis respecto al mantenimiento, monitoreo y análisis de evidencias obtenidas mediante los registros de auditoría**	**6.1**	Utilizar tres fuentes de tiempo sincronizadas	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.4.4** Sincronización del reloj
		6.2	Activar registros de auditoría	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.4.1** Registro, protección y revisión periódico de las eventos relacionados con los usuarios
		6.3	Habilitar registros detallados	N/A	No se encuentra en la comparación

CIS				ISO 27001	
Control		Sub control		Dominio	Control
		6.4	Asegurar almacenamiento adecuado para registros	N/A	No se encuentra en la comparación
		6.5	Gestión centralizada de registros	N/A	No se encuentra en la comparación
		6.6	Desplegar herramientas de Gestión de información de seguridad y eventos o de Análisis de registros	N/A	No se encuentra en la comparación
		6.7	Revisar regularmente los registros	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.4.3** Registro, protección y revisión de las actividades realizadas por el administrador del sistema
		6.8	Ajustar regularmente el Sistema de Gestión de información de seguridad y eventos	N/A	No se encuentra en la comparación
7	**7. Protecciones de correo electrónico y navegador web**	**7.1**	Asegurar que solo los navegadores web y clientes de correo electrónico que cuenten con el soporte	**A.8** Administración de los activos de hardware y software	**A.8.1.3** Identificar, documentar e implementar los activos de hardware y software
		7.2	Desinstalar o deshabilitar plugins no requeridos para las tareas de navegadores o clientes de correo electrónico	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.6.2** Establecer y administrar reglas que permitan la instalación de software
		7.3	Asegurar que solo los lenguajes de scripting habilitados en navegadores web y clientes de correo electrónico se ejecuten correctamente	N/A	No se encuentra en la comparación
		7.4	Mantener y aplicar filtros de URL que impidan la conexión a sitios web no utilizados	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		7.5	Suscribirse a servicios de categorización de URL	N/A	No se encuentra en la comparación
		7.6	Registrar todas las peticiones de URLs	N/A	No se encuentra en la comparación
		7.7	Utilizar servicios de filtrado DNS	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
				A. 12 Seguridad en las	**A.12.2.1** Controles de detección, prevención y

CIS				ISO 27001	
Control		Sub control		Dominio	Control
				operaciones que desarrolla TI	recuperación contra el código considerado malicioso
		7.8	Implementar políticas a los dominios Domain-based Message Authentication, Reporting and Conformance - DMARC y la verificación del lado del receptor	**A.13** Protección de la seguridad redes	**A.13.2.3** Mensajería electrónica
		7.9	Bloquear tipos de archivos innecesarios	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		7.10	Utilizar técnicas de cajas de arena para el análisis de loa archivos los adjuntos de correo electrónico	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.2.1** Controles de detección, prevención y recuperación contra el código considerado malicioso
8	**8. Defensas de malware**	**8.1**	Utilizar software antimalware de gestión centralizada	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.2.1** Controles de detección, prevención y recuperación contra el código considerado malicioso
		8.2	Asegurar que el software antimalware y las firmas de la organización se actualicen de forma periódica	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.2.1** Controles de detección, prevención y recuperación contra el código considerado malicioso
		8.3	Habilitar características anti- explotación de sistemas operativos / implementar tecnologías anti-explotación	N/A	No se encuentra en la comparación
		8.4	Configurar escaneo anti-malware de dispositivos removibles	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.2.1** Controles de detección, prevención y recuperación contra el código considerado malicioso
		8.5	Configurar equipos para no auto-ejecutar contenido	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.2.1** Controles de detección, prevención y recuperación contra el código considerado malicioso

CIS				ISO 27001	
Control		Sub control		Dominio	Control
		8.6	Centralizar los registros anti- malware	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.4.1** Registro, protección y revisión periódico de las eventos relacionados con los usuarios
				A. 12 Seguridad en las operaciones que desarrolla TI	**A.12.2.1** Controles de detección, prevención y recuperación contra el código considerado malicioso
		8.7	Habilitar registros de consultas DNS	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.4.1** Registro, protección y revisión periódico de las eventos relacionados con los usuarios
		8.8	Habilitar registros de auditoría de línea de comandos	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.4.1** Registro, protección y revisión periódico de las eventos relacionados con los usuarios
9	**9. Administración y configuración correcta de puertos de red, protocolos y servicios levantados en la red**	**9.1**	Asociación de puertos, servicios y protocolos activos al inventario de equipos de cómputo (hardware)	**A.13** Protección de la seguridad redes	**A.13.1.2** Identificar mecanismos de seguridad de acuerdo a los servicios de red
		9.2	Asegurar que en cada sistema solo se ejecuten puertos, protocolos y servicios aprobados	**A.13** Protección de la seguridad redes	**A.13.1.3** Gestión de servicios que permitan la segregación de redes grandes en sub redes
		9.3	Realizar regularmente escaneos automatizados de puertos	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		9.4	Implementación de cortafuegos basados en host o realizar filtrado de puertos	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		9.5	Implementación de cortafuegos de aplicación	N/A	No se encuentra en la comparación
10	**10. Capacidades de recuperación de datos**	**10.1**	Asegurar los respaldos regulares automatizados	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.3.1** Aseguramiento de respaldos de SI
		10.2	Asegurarse de respaldos completos en los sistemas operativos	N/A	No se encuentra en la comparación

CIS				ISO 27001	
Control		Sub control		Dominio	Control
		10.3	Asegurarse que medios de respaldo funcionan correctamente y la correcta integridad de la información	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.3.1** Aseguramiento de respaldos de SI
		10.4	Asegurar el correcto almacenamiento y protección de las copias de respaldo	N/A	No se encuentra en la comparación
		10.5	Asegurar que las respaldo de información tengan al menos un destino que no esté disponible	N/A	No se encuentra en la comparación
11	**11. Configuración segura para dispositivos de red, como cortafuegos, enrutadores y switch**	**11.1**	Administrar configuraciones de seguridad estandarizadas en equipos de red autorizados	N/A	No se encuentra en la comparación
		11.2	Documentar las reglas de configuración de tráfico	N/A	No se encuentra en la comparación
		11.3	Utilizar herramientas automatizadas para verificar configuraciones de equipos y detectar cambios	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.1.2** Procedimientos que permitan gestionar los cambios de la organización
		11.4	Instalación de versiones estables con las actualizaciones de seguridad en todos los equipos conectados en la red	N/A	No se encuentra en la comparación
		11.5	Gestión de equipos de red mediante autenticación multi-factor y sesiones cifradas	N/A	No se encuentra en la comparación
		11.6	Establecer máquinas dedicadas para la ejecución de las tareas administrativas en la red	N/A	No se encuentra en la comparación
		11.7	Administrar la infraestructura de red mediante conexiones de red dedicada	**A.13** Protección de la seguridad redes	**A.13.1.3** Gestión de servicios que permitan la segregación de redes grandes en sub redes
12	**12. Defensa de límites**	**12.1**	Mantener un inventario de las red perimetrales y DMZ	N/A	No se encuentra en la comparación
		12.2	Escaneo de conexiones no autorizadas en las	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes

CIS				ISO 27001	
Control		Sub control		Dominio	Control
			redes perimetrales o DMZ confiables		
		12.3	Denegar comunicaciones con direcciones IPs maliciosas conocidas	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		12.4	Denegar comunicaciones sobre puertos no autorizados	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		12.5	Configurar sistemas de monitoreo para registro paquetes que se transfieran a través de redes perimetrales	N/A	No se encuentra en la comparación
		12.6	Desplegar sensores IDS basados en red	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		12.7	Desplegar IPS basado en red	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		12.8	Desplegar colectores de trafico de red en equipos conectados a las redes perimetrales	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		12.9	Desplegar servidor proxy de filtrado de capa de aplicación	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		12.10	Análisis del tráfico que pasa por la red a través del proxy	N/A	No se encuentra en la comparación
		12.11	Requerir autenticación de tipo multi-factor en los inicios de sesión de forma remota	**A.9** Implementación de controles de los accesos de los usuarios	**A.9.4.2** Política para el control de acceso seguros de inicio de sesión a sistemas y aplicaciones
		12.12	Administración de los dispositivos que se conectan a la red interna de manera remota	**A.9** Implementación de controles de los accesos de los usuarios	**A.9.4.2** Política para el control de acceso seguros de inicio de sesión a sistemas y aplicaciones
13	**13. Protección de Datos**	**13.1**	Levantar y administrar un inventario con la información catalogada como sensible	**A.8 Administración de los activos de hardware y software**	**A.8.2.1** Clasificación de la importancia de la información
		13.2	Eliminación de datos o sistemas catalogados como sensibles con bajo nivel de acceso en la organización	N/A	No se encuentra en la comparación
		13.3	Monitoreo y bloqueo automatizado de tráfico no autorizado en la red	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes

CIS				ISO 27001	
Control		Sub control		Dominio	Control
		13.4	Establecer controles que permitan el acceso de proveedores de servicios de nube o correo autorizados	**A.13** Protección de la seguridad redes	**A.13.2.3** Mensajería electrónica
		13.5	Monitoreo y detección de cualquier uso no autorizado de cifrado de información	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		13.6	Cifrado de discos duros y de dispositivos móviles	**A.6** Organización de la seguridad de la información	**A.6.2.1** Política de dispositivos móviles
		13.7	Gestión de los dispositivos USB	**A.8** Administración de los activos de hardware y software	**A.8.3.1** Administración de medios de soporte extraíbles
		13.8	Administración de configuraciones lectura/escritura medios removibles externos en los sistemas informáticos	**A.8** Administración de los activos de hardware y software	**A.8.3.1** Administración de medios de soporte extraíbles
		13.9	Cifrar los datos en dispositivos de almacenamiento USB	**A.10** Métodos de Criptografía	**A.10.1.1** Política de manejo e implementación de medios criptográficos
14	**14. Acceso controlado basado en la necesidad de saber**	**14.1**	Segmentación de la red basado el nivel de sensibilidad de la información	**A.13** Protección de la seguridad redes	**A.13.1.3** Gestión de servicios que permitan la segregación de redes grandes en sub redes
		14.2	Habilitar filtrado de paquetes entre los cortafuegos de las redes virtuales	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		14.3	Deshabilitar comunicaciones entre estaciones de trabajo	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		14.4	Cifrar toda la información sensible que se transmite a través de la red	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
				A.10 Métodos de Criptografía	**A.10.1.1** Política de manejo e implementación de medios criptográficos
		14.5	Utilización de herramientas que permitan identificar los datos sensibles	N/A	No se encuentra en la comparación
		14.6	Proteger los datos almacenados de los	**A.9** Implementación de controles de	**A.9.1.1** Documentación y revisión de política

CIS				ISO 27001	
Control		Sub control		Dominio	Control
			sistemas mediante lista de control de acceso	los accesos de los usuarios	que administren los controles de acceso
		14.7	Aplicar controles de acceso a los datos mediante el uso de herramientas automatizadas que evite la perdida de datos Data Loss Prevention - DLP	N/A	No se encuentra en la comparación
		14.8	Cifrar información sensible	**A.10** Métodos de Criptografía	**A.10.1.1** Política de manejo e implementación de medios criptográficos
		14.9	Implementar un registro detallado de accesos o cambios en la información sensible del sistema	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.4.3** Registro, protección y revisión de las actividades realizadas por el administrador del sistema
15	**15. Control de acceso inalámbrico**	**15.1**	Gestionar el inventario con los puntos de acceso inalámbrico que se encuentran autorizados	**A.8** Administración de los activos de hardware y software	**A.8.1.1** Levantamiento de un inventario de activos relacionados con el ciclo de vida de seguridad de información
		15.2	Configuración de herramientas que explore vulnerabilidades en puntos de acceso inalámbricos conectados a la red	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		15.3	Uso de sistema inalámbrico de detección de intrusos a través de puntos de acceso inalámbricos conectados a la red cableada	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		15.4	Deshabilitar el acceso inalámbrico en dispositivos requieran conexión en la red	**A.8** Administración de los activos de hardware y software	**A.8.1.3** Identificar, documentar e implementar los activos de hardware y software
		15.5	Limitar el acceso de dispositivos a través de la red inalámbrico	**A.8** Administración de los activos de hardware y software	**A.8.1.3** Identificar, documentar e implementar los activos de hardware y software

CIS				ISO 27001	
Control		Sub control		Dominio	Control
		15.6	Inhabilitar las configuraciones establecidas en la red inalámbrica punto a punto de los clientes conectados	**A.8** Administración de los activos de hardware y software	**A.8.1.3** Identificar, documentar e implementar los activos de hardware y software
		15.7	Usar estándares de cifrado avanzado (AES) para cifrar datos de dispositivos conectados en redes inalámbricas	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
				A.10 Métodos de Criptografía	**A.10.1.1** Política de manejo e implementación de medios criptográficos
		15.8	Usar protocolos de autenticación en redes inalámbricas que al momento de conexión requieran autenticación multi-factor	**A.13** Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		15.9	Deshabilitar el acceso periférico inalámbrico de dispositivos	**A.8 Administración de los activos de hardware y software**	**A.8.1.3** Identificar, documentar e implementar los activos de hardware y software
		15.10	Creación de redes inalámbricas separadas de dispositivos confiables y no confiables	**A.13** Protección de la seguridad redes	**A.13.1.3** Gestión de servicios que permitan la segregación de redes grandes en sub redes
16	**16. Control y monitoreo de la cuenta**	**16.1**	Mantener un inventario de sistemas de autenticación	**A.8** Administración de los activos de hardware y software	**A.8.1.1** Levantamiento de un inventario de activos relacionados con el ciclo de vida de seguridad de información
		16.2	Configurar un punto de autenticación centralizado	N/A	No se encuentra en la comparación
		16.3	Requerir Autenticación Multi- factor	N/A	No se encuentra en la comparación
		16.4	Utilizar un cifrado o códigos hash en los métodos y herramientas de autenticación	**A.10** Métodos de Criptografía	**A.10.1.1** Política de manejo e implementación de medios criptográficos
		16.5	Cifrado en la transferencia de datos que permitan la autenticación	**A.10** Métodos de Criptografía	**A.10.1.1** Política de manejo e implementación de medios criptográficos

CIS				ISO 27001	
Control		Sub control		Dominio	Control
				A.13 Protección de la seguridad redes	**A.13.1.1** Gestión y Control de redes
		16.6	Mantenimiento de un inventario de cuentas de usuario creados y modificados	**A.9** Implementación de controles de los accesos de los usuarios	**A.9.2.1** Control y administración del registro y la baja de los usuario
		16.7	Establecer un proceso para revocar el acceso a los usuarios dados de baja	**A.9** Implementación de controles de los accesos de los usuarios	**A.9.2.6** Revisión de permisos para el retiro o la reasignación de los accesos
		16.8	Deshabilitar cuentas no asociadas con el proceso de negocio	N/A	No se encuentra en la comparación
		16.9	Deshabilitar todas las cuentas inactivas en el proceso	N/A	No se encuentra en la comparación
		16.10	Programar o implementar métodos con fecha de caducidad de las cuentas	N/A	No se encuentra en la comparación
		16.11	Bloqueo automático de sesiones en la estaciones de después de un tiempo de inactividad	**A.8** Administración de los activos de hardware y software	**A.8.1.3** Identificar, documentar e implementar los activos de hardware y software
		16.12	Monitoreo de accesos no autorizados a través de cuentas desactivadas	N/A	No se encuentra en la comparación
		16.13	Monitoreo y Alerta de comportamiento no asociados con el inicio de sesión de cuentas	N/A	No se encuentra en la comparación
17	**17. Formalizar un programa continuo de concientización e instrucción del personal de la organización en temas de seguridad informática**	**17.1**	Realizar un análisis de brecha de habilidades	N/A	No se encuentra en la comparación
		17.2	Implementar programas de capacitación para cubrir la deficiencia de habilidades del personal	**A.7** Requisitos relacionados con el antes, durante y finalización de la relación laboral con la organización	**A.7.2.2** Concienciación, educación y capacitación en seguridad informática
		17.3	Implementar un programa de concienciación de seguridad	**A.7** Requisitos relacionados con el antes, durante y finalización de la relación laboral con la organización	**A.7.2.2** Concienciación, educación y capacitación en seguridad informática
		17.4	Actualice el contenido de concienciación con frecuencia	**A.7** Requisitos relacionados con el antes, durante	**A.7.2.2** Concienciación, educación y

CIS				ISO 27001	
Control		Sub control		Dominio	Control
				y finalización de la relación laboral con la organización	capacitación en seguridad informática
		17.5	Capacitación sobre la implementación de autenticación segura	**A.7** Requisitos relacionados con el antes, durante y finalización de la relación laboral con la organización	**A.7.2.2** Concienciación, educación y capacitación en seguridad informática
		17.6	Capacitar referente a los ataques de ingeniería social	**A.7** Requisitos relacionados con el antes, durante y finalización de la relación laboral con la organización	**A.7.2.2** Concienciación, educación y capacitación en seguridad informática
		17.7	Capacitar sobre el manejo de información catalogada como sensibles	**A.7** Requisitos relacionados con el antes, durante y finalización de la relación laboral con la organización	**A.7.2.2** Concienciación, educación y capacitación en seguridad informática
		17.8	Capacitación en temas de exposición involuntaria de datos	**A.7** Requisitos relacionados con el antes, durante y finalización de la relación laboral con la organización	**A.7.2.2** Concienciación, educación y capacitación en seguridad informática
		17.9	Capacitación de identificación y reporte de incidentes	**A.7** Requisitos relacionados con el antes, durante y finalización de la relación laboral con la organización	**A.7.2.2** Concienciación, educación y capacitación en seguridad informática
18	**18. Procedimientos de pruebas de seguridad a programas informáticos (software) de la organización**	**18.1**	Establecer prácticas seguras de codificación	**A.14** Compra, desarrollo y mantenimiento de sistemas de la organización	**A.14.2.1** Política para el desarrollo seguro se sistemas
		18.2	Documentación en la verificación de errores con relacional software desarrollado internamente en la organización	N/A	No se encuentra en la comparación
		18.3	Verificar del tiempo de soporte del software adquirido	N/A	No se encuentra en la comparación
		18.4	Verificación que los componentes adquiridos a terceros	N/A	No se encuentra en la comparación

CIS				ISO 27001	
Control		Sub control		Dominio	Control
			tienen actualización y son de confianza		
		18.5	Algoritmos que permita el cifrado sean revisados y estén estandarizados	**A.10** Métodos de Criptografía	**A.10.1.**1 Política de manejo e implementación de medios criptográficos
		18.6	Capacitación en programación segura al personal de desarrollo de software	N/A	No se encuentra en la comparación
		18.7	Implementación de herramientas que permita el análisis de código de forma estática y forma dinámica	N/A	No se encuentra en la comparación
		18.8	Gestionar procesos de aceptación y tratamiento de reportes de vulnerabilidades del software	N/A	No se encuentra en la comparación
		18.9	Separación de ambientes de desarrollo y producción	**A. 12** Seguridad en las operaciones que desarrolla TI	**A.12.1.4** Reducción de riesgos de acceso no autorizado mediante la separación de los recursos de desarrollo, prueba y operación
		18.10	Implementación de cortafuegos de aplicación basados en Web (WAFs)	N/A	No se encuentra en la comparación
		18.11	Configuración de hardening para bases de datos	N/A	No se encuentra en la comparación
19	**19. Respuesta y manejo de incidentes de ciberseguridad**	**19.1**	Documentación de los procedimientos de respuestas a incidentes de seguridad	**A.16** Administración de acontecimientos relacionados con la seguridad de la información	**A.16.1.1** Establecimiento de respuesta rápida para las responsabilidades y los procedimientos
		19.2	Asignación de cargos y responsabilidades de los usuarios para la respuesta a incidentes	N/A	No se encuentra en la comparación
		19.3	Designación del personal de apoyo en el manejo de incidentes	N/A	No se encuentra en la comparación
		19.4	Implementar modelos de reporte de incidentes para la organización	**A.16** Administración de acontecimientos	**A.16.1.3** Comunicación de los incidentes respecto a los

CIS				ISO 27001	
Control		Sub control		Dominio	Control
				relacionados con la seguridad de la información	puntos débiles de la seguridad
		19.5	Establecer y mantener contactos de respuesta a incidentes de seguridad	**A.6** Organización de la seguridad de la información	**A.6.1.3** Mecanismos de contacto con alta gerencia
		19.6	Publicación de información relacionada con los incidentes en seguridad de la información	N/A	No se encuentra en la comparación
		19.7	Manejar escenarios para la gestión de los incidentes de seguridad	N/A	No se encuentra en la comparación
		19.8	Creación de esquema que prioricen los incidentes	N/A	No se encuentra en la comparación
20	**20. Pruebas de defensa contra ataques de penetración a los sistemas de la organización y ejercicios de hackeo ético conocidos como equipo rojo**	**20.1**	Establecer un programa de prueba de penetración	N/A	No se encuentra en la comparación
		20.2	Llevar a cabo pruebas periódicas de penetración externa e interna	N/A	No se encuentra en la comparación
		20.3	Realizar Ejercicios Periódicos del Equipo Rojo	N/A	No se encuentra en la comparación
		20.4	Incluir pruebas que verifiquen la existencia de información y artefactos no protegidos de sistema	N/A	No se encuentra en la comparación
		20.5	Creación de bancos de pruebas de elementos en ambiente de producción	N/A	No se encuentra en la comparación
		20.6	Uso de herramientas de penetración y exploración de vulnerabilidades	N/A	No se encuentra en la comparación
		20.7	Documentar resultados de la prueba de penetración	N/A	No se encuentra en la comparación
		20.8	Controlar y monitorear las cuentas asociadas con las pruebas de penetración	N/A	No se encuentra en la comparación

Tabla 5: Mapeo de controles entre CIS e ISO 27001
Fuente: (CIS, 2019)

1.9. Estándar de Calidad ISO 9001

La norma ISO 9001 en el levantamiento de procesos que garanticen una cadena efectiva de desarrollo de productos y servicios mediante el cumplimiento de estándares que ofrece a fin

de que el cliente se mantenga satisfecho, no es exclusiva para un sector que preste determinados servicios, pudiéndose aplicar en cualquier sector (Normas9000, 2018). Al ser la ISO una institución no gubernamental no puede exigir el cumplimiento de sus normas, pero los clientes o consumidores prefieren una institución que cuente con esta certificación porque de esa manera se aseguran que tiene la garantía que cumplen procedimientos de calidad con el apoyo del SGC. Según (Martínez, 2015) existen beneficios con la aplicación de esta Norma en su versión ISO 9001:2015 que son:

a. La capacidad de satisfacción al cliente, así como el cumplimiento de requisitos legales y reglamentarios exigidos en cada sector con la entrega de productos y servicios;
b. Evaluación y mejora de procesos que permitan aumentar el grado de satisfacción de los clientes;
c. Evalúa riesgos y coyunturas que pueden ser mejoradas en el contexto y objetivos;
d. La capacidad de demostrar la conformidad con requisitos establecidos en el SGC especificados

Esta norma se enfoca en el levantamiento de actividades mediante las etapas Planificar, Hacer, Verificar, Actuar (PHVA), además del pensamiento basado en riesgos. EL ciclo PHVA permite a la institución, organización o empresa que esté aplicando esta norma asegurarse de que sus procesos tengan los recursos necesarios y la gestión de los mismos sea la adecuada (Martínez, 2015).

