UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERIA

MAESTRIA EN GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA INFORMACIÓN

“Elaboración de las Políticas de Seguridad de la Información para el Consejo Nacional Electoral del Ecuador”

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR:

Ing. Jeffrey Badí Quinteros Basantes

DIRECTOR:

Ing. Diego Arturo Ponce Vásquez, PhD.

CUENCA-ECUADOR

2017

Resumen

Este trabajo evalúa las medidas de seguridad de la Información del Consejo Nacional Electoral del Ecuador (CNE) con el fin de mejorar sus niveles de seguridad en los procesos electorales y no electorales.

El Consejo Nacional Electoral tiene la responsabilidad de "… vigilar y garantizar, de manera transparente, los procesos electorales…" (Asamblea Nacional Constituyente, 2008), por lo que es necesario implementar políticas de seguridad de la información, las cuales permitirán tener normativas que ayuden a gestionar de forma eficaz la seguridad de la información, de tal forma de que se logre contrarrestar: amenazas, evaluar riesgos, e incrementar controles que permitan garantizar la confidencialidad, integridad y disponibilidad de la información de la cual es responsable el Consejo Nacional Electoral.

Este trabajo pretende la crear las Políticas de Seguridad de la Información para el Consejo Nacional Electoral del Ecuador usando como base la normativa ISO/IEC 27001:2013, estas políticas propenden la protección de los datos desde la parte informática, su acceso físico y restricciones de uso, responsabilidad de los servidores y servidoras que forma parte del CNE, entre otros.

Se ha considerado además que en el Ecuador se han elaborado Normas Técnicas Ecuatorianas como la NTE INEN-ISO/IEC 27000 para la gestión de la Seguridad de la Información. Además, se tomará en cuenta el Esquema Gubernamental de Seguridad de la Información[1] como fuente relevante para la elaboración de las Políticas de Seguridad de la Información, ya que este esquema es usado por la Función Ejecutiva del Ecuador.

Pablaras Clave: Consejo Nacional Electoral, ISO/IEC 27001:2013, Ecuador, Seguridad de la Información

[1] EGSI

Abstract

This work evaluates information security measures of the National Electoral Council of Ecuador (NEC) in order to improve its security level in electoral and non-electoral processes. The National Electoral Council of Ecuador holds the responsibility of "…monitor and guarantee, in a transparent way, the electoral processes…" (Constituent National Assembly, 2008), so it is necessary to implement information security policies, which will allow to have regulations that help manage the information security in an effective way, so that treats and risks can be diminished; better yet, to increase control that guarantees confidentiality, integrity, and availability of the information which the National Electoral Council is responsible for.

Therefore, this work builds up Security Information Policies for the National Electoral Council of Ecuador using ISO/IEC 27001:2013 regulations, which tend to protect computer data, its physical access and use restrictions, responsibility from public servants that are part of the NEC, among others.

In addition, it has been taken into consideration that Technical Norms have been elaborated in Ecuador; for instance, NTE INEN-ISO/IEC 27000 to manage Information Security fields. Moreover, the government's Information Security scheme was taken into account as a relevant source for the development of the Information Security Policies since they are used by the Executive Function of Ecuador.

KEYWORDS: National Electoral Council, ISO/IEC 27001:2013, Ecuador, Information Security.

Índice

Jeffrey Badí Quinteros Basantes, autor de la tesis "Elaboración de las Políticas de Seguridad de la Información para el Consejo Nacional Electoral del Ecuador", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de MAGISTER EN GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA INFORMACIÓN. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor/a

Cuenca, 8 de marzo del 2017

Jeffrey Badí Quinteros Basantes

C.I: 0102966546

Jeffrey Badí Quinteros Basantes, autor de la tesis "Elaboración de las Políticas de Seguridad de la Información para el Consejo Nacional Electoral del Ecuador", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor/a.

Cuenca, 8 de marzo del 2017