Figura 8: Ciclo de implementación de mejora continua propuesta en Deming (Planear, Hacer, Actuar y Verificar)
Fuente: (ALPHA, 2017)

El pensamiento basado en riesgos permite alcanzar los resultados deseados, identificando los posibles problemas que puedan presentarse en los procesos y en el SGC, además de ejecutar procedimientos preventivos minimizando la aparición de estos posibles problemas (Martínez, 2015).

1.10. Estándar de Calidad ISO/TS 17582

La norma ISO/TS 17582 fue creada específicamente para el Sistema de Gestiona de Calidad en procesos electorales. A diferencia de la norma ISO 9001 que se puede aplicar en cualquier sector, la ISO/TS 17582 es para un sector en específico (ISOTools, 2018). Ambas normativas buscan el proveer un servicio de calidad y busca la satisfacción de los clientes. La norma se enfoca en 8 puntos importantes en el proceso electoral (OEA, 2020):

1. **Registro de los votantes. –** Levantar y evaluar procedimientos que identifiquen a las ciudadanas y ciudadanos que de acuerdo a la constitución y leyes se encuentren habilitados para votar.
2. **Levantamiento y mantenimiento de información de las organizaciones políticas y de los candidatos. –** Levantar y evaluar procedimientos que registren y mantengan la información y documentación de las organizaciones políticas y candidaturas en el organismo a cargo de la gestión electoral
3. **Logística electoral. -** Levantar los procedimientos que administren el armado y despacho de los materiales electorales en cada uno de los puntos de recepción del sufragio.
4. **Sufragio. -** Establecer los procedimientos que hagan efectivo el derecho al sufragio en los votantes habilitados para hacerlo.
5. **Escrutinio y declaración de los resultados. -** Definir los procedimientos para el escrutinio de los votos en los puntos de votación, cómputo y presentación de los resultados, se establece como el parte medular del proceso en el cual se mide el éxito del proceso electoral.
6. **Educación electoral. -** Establecer los procedimientos y métricas en los que se implementen diferentes medios de capacitación a los diferentes actores electorales.
7. **Fiscalización del financiamiento político. -** Establecer los procedimientos para el control del financiamiento utilizado por las organizaciones políticas (partidos y movimientos) durante la campaña electoral.
8. **Resolución de disputas electorales. -** Definir los procedimientos que permitan la resolución de inconformidades en los resultados electorales, así como la asignación de los escaños que le corresponda según la votación obtenida en la jornada electoral.

Al igual que todas las normas ISO, la aplicación de la norma ISO/TS 17582 es voluntaria, se pueden implementar infinidad de procesos, pero es indispensable que el organismo electoral visualice los procedimientos para los 8 procesos descritos con anterioridad. La implementación de la norma ISO/TS 17582 busca que los organismos electorales brinden

mayor confianza y los votantes, ya que garantiza que los procesos son realizados con calidad, sin embargo, no se implementa una norma relacionada con la seguridad de la información.

1.11. Certificación de las instituciones electorales

Los organismos electorales con la finalidad de ofrecer confianza en los electores buscan la implementación de normas de calidad, que permitan garantizar la transparencia en las actividades relacionadas con el procesos electorales, de acuerdo a la tesis presentada por (Basantes, 2017) el tabla 6 presenta una lista de organismos electorales que han implementado normas de calidad.

País	Organismo Electoral	Norma	Alcance
México	Comisión Estatal Electoral Nuevo León	ISO 9001:2008	1. Planificación, alta dirección, organización, vigilancia y ejecución de los procesos electorales. 2. Educación en valores democráticos. 3. Sistema de privilegios y la fiscalización de actividades a partidos políticos
Panamá	Tribunal Electoral de Panamá	ISO 9001:2008	1. Diseño y Gestión del Soporte y Tecnología Informática 2. Servicios asociados con el Registro Civil, servicios de cedulación, Residencia Electoral. 3. Organización Electoral: Servicios Administrativos Electorales, 4. Registros de Adherentes a Partidos Políticos, 5. Levantamiento de cartografía electoral 6. Distribución de Centros de Votación
México	Tribunal Electoral del Poder Judicial de la Federación	ISO 9001:2008	1. Recepción y trámite de impugnaciones a requerimientos electorales
México	Tribunal Electoral del Poder Judicial de la Federación	ISO 9001:2008	1. Atención y trámite de impugnaciones órgano electoral de carácter superior
Perú	Jurado Nacional de Elecciones de Perú	ISO 9001:2008 ISO 27001:2013	1. Atención al ciudadano, formación cívica ciudadana 2. Registro de organizaciones políticas. 3. Proceso de aprovisionamiento de material electoral 4. Talento Humano 5. Seguridad de la información
Costa Rica	Tribunal Supremo de Elecciones	ISO 9001:2008	1. Emisión de padrón nacional electoral. 2. Registro Civil
República Dominicana	Junta Central Electoral de la República Dominicana	ISO 9001:2008 e ISO/TS 17582:2014	1. Registro Electoral y Cedulación 2. Legalización de Partidos Políticos 3. Aprovisionamiento de material electoral 4. Proceso de Votación; Escrutinio y Emisión de Boletines 5. Asignación de Fondo Económico a los Partidos

País	Organismo Electoral	Norma	Alcance
			por parte del estado 6. Fiscalización del Gastos realizado por los Partidos
Ecuador	Consejo Nacional Electoral	ISO/TS 17582:2014 ISO 9001:2008	1. Procesos determinados en la norma ISO 17582 2. Registro Electoral, reconocimiento de partidos y movimientos políticos, inscripción de candidatos, elecciones, disputas, capacitación, fiscalización y acciones administrativas de queja

Tabla 6: Instituciones electorales en América Latina que han implementado la norma ISO 9001:2008 para la implementación de sistemas de gestión de la calidad, norma ISO/TS 17582:2014 enfocada a sistemas electorales y seguridad informática bajo la norma ISO 27001:2013 que implementa sistemas de gestión de seguridad de la información
Fuente: (Basantes, 2017)

1.12. Sistemas de Informático de escrutinios

El sistema informático de escrutinio utilizado por el organismo electoral conocido en Ecuador como Sistema de Transmisión y Publicación de Resultados STPR, ha sido implementado desde el año 2017 para los procesos electorales: “Elecciones Generales 2017”; “Referéndum y Consulta Popular 2018”; y, “Elecciones Seccionales 2019 y Elección de Consejeras y Consejeros al Consejo de Participación Ciudadana y Control Social”. El sistema consta de varios módulos entre ellos:

a) Módulo de escaneo
b) Módulo de cortes
c) Módulo de reconocimiento inteligente de caracteres (ICR)
d) Módulo de digitación
e) Módulo de verificación de firmas
f) Módulo de computo de resultados
g) Módulo de publicación de resultados

A la fecha el sistema sigue siendo utilizado para los procesos electorales, sin embargo mediante informe de Contraloría General del Estado DNA1-2019-0051 (Contraloría General del Estado, 2019), solicita al Consejo Nacional Electoral la realización de un nuevo sistema de escrutinios en base a observaciones en cuanto a los procedimientos implementados, por los que para el proceso electoral del año 2021 el organismo electoral se encuentra realizando una reingeniería del sistema informático mediante la actualización de varios módulos del proceso ya definido con anterioridad en base a las observaciones realizadas por la Contraloría General del Estado. La misma institución dentro del informe DNA1-0054-2020 (Contraloría General del Estado, 2020) solicita la implementación de controles automáticos de verificación

de las actas levantadas en las JRV, así como la corrección de las observaciones realizadas en el informe DNA1-2019-0051.

1.13. Controles de Acceso

Los controles de acceso son mecanismos que garantizan el correcto ingreso de una persona habilitada a un equipo informático, sistema operativo, aplicación, base de datos, a fin de que no se permitan accesos de personas ajenas a la institución o departamento, evitando en lo posterior que estas personas no autorizadas cometan acciones ilícitas contra la organización, como denegaciones de servicio o robo de la información y se garantice su confidencialidad, integridad y disponibilidad.

1.13.1. Etapas

Los controles de acceso se basan en tres etapas (identificación, autentificación, autorización).

1. **Identificación. –** Etapa en la que el usuario determina ser el titular de las credenciales de acceso, y que permite distinguir una persona de otra en la cual al usuario

2. **Autenticación. -** Comprobación de los datos del usuario con aquellos datos que se almacenan en el sistema mediante siguientes técnicas:

   a) **Lo que es usuario sabe. -** contraseñas o claves de acceso.

   b) **Lo que el usuario tiene. -** dispositivos como tokens, firmas digitales o tarjetas de acceso, magnéticas.

   c) **Lo que el usuario posee. -** características propias del usuario como medios de identificación biométrica como huella dactilar, patrones de voz, patrones de la retina.

   A diferencia del tercer medio de identificación que es algo propio del usuario, los anteriores debe mantenerse con mayor precaución debido a la utilización de técnicas para su robo o suplantación.

3. **Autorización. -** Comprobada las credenciales que identifiquen al usuario el sistema aprueba el acceso hacia los recursos con los permisos referentes al nivel de acceso:

   Lectura del archivo

   Escribir un archivo (añadir, actualizar, borrar, renombrar el archivo)

1.13.2. Elementos

Para establecer los elementos debemos basarnos en dos términos ¿Quiénes van a trabajar sobre los recursos del sistema?, y ¿sobre qué recursos del sistema se trabajan?

a. **Sujetos:** Se consideran como sujetos los términos que operan sobre los recursos: programas, usuarios o hilos.
b. **Objetos:** Son los recursos con los que cuenta el sistema, es decir los recursos del sistema son archivos, carpetas o directorios, servicios del sistema, dispositivos de entrada/salida, puertos TCP/UDP.

1.13.3. Modelos

Es el conjunto definido de criterios que debe aplicar un administrador del sistema para puntualizar los permisos asignados a los usuarios del sistema. Existen tres tipos de modelos:

1. **Control de acceso mandatorio (Mandatory Access Control, MAC). –** Consiste en el "etiquetado" de cada elemento del sistema en los que se aplicarán las políticas de control de acceso.
2. **Control de acceso discrecional (Discretionary Access control, DAC):** método de restricción de acceso a objetos basándose en la identidad de los sujetos que pretenden operar o acceder sobre ellos.
3. **Control de acceso basado en roles (Role Base Access Control, RBAC). -** Definición de perfiles (roles) a los que se les atribuyen una serie de características que aplican sobre los permisos y acciones que pueden llevar a cabo, incluyendo el control sobre otros perfiles

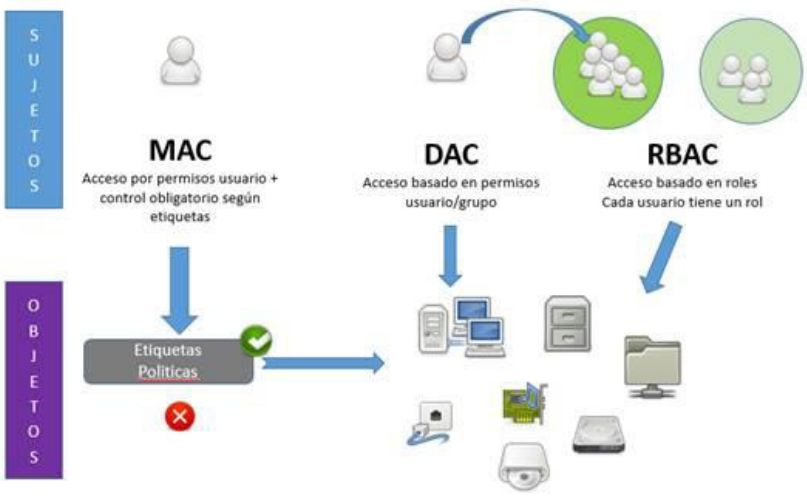


Figura 9: Descripción de los modelos de control de acceso
Fuente: (INCIBE, 2014)

1.13.4. Tipos de autenticación

1. **Autenticación Básica. –** La autentificación permite el envió del usuario y la contraseña en la aplicación a través de la cabecera del portal web mediante peticiones GET.

Ventajas y Desventajas

Ventajas	Desventajas
Fácil de implementar	La facilidad de la programación de este tipo de autentificación permite que las credenciales de acceso sean enviadas por la cabecera mediante peticiones GET o POST por lo que los secuestros de información son más factibles haciendo vulnerable el sistema
Las contraseñas pueden ser almacenadas con cifrado de contraseña en la base de datos	
La autentificación permite el acceso mediante una consulta a la base de datos	

Tabla 7: Ventajas y desventajas de la autentificación básica
Fuente: Análisis de ventajas y desventajas de autentificación básica

2. **Autentificación Digest. -** Método de protección de las credenciales de acceso mediante el cifrado en base de datos de tipo Hash MD5**.**

Inconvenientes

a. Se encuentran expuestos a ataques de sniffing
b. Los mensajes pueden ser interceptados mediante ataque de man in the middle

3. **Inicio de sesión único (Single Sign On- SSO).** – Autentificación que permite que los usuarios puedan tener acceso a todas las aplicaciones, programas sistemas y recursos asociados con un solo usuario y contraseña. Para ejemplificar podemos tomar como referencia los distintos servicios con los que cuenta Google (Google +, Gmail, Drive, Calendario) con el cual el usuario accede a todos los servicios con un solo inicio de sesión.

Características

Características	Descripción
Fácil de gestionar	Permite gestionar las contraseñas e información de los simplificando el acceso a los todas las plataformas y recursos que forman parte del sistema o servicio.
Seguridad	Mejoras en la seguridad de la red y de las aplicaciones, esta autentificación permite identificar de manera evidente a un usuario que cumple con normas más exigentes respecto a la seguridad ya que la información se encuentra cifrada.

Fácil de usar	Mejoran la experiencia del usuario evitando volver a solicitar contraseñas en infinidad de ocasiones que permitan acceder a todas las herramientas informáticas, ya que el usuario se autentica una sola vez permitiendo posteriormente el acceso a todos los recursos que se hayan autorizado al usuario.
Transparente	El usuario no visualiza la autenticación de todos los servicios por lo que las autorizaciones de acceso se realizan de manera transparente.

Tabla 8: Características de la implementación Single Sing On
Fuente: Análisis de características de autentificación Single Sing On

Ventajas y desventajas

Ventajas	Desventajas
Facilidad del usuario al utilizar los servicios	El solo usar una contraseña para todos los servicios aumenta el riesgo de vulnerabilidad en el robo de la contraseña
Reduce la capacidad de que el usuario recuerde varias contraseñas	Si se produce un error en la disponibilidad falla todo el sistema provocando que el usuario queden sin acceso a todos los servicio asociados
Al recordar un solo usuario reduce el tiempo de asistencia por soporte técnico	Si un usuario no autorizado vulnera las seguridades corre el riesgo de acceder a más de una aplicación

Tabla 9: Ventajas y desventajas de la autentificación Single Sing On
Fuente: Análisis de ventajas y desventajas de autentificación Single Sing On

1.13.5. Protocolos de autenticación

1. **Kerberos. -** Protocolo de seguridad a través de la emisión de tickets para el acceso a los servicios en los cuales el servidor emite un conjunto de información electrónica a los usuarios que quieren acceder a la red, buscando evitar la interceptación de las contraseñas.

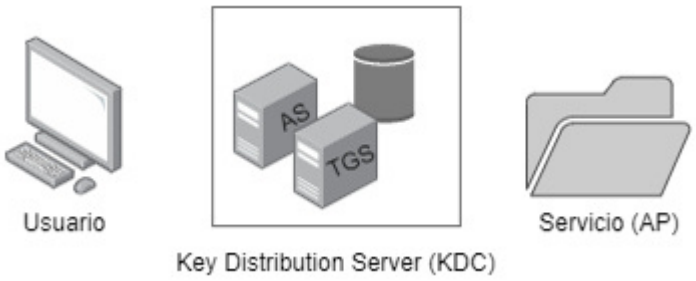


Figura 10: Protocolo Kerberos
Fuente: (ICEAuditor, 2020)

Ventajas y Desventajas

Ventajas	Desventajas
La red en la que se instala kerberos no debe encontrarse en acceso directo o a la vista de usuarios ajenos a su administración por lo que los usuarios que acceden a la red deben ser de confianza	La autentificación se puede volver complicada para el usuario desde el ingreso de contraseñas hasta su autorización
Ofrece un medio de conexión a una red segura, entendiéndose que el momento que se habilite el acceso por internet esta se vuelve insegura	Kerberos inicialmente presume que las peticiones realizadas son de confianza, por lo que puede ser que un usuario no correctamente identificados obtengan credenciales de acceso
El objetivo de kerberos es eliminar la transmisión de información a través de red tratando de erradicar la intercepción de mensajes	Si se usa kerberos y se realiza la transmisión de paquetes a un servicio que no utilice la mismo protocolo se corre el riego que pueda ser interceptado

Figura 11: Ventajas y desventajas referente al uso de kerberos
Fuente: (Massachusetts Institute of Technology, 2020)

2. **Open ID. -** Protocolo de autentificación que permite el ingreso de los usuarios por intermedio de sitios web liberando así la responsabilidad de los programadores y administradores de red de almacenamiento y administración de contraseñas de los posibles solicitantes debido a la gran cantidad de personas que tienen acceso a internet es posible que se busque la saturación de cuentas en beneficio personal.

Ventajas y desventajas

Ventajas	Desventajas
Puede ser utilizado por los programadores de forma libre el mismo que es descargado desde el portal oficial	La fiabilidad de los proveedores de identidad que usan Open ID no está garantizada
El código de implementación es factible, fiable y seguro	Hay muchos proveedores de identidad que trabajan con Open ID, pero pocos proveedores de servicios que lo acepten
Se libera la responsabilidad de al verse comprometido el sistema la información de contraseñas de los usuarios no se encuentran en los servidores	

Tabla 10: Ventajas y desventajas de Open ID
Fuente: (Open ID, 2020)

3. **Protocolo de Acceso Ligero a Directorios (LDAP). –** Conjunto de protocolos de utilizados para el acceso a la información almacenada de forma centralizada en la red conectados mediante una red LAN, basada en una estructura jerárquica de árbol.

Características

Características	Descripción
Escalabilidad	Facilita la configuración simple en hardware y software
Disponibilidad	Permite replicar la información en espejo en varios servidores en la cual facilita la consulta en varios servidores simplificando en una gestión distribuida
Seguridad	Garantiza no permitir el acceso no autorizado de entidades a usuarios externos mediante los requisitos que permitan el acceso
Gestión	Permiten la administración de permisos de manera grafica

Tabla 11: Características de LDAP
Fuente: (Jose Teodoro Mejia Viteri, 2016)

Versiones

Windows: Active Directory

Linux: Open LDAP

Capítulo 2 – Metodología MSIPE

Este capítulo describe las etapas y los pasos en los que se planificará e implementará la metodología enfocada en cuatro normativas y mejores prácticas:

1. ISO 9001 (Enfoque de calidad y adaptación al ciclo PHVA de DEMING).
2. ISO/TS 17582 (Enfoque de calidad para organización de procesos electorales de cual se utilizará en el proceso de **Escrutinio y declaración de los resultados**.
3. ISO 27001 (Los dominios referentes a control de accesos).
4. Controles CIS (Análisis de los controles enfocados en prácticas que garanticen el acceso a usuarios habilitados a operar los sistemas).

La metodología inicia en una primera etapa de **ANÁLISIS** en la cual se analizan tres aspectos que determinen la factibilidad de implementación de la metodología en el proceso electoral. En esta etapa se realiza un **análisis técnico** en la que se realiza la comparativa de los Controles CIS y el proceso de escrutinios y presentación de resultados de la norma ISO/TS 17582 presentadas en cuanto al alcance de la implementación de la metodología, en un **análisis normativo** se especifican los artículos de la Constitución del Ecuador, las Leyes relacionadas con el sistema democrático del país, y los reglamentos asociados a los sistemas informáticos, y finalmente un **análisis político** que es la parte importante de esta etapa, en la cual se analiza el nivel de confianza en la institución y sistemas utilizados. Con la información recopilada se procederá con la segunda etapa de **PLANIFICACIÓN** con un análisis de factibilidad de la aplicación en razón de los datos analizados en la etapa anterior, la **autorización** del organismo electoral, el **levantamiento del plan** que se aplicará en la metodología y la **recopilación de la documentación** a analizar. En una tercera etapa se realizará la **EJECUCIÓN** de la metodología mediante la **evaluación** y levantamiento de **observaciones**. Finalmente, en una última etapa denominada **INFORME** se realizará la **ejecución** y **presentación** del informe que podrá ser utilizado en una retroalimentación a un siguiente proceso.

2.1. Metodología de implementación

En el ciclo de Deming es un proceso de mejora continua en la que se reinicia con la retroalimentación de las experiencias u observaciones recopiladas, que han sido implementadas en las normas gestión de la ISO.

Las fases sobre las que se va a realizar el trabajo son:

Ciclo Deming	MSIPE
Hacer	Análisis
Planificar	Planificación
Actuar	Ejecución
Verificar	Informe

Tabla 12: Comparativa de etapas del Ciclo de Deming **(Normas9000, 2018)** y Metodología MSIPE
Fuente: propia

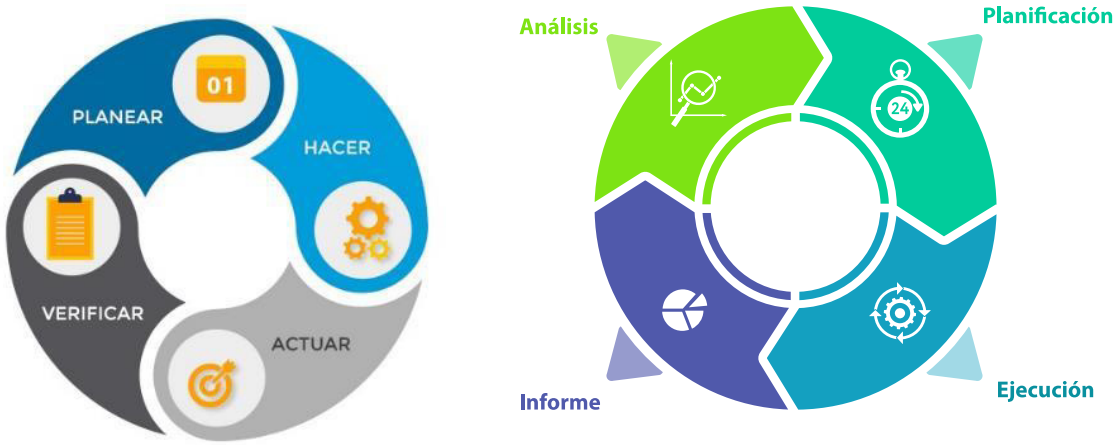


Figura 12: Comparativa entre el ciclo de Deming y la metodología de seguridad informática para procesos electorales
Fuente: propia

El proceso se describe de la siguiente manera:

Etapa	Actividad	Descripción	Componente
Análisis	**1. Análisis Técnico**	Determinar los Controles CIS a utilizar en razón del alcance de la metodología. Determinar los procesos respecto a la norma ISO/TS 17582 en el cual se va a aplicar la metodología	Técnico
	2. Análisis Normativo	Analizar los artículos de la CRE relacionados con el sistema democrático Analizar la norma legal en la cual se autorice uso de sistemas informáticos Determinar si existen reglamentos relacionados con el uso de los sistemas informáticos y realizar el análisis de los mismos	Técnico
	3. Análisis Político	Analizar el nivel de confianza del organismo electoral respecto a su administración y uso de herramientas informáticas	Técnico y Político
Planificación	**4. Análisis de Factibilidad**	Determinar la factibilidad de implementación de la metodología de acuerdo a los resultados planteados en los apartados de análisis técnico, normativo y político De ser factible se proceder con el paso 5 del proceso, caso contrario dar por terminado el proceso	Técnico

Etapa	Actividad	Descripción	Componente
	5. Autorización	Autorizar por parte del organismo electoral la implementación de la metodología de acuerdo al alcance determinado en el análisis De ser factible se proceder con el paso 6 del proceso, caso contrario dar por terminado el proceso	Político
	6. Levantamiento del plan	Levantar las actividades y tiempos para el desarrollo de la metodología	Técnico
	7. Recopilación de documentación	Levantar la documentación necesaria para el desarrollo de la metodología Solicitar a las unidades técnicas la documentación necesaria para el correcto análisis	Técnico
Ejecución	**8. Evaluación**	Evaluar los aspectos relacionados con el alcance de la metodología	Técnico
	9. Observaciones	Levantar las observaciones que se consideren que pueden ser corregidas o mejoradas	Técnico
Informe	**10. Preparación de informe**	Elaborar el informe de acuerdo a los establecido en el alcance de implementación de la metodología	Técnico
	11. Presentación de informe	Presentar el informe a las autoridades del organismo electoral	Técnico

Tabla 13: Descripción de la metodología MSIPE
Fuente: Propia

Figura 13: Actividades contempladas en la metodología MSIPE
Fuente: Propia

Para mayor explicación de la imagen descrita en la figura 13 se realizará la descripción en el siguiente diagrama de flujo descrito en la figura 14.

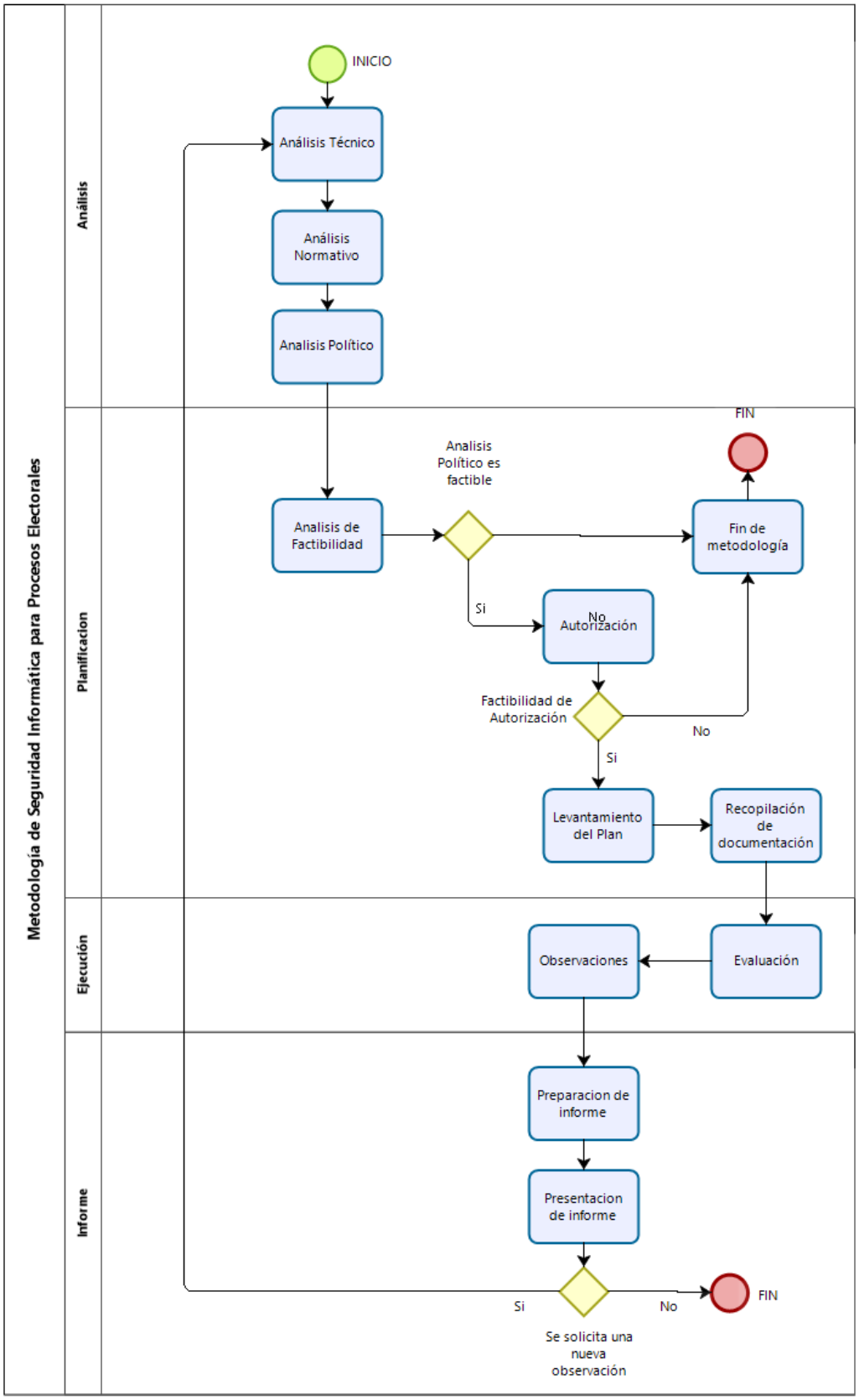


Figura 14: Diagrama de flujo del proceso para la implementación de la metodología MSIPE en Fuente: Propia

2.2. Descripción de la Metodología

Como se ha podido observar la metodología consta de 4 pasos en los cuales se describe el desarrollo de la metodología:

2.2.1. Análisis

El análisis es el inicio del desarrollo de la metodología, en la cual el observador permitirá recopilar las herramientas para la etapa de planificación. Esta etapa se analizarán los aspectos técnicos, normativos y políticos que influyen en un proceso electoral y permitirán establecer la factibilidad de continuidad de la implementación, previo a un análisis de implementaciones anteriores, de existir aplicaciones anteriores es necesario incluir en el proceso los informes levantados a fin de integrarlos en el análisis técnico a realizar.

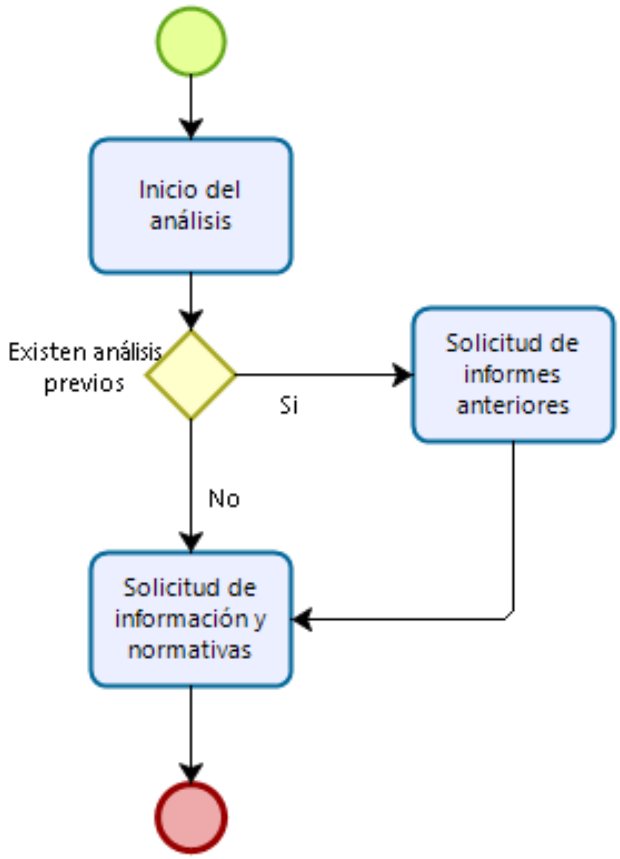


Figura 15: Procedimiento de la etapa de análisis e inicio de la implementación de la metodología MSIPE
Fuente: Propia

La etapa de análisis describe tres actividades explicadas en la figura 16, en la cual la base del análisis corresponde a la aceptación de la ciudadanía y actores electorales respecto del organismo electoral en el país en el que se realicen procesos democráticos, en muchos casos la ciudadanía manifiesta su inconformidad con estas instituciones y pero aun su inconformidad contra de las autoridades que realizan la administración de estas instituciones, ya que eso

deriva en el uso de las herramientas tecnológicas o procedimientos que permitan garantizar la transparencia en las autoridades ocasionando así su implementación. De aceptarse el riesgo político de implementación de la metodología es necesaria el análisis de las normas constitucionales, legales y reglamentarias que regulan el sistema democrático, para la aprobación de estos documentos en muchos casos es necesario los acuerdos políticos en las que los actores lleguen a tener para la gobernabilidad, en muchos casos existen normativas que beneficiarían el mejoramiento de los procesos y que al no llegar a un acuerdo político estas no llegan a aprobarse. En última instancia se encuentra el aspecto técnico que agrupa los procedimientos, manuales y experiencias recopiladas en el mejoramiento constante de los procesos electorales, estos deben ser adaptados a la realidad normativa aprobada por lo que en muchos casos se debe apreciar una serie de versiones en los documentos que administran el proceso, es ahí que primero se necesita el acuerdo político que genere la elaboración de cuerpos normativos y la adaptabilidad de los aspectos técnicos de un proceso electoral.

Figura 16: Análisis de implementación de la primera etapa de la metodología MSIPE
Fuente: Propia

A continuación, se describirá a detalle la descripción de cada uno de los aspectos en la etapa de análisis.

a. Técnico

La evaluación técnica corresponde a la comparativa de los Controles CIS y el proceso de escrutinios y presentación de resultados de la norma ISO/TS 17582 presentadas en cuanto al alcance de la implementación de la metodología, en este caso analizaremos las herramientas propuestas para el respectivo análisis.

i. ALCANCE

Adoptando el principio de Pareto aplicado a la seguridad informática podemos establecer que en el campo de la ciberseguridad es posible obtener la garantía que el 80% de los riegos asociados a la seguridad informática podrán ser mitigados con el 20% de los controles (ESET, 2011), es decir que el análisis y aplicación de una cantidad mínima de controles garantizarán la minimización de las vulnerabilidades en un 80% para los cual analizaremos los controles CIS descritos y los controles establecidos en el documento conocido como "Anexo A" adjunto a la norma técnica ISO 27001. Para determinar la importancia en la etapa de análisis en los tres componentes, como se describe en la figura 16 se muestra (redactar gráfico) la base del análisis es el ámbito político en el cual se toman las decisiones respecto a la implementación, la parte normativa es acoplable a las decisiones políticas y el complemento se establece como la parte técnica que es adaptable a las condiciones impuestas en el organismo electoral.

ii. CONTROLES CIS

En base a lo descrito en por la (Center for Internet Security, 2019) los controles son revisados y modificados en base a las realidades y prácticas establecidas por las organizaciones y comunidades de expertos que versionan contantemente el documentos. los controles a ser aplicados se describen en la tabla 13:

Control	Titulo	Sub control	Descripción	Si/No
1	**Custodiar un inventario y control de equipos informáticos (hardware)**	**1.1**	Manejo de herramientas que permitan el descubrimiento de equipos informáticos conectados a la red	Si
		1.2	Manejo de herramientas que permitan el descubrimiento de equipos informáticos conectados a la red de forma pasiva	Si
		1.3	Manejo de logging para DHCP Logging que permita la actualización del inventario de equipos informáticos	Si
		1.4	Manejo de un inventario de equipos informáticos detallado	Si
		1.5	Gestionar el detalle de información respacto al catálogo o inventario de equipos informáticos	Si
		1.6	Gestionar el detalle de los equipos informáticos no autorizados en la red	Si
		1.7	Implementación de controles de acceso a nivel de puerto para evitar ingresos no autorizados	Si
		1.8	Utilizar certificados clientes que permitan la autenticación de los equipos informáticos hardware	Si
2	**2. Custodiar un inventario y control de programas de**	**2.1**	Mantener un inventario de programas de computación (software) autorizado	Si
		2.2	Asegurarse que los programas de computación (software) cuenten con el soporte del fabricante	Si

Control	Titulo	Sub control	Descripción	Si/No
	computación (software)	**2.3**	Utilizar herramientas para el inventario de programas de computación (software)	Si
		2.4	Rastrear información referente al inventario de los programas de computación (software)	Si
		2.5	Integrar un catálogo o inventarios de activos de equipos de computación (hardware) y programas de computación (software)	Si
		2.6	Controlar los programas de computación (software) no aprobado	Si
		2.7	Implementar una lista blanca de uso de aplicaciones seguras	Si
		2.8	Implementar lista blanca de uso de librerías	Si
		2.9	Implementar lista blanca de uso de scripts	Si
		2.10	Separar las aplicaciones que supongan un alto riesgo tanto a nivel físico como lógico	Si
3	**3. Gestión de las vulnerabilidades de red**	**3.1**	Ejecutar herramientas de escaneo automatizados de vulnerabilidades	Si
		3.2	Realizar análisis de vulnerabilidades autenticados	Si
		3.3	Uso de cuentas específicas para escaneo de vulnerabilidades y auditorias de seguridad	Si
		3.4	Manejo de herramientas que permitan la gestión automatizada de parches para los sistemas operativos	Si
		3.5	Manejo de herramientas que realicen la gestión automatizada de parches de programas de computación (software)	Si
		3.6	Comparar escaneos de vulnerabilidades consecutivos	Si
		3.7	Utilizar un proceso de calificación de riesgo	Si
4	**4. Administración de los Privilegios Administrativos de los sistemas**	**4.1**	Mantener un inventario de cuentas administrativas	Si
		4.2	Cambiar contraseñas por defecto	Si
		4.3	Asegurar el uso de cuentas administrativas dedicadas	Si
		4.4	Usar contraseñas únicas	Si
		4.5	Usar autenticación multifactor para todo acceso administrativo	Si
		4.6	Usar máquinas específicas que permitan la gestión de las tareas administrativas	Si
		4.7	Limitar el acceso a usuarios administrativos con herramientas de scripts	Si
		4.8	Configuración de sistemas que registren y alerten los cambios de los miembros del grupo que tenga asignados privilegios administrativos	Si
		4.9	Manejo de los Registros y alertas sobre los inicios de sesión fallidos en cuentas administrativas	Si

Control	Titulo	Sub control	Descripción	Si/No
15	15. Control de acceso inalámbrico	15.1	Gestionar el inventario con los puntos de acceso inalámbrico que se encuentran autorizados	Si
		15.2	Configuración de herramientas que explore vulnerabilidades en puntos de acceso inalámbricos conectados a la red	Si
		15.3	Uso de sistema inalámbrico de detección de intrusos a través de puntos de acceso inalámbricos conectados a la red cableada	Si
		15.4	Deshabilitar el acceso inalámbrico en dispositivos que no requieran conexión en la red	Si
		15.5	Limitar el acceso de dispositivos a través de la red inalámbrico	Si
		15.6	Inhabilitar las configuraciones establecidas en la red inalámbrica punto a punto de los clientes conectados	Si
		15.7	Usar estándares de cifrado avanzado (AES) para cifrar datos de dispositivos conectados en redes inalámbricas	Si
		15.8	Usar protocolos de autenticación en redes inalámbricas que al momento de conexión requieran autenticación multi-factor	Si
		15.9	Deshabilitar el acceso periférico inalámbrico de dispositivos	Si
		15.10	Creación de redes inalámbricas separadas de dispositivos confiables y no confiables	Si
16	16. Control y monitoreo de la cuenta	16.1	Mantener un inventario de sistemas de autenticación	Si
		16.2	Configurar un punto de autenticación centralizado	Si
		16.3	Requerir Autenticación Multi- factor	Si
		16.4	Utilizar un cifrado o códigos hash en los métodos y herramientas de autenticación	Si
		16.5	Cifrado en la transferencia de datos que permitan la autenticación	Si
		16.6	Mantenimiento de un inventario de cuentas de usuario creados y modificados	Si
		16.7	Establecer un proceso para revocar el acceso a los usuarios dados de baja	Si
		16.8	Deshabilitar cuentas no asociadas con el proceso de negocio	Si
		16.9	Deshabilitar todas las cuentas inactivas en el proceso	Si
		16.10	Programar o implementar métodos con fecha de caducidad de las cuentas	Si
		16.11	Bloqueo automático de sesiones en la estaciones de después de un tiempo de inactividad	Si
		16.12	Monitoreo de accesos no autorizados a través de cuentas desactivadas	Si

Control	Titulo	Sub control	Descripción	Si/No
		16.13	Monitoreo y Alerta de comportamiento no asociados con el inicio de sesión de cuentas	Si
17	**17. Formalizar un programa continuo de concientización e instrucción del personal de la organización en temas de seguridad informática**	**17.1**	Realizar un análisis de brecha de habilidades	Si
		17.2	Implementar programas de capacitación para cubrir la deficiencia de habilidades del personal	Si
		17.3	Implementar un programa de concienciación de seguridad	Si
		17.4	Actualice el contenido de concienciación con frecuencia	Si
		17.5	Capacitación sobre la implementación de autenticación segura	Si
		17.6	Capacitar referente a los ataques de ingeniería social	Si
		17.7	Capacitar sobre el manejo de información catalogada como sensibles	Si
		17.8	Capacitación en temas de exposición involuntaria de datos	Si
		17.9	Capacitación de identificación y reporte de incidentes	Si

Tabla 14: Cuadro de controles y sub controles aplicados a la metodología
Fuente: (Center for Internet Security, 2019)

iii. ISO/TS 17582

De los 8 procesos relacionados con la normativa la parte considerada más importante es la relacionada con el proceso número 5 “Escrutinio y declaración de los resultados”

a. Normativo

Este apartado corresponde al análisis de la normativa legal con el que cuenta el organismo electoral de un país, en cuanto a la Constitución, Leyes, Reglamentos, instructivos y procedimientos que aprueben el uso de las TIC en una o varias etapas del proceso, existen normativas legales en las cuales el uso de votación electrónica facilita la implementación de voto electrónico, en cambio en otros países el uso de las TIC se limita al cómputo de resultados, transmisión y publicación de las mismas[2]

b. Político

Corresponde al nivel de aceptación que tienen los actores políticos con respecto a la implementación de la metodología establecida en razón de los posibles resultados que se puedan levantar con la observación, ya que dependerá de su aceptación para la publicación de los resultados en base al nivel de confianza que tengan a nivel de la ciudadanía[3]. Es posible

[2] En el caso ecuatoriano, artículo 63 de la CRE en su y el artículo 11 de la LOE (Registro Oficial de Ecuador, 2009), determinan que una vez realizado el sufragio en el Ecuador los votos son **escrutados públicamente**, para lo cual la autoridad electoral inicia con la conformación de la JRV y el conteo de los votos frente a delegados políticos.

[3] De acuerdo a los análisis presentados en las figuras 4 y 5 del año 2020, existe una baja confianza de parte de la ciudadanía en el organismo electoral y en quien preside el mismo, por lo que dependiendo de cada país se podrá o no implementar la metodología

que el organismo electoral no permita la observación con lo cual se dará por terminada la misma.

2.2.2. Planificación

a. Análisis de Factibilidad

Con la recopilación de la información se presenta un análisis de factibilidad del desarrollo de la metodología la cual permitirá realizar una presentación al organismo electoral y se solicitará su autorización para la realización de la misma, el documento recopilará los datos obtenidos en la etapa de análisis técnico, normativo y político.

b. Autorización

Al igual que la etapa de análisis político esta actividad determina el punto crítico en el desarrollo de la metodología ya que sin la autorización del organismo electoral se da por concluida la aplicación de la metodología, al aceptar la metodología la autoridad electoral da por conocido la documentación presentada en el informe de análisis, y designa al oficial de seguridad o responsable implementación de seguridad informática en la organización para determinar el calendario de implementación del plan.

c. Levantamiento del Plan

El observador en conjunto con el funcionario responsable, realiza el levantamiento de las actividades a realizar con el respectivo cronograma de implementación el cual se anexará al informe final.

d. Recopilación de la documentación

En base a los análisis realizados en la primera etapa el observador considerara la solicitud de documentación que faculte la revisión de los controles descritos en la etapa de análisis técnico, así como las observaciones relacionadas con los reglamentos, instructivos y procedimientos que sustenten el proceso de escrutinios y presentación de resultados.

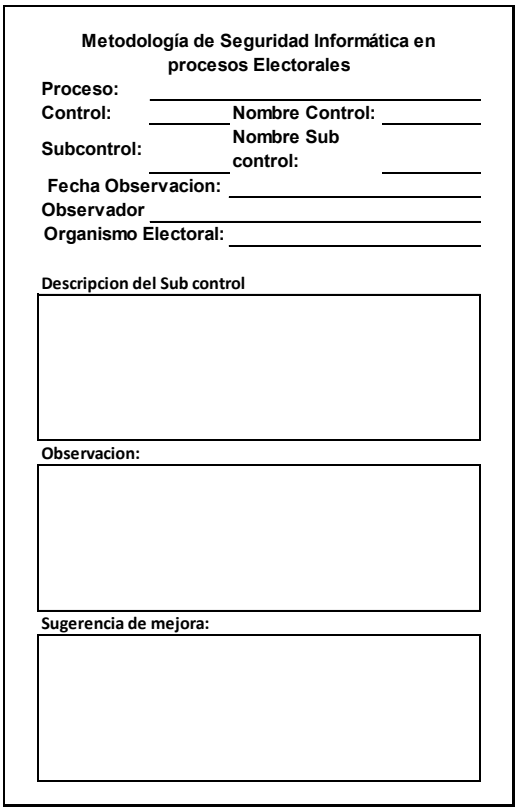
2.2.3. Ejecución

a. Evaluación

En base a los controles específicos y la documentación solicitada se procede con las entrevistas o análisis de los controles establecidos a fin de encontrar observaciones que permitan determinar el grado de madurez de la seguridad informática en el proceso de escrutinios.

b. Levantamiento de observaciones

El observador en base de los criterios establecidos en los controles específicos, el observador levantará oportunidades de mejora en cuanto al proceso electoral, que serán plasmados en el informe final para su aplicación en procesos posteriores si el organismo electoral lo considera en razón de que no es obligatorio la aplicación de la misma.


Metodología de Seguridad Informática en procesos Electorales

Proceso:

Control: Nombre Control:

Subcontrol: Nombre Sub control:

Fecha Observacion:

Observador

Organismo Electoral:

Descripcion del Sub control

Observacion:

Sugerencia de mejora:

Figura 17: Modelo de formato de levantamiento de observaciones en el desarrollo de la metodología MSIPE al encontrarse observaciones que pueden ser mejoradas
Fuente: Propia

2.2.4. Informe

a. Elaboración del informe

Con la información levantada y las observaciones recopiladas el observador realizará el informe con los siguientes elementos:

1. Datos de la institución electoral
2. Objetivos
3. Antecedentes
4. Normativa legal
5. Descripción de la metodología
6. Implementación y análisis
7. Observaciones
8. Conclusiones
9. Recomendaciones (Mejoras a ser consideradas en próximos procesos electorales)

b. Presentación del informe

El observador presentara el informe a las autoridades del organismo electoral a fin de que se den por conocidas las observaciones y estas puedan ser implementadas en el siguiente proceso electoral si ellos lo consideran pertinente.

2.2.5. Retroalimentación

Con la información obtenida el organismo electoral podrá considerar las recomendaciones de mejora para su aplicación las cuales en el siguiente proceso electoral podrán ser verificadas y así dar a conocer a la ciudadanía que el organismo electoral permite garantizar la transparencia y la seguridad informática en los procesos electorales

2.2.6. Puntos críticos

Los puntos críticos de la metodología son aquellos en los cuales se puede dar por terminada el desarrollo de la metodología en razón de la importancia que se quiera dar a la observación, estas etapas son:

Análisis político (Ver 2.2.1 ítem b)

Autorización (Ver 2.2.2 ítem b)

Capítulo 3 – Experimentación

En este capítulo se realiza la experimentación de la Metodología de Seguridad Informática para procesos electorales en el sistema informático de presentación de resultados de Ecuador, en las etapas de análisis, planificación, ejecución e informe, estableciendo como alcance los accesos al Sistema de Transmisión y Publicación de Resultados STPR por parte de los usuarios habilitados al mismo, para ello se utilizarán los controles CIS detallados en los números 1,2,3,4,15,16 y 17 que permitirán determinar que solo las personas autorizadas para el acceso son aquellas que se encuentran operando el mismo, ante ello de acuerdo a los procesos que exige la norma ISO/TS 17582 se utilizara el proceso relacionado con el escrutinios y presentación de resultados, el análisis de los artículos 61,62,217,218,219,220 y 221 de la CRE[4], artículos 2,11,24,25,63,70,89,90 y 91 de la LOE[5], el reglamento de uso de sistema informático y la aceptación de parte de la sociedad para la posterior aplicación y análisis del trabajo.

3.1. Análisis

3.1.1. Técnico

3.1.1.1. CIS

Primero se realizará el análisis de los controles a utilizar en la metodología, que como se explicó en el apartado 2.1.1. del análisis técnico, se tomarán los controles y sub controles CIS números:

1. Custodiar un inventario y control de equipos informáticos (hardware)

2. Custodiar un inventario y control de programas de computación (software)

3. Gestión de las vulnerabilidades de red

4. Administración de los Privilegios Administrativos de los sistemas

15. Control de acceso inalámbrico

16. Control y monitoreo de la cuenta

[4] Constitución de la República del Ecuador
[5] Ley Orgánica Electoral y de Organizaciones Políticas de la República del Ecuador, Código de la Democracia

17. Formalizar un programa continuo de concientización e instrucción del personal de la organización en temas de seguridad informática

Estos controles permitirán determinar los accesos realizados al sistema a través de los diferentes medios, como software que se utiliza, y el personal habilitado para hacerlo.

3.1.1.2. ISO/TS 17582

El proceso a ser analizado es el número 5 "Escrutinio y declaración de los resultados" que es la etapa más importante del proceso electoral, en la cual la tensión política se verá enfocada y permitirá la evaluación de la confianza de los actores electorales y determinará la transparencia del mismo

3.1.2. Normativo

A nivel normativo el organismo electoral cuenta con los siguientes cuerpos:

Ord	Cuerpo Normativo	Descripción
1	Constitución de la República del Ecuador	**Art. 61** Derechos de Participación "*1. Elegir y ser elegido* *2. Participar en asuntos de interés publico* *4. Ser Consultados* *6. Revocar el mandato que hayan conferido a las autoridades de elección popular*." **Art. 62** Goce de los Derechos de Participación *"1. Obligatorio entre 18 y 65 años y Personas Privadas de Libertad (PPLs) sin sentencia condenatoria ejecutoriada entre 18 y 65* *2. Voluntario: Entre 16 y 18 años, mayores de 65 años, policías y militares en servicio activo, residentes en el exterior, extranjeros con residencia mayor a 5 años en el Ecuador y personas con discapacidad"* **Art. 217** Conformación de la Función Electoral FE **Art. 218** Integración del Consejo Nacional Electoral CNE **Art. 219** Funciones del CNE **Art. 220** Integración del Tribunal Contencioso Electoral TCE **Art. 221** Funciones del TCE
2	Ley Orgánica Electoral y de Organizaciones Políticas de la República del Ecuador, Código de la Democracia	**Art. 2** Derechos de Participación **Art. 11** Goce de los Derechos de Participación **Art. 24** Integración del CNE **Art. 25** Funciones del CNE **Art. 63** Integración del TCE **Art. 70** Funciones del TCE **Art. 89** Elecciones Generales (Autoridades Nacionales) **Art. 90** Elecciones Seccionales (Autoridades Locales) **Art. 91** fechas de posesión 24 de mayo Presidente y Vicepresidente 19 de mayo Parlamentarios Andinos 14 de mayo Asambleístas 14 de mayo otras dignidades **Art. 127** Posibilidad de automatizar el proceso de escrutinios (Se debe considerar que el escrutinio debe hacerse de manera pública)

Ord	Cuerpo Normativo	Descripción
3	Reglamento de integración, implementación y funcionamiento del Sistema de Transmisión y Publicación de Resultados STPR	Implementación del sistema

Tabla 15: Análisis normativo
Fuente: Propia

3.1.3. Político

3.1.3.1. La confianza ciudadana

El Consejo Nacional Electoral al 2020 a nivel ciudadano no cuenta con una aceptación en cuanto a la transparencia en la organización de procesos electorales esto se comprueba con los resultados presentados en la figura 4 del presente documento, en la cual hace referencia a la encuesta realizada por (CEDATOS, 2020), demostrando que el 19% de los encuestados SI CONFÍA en el organismo mientras que el 81% NO CONFÍA; y, en cuanto a la máxima autoridad del organismo, los resultados presentados en la misma encuesta son más desalentadores, estos son presentados en la figura 5 determinando que el 15% SI CONFÍA, mientras que el 85% NO CONFÍA, es decir 4 puntos menos con respecto a los análisis de la figura 4. Estos resultados deben considerarse en razón de que la cabeza de la institución que es quien debe llevar a cabo la implementación de las actividades del proceso, y cualquier actividad que implementen para la mejora de la transparencia serán objeto de cuestionamientos por parte de los actores políticos, ocasionando desconfianza en los resultados que se presente como decisión de los electores el día del sufragio. Muchos medios de información del Ecuador determinan que el término confianza *"No es la primera palabra que muchos piensan cuando hablan del Consejo Nacional Electoral (CNE)"* (Diario Expreso, 2019), por los que el primer objetivo estratégico planteado por la institución en el Plan Estratégico Institucional 2018-2021 (CNE, 2017) determina el Incrementar la eficiencia y transparencia en la organización de los procesos electorales a fin de no caer en la desconfianza en el sistema democrático y la implementación de soluciones, que se verá reflejado en las acciones que se tomen posterior a la presentación de los resultados en el proceso electoral 2021.

3.1.3.2. Sistemas Informáticos

En cuanto al sistema informático utilizado el organismo electoral ha sufrido cuestionamientos por parte del organismo de control de los recursos públicos, en informes DNA1-2019-0051 la (Contraloria General del Estado, 2019) determina observaciones al Sistema de Transmisión y Publicación de Resultados STPR en el cual menciona que no se han establecido mecanismos para el control y la supervisión del proceso de conteo de votos y emisión de las actas de escrutinio no mencionándose problemas con los acceso al sistema

pero generando desconfianza en los actores electorales. Así mismo DNA1-0054-2020 (Contraloria General del Estado, 2020) visibiliza problemas con la publicación de las actas debido a una saturación en las consultas realizadas al portal web, sin embrago no realiza observaciones a los accesos del sistema pero generando desconfianza en los actores electorales.

3.2. Planificación

3.2.1. Análisis de factibilidad

3.2.1.1. Técnico

Existe la factibilidad técnica de la metodología sin embargo hay que considerar el análisis político para verificar su implementación, existen las herramientas para su aplicación en el Consejo Nacional Electoral.

3.2.1.2. Normativo

Se cuenta con los cuerpos legales para realizar la aplicación de la metodología, el Código de la Democracia faculta al organismo electoral el uso de las TIC en una o varias etapas del proceso electoral siempre garantizando que el escrutinio que se realice en las Juntas Receptoras del Voto JRV se haga de manera pública, es decir el secretario leerá en voz alta el resultado de la papeleta y la mostrara a los asistentes para que se realice su contabilización, se levantará un acta que será examinada de manera individualizada por la Junta Provincial Electoral JPE en el caso del territorio nacional o la Junta Especial en el Exterior JEE, para el caso del resto de países donde residan ecuatorianos para su contabilización en el sistema informático. Los sistemas desarrollados deben ser implementados bajo esa característica, para lo cual el acceso al sistema habilitado se considera solo al personal estrictamente necesario del CNE.

3.2.1.3. Político

La confianza en las actividades que desarrolla el CNE y sus sistemas informáticos es relativamente baja por lo que cualquier actividad realizada en pro de seguridad de la información causará desconfianza entre los actores electorales así lo recopilan las tres publicaciones de los diarios: (Diario Expreso, 2019), (Diario el Comercio, 12), (Diario el Telégrafo, 12) , por lo que es necesario que se implementen múltiples herramientas de control con el acompañamiento de los actores electorales durante los procesos electorales que vienen en los años 2021, 2023, 2025 en los cuales la institución debe proyectarse a aumentar el nivel de confianza que no es en el presente proceso electoral.

Con respecto al Sistema de Transmisión y Publicación de Resultados, a la fecha existen fuertes cuestionamientos por parte de las ciudadanas y ciudadanos electores, así como de la

entidad de control así como lo presenta el informe de Contraloría General del Estado DNA1-2019-0051 (Contraloría General del Estado, 2019), en la que solicita al Consejo Nacional Electoral la realización de un nuevo sistema de escrutinios en base a observaciones en cuanto a los procedimientos implementados, por los que para el proceso electoral del año 2021 el organismo electoral se encuentra realizando una reingeniería del sistema informático mediante la actualización de varios módulos del proceso ya definido con anterioridad en base a las observaciones realizadas por la Contraloría General del Estado. La misma institución dentro del informe DNA1-0054-2020 (Contraloría General del Estado, 2020) solicita la implementación de controles automáticos de verificación de las actas levantadas en las JRV, así como la corrección de las observaciones realizadas en el informe DNA1-2019-0051. A pesar de que estos controles no revelan inconvenientes en cuanto a los accesos el sistema no es muy bien visto por los actores electorales (Diario El Universo, 2020), que a pesar de ser un tema técnico el uso del mismo lo vuelve un tema de discusión muy álgido convirtiéndose en un punto de decisión política ya que las autoridades del CNE manifiestan hacer un reingeniería del proceso que a pesar de su necesidad, este se encontrara listo en el mes de diciembre del año 2020, previo a las elecciones de 7 de febrero de 2021, a pesar de esto se muestra publicaciones de (Diario la Hora, 2020) o como se menciona en publicación de (Diario El Comercio, 2020) *"no alcanzaría a configurar un sistema informático nuevo, sino que se "parchará"",* causando serios inconvenientes en su aplicación.

3.3. Ejecución

3.3.1. Evaluación y observaciones

3.3.1.1. Sistema Informático

El sistema informático de escrutinio utilizado por el organismo electoral conocido en Ecuador como Sistema de Transmisión y Publicación de Resultados STPR, ha sido implementado desde el año 2017 para los procesos electorales: *"Elecciones Generales 2017"*; *"Referéndum y Consulta Popular 2018"*; y, *"Elecciones Seccionales 2019 y Elección de Consejeras y Consejeros al Consejo de Participación Ciudadana y Control Social"*. El sistema consta de varios módulos entre ellos:

a) Módulo de escaneo

b) Módulo de cortes

c) Módulo de reconocimiento inteligente de caracteres (ICR)

d) Módulo de digitación

e) Módulo de verificación de firmas

f) Módulo de computo de resultados

g) Módulo de publicación de resultados

El Sistema de Transmisión y Publicación de Resultados comprende el conjunto de normas, procedimientos y herramientas tecnológicas que permiten el escaneo de las actas de escrutinio que son levantadas por las JRV, la transmisión de las actas desde los recintos de transmisión y publicación de actas desde son escaneadas hasta los centros de datos. En los centros de datos se realiza el proceso de reconocimiento de caracteres y el corte de imágenes de las actas para su transmisión hacia los centros de procesamiento de resultados los cuales mediante controles humanos se realiza el procesamiento de los datos registrados en las actas para su inspección por parte de la JPE en el caso de dignidades nacionales o JEE en el caso de dignidades en el exterior. Con la aprobación de la JPE o JEE se realizará el computo de resultados y la publicación de los mismos en el portal web.

La red sobre la cual opera el sistema se encuentra separada de la red administrativa, en la cual se realizan aquellas actividades ordinarias propias de la gestión operativa de la institución, esta red es conocida como red electoral.

Red Administrativa

Control	Titulo	Sub control	Descripción	Si/No
1	**Custodiar un inventario y control de equipos informáticos (hardware)**	**1.1**	La institución maneja herramientas que permitan el descubrimiento de equipos informáticos conectados a la red	Si
		1.2	La institución maneja herramientas que permitan el descubrimiento de equipos informáticos conectados a la red de forma pasiva	No
		1.3	La institución maneja herramientas de logging para *"DHCP Logging"* que permita la actualización del inventario de equipos informáticos	No
		1.4	La institución maneja un inventario de equipos informáticos detallado	Si
		1.5	La institución mantiene el detalle de información del inventario de equipos informáticos	Si
		1.6	La institución gestiona los equipos informáticos no autorizados	No
		1.7	Se Implementan controles de acceso a nivel de puerto para evitar ingresos no autorizados	No
		1.8	La institución utiliza certificados clientes que permitan la autenticación de los equipos informáticos hardware	Si

Control	Titulo	Sub control	Descripción	Si/No
2	2. Custodiar un inventario y control de programas de computación (software)	2.1	La institución mantiene un inventario de programas de computación (software) autorizado	No
		2.2	La institución se asegura que los programas de computación (software) cuenten con el soporte del fabricante	No
		2.3	La institución utiliza herramientas para el inventario de programas de computación (software)	No
		2.4	La institución rastrea información referente al inventario de los programas de computación (software)	No
		2.5	La institución integra inventarios de activos de equipos de computación (hardware) y programas de computación (software)	No
		2.6	La institución controla los programas de computación (software) no aprobado	No
		2.7	La institución utiliza una lista blanca de aplicaciones	No
		2.8	La institución implementa una lista blanca de librerías	No
		2.9	La institución implementar lista blanca de scripts	No
		2.10	La institución separa las aplicaciones que supongan un alto riesgo tanto a nivel físico como lógico	No
3	3. Gestión de las vulnerabilidades de red	3.1	La institución ejecuta herramientas de escaneo automatizados de vulnerabilidades	Si
		3.2	La institución realiza el análisis de vulnerabilidades autenticados	Si
		3.3	Se hacen uso de cuentas específicas para escaneo de vulnerabilidades y auditorias de seguridad	Si
		3.4	Se maneja herramientas que permitan la gestión automatizada de parches para los sistemas operativos	No
		3.5	Se administran de herramientas que realicen la gestión automatizada de parches de programas de computación (software)	No
		3.6	Se realiza comparación de escaneos de vulnerabilidades consecutivos	No
		3.7	Se utiliza un proceso de calificación de riesgo	Si
4	4. Administración de los Privilegios	4.1	La institución mantiene un inventario de cuentas administrativas	Si
		4.2	Se cambian las contraseñas por defecto	Si

Control	Titulo	Sub control	Descripción	Si/No
	Administrativos de los sistemas	**4.3**	El personal técnico asegurar el uso de cuentas administrativas dedicadas	Si
		4.4	Se usan contraseñas únicas	Si
		4.5	La unidad técnica usa métodos de autenticación multifactor para todo acceso administrativo	No
		4.6	Se hacen uso de máquinas específicas que permitan la gestión de las tareas administrativas	No
		4.7	Se limita el acceso a usuarios administrativos con herramientas de scripts	No
		4.8	En la institución se configuran sistemas que registren y alerten los cambios de los miembros del grupo que tenga asignados privilegios administrativos	Si
		4.9	Se manejan registros y alertas sobre los inicios de sesión fallidos en cuentas administrativas	Si
15	**15. Control de acceso inalámbrico**	**15.1**	Se gestiona el inventario con los puntos de acceso inalámbrico que se encuentran autorizados	No
		15.2	Se configuran herramientas que explore vulnerabilidades en puntos de acceso inalámbricos conectados a la red	No
		15.3	Se usan sistemas inalámbrico de detección de intrusos a través de puntos de acceso inalámbricos conectados a la red cableada	No
		15.4	Se deshabilitan los accesos inalámbricos en dispositivos que no requieran conexión en la red	No
		15.5	La unidad informática limita el acceso de dispositivos a través de la red inalámbrico	Si
		15.6	Se inhabilitan las configuraciones establecidas en la red inalámbrica punto a punto de los clientes conectados	No
		15.7	Se usan estándares de cifrado avanzado (AES) para cifrar datos de dispositivos conectados en redes inalámbricas	Si
		15.8	Se usan protocolos de autenticación en redes inalámbricas que al momento de conexión requieran autenticación multi-factor	No
		15.9	Se deshabilitan los accesos periféricos inalámbrico de dispositivos	No
		15.10	Se crean redes inalámbricas separadas de dispositivos confiables y no confiables	Si

Control	Titulo	Sub control	Descripción	Si/No
16	16. Control y monitoreo de la cuenta	16.1	Se mantiene un inventario de sistemas de autenticación	No
		16.2	Se configuran punto de autenticación centralizado	Si
		16.3	Se cuenta con autenticación Multi-factor	No
		16.4	Se utilizan cifrados o códigos hash en los métodos y herramientas de autenticación	Si
		16.5	Se realiza cifrado en la transferencia de datos que permitan la autenticación	No
		16.6	Se hace un mantenimiento de un inventario de cuentas de usuario creados y modificados	Si
		16.7	Se establece un proceso para revocar el acceso a los usuarios dados de baja	No
		16.8	Se deshabilitan las cuentas no asociadas con el proceso de negocio	Si
		16.9	Se deshabilitan todas las cuentas inactivas en el proceso	Si
		16.10	Se programan o implementan métodos con fecha de caducidad de las cuentas	No
		16.11	Se realiza el bloqueo automático de sesiones en la estaciones de después de un tiempo de inactividad	No
		16.12	Se monitorean los accesos no autorizados a través de cuentas desactivadas	No
		16.13	Se monitorean y alertan los comportamientos no asociados con el inicio de sesión de cuentas	No
17	17. Formalizar un programa continuo de concientización e instrucción del personal de la organización en temas de seguridad informática	17.1	Al personal se realiza un análisis de brecha de habilidades	No
		17.2	Al personal se capacita para llenar las brechas de habilidades	No
		17.3	La institución implementa un programa de concienciación de seguridad	No
		17.4	Se actualiza el contenido de concienciación con frecuencia	No
		17.5	Se capacita al personal sobre la implementación de autenticación segura	No
		17.6	La institución realiza programas de capacitación referente a los ataques de ingeniería social	No
		17.7	Se capacita sobre el manejo de información catalogada como sensibles	No
		17.8	Se capacita en temas de exposición involuntaria de datos	No
		17.9	Se realiza capacitación de identificación y reporte de incidentes	Si

Tabla 16: Análisis de la implementación de controles de acceso en el STPR, red administrativa del Consejo Nacional Electoral
Fuente: Propia

Red Electoral

Control	Titulo	Sub control	Descripción	Si/No
1	Custodiar un inventario y control de equipos informáticos (hardware)	1.1	La institución maneja herramientas que permitan el descubrimiento de equipos informáticos conectados a la red	Si
		1.2	La institución maneja herramientas que permitan el descubrimiento de equipos informáticos conectados a la red de forma pasiva	No
		1.3	La institución maneja herramientas de logging para *"DHCP Logging"* que permita la actualización del inventario de equipos informáticos	Si
		1.4	La institución maneja un inventario de equipos informáticos detallado	Si
		1.5	La institución mantiene el detalle de información del inventario de equipos informáticos	Si
		1.6	La institución gestiona los equipos informáticos no autorizados	No
		1.7	Se Implementan controles de acceso a nivel de puerto para evitar ingresos no autorizados	Si
		1.8	La institución utiliza certificados clientes que permitan la autenticación de los equipos informáticos hardware	Si
2	2. Custodiar un inventario y control de programas de computación (software)	2.1	La institución mantiene un inventario de programas de computación (software) autorizado	No
		2.2	La institución se asegura que los programas de computación (software) cuenten con el soporte del fabricante	No
		2.3	La institución utiliza herramientas para el inventario de programas de computación (software)	No
		2.4	La institución rastrea información referente al inventario de los programas de computación (software)	No
		2.5	La institución integra inventarios de activos de equipos de computación (hardware) y programas de computación (software)	No
		2.6	La institución controla los programas de computación (software) no aprobado	No
		2.7	La institución utiliza una lista blanca de aplicaciones	No
		2.8	La institución implementa una lista blanca de librerías	No

Control	Titulo	Sub control	Descripción	Si/No
		2.9	La institución implementar lista blanca de scripts	No
		2.10	La institución separa las aplicaciones que supongan un alto riesgo tanto a nivel físico como lógico	No
3	**3. Gestión de las vulnerabilidades de red**	**3.1**	La institución ejecuta herramientas de escaneo automatizados de vulnerabilidades	Si
		3.2	La institución realiza el análisis de vulnerabilidades autenticados	Si
		3.3	Se hacen uso de cuentas específicas para escaneo de vulnerabilidades y auditorias de seguridad	Si
		3.4	Se maneja herramientas que permitan la gestión automatizada de parches para los sistemas operativos	No
		3.5	Se administran de herramientas que realicen la gestión automatizada de parches de programas de computación (software)	No
		3.6	Se realiza comparación de escaneos de vulnerabilidades consecutivos	No
		3.7	Se utiliza un proceso de calificación de riesgo	Si
4	**4. Administración de los Privilegios Administrativos de los sistemas**	**4.1**	La institución mantiene un inventario de cuentas administrativas	Si
		4.2	Se cambian las contraseñas por defecto	Si
		4.3	El personal técnico asegurar el uso de cuentas administrativas dedicadas	Si
		4.4	Se usan contraseñas únicas	Si
		4.5	La unidad técnica usa métodos de autenticación multifactor para todo acceso administrativo	No
		4.6	Se hacen uso de máquinas específicas que permitan la gestión de las tareas administrativas	No
		4.7	Se limita el acceso a usuarios administrativos con herramientas de scripts	No
		4.8	En la institución se configuran sistemas que registren y alerten los cambios de los miembros del grupo que tenga asignados privilegios administrativos	Si
		4.9	Se manejan registros y alertas sobre los inicios de sesión fallidos en cuentas administrativas	Si

Control	Titulo	Sub control	Descripción	Si/No
15	15. Control de acceso inalámbrico	15.1	Se gestiona el inventario con los puntos de acceso inalámbrico que se encuentran autorizados	No
		15.2	Se configuran herramientas que explore vulnerabilidades en puntos de acceso inalámbricos conectados a la red	No
		15.3	Se usan sistemas inalámbrico de detección de intrusos a través de puntos de acceso inalámbricos conectados a la red cableada	No
		15.4	Se deshabilitan los accesos inalámbricos en dispositivos que no requieran conexión en la red	No
		15.5	La unidad informática limita el acceso de dispositivos a través de la red inalámbrico	Si
		15.6	Se inhabilitan las configuraciones establecidas en la red inalámbrica punto a punto de los clientes conectados	No
		15.7	Se usan estándares de cifrado avanzado (AES) para cifrar datos de dispositivos conectados en redes inalámbricas	Si
		15.8	Se usan protocolos de autenticación en redes inalámbricas que al momento de conexión requieran autenticación multi-factor	No
		15.9	Se deshabilitan los accesos periféricos inalámbrico de dispositivos	No
		15.10	Se crean redes inalámbricas separadas de dispositivos confiables y no confiables	Si
16	16. Control y monitoreo de la cuenta	16.1	Se mantiene un inventario de sistemas de autenticación	No
		16.2	Se configuran punto de autenticación centralizado	Si
		16.3	Se cuenta con autenticación Multi-factor	No
		16.4	Se utilizan cifrados o códigos hash en los métodos y herramientas de autenticación	Si
		16.5	Se realiza cifrado en la transferencia de datos que permitan la autenticación	No
		16.6	Se hace un mantenimiento de un inventario de cuentas de usuario creados y modificados	Si
		16.7	Se establece un proceso para revocar el acceso a los usuarios dados de baja	No
		16.8	Se deshabilitan las cuentas no asociadas con el proceso de negocio	Si

Control	Titulo	Sub control	Descripción	Si/No
		16.9	Se deshabilitan todas las cuentas inactivas en el proceso	Si
		16.10	Se programan o implementan métodos con fecha de caducidad de las cuentas	No
		16.11	Se realiza el bloqueo automático de sesiones en la estaciones de después de un tiempo de inactividad	No
		16.12	Se monitorean los accesos no autorizados a través de cuentas desactivadas	No
		16.13	Se monitorean y alertan los comportamientos no asociados con el inicio de sesión de cuentas	No
17	**17. Formalizar un programa continuo de concientización e instrucción del personal de la organización en temas de seguridad informática**	**17.1**	Al personal se realiza un análisis de brecha de habilidades	No
		17.2	Al personal se capacita para llenar las brechas de habilidades	No
		17.3	La institución implementa un programa de concienciación de seguridad	No
		17.4	Se actualiza el contenido de concienciación con frecuencia	No
		17.5	Se capacita al personal sobre la implementación de autenticación segura	No
		17.6	La institución realiza programas de capacitación referente a los ataques de ingeniería social	No
		17.7	Se capacita sobre el manejo de información catalogada como sensibles	No
		17.8	Se capacita en temas de exposición involuntaria de datos	No
		17.9	Se realiza capacitación de identificación y reporte de incidentes	Si

Tabla 17: Análisis de la implementación de controles de acceso en el STPR, red administrativa del Consejo Nacional Electoral
Fuente: Propia

3.4. Informe del sistema

El Sistema de Transmisión y Publicación de Resultados comprende el conjunto de normas, procedimientos y herramientas tecnológicas que permiten el escaneo de las actas de escrutinio que son levantadas por las JRV, la transmisión de las actas desde los recintos de transmisión y publicación de actas desde son escaneadas hasta los centros de datos. En los centros de datos se realiza el proceso de reconocimiento de caracteres y el corte de imágenes de las actas para su transmisión hacia los centros de procesamiento de resultados los cuales mediante controles humanos se realiza el procesamiento de los datos registrados en las actas para su inspección por parte de la JPE en el caso de dignidades nacionales o JEE en el caso

de dignidades en el exterior. Con la aprobación de la JPE o JEE se realizará el computo de resultados y la publicación de los mismos en el portal web. Si bien las partes sensibles del sistema se encuentran separados en una red privada en la cual se conectarán exclusivamente los equipos destinados al proceso como son: equipos de los recintos de transmisión y publicación de actas, centro de datos y centros de procesamiento de resultados, conocido como red electoral, de la red administrativa, las dos redes cuentas con ciertos controles que, a pesar de generar un nivel de seguridad, no garantiza que en algún momento se presenten fallos. **1.** El sistema se debe **reforzar con el inventario de hardware y software** que use la institución, de manera que se pueda garantizar por un lado su contante mantenimiento y nuevas adquisiciones para reemplazar aquellos equipos que hayan cumplido su vida útil, y por otro la adquisición de licencias de programas o aplicaciones informáticos a fin de no generar problemas posteriores con las empresas proveedoras de software o vulnerabilidades en esos programas, ya que se ha visualizado la existencia de software que no cuenta con el licenciamiento adecuado exponiendo un grave problema de seguridad, esperándose que durante el proceso electoral se realice la adquisición de los mismos. **2.** Se ha identificado que existe un sistema de acceso a través de Single Sing On, con el cual se pueden acceder a todos los servicios en los cuales se encuentre habilitado el usuario, si el usuario se le confiere acceso a un módulo del sistema de escrutinios este debe encontrarse habilitado en el Directorio Activo o Active Directory, sin embargo, para reforzar la seguridad se pueden **implementar procedimientos de autentificaciones multifactor** que den mayor seguridad en el acceso. **3.** Se identificó que existen módulos del sistema que funcionan en una red independiente conocido como red electoral, en la cual se determina el número de equipos que va a encontrarse conectados, de esta asignación en procedimientos de verificación o auditoria se identificó que equipos pertenecientes a una red administrativa y con un usuario designado para el acceso al sistema se produjo un acceso al mismo por lo que se puede mejorar el **control de loggin de sesión de equipos exclusivamente designados a la red electoral**, controlando de esta manera los acceso de equipos no autorizados , así como la **separación de acceso que se realiza a través de red cableada de aquella que se realiza por medio de una red inalámbrica**. **4.** Existe una configuración específica para los equipos que se destinaran al sistema electoral, del cual se manifiesta que para su configuración se destinan imágenes de software que deben instalarse en estos equipos, se ha comprobado que se han omitido la configuración para el uso de entradas USB, por lo que se debe mejorar los procesos **de auditorías o identificación de vulnerabilidades en los equipos destinados a red electoral en la cual se examinen las entradas de USB 5.** Se ha identificado que existen procedimientos levantados para dar de baja a los funcionarios separados de la institución es necesario que **se automaticen estos procedimientos mediante la implementación de herramientas que aceleren el retiro de privilegios de estos funcionarios en todos los**

sistemas a los que tengan acceso 6. Si bien existe un Comité de Seguridad de la Información, un Oficial de Seguridad y una dirección de seguridad de la información nombrada como Dirección Nacional de Seguridad y Proyectos de Tecnología Informática Electorales en base al "*Estatuto orgánico de gestión organizacional por procesos del Consejo Nacional Electoral",* aprobado por el Pleno del Consejo Nacional Electoral mediante resolución PLE-CNE-2-26-4-2018 y publicada en el (Registro Oficial Ecuador, 2018), que monitorea los equipos asignados a la seguridad informática es necesario que se **establezcan políticas de concienciación en seguridad de la información y ataques informáticos e ingeniería social de manera que prevengan este tipo de actividades y mejore la seguridad en la institución** no solo en el proceso electoral, es decir debe enfocarse en todas las actividades de tipo ordinario y electoral. Deben **implementarse programas continuos de concienciación en seguridad de la información y ataques informáticos e ingeniería social** para el ingreso del personal

Conclusión

Los organismos electorales en América Latina no gozan de aceptación. En Ecuador la realidad no es diferente ya que el nivel de aceptación es inferior al 20%. Ello dificulta la transparencia en la organización de procesos electorales en especial el próximo proceso electoral del año 2021. El organismo electoral debe implementar una serie de procesos, normativa y metodologías que permitan el acompañamiento de los diferentes actores electorales de manera que puedan permitir la confianza en las personas que administran las instituciones. En América Latina muchas instituciones buscan la implementación de normas que visibilicen la gestión de la calidad como son normas de calidad basados en el estándar ISO-9001 o bien la norma ISO/TS 17582 que implementan Sistemas de Gestión de Calidad SGC. Sin embargo, considerando que la parte más importante del proceso electoral es la etapa de escrutinio y presentación de resultados, las normas de calidad que garantizan que los procesos se realicen de acuerdo a como fueron descritos en el manual de gestión de la calidad sin considerar la seguridad de la información. Ello deja un vacío en la confianza de los ciudadanos. De manera paralela existen metodologías respecto a la seguridad de información que a criterio de las instituciones pueden ser implementadas como son los controles CIS e ISO 27001. La metodología de seguridad de la información para procesos electorales MSIPE presentada en esta investigación ha resultado ser una magnifica herramienta que garantiza mejorar la seguridad de la información recogiendo las mejores prácticas de otras metodologías y controles. Esta novedosa metodología podrá utilizarse como una herramienta apropiada en los procesos electorales. La metodología es una herramienta que garantiza la comparación de las diferentes herramientas en el campo de seguridad de la información adoptando las mejores prácticas de cada herramienta y enfocándolas en el campo de procesos electorales. Como se ha podido apreciar, el sistema informático empleado para el proceso de escrutinios en el Ecuador no goza de la aceptación de los diferentes actores electorales y ha tenido observaciones en cuanto a su aplicación por parte de la entidad de control mediante los exámenes especiales realizados en los años 2019 y 2020, sin embargo no se han identificado observaciones o vulnerabilidades en cuanto a los accesos a los sistemas, con la aplicación de la metodología MSIPE se han identificado puntos que deben considerarse en la reingeniería del sistema.

Trabajo futuro

El presente trabajo plantea las siguientes mejoras: **1.** Plantea la posibilidad de hacer un estudio más amplio y detallado en seguridad de la información con respecto a los procesos electorales, con el análisis y mejora de la normativa ISO/TS 17582 en sus 8 procesos de manera que abarque un sistema de gestión de seguridad de la información y un sistema de gestión de calidad integrado para procesos electorales. **2.** Plantear a parte de la metodología de seguridad de la información un modelo de observación en la transparencia electoral por parte de organismos electorales internacionales, mediante misiones de observación. **3.** Mejorar el alcance planteado en la fase de análisis de vulnerabilidades de manera que abarque no solo los accesos del sistema de escrutinios, de manera que pueda ser implementado en otros procesos que involucren información sensible como por ejemplo el registro electoral, proceso número 1 en la norma ISO/TS 17582 u otros procesos del organismo. **4.** Se puede realizar un estudio de implementación de la metodología MSIPE en otros organismos a electorales de la región que permita la mejora en la aplicación de la misma.

Bibliografía

The Cocktail Analysis. (04 de 2019). *OSPI.* Obtenido de OSPI: https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

ALPHA. (16 de 08 de 2017). *ALPHA Consultoria y Asesoria*. Obtenido de ALPHA Consultoria y Asesoria: https://www.alpha-sgsst.com.co/modelo-plan-basico-legal/

Banco Interamericano de Desarrollo. (2020). *Reporte Ciberseguridad 2020 riesgo, avances y el camino a seguir en America Latina y el Caribe.* Washington D.C.: Banco Interamericano de Desarrollo.

Barredo, A. (16 de 05 de 2017). *La Vanguardia*. Obtenido de La Vanguardia: https://www.lavanguardia.com/tecnologia/20170516/422622391424/seguridad-windows-android-adobe-apple-linux.html

Basantes, J. B. (2017). *Universidad de Cuenca.* Obtenido de www.ucuenca.edu.ec: http://dspace.ucuenca.edu.ec/bitstream/123456789/26968/1/Tesis%20V2.5%20.pdf

Boletin Oficial del Estado. (s.f.). *Boletin Oficial del Estado*. Obtenido de Boletin Oficial del Estado: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=038_Codigo_Penal_y_legislacion_complementaria&tipo=C&modo=2

CEDATOS. (26 de 02 de 2020). *https://cedatos.com.ec*. Obtenido de https://cedatos.com.ec: https://cedatos.com.ec/blog/2020/02/26/cedatos-escenario-hacia-las-elecciones-de-2021/

Center for Internet Security. (2018). *CIS Center for Internet Security*. Obtenido de https://www.cisecurity.org/

Center for Internet Security. (04 de 2019). *cisecurity.org.* Obtenido de cisecurity.org: https://www.cisecurity.org/controls/

Centro de Asesoría y Promoción Electoral CAPEL. (2017). *Diccionario Electoral* (Tercera Edición ed., Vol. 1). San José de Costa Rica, Costa Rica: IIDH/CAPEL.

CIS. (18 de 7 de 2019). *Center for Internet Security.* Obtenido de Center for Internet Security: https://www.cisecurity.org/white-papers/cis-controls-and-sub-controls-mapping-to-iso-27001/

CIS. (2020). *Cibersecurity*. Obtenido de Cibersecurity: https://www.cisecurity.org/white-papers/cis-controls-and-sub-controls-mapping-to-iso-27001/

CNE. (22 de 08 de 2017). *Consejo Nacional Electoral.* Obtenido de Consejo NAcional Electoral: http://institutodemocracia.gob.ec/wp-content/uploads/2020/01/Plan_Estrategico_2018-2021.pdf

Consejo Electoral Nacional. (2014). *Proyecto de implementacion de infraestructura de tecnologias de informacion y comunicaciones del consejo electoral nacional*. Obtenido de http://cne.gob.ec/documents/lotaip/6.planificacion_institucional/2014/6

Contraloria General del Estado. (26 de 07 de 2019). *CGE.* Obtenido de CGE: https://www.contraloria.gob.ec/Consultas/InformesAprobados

Contraloría General del Estado. (2019). *Informe al sistema de escrutinios.* Quito.

Contraloria General del Estado. (20 de 08 de 2020). *CGE.* Obtenido de CGE: https://www.contraloria.gob.ec/Consultas/InformesAprobados

Corporacion Latinobarometro. (2018). *Informe Latinobarometro.* Santiago de Chile: Latinobarometro. Obtenido de https://www.latinobarometro.org/latOnline.jsp

Corporacion Latinobarometro. (2018). *Informe Latinobarometro.* Santiago de Chile: Latinobarometro. Obtenido de https://www.latinobarometro.org/latOnline.jsp

DELOITE. (2017). *Seguridad de la Información en Ecuador 2017.* Quito: DELOITE Ecuador.

Diario el Comercio. (2020 de 02 de 12). *elcomercio.com*. Obtenido de elcomercio.com: https://www.elcomercio.com/opinion/confianza-fetichismo-legal-consejo-electoral.html

Diario El Comercio. (29 de 08 de 2020). *elcomercio.com*. Obtenido de elcomercio.com: https://www.elcomercio.com/actualidad/reingenieria-tecnologica-comisios-cne-elecciones.html

Diario el Telégrafo. (2020 de 03 de 12). *eltelegrafo.com*. Obtenido de eltelegrafo.com: https://www.eltelegrafo.com.ec/noticias/politica/3/cne-imagen-institucional-comicios2021

Diario El Universo. (25 de 08 de 2020). *eluniverso.com*. Obtenido de eluniverso.com: https://www.eluniverso.com/noticias/2020/08/24/nota/7953775/elecciones-presidenciales-ecuador-2021-contraloria-general-consejo

Diario Expreso. (03 de 12 de 2019). *Expreso.* Obtenido de Expreso: https://www.expreso.ec/actualidad/confianza-brilla-consejo-nacional-electoral-655.html

Diario la Hora. (19 de 02 de 2020). *lahora.com.ec*. Obtenido de lahora.com.ec: https://lahora.com.ec/quito/noticia/1102307050/incertidumbre-sobre-reingenieria-del-sistema-informatico-del-cne

EmprendePyme. (2016). Obtenido de ¿Cómo conseguir un certificado de calidad en tu negocio?: https://www.emprendepyme.net/como-conseguir-un-certificado-de-calidad-en-tu-negocio.html

ESET. (8 de 3 de 2011). *Welive security*. Obtenido de Welive security: https://www.welivesecurity.com/la-es/2011/03/08/principio-pareto-seguridad-informatica/#:~:text=Seg%C3%BAn%20el%20Principio%20de%20Pareto,amenazas%20inform%C3%A1ticas%20en%20la%20empresa.

Eureknow. (2009). *Eureknow.* Obtenido de Eureknow: https://www.eureknow.com/

ICEAuditor. (25 de 06 de 2020). *ICEAuditor*. Obtenido de ICEAuditor: https://blog.isecauditors.com/2020/06/kerberos-el-perro-de-tres-cabezas.html

INCIBE. (27 de 11 de 2014). *Centro de respuesta a incidentes de seguridad* . Obtenido de Centro de respuesta a incidentes de seguridad : https://www.incibe-cert.es/blog/control-acceso

Instituto Nacional de Estadistica INE - España. (16 de 10 de 2012 - 2019). *Encuesta sobre el equipamiento y uso de Tecnologías de la Información y Comunicación en los hogares.* Madrid: Instituto Nacional de Estadistica. Obtenido de Instituto Nacional de Estadistica: https://www.ine.es/prensa/tich_2019.pdf

Instituto Nacional de Estadísticas y Censos INEC - Ecuador. (2012 -2019). *Ecuador en cifras.* Obtenido de Ecuador en cifras: https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic/

ISO. (20 de 11 de 2014). ISO/TS 17582. *Sistemas de gestión de la calidad. Requisitos específicos para la aplicación de la Norma ISO 9001:2008 a organizaciones electorales en todos los niveles de gobierno*.

ISO. (2018). *ISO, Organización Internacional de Normalización: Historia, Funciones y Estructura*. Obtenido de https://www.isotools.org/2013/06/20/iso-organizacion-internacional-de-normalizacion-historia-funciones-y-estructura/

ISOTools. (2018). *8 requisitos de la ISO/TS 17582Ñ2014 para procesos electorales*. Obtenido de https://www.isotools.org/2018/06/26/8-requisitos-iso-ts-175822014/

ISOTools. (s.f.). *International Organization for Standardization*. Obtenido de https://www.iso.org/home.html

ITIL, D. (2018). *ISO-27001:2013 ¿Qué hay de nuevo?* | *Magazcitum*. Obtenido de http://www.magazcitum.com.mx/?p=2397

Jose Teodoro Mejia Viteri, M. I. (2016). Gestion de Usuarios Con LDAP (Lightweight Directory Access Protocol) para el Acceso a los servicios Tecnológicos y a la información en la Empresas. *Journal of Science and Research: Revista Ciencia e Investigacion*, 10-15.

LEAD. (2018). *La ISO. LEAD de Bureau Veritas*. Obtenido de https://es.lead.bureauveritas.com/breve-historia-iso

Lincoln, A. (1863). Ex Presidente de Estados Unidos. En C. Centro de Asesoría y Promoción Electoral, *Diccionario Electoral de CAPEL* (Tercera Edicion ed., Vol. Primer Volumen, pág. 249). San José, Costa Rica: Centro de Asesoría y Promoción Electoral de Instituto Interamericano de Derechos Humanos. Recuperado el 26 de 04 de 2020, de https://www.iidh.ed.cr/capel/diccionario/index.html

Martínez, J. A. (2015). Guía para la aplicación de UNE-EN ISO 9001: 2015.

Massachusetts Institute of Technology. (20 de 07 de 2020). *MIT*. Obtenido de MIT: https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-kerberos.html

Naciones Unidas. (10 de diciembre de 1948). *Naciones Unidas.* Obtenido de www.un.org/: https://www.un.org/es/universal-declaration-human-rights/

Normas9000. (2018). *Qué es ISO | Normas9000.com*. Obtenido de http://www.normas9000.com/content/que-es-iso.aspx

Odar, B. b. (Dirección). (2014). *Hackers, ningun sistema es seguro* [Película].

OEA. (23 de 11 de 2001). *Organizacion de Estados Americanos.* Recuperado el 30 de 07 de 2020, de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

OEA. (2018). *OAS: Quiénes Somos*. Obtenido de http://www.oas.org/es/acerca/quienes_somos.asp

OEA. (20 de 05 de 2020). *Organizacion de Estados Americanos*. Obtenido de Organizacion de Estados Americanos: https://www.oas.org/es/sap/deco/NormasISO.asp

Open ID. (2020). *Open ID*. Obtenido de Open ID: https://openid.net/connect/faq/

Organización de las Naciones Unidas. (27 de Enero de 2015). Recuperado el 20 de Abril de 2020, de http://www.unodc.org/documents/congress/Documentation/A-CONF.222-8/ACONF222_8_s_V1500541.pdf

Organizacion de las Naciones Unidas ONU. (10 de Diciembre de 1948). Organizacion de las Naciones Unidas. *Carta Universal de Derechos Humanos*. Paris, Francia: Organizacion de las Naciones Unidas. Recuperado el 20 de Abril de 2020, de Organizacion de las Naciones Unidas: http://www.un.org/es/documents/index.html

Quinteros Basantes, J. B., & Pozo Bahamonde, J. P. (2017). Beneficios de la aplicación de normas internacionales ISO en procesos electorales. *Revista Derecho Electoral*, 55-72.

Registro Oficial de Ecuador. (27 de 04 de 2009). *Registro Oficial de Ecuador*. Recuperado el 20 de 05 de 2020, de Registro Oficial de Ecuador: https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/4351-suplemento-al-registro-oficial-no-578.html

Registro Oficial de Ecuador. (23 de Enero de 2017). Recuperado el 20 de Abril de 2020, de www.registroficial.gob.ec

Registro Oficial de Ecuador. (10 de 2 de 2017). *Registro Oficial.* Obtenido de Registro Oficial: https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/2215-suplemento-al-registro-oficial-no-180.html

Registro Oficial Ecuador. (20 de 10 de 2008). *Registro Oficial.* Obtenido de Registro Oficial: https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/registro-oficial/item/4864-registro-oficial-no-449

Registro Oficial Ecuador. (11 de 05 de 2018). *Registro Oficial*. Obtenido de Registro Oficial: https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/ediciones-especiales/item/10439-edici%C3%B3n-especial-no-408

Romero, A. S. (Febrero de 2016). Formación de Auditores Internos para Auditoría del Sistema de Gestión de Calidad ISO/TS 17582:2014 /ISO 19011:2011 . *Formación de Auditores Internos para Auditoría del Sistema de Gestión de Calidad ISO/TS 17582:2014 /ISO 19011:2011* . Quito, Pichincha, Ecuador.

Ronquillo, S. (2014). *CONTROLES EN LA SEGURIDAD DE LA INFORMACION*. Obtenido de https://prezi.com/gkwjvmaeivtc/controles-en-la-seguridad-de-la-informacion/

SANS. (2018). *SANS Institute - CIS Critical Security Controls*. Obtenido de https://www.sans.org/critical-security-controls

Tripwire, I. (2018). *Make the Most of the New Centre for Internet Security (CIS) Controls v7*. Obtenido de https://www.tripwire.com/state-of-security/security-data-protection/security-controls/cis-top-20-critical-security-controls/

Universitat de Barcelona. (2018). *Seguridad de la información, un conocimiento imprescindible*. Obtenido de https://www.obs-edu.com/int/blog-investigacion/sistemas/seguridad-de-la-informacion-un-conocimiento-imprescindible

Anexo 1

Artículo de investigación

Nueva metodología de seguridad informática para procesos electorales (MSIPE) en Ecuador

Carlos Fabricio Espín Armijo

Universidad Internacional de la Rioja, Logroño (España)

23 de septiembre de 2020

Resumen

En el presente trabajo de investigación se busca implementar una Nueva Metodología de Seguridad Informática para Procesos Electorales (MSIPE) en Ecuador. La metodología MSIPE se asienta en los controles de seguridad determinados por el (Center for Internet Security) en adelante CIS y en los estándares de calidad ISO17582 alineados a procesos electorales, aprobados por la Organización de Estados Americanos en adelante OEA. Este trabajo realiza una metodología eficiente que permita el control de accesos al Sistema Informático de Resultados Electorales del organismo electoral de Ecuador. Ello contribuirá efectivamente la implementación con el aseguramiento de la "confidencialidad", "integridad" y "disponibilidad" del sistema, asegurando la seguridad informática de las elecciones en Ecuador.

Palabras Clave

Metodología de seguridad informática para elecciones, Accesos a sistemas informáticos, Auditoría Informática

I. Introducción

La toma de decisiones libres y voluntarias, así como la representatividad de un pueblo, ha sido adoptada como un sistema y una forma de organización política actualmente conocida por todos nosotros como Democracia. Si bien el término Democracia, fue acuñado desde antigua Grecia con la palabra *"dēmokratía"*, cuyos vocablos: *"demos"* significa pueblo; y *"kratos"* significa gobierno, establece que democracia es el *"gobierno del pueblo"*. Etimología que fue perfeccionada y definida en el discurso de (Lincoln, 1863) como *"el gobierno del pueblo, por el pueblo y para el pueblo"* (Centro de Asesoría y Promoción Electoral CAPEL, 2017, p. 249). Para ejercer la democracia es necesario establecer el derecho al sufragio como uno de los principios de los derechos humanos, el cual transcribo de la (Organizacion de las Naciones Unidas ONU, 1948) *"Artículo 21.- 1. Toda persona tiene derecho a participar en el gobierno de su país, directamente o por medio de representantes libremente escogidos. 3. La voluntad del pueblo es la base de la autoridad del poder público; esta voluntad se expresará mediante elecciones auténticas que habrán de celebrarse periódicamente, por sufragio universal e igual y por voto secreto u otro procedimiento equivalente que garantice la libertad del voto*". Los países que reconocen la Carta Universal de Derechos Humanos de las Naciones Unidas, adoptan en sus constituciones el sufragio bajo los principios del democráticos de elecciones libres, a fin de garantizar la transparencia, estabilidad y el progreso de los sistemas democráticos adoptados en cada estado soberano. Para la aplicación de este derecho, los organismos electorales de cada país deben transparentar las acciones que realicen, en todas o en alguna etapa del proceso electoral. En especial en el escrutinio y presentación de resultados que es la parte más importante de un proceso electoral, la rapidez y transparencia de esta etapa determinan la efectividad de los organismos electorales en los países que realizan las elecciones de manera periódica respetando los principios democráticos. En ocasiones, los diferentes actores electorales y han manifestado su desconfianza en los organismos públicos con la función y responsabilidad de la organización, dirección, vigilancia de procesos electivos de dignatarios transparentes y eficaces. El termino confianza que deben tener los actores electorales deriva de la satisfacción que tiene la ciudadanía hacia el organismo electoral de su país, la cual ha venido decayendo a lo largo del tiempo. Para esta investigación se ha elaborado la gráfica de la Figura 1, en donde se ven reflejados los informes presentados por la (Corporacion Latinobarometro, 2018) desde el año 1996 al 2018. La confianza en la democracia en el Ecuador refleja la desconfianza en las instituciones electorales, los procesos que organiza y los sistemas informáticos utilizados.

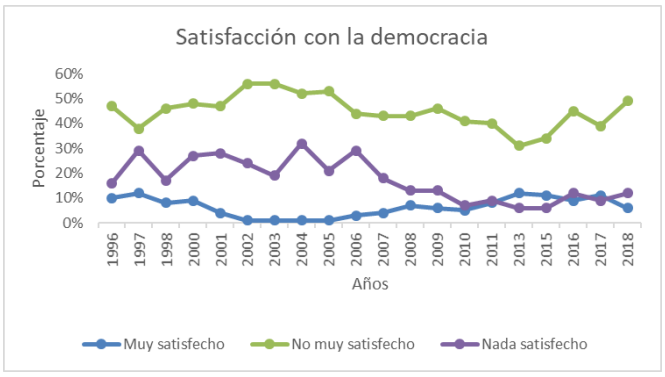


Fig. 1: Satisfacción de la ciudadanía con la democracia en el Ecuador del año 1996 al 2018 Fuente: (Corporacion Latinobarometro, 2018)

Como podemos observar en la figura 1, el informe muestra que la confianza en la democracia tiene un promedio del 6% comparativamente bajo con respecto a la desconfianza que entre los criterios de no muy satisfecho y nada satisfecho tiene un promedio de 62% en los años de estudio de presentación de los informes. Así mismo, en la figura número 2 se analiza la confianza en el organismo electoral. Esta institución tenia por nombre hasta el 2009 como Tribunal Supremo Electoral. Con la aprobación de la nueva Constitución y publicación en el número 449 del (Registro Oficial

Ecuador, 2008) de fecha 20 de octubre del año 2008, la institución paso a llamarse Consejo Nacional Electoral del Ecuador como se establece la (Constitución de la República del Ecuador, 2008) en su artículo 217, nombre que lleva hasta el día de hoy. La grafica muestra estudios aplicados durante los años 2006, 2007, 2010, 2015, 2016, 2017 y 2018 en la cual se representa el nivel de confianza con respecto al organismo electoral, el parámetro "Mucha confianza" refleja un promedio del 4%, el parámetro "Algo de confianza" refleja un promedio del 22%, el parámetro "Poca confianza" refleja un promedio del 40%, y el parámetro "Ninguna confianza" refleja un promedio del 31%, demostrando una gran serie de inconvenientes al momento de organizar procesos electorales.

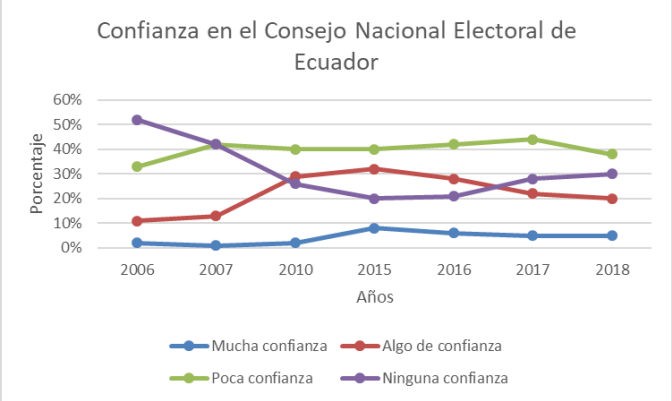


Fig. 2: Confianza en el organismo electoral ecuatoriano Fuente: (Corporacion Latinobarometro, 2018)

La información se ratifica en el año 2019 a través de un informe presentado por la empresa (Eureknow, 2009) que realiza análisis de mercados, quien publica un estudio referente al nivel de confianza del organismo electoral por parte de la ciudadanía, como se puede apreciar en la figura 3, se realiza un estudio sobre las instituciones públicas del Ecuador, en el cual la aceptación del Consejo Nacional Electoral es del 79% baja, 15% es regular y 6% es alta.

Fig. 3: Evaluación de la confianza en las instituciones del Ecuador 2019 Fuente: (Eureknow, 2009)

Por su parte la empresa (CEDATOS, 2020) en el año 2020 presenta el análisis realizado a los ecuatorianos y ecuatorianas respecto al proceso electoral que debe organizar el CNE en el mes de febrero de 2021 en el que indica "En una sola palabra, díganos: ¿Usted CONFÍA o NO CONFÍA en la gestión que realiza el Consejo Nacional Electoral para las elecciones del próximo año 2021?", los resultados de la figura 4 muestran los siguientes resultados: SI CONFÍA : 19%; NO CONFÍA: 81%.

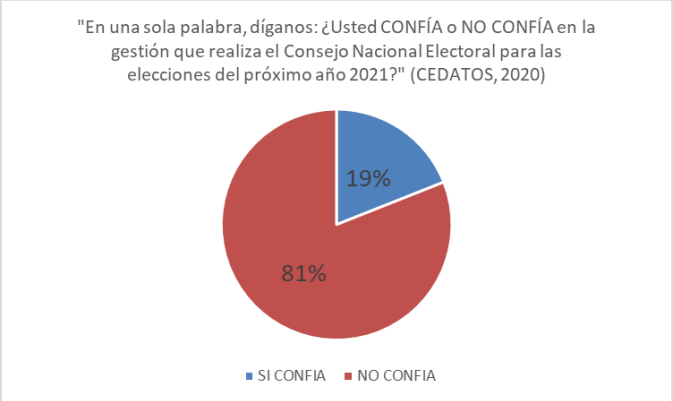


Fig. 4: Confianza en el organismo electoral Fuente: (CEDATOS, 2020)

En la misma encuesta de (CEDATOS, 2020) se pregunta "Concretamente: ¿Usted CONFÍA o NO CONFÍA en la gestión de la Presidenta del Consejo Nacional Electoral, Diana Atamaint?" ante lo cual los encuestados responden: SI CONFÍA, 15%; NO CONFÍA, 85% como se presenta en la información detallada de la figura 5.

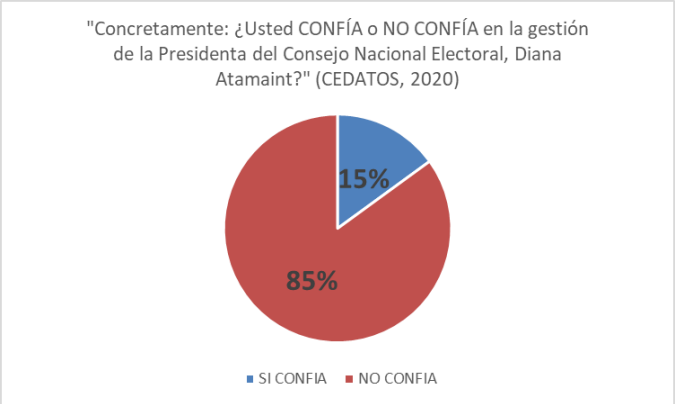


Fig. 5: Confianza en la máxima autoridad del organismo electoral Fuente: (CEDATOS, 2020)

Estos antecedentes derivan de la misma manera en la desconfianza hacia el uso de las Tecnologías de la Información y Comunicación TIC respecto al cómputo de resultados, generando cuestionamientos en los actores electorales, quienes describiendo el principio de seguridad de seguridad de la información que ningún sistema puede ofrecer una confiabilidad total de seguridad o *"ningún sistema es seguro"* (Odar, 2014) concluyen que los sistemas creados para transmisión y publicación de resultado son fácilmente alterados, viciando así la transparencia del proceso electoral, ya que en alguna etapa de desarrollo o implementación del software, todo sistema puede verse comprometido. Estas variables hacen que el sistema informático se vea afectado, para lo cual el organismo electoral debe asegurar a los actores electorales una normativa o procedimiento enfocado en ciberseguridad o seguridad informática, en el que se establecen las normas claras de defensa de los sistemas; que concluyan en la confianza de la organización del proceso electoral. Con lo expuesto, el presente trabajo busca la implementación de una nueva metodología de controles de accesos a sistemas de información que mitiguen falencias normativas y procedimentales que deben ser verificados en uno o varios sistemas del que principalmente debe prevalecer el sistema de escrutinios, de manera que permita generar confianza y seguridad, en cuanto a calidad y seguridad informática.

II. GLOSARIO

FE Función Electoral
CNE Consejo Nacional Electoral
TCE Tribunal Contencioso Electoral
DPE Delegación Provincial Electoral
JPE Junta Provincial Electoral
JEE Junta Especial en el Exterior
JRV Juntas Receptoras del Voto
MJRV Miembros de Juntas Receptoras del Voto
PPL Personas Privadas de Libertad
STPR Sistema de Transmisión y Publicación de Resultados
SG Secretaria General
CNTPE Coordinación Nacional Técnica de Procesos Electorales
CNSIPTE Coordinación Nacional de Seguridad Informática y Proyectos Tecnológicos Electorales
DNITCE Dirección Nacional de Infraestructura Tecnológica y Comunicaciones Electorales
DNSIE Dirección Nacional de Sistemas e Informática Electoral
DNSMIR Dirección Nacional de Seguridad y Manejo integral de Riesgos
OSI Oficial de Seguridad de la Información
TIC Tecnologías de la Información y Comunicación
CRE Constitución de la República del Ecuador
RO Registro Oficial de Ecuador
BOE Boletín Oficial del Estado España
LOE Ley Orgánica Electoral y de Organizaciones Políticas de ña República del Ecuador, Código de la Democracia
ISO Organización Internacional de Estandarización (International Standardization Organization)
CIS Centro para la Seguridad de la Información (Center for Information Security)
ONU Organización de Naciones Unidas
OEA Organización de Estados Americanos
CAPEL Centro de Asesoría y Promoción Electoral
INEC Instituto Nacional de Estadísticas y Censos (Ecuador)
INE Instituto Nacional de Estadística (España)
CGE Contraloría General del Estado
SGC Sistema de Gestión de Calidad
SGSI Sistema de Gestión de Seguridad de la Información

III. ESTADO DEL ARTE

Se debe primero establecer la comparativa entre el uso de las Tecnologías de la Información y la Comunicación entre los años 2012 al 2019 y aceptación de la Seguridad Informática en Ecuador y España

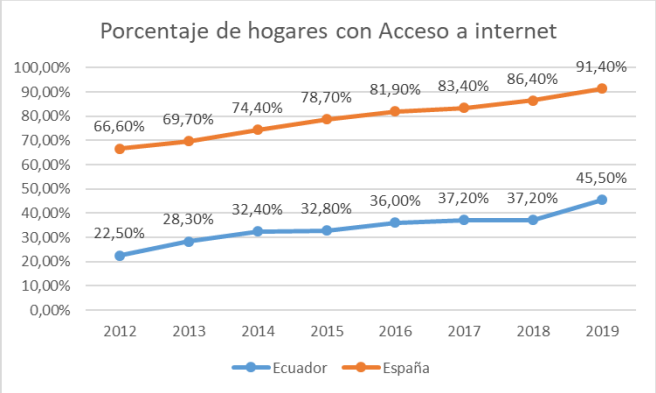


Fig. 6: Uso de las Tecnologías de la Información y la Comunicación entre los años 2012 al 2019 entre Ecuador y España

Fuente: (Instituto Nacional de Estadísticas y Censos INEC - Ecuador, 2012 -2019) e (Instituto Nacional de Estadistica INE - España, 2012 - 2019)

Como se puede visualizar en la figura 6 en el país español la aceptación de esta tecnología es mucho mayor con respecto a la realidad ecuatoriana, reflejando una diferencia promedio del 45%, entre los dos países, realidad que no es ajena al aspecto de seguridad informática puesto que el país español tiene una mayor preparación en los aspectos de seguridad informática y normativa que previene y sanciona los delitos informáticos. Con respecto al estado español cuenta con una ley relacionada con la Protección de Datos de Carácter Personal conocida como Ley Orgánica 15/1999, una ley relacionada con los servicios de la información y el comercio electrónico conocida como Ley 34/2002 y una ley relacionada con los delitos informáticos tipificados en la Ley Orgánica Código Penal conocida como Ley Orgánica 10/1995. Sin embargo, el estado ecuatoriano solo cuenta con una ley que sanciona los delitos informáticos cometido en el territorio teniendo una deficiencia en privacidad de datos determinado que en Ecuador existe una deficiencia en la normativa legal relacionada con la seguridad informática y una desconfianza en los organismos electorales, ocasionando suspicacia respecto a vulnerabilidades en los sistemas informáticos utilizados para los procesos electorales, por lo que es necesario implementar herramientas que mitiguen los riesgos de vulnerabilidades contemplando en el estudio la planificación e implementación de mejores prácticas enfocadas en tres normativas o documentos:

1. ISO 9001:2015 (Enfoque de calidad y adaptación al ciclo PHVA de DEMING).

2. ISO/TS 17582:2014 (Enfoque de calidad para organización de procesos electorales).

3. Controles CIS v7.1 (Análisis de los controles enfocados en prácticas que garanticen el acceso a usuarios habilitados a operar los sistemas), con la comparativa de los controles del Anexo A de la normativa ISO 27001:2013 en la cual se identifiquen similitudes que justifiquen el uso de CIS.

Finalmente, la propuesta de una metodología efectiva a ser implementada en los organismos electorales principalmente en el Ecuador.

IV. OBJETIVOS Y METODOLOGÍA

El trabajo tiene como objetivo general el ofrecer una metodología de seguridad de la información que mitigue los riesgos de accesos no

autorizados a través de su control en el sistema manejado en los procesos electorales que garantice la transparencia del sufragio durante el proceso electoral del Ecuador.

Los objetivos específicos los describimos como:

1. Establecer la metodología de análisis de un proceso electoral mediante controles de acceso de la seguridad informática.

2. Evaluar la seguridad de la información del sistema utilizado en los escrutinios del organismo electoral de Ecuador.

3. Experimentar la metodología de seguridad informática aplicado al sistema informático aplicado en los procesos de escrutinios del organismo electoral de Ecuador y descripción de los resultados presentados.

La metodología como se describe en la figura 6 inicia en una primera etapa de **ANÁLISIS** en la cual se analizan tres aspectos que determinen la factibilidad de implementación de la metodología en el proceso electoral. En esta etapa se realiza un análisis técnico en la que se realiza la comparativa de los Controles CIS y el proceso de escrutinios y presentación de resultados de la norma ISO/TS 17582 presentadas en cuanto al alcance de la implementación de la metodología, en un análisis normativo se especifican los artículos de la Constitución del Ecuador, las Leyes relacionadas con el sistema democrático del país, y los reglamentos asociados a los sistemas informáticos, y finalmente un análisis político que es la parte importante de esta etapa, en la cual se analiza el nivel de confianza en la institución y sistemas utilizados. Con la información recopilada se procederá con la segunda etapa de **PLANIFICACIÓN** con un análisis de factibilidad de la aplicación en razón de los datos analizados en la etapa anterior, la autorización del organismo electoral, el levantamiento del plan que se aplicará en la metodología y la recopilación de la documentación a analizar. En una tercera etapa se realizará la **EJECUCIÓN** de la metodología mediante la evaluación y levantamiento de observaciones. Finalmente, en una última etapa denominada **INFORME** se realizará la ejecución y presentación del informe que podrá ser utilizado en una retroalimentación a un siguiente proceso.

Fig. 6 Actividades contempladas en la metodología MSIPE Fuente: Propia

V. EXPERIMENTACION

A. *Análisis*

Técnico. - Primero se realizará el análisis de los controles a utilizar en la metodología en base a los controles CIS establecidos en los puntos:

1. Custodiar un inventario y control de equipos informáticos (hardware)

2. Custodiar un inventario y control de programas de computación (software)

3. Gestión de las vulnerabilidades de red

4. Administración de los Privilegios Administrativos de los sistemas

15. Control de acceso inalámbrico

16. Control y monitoreo de la cuenta

17. Formalizar un programa continuo de concientización e instrucción del personal de la organización en temas de seguridad informática.

Posteriormente se determinará el alcance de la metodología MSIPE con el análisis de la normativa ISO/TS 17582, en la cual se establece el proceso número 5 bajo el nombre de *"Escrutinio y declaración de los resultados"*

Normativo. – Se analizaron los artículos 61, 62, 217, 218, 219, 220 y 221 de la Constitución de la República del Ecuador relacionados con el derecho al voto, los organismos que componen la función electoral y las funciones de cada una de ellas. Los artículos 2, 11, 24, 25, 63, 70, 89, 90, 91 y 127 de la Ley Orgánica Electoral y de Organizaciones Políticas de la República del Ecuador, Código de la Democracia relacionados con los organismos que componen la función electoral y las funciones de cada una, las elecciones a realizarse en cada proceso, fechas de posesión de autoridades y la facultad de uso de las TIC en una o varias fases del proceso.

Político. – Se realiza un análisis respecto a la confianza ciudadana en la cual el Consejo Nacional Electoral al 2020 a nivel ciudadano no cuenta con una aceptación en cuanto a la transparencia en la organización de procesos electorales esto se comprueba con los resultados presentados en la figura 4 del presente documento, en la cual hace referencia a la encuesta realizada por (CEDATOS, 2020), demostrando que el 19% de los encuestados SI CONFÍA en el organismo mientras que el 81% NO CONFÍA; y, en cuanto a la máxima autoridad del organismo, los resultados presentados en la misma encuesta son más desalentadores, estos son presentados en la figura 5 determinando que el 15% SI CONFÍA, mientras que el 85% NO CONFÍA, es decir 4 puntos menos con respecto a los análisis de la figura 4. Estos resultados deben considerarse en razón de que la cabeza de la institución que es quien debe llevar a cabo la implementación de las actividades del proceso, y cualquier actividad que implementen para la mejora de la transparencia serán objeto de cuestionamientos por parte de los actores políticos, ocasionando desconfianza en los resultados que se presente como decisión de los electores el día del sufragio. Muchos medios de información del Ecuador determinan que el término confianza *"No es la primera palabra que muchos piensan cuando hablan del Consejo Nacional Electoral (CNE)"* (Diario Expreso, 2019), por los que el primer objetivo estratégico planteado por la institución en el Plan Estratégico Institucional 2018-2021 (CNE, 2017) determina el Incrementar la eficiencia y transparencia en la organización de los procesos electorales a fin de no caer en la desconfianza en el sistema democrático y la implementación de soluciones, que se verá reflejado en las acciones que se tomen posterior a la presentación de los resultados en el proceso electoral 2021. En cuanto al sistema informático utilizado el organismo electoral ha sufrido cuestionamientos por parte del organismo de control de los recursos públicos, en informes DNA1-2019-0051 la (Contraloria General del Estado, 2019) determina observaciones al Sistema de Transmisión y Publicación de Resultados STPR en el cual menciona que no se han establecido mecanismos para el control y la supervisión del proceso de conteo de votos y emisión de las actas de escrutinio no mencionándose problemas con los acceso al sistema pero generando desconfianza en los actores electorales. Así mismo DNA1-0054-2020 (Contraloria General del Estado, 2020) visibiliza problemas con la publicación de las actas debido a una saturación en las consultas realizadas al portal web, sin embrago no realiza observaciones a los accesos del sistema, pero generando desconfianza en los actores electorales

B. *Planificación*

1. Existe la factibilidad técnica de la metodología sin embargo hay que considerar el análisis político para verificar su implementación, existen las herramientas para su aplicación en el Consejo Nacional Electoral.

2. Se cuenta con los cuerpos legales para realizar la aplicación de la metodología, el Código de la Democracia faculta al organismo electoral el uso de las TIC en una o varias etapas del proceso electoral siempre garantizando que el escrutinio que se realice en las Juntas Receptoras del Voto JRV se haga de manera pública, es decir el secretario leerá en voz alta el resultado de la papeleta y la mostrara a los asistentes para que se realice su contabilización, se levantará un acta que será examinada de manera individualizada por la Junta Provincial Electoral JPE en el caso del territorio nacional o la Junta Especial en el Exterior JEE, para el caso del resto de países donde residan ecuatorianos para su contabilización en el sistema informático. Los sistemas desarrollados deben ser implementados bajo esa característica, para lo cual el acceso al sistema habilitado se considera solo al personal estrictamente necesario del CNE.

3. La confianza en las actividades que desarrolla el CNE y sus sistemas informáticos es relativamente baja por lo que cualquier actividad realizada en pro de seguridad de la información causará desconfianza entre los actores electorales así lo recopilan las tres publicaciones de los diarios: (Diario Expreso, 2019), (Diario el Comercio, 2020), (Diario el Telégrafo, 2020), por lo que es necesario que se implementen múltiples herramientas de control con el acompañamiento de los actores electorales durante los procesos electorales que vienen en los años 2021, 2023, 2025 en los cuales la institución debe proyectarse a aumentar el nivel de confianza que no es en el presente proceso electoral. Con respecto al Sistema de Transmisión y Publicación de Resultados, a la fecha existen fuertes cuestionamientos por parte de las ciudadanas y ciudadanos electores, así como de la entidad de control así como lo presenta el informe de Contraloría General del Estado DNA1-2019-0051 la (Contraloria General del Estado, 2019)), en la que solicita al Consejo Nacional Electoral la realización de un nuevo sistema de escrutinios en base a observaciones en cuanto a los procedimientos implementados, por los que para el proceso electoral del año 2021 el organismo electoral se encuentra realizando una reingeniería del sistema informático mediante la actualización de varios módulos del proceso ya definido con anterioridad en base a las observaciones realizadas por la Contraloría General del Estado. La misma institución dentro del informe DNA1-0054-2020 (Contraloria General del Estado, 2020) visibiliza solicita la implementación de controles automáticos de verificación de las actas levantadas en las JRV, así como la corrección de las observaciones realizadas en el informe DNA1-2019-0051. A pesar de que estos controles no revelan inconvenientes en cuanto a los accesos el sistema no es muy bien visto por los actores electorales (Diario El Universo, 2020), que a pesar de ser un tema técnico el uso del mismo lo vuelve un tema de discusión muy álgido convirtiéndose en un punto de decisión política ya que las autoridades del CNE manifiestan hacer un reingeniería del proceso que a pesar de su necesidad, este se encontrara listo en el mes de diciembre del año 2020, previo a las elecciones de 7 de febrero de 2021, a pesar de esto se muestra publicaciones de (Diario la Hora, 2020) o como se menciona en publicación de (Diario El Comercio, 2020) “no alcanzaría a configurar un sistema informático nuevo, sino que se “parchará””, causando serios inconvenientes en su aplicación

C. Ejecución

El Sistema de Transmisión y Publicación de Resultados comprende el conjunto de normas, procedimientos y herramientas tecnológicas que permiten el escaneo de las actas de escrutinio que son levantadas por las JRV, la transmisión de las actas desde los recintos de transmisión y publicación de actas desde son escaneadas hasta los centros de datos. En los centros de datos se realiza el proceso de reconocimiento de caracteres y el corte de imágenes de las actas para su transmisión hacia los centros de procesamiento de resultados los cuales mediante controles humanos se realiza el procesamiento de los datos registrados en las actas para su inspección por parte de la JPE en el caso de dignidades nacionales o JEE en el caso de dignidades en el exterior. Con la aprobación de la JPE o JEE se realizará el computo de resultados y la publicación de los mismos en el portal web.

La red sobre la cual opera el sistema se encuentra separada de la red administrativa, en la cual se realizan aquellas actividades ordinarias propias de la gestión operativa de la institución, esta red es conocida como red electoral, levantándose las observaciones detalladas en el punto D Informes.

D. Informes

El Sistema de Transmisión y Publicación de Resultados comprende el conjunto de normas, procedimientos y herramientas tecnológicas que permiten el escaneo de las actas de escrutinio que son levantadas por las JRV, la transmisión de las actas desde los recintos de transmisión y publicación de actas desde son escaneadas hasta los centros de datos. En los centros de datos se realiza el proceso de reconocimiento de caracteres y el corte de imágenes de las actas para su transmisión hacia los centros de procesamiento de resultados los cuales mediante controles humanos se realiza el procesamiento de los datos registrados en las actas para su inspección por parte de la JPE en el caso de dignidades nacionales o JEE en el caso de dignidades en el exterior. Con la aprobación de la JPE o JEE se realizará el computo de resultados y la publicación de los mismos en el portal web. Si bien las partes sensibles del sistema se encuentran separados en una red privada en la cual se conectarán exclusivamente los equipos destinados al proceso como son: equipos de los recintos de transmisión y publicación de actas, centro de datos y centros de procesamiento de resultados, conocido como red electoral, de la red administrativa, las dos redes cuentas con ciertos controles que, a pesar de generar un nivel de seguridad, no garantiza que en algún momento se presenten fallos. **1.** El sistema se debe **reforzar con el inventario de hardware y software** que use la institución, de manera que se pueda garantizar por un lado su contante mantenimiento y nuevas adquisiciones para reemplazar aquellos equipos que hayan cumplido su vida útil, y por otro la adquisición de licencias de programas o aplicaciones informáticos a fin de no generar problemas posteriores con las empresas proveedoras de software o vulnerabilidades en esos programas, ya que se ha visualizado la existencia de software que no cuenta con el licenciamiento adecuado exponiendo un grave problema de seguridad, esperándose que durante el proceso electoral se realice la adquisición de los mismos. **2.** Se ha identificado que existe un sistema de acceso a través de Single Sing On, con el cual se pueden acceder a todos los servicios en los cuales se encuentre habilitado el usuario, si el usuario se le confiere acceso a un módulo del sistema de escrutinios este debe encontrarse habilitado en el Directorio Activo o Active Directory, sin embargo, para reforzar la seguridad se pueden **implementar procedimientos de autentificaciones multifactor** que den mayor seguridad en el acceso. **3.** Se identificó que existen módulos del sistema que funcionan en una red independiente conocido como red electoral, en la cual se determina el número de equipos que va a encontrarse conectados, de esta asignación en procedimientos de verificación o auditoria se identificó que equipos pertenecientes a una red administrativa y con un usuario designado para el acceso al sistema se produjo un acceso al mismo por lo que se puede mejorar el **control de loggin de sesión de equipos exclusivamente designados a la red electoral**, controlando de esta manera los acceso de equipos no autorizados , así como la **separación de acceso que se realiza a través de red cableada de aquella que se realiza por medio de una red inalámbrica**. **4.** Existe una configuración específica para los equipos que se destinaran al sistema electoral, del cual se manifiesta que para su configuración se destinan imágenes de software que deben instalarse en estos equipos, se ha comprobado que se han omitido la configuración para el uso de entradas USB, por lo que se debe mejorar los procesos de **auditorías o identificación de vulnerabilidades en los equipos destinados a red electoral en la**

cual se examinen las entradas de USB 5. Se ha identificado que existen procedimientos levantados para dar de baja a los funcionarios separados de la institución es necesario que se **automaticen estos procedimientos mediante la implementación de herramientas que aceleren el retiro de privilegios de estos funcionarios en todos los sistemas a los que tengan acceso 6.** Si bien existe un Comité de Seguridad de la Información, un Oficial de Seguridad y una dirección de seguridad de la información nombrada como Dirección Nacional de Seguridad y Proyectos de Tecnología Informática Electorales en base al "Estatuto orgánico de gestión organizacional por procesos del Consejo Nacional Electoral", aprobado por el Pleno del Consejo Nacional Electoral mediante resolución PLE-CNE-2-26-4-2018 y publicada en el (Registro Oficial Ecuador, 2018), que monitorea los equipos asignados a la seguridad informática es necesario que se **establezcan políticas de concienciación en seguridad de la información y ataques informáticos e ingeniería social de manera que prevengan este tipo de actividades y mejore la seguridad en la institución** no solo en el proceso electoral, es decir debe enfocarse en todas las actividades de tipo ordinario y electoral. Deben implementarse **programas continuos de concienciación en seguridad de la información y ataques informáticos e ingeniería social** para el ingreso del personal

VI. Conclusiones

Los organismos electorales en América Latina no gozan de aceptación. En Ecuador la realidad no es diferente ya que el nivel de aceptación es inferior al 20%. Ello dificulta la transparencia en la organización de procesos electorales en especial el próximo proceso electoral del año 2021. El organismo electoral debe implementar una serie de procesos, normativa y metodologías que permitan el acompañamiento de los diferentes actores electorales de manera que puedan permitir la confianza en las personas que administran las instituciones. En América Latina muchas instituciones buscan la implementación de normas que visibilicen la gestión de la calidad como son normas de calidad basados en el estándar ISO-9001 o bien la norma ISO/TS 17582 que implementan Sistemas de Gestión de Calidad SGC. Sin embargo, considerando que la parte más importante del proceso electoral es la etapa de escrutinio y presentación de resultados, las normas de calidad que garantizan que los procesos se realicen de acuerdo a como fueron descritos en el manual de gestión de la calidad sin considerar la seguridad de la información. Ello deja un vacío en la confianza de los ciudadanos. De manera paralela existen metodologías respecto a la seguridad de información que a criterio de las instituciones pueden ser implementadas como son los controles CIS e ISO 27001. La metodología de seguridad de la información para procesos electorales MSIPE presentada en esta investigación ha resultado ser una magnifica herramienta que garantiza mejorar la seguridad de la información recogiendo las mejores prácticas de otras metodologías y controles. Esta novedosa metodología podrá utilizarse como una herramienta apropiada en los procesos electorales. La metodología es una herramienta que garantiza la comparación de las diferentes herramientas en el campo de seguridad de la información adoptando las mejores prácticas de cada herramienta y enfocándolas en el campo de procesos electorales. Como se ha podido apreciar, el sistema informático empleado para el proceso de escrutinios en el Ecuador no goza de la aceptación de los diferentes actores electorales y ha tenido observaciones en cuanto a su aplicación por parte de la entidad de control mediante los exámenes especiales realizados en los años 2019 y 2020, sin embargo no se han identificado observaciones o vulnerabilidades en cuanto a los accesos a los sistemas, con la aplicación de la metodología MSIPE se han identificado puntos que deben considerarse en la reingeniería del sistema.

Referencias

The Cocktail Analysis. (04 de 2019). *OSPI.* Obtenido de OSPI: https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

Abrahams, S., Hafner, D., Erwitt, E., & Scarpinelli, A. (2016). *TensorFlow for Machine Intelligence: A Hands-on Introduction to Learning Algorithms.* Bleeding Edge Press.

Al Imran, A., Amin, M. N., & Johora, F. T. (2018). Classification of Chronic Kidney Disease using Logistic Regression, Feedforward Neural Network and Wide & Deep Learning. *2018 International Conference on Innovation in Engineering and Technology*, 1-6.

Banco Interamericano de Desarrollo. (2020). *Reporte Ciberseguridad 2020 riesgo, avances y el camino a seguir en America Latina y el Caribe.* Washington D.C.: Banco Interamericano de Desarrollo.

Bishop, C. M. (1995). Regularization and complexity control in feed-forward networks. *Proceedings International Conference on Artificial Neural Networks*, 141–148.

Breiman, L. (1994). Bagging predictors. *Machine Learning, 24*(2), 123-140.

Breiman, L. (2001). Random forests. *Machine Learning, 45*, 5-32.

Cao, Y., Hu, Z. D., Liu, X. F., Deng, A. M., & Hu, C. J. (2013). An MLP classifier for prediction of HBV-induced liver cirrhosis using routinely available clinical parameters. *Disease markers, 35*(6), 653-660.

CEDATOS. (26 de 02 de 2020). *https://cedatos.com.ec*. Obtenido de https://cedatos.com.ec: https://cedatos.com.ec/blog/2020/02/26/cedatos-escenario-hacia-las-elecciones-de-2021/

Center for Internet Security. (04 de 2019). *cisecurity.org.* Obtenido de cisecurity.org: https://www.cisecurity.org/controls/

Centro de Asesoría y Promoción Electoral CAPEL. (2017). *Diccionario Electoral* (Tercera Edición ed., Vol. 1). San José de Costa Rica, Costa Rica: IIDH/CAPEL.

Chapman, P., Clinton, J., Kerber, R., Khabaza, T., Reinartz, T., Shearer, C., & Wirth, R. (2000). *CRISP-DM 1.0: Step-by-step data mining guide.*

Chapman, P., Clinton, J., Kerber, R., Khabaza, T., Reinartz, T., Shearer, C., & Wirth, R. (2000). *Step-by-step data mining guide.*

CIS. (2020). *Cibersecurity*. Obtenido de Cibersecurity: https://www.cisecurity.org/white-papers/cis-controls-and-sub-controls-mapping-to-iso-27001/

CNE. (22 de 08 de 2017). *Consejo Nacional Electoral.* Obtenido de Consejo NAcional Electoral: http://institutodemocracia.gob.ec/wp-content/uploads/2020/01/Plan_Estrategico_2018-2021.pdf

Contraloria General del Estado. (26 de 07 de 2019). *CGE.* Obtenido de CGE:

https://www.contraloria.gob.ec/Consultas/InformesAprobados

Contraloria General del Estado. (20 de 08 de 2020). *CGE*. Obtenido de CGE: https://www.contraloria.gob.ec/Consultas/InformesAprobados

Corporacion Latinobarometro. (2018). *Informe Latinobarometro*. Santiago de Chile: Latinobarometro. Obtenido de https://www.latinobarometro.org/latOnline.jsp

Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine learning, 20*(3), 273-297.

DANE. (11 de mayo de 2019). *Proyecciones de población.* Obtenido de https://www.dane.gov.co/index.php/estadisticas-por-tema/demografia-y-poblacion/proyecciones-de-poblacion

DELOITE. (2017). *Seguridad de la Información en Ecuador 2017*. Quito: DELOITE Ecuador.

Dessai, I. S. (2013). Intelligent heart disease prediction system using probabilistic neural network. *International Journal on Advanced Computer Theory and Engineering (IJACTE), 2*(3), 2319-2526.

Diario el Comercio. (2020 de 02 de 12). *elcomercio.com*. Obtenido de elcomercio.com: https://www.elcomercio.com/opinion/confianza-fetichismo-legal-consejo-electoral.html

Diario El Comercio. (29 de 08 de 2020). *elcomercio.com.* Obtenido de elcomercio.com: https://www.elcomercio.com/actualidad/reingenieria-tecnologica-comisios-cne-elecciones.html

Diario el Telégrafo. (2020 de 03 de 12). *eltelegrafo.com*. Obtenido de eltelegrafo.com: https://www.eltelegrafo.com.ec/noticias/politica/3/cne-imagen-institucional-comicios2021

Diario El Universo. (25 de 08 de 2020). *eluniverso.com.* Obtenido de eluniverso.com: https://www.eluniverso.com/noticias/2020/08/24/nota/7953775/elecciones-presidenciales-ecuador-2021-contraloria-general-consejo

Diario Expreso. (03 de 12 de 2019). *Expreso.* Obtenido de Expreso: https://www.expreso.ec/actualidad/confianza-brilla-consejo-nacional-electoral-655.html

Diario la Hora. (19 de 02 de 2020). *lahora.com.ec*. Obtenido de lahora.com.ec: https://lahora.com.ec/quito/noticia/1102307050/incertidumbre-sobre-reingenieria-del-sistema-informatico-del-cne

ESET. (8 de 3 de 2011). *Welive security*. Obtenido de Welive security: https://www.welivesecurity.com/la-es/2011/03/08/principio-pareto-seguridad-informatica/#:~:text=Seg%C3%BAn%20el%20Principio%20de%20Pareto,amenazas%20inform%C3%A1ticas%20en%20la%20empresa.

Eureknow. (2009). *Eureknow.* Obtenido de Eureknow: https://www.eureknow.com/

Fawcett, T. (2006). An introduction to ROC analysis. *Pattern Recognition Letters, 27*(8), 861–874.

Flores, J. C., Alvo, M., Borja, H., Morales, J., Vega, J., Zúñiga, C., . . . Münzenmayer, J. (2009). Enfermedad renal crónica: Clasificación, identificación, manejo y complicaciones. *Revista médica de Chile, 137*(1), 137-177.

Fondo Colombiano de Enfermedades de Alto Costo. (2014). *Enfermedad Renal Crónica ERC*. Obtenido de http://www.cuentadealtocosto.org/index.php/patologias/9-patologias/35-enfermedad-renal-cronica-erc

Fondo Colombiano de Enfermedades de Alto Costo. (2017). *Situación de la enfermedad renal crónica, la hipertensión arterial y la diabetes mellitus en Colombia.* Bogotá.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

Gulli, A., & Pal, S. (2017). *Deep Learning with Keras.* Packt Publishing Ltd.

Hinton, G. (2012). Neural networks for machine learning. *Coursera, video lectures*.

Hinton, G. E., Osindero, S., & Teh, Y. (2006). A fast learning algorithm for deep belief nets. *Neural Computation, 18*, 1527–1554.

Hore, S., Chatterjee, S., Shaw, R. K., Dey, N., & Virmani, J. (2018). Detection of chronic kidney disease: A NN-GA-based approach. *Nature Inspired Computing*, 109-115.

Hornik, K., Stinchcombe, M., & White, H. (1989). Multilayer feedforward networks are universal approximators. *Neural Networks, 2*, 359-366.

Hornik, K., Stinchcombe, M., & White, H. (1989). Multilayer feedforward networks are universal approximators. *Neural Networks, 2*, 359-366.

IBM Corporation. (2012). *Manual CRISP-DM de IBM SPSS.*

ICEAuditor. (25 de 06 de 2020). *ICEAuditor*. Obtenido de ICEAuditor: https://blog.isecauditors.com/2020/06/kerberos-el-perro-de-tres-cabezas.html

INCIBE. (27 de 11 de 2014). *Centro de respuesta a incidentes de seguridad* . Obtenido de Centro de respuesta a incidentes de seguridad : https://www.incibe-cert.es/blog/control-acceso

Instituto Nacional de Estadistica INE - España. (16 de 10 de 2012 - 2019). *Encuesta sobre el equipamiento y uso de Tecnologías de la Información y Comunicación en los hogares.* Madrid: Instituto Nacional de Estadistica. Obtenido de Instituto Nacional de Estadistica: https://www.ine.es/prensa/tich_2019.pdf

Instituto Nacional de Estadísticas y Censos INEC - Ecuador. (2012 - 2019). *Ecuador en cifras.* Obtenido de Ecuador en cifras: https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic/

James, G., Witten, D., Hastie, T., & Tibshirani, R. (2013). *An Introduction to Statistical Leaerning with Applications in R.* New York: Springer.

Jarrett, K., Kavukcuoglu, K., & LeCun, Y. (2009). What is the best multi-stage architecture for object recognition? *2009 IEEE 12th international conference on computer vision*, 2146-2153.

Jose Teodoro Mejia Viteri, M. I. (2016). Gestion de Usuarios Con LDAP (Lightweight Directory Access Protocol) para el Acceso a los servicios Tecnológicos y a la información en la Empresas. *Journal of Science and Research: Revista Ciencia e Investigacion*, 10-15.

Kingma, D. P., & Ba, J. (2014). Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*.

Kriplani, H., Patel, B., & Roy, S. (2019). Prediction of Chronic Kidney Diseases Using Deep Artificial Neural Network Technique. *Computer Aided Intervention and Diagnostics in Clinical and Medical Images*, 179-187.

Kumar, K., & Abhishek, B. (2009). Artificial neural networks for diagnosis of kidney stones disease. *Information Technology and Computer Science, 1*, 41-48.

Lincoln, A. (1863). Ex Presidente de Estados Unidos. En C. Centro de Asesoría y Promoción Electoral, *Diccionario Electoral de CAPEL* (Tercera Edicion ed., Vol. Primer Volumen, pág. 249). San José, Costa Rica: Centro de Asesoría y Promoción Electoral de Instituto Interamericano de Derechos Humanos. Recuperado el 26 de 04 de 2020, de https://www.iidh.ed.cr/capel/diccionario/index.html

Magnin, B., Mesrob, L., Kinkingnéhun, S., Pélégrini-Issac, M., Colliot, O., Sarazin, M., & Benali, H. (2009). Support vector machine-based classification of Alzheimer's disease from whole-brain anatomical MRI. *Neuroradiology, 51*(2), 73-83.

Maltarollo, V. G., Honório, K. M., & da Silva, A. F. (2013). Applications of artificial neural networks in chemical problems. *Artificial neural networks-architectures and applications*, 203-223.

Massachusetts Institute of Technology. (20 de 07 de 2020). *MIT*. Obtenido de MIT: https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-kerberos.html

McCulloch, W. S., & Pitts, W. (1943). A logical calculus of ideas immanent in nervous. *Bulletin of Mathematical Biophysics, 5*, 115–133.

Ministerio de Salud y Protección Social. (2016). *Guía de Práctica Clínica para el diagnóstico y tratamiento de la Enfermedad Renal Crónica.* Bogotá.

Ministerio de Salud y Protección Social. (13 de mayo de 2019). *Misión Institucional*. Obtenido de https://www.minsalud.gov.co/Ministerio/Institucional/Paginas/mision-vision-principios.aspx

Ministerio de Salud y Protección Social. (13 de mayo de 2019). *Resolución 3374 de 2000.* Obtenido de https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/DIJ/Resoluci%C3%B3n_3374_de_2000.pdf

Ministerio de Salud y Protección Social. (13 de mayo de 2019). *Sistema de Información de Prestaciones de Salud*. Obtenido de https://www.minsalud.gov.co/proteccionsocial/Paginas/rips.aspx

Ministerio de Salud y Protección Social. (28 de abril de 2019). *Sistema Integrado de Información de la Protección Social*. Obtenido de https://www.sispro.gov.co/Pages/Home.aspx

Nielsen, M. (2015). *Neural Networks and Deep Learning*. San Francisco, CA, USA: Determination press.

Odar, B. b. (Dirección). (2014). *Hackers, ningun sistema es seguro* [Película].

OEA. (23 de 11 de 2001). *Organizacion de Estados Americanos.* Recuperado el 30 de 07 de 2020, de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

OEA. (20 de 05 de 2020). *Organizacion de Estados Americanos*. Obtenido de Organizacion de Estados Americanos: https://www.oas.org/es/sap/deco/NormasISO.asp

Open ID. (2020). *Open ID*. Obtenido de Open ID: https://openid.net/connect/faq/

Organizacion de las Naciones Unidas ONU. (10 de Diciembre de 1948). Organizacion de las Naciones Unidas. *Carta Universal de Derechos Humanos*. Paris, Francia: Organizacion de las Naciones Unidas. Recuperado el 20 de Abril de 2020, de Organizacion de las Naciones Unidas: http://www.un.org/es/documents/index.html

Organización Panamericana de la Salud. (2015). *La OPS/OMS y la Sociedad Latinoamericana de Nefrología llaman a prevenir la enfermedad renal y a mejorar el acceso al tratamiento*. Obtenido de https://www.paho.org/hq/index.php?option=com_content&view=article&id=10542:2015-opsoms-sociedad-latinoamericana-nefrologia-enfermedad-renal-mejorar-tratamiento&Itemid=1926

Rady, E. H., & Anwar, A. S. (2019). Prediction of kidney disease stages using data mining algorithms. *Informatics in Medicine Unlocked*, 100178.

Registro Oficial de Ecuador. (27 de 04 de 2009). *Registro Oficial de Ecuador*. Recuperado el 20 de 05 de 2020, de Registro Oficial de Ecuador: https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/4351-suplemento-al-registro-oficial-no-578.html

Registro Oficial de Ecuador. (10 de 2 de 2017). *Registro Oficial.* Obtenido de Registro Oficial: https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/2215-suplemento-al-registro-oficial-no-180.html

Registro Oficial Ecuador. (20 de 10 de 2008). *Registro Oficial.* Obtenido de Registro Oficial: https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/registro-oficial/item/4864-registro-oficial-no-449

Registro Oficial Ecuador. (11 de 05 de 2018). *Registro Oficial*. Obtenido de Registro Oficial: https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/ediciones-especiales/item/10439-edici%C3%B3n-especial-no-408

Ren, Y., Fei, H., Liang, X., Ji, D., & Cheng, M. (2019). A hybrid neural network model for predicting kidney disease in hypertension patients based on electronic health records. *BMC Medical Informatics and Decision Making, 19*(2), 51.

Rodríguez, L., Díaz, M. E., Ruiz, V., Hernández, H., Herrera, V., & Montero, M. (2014). Factores de riesgo cardiovascular y su relación con la hipertensión arterial en adolescentes. *Revista Cubana de Medicina, 53*(1), 25-36.

Rumelhart, D., Hinton, G., & Williams, R. (1986). Learning representations by back-propagating errors. *Nature, 323*, 533–536.

Samuel, A. (1959). Some Studies in Machine Learning Using the Game of Checkers. *IBM Journal of Research and Developmen, 3*(3), 210-29.

Soldevila, A. (2017). *Análisis de la progresión de la enfermedad renal crónica avanzada mediante técnicas de aprendizaje máquina.* Valencia.

Srivastava, N. (2013). Improving neural networks with dropout. *Universidad de Toronto*.

Tretyakov, K. (2004). Machine learning techniques in spam filtering. *Data Mining Problem-oriented Seminar, MTAT, 3*(177), 60-79.

Vapnik, V. (1982). *Estimation of Dependences Based on Empirical Data.* New York: Springer-Verlag.

West, D., & West, V. (2000). Improving diagnostic accuracy using a hierarchical neural network to model decision subtasks. *International journal of medical informatics, 57*(1), 41-55.

Xiao, J., Ding, R., Xu, X., Guan, H., Feng, X., Sun, T., & Ye, Z. (2019). Comparison and development of machine learning tools in the prediction of chronic kidney disease progression. *Journal of translational medicine, 17*(1), 119.

Yang, J., & Yang, G. (2018). Modified Convolutional Neural Network Based on Dropout and the Stochastic Gradient Descent Optimizer. *Algorithms, 11*(3), 28.

Yu, W., Liu, T., Valdez, R., Gwinn, M., & Khoury, M. J. (2010). Application of support vector Machine modeling for prediction of common diseases: the case of diabetes and pre-diabetes. *BMC medical informatics and decision making, 10*(1), 16.

Zhang, H., Hung, C. L., Chu, W. C., Chiu, P. F., & Tang, C. Y. (2018). Chronic Kidney Disease Survival Prediction with Artificial Neural Networks. *2018 IEEE International Conference on Bioinformatics and Biomedicine*, 1351-1356.

Zhou, Z. H., Jiang, Y., Yang, Y. B., & Chen, S. F. (2002). Lung cancer cell identification based on artificial neural network ensembles. *Artificial Intelligence in Medicine, 24*(1), 25-36.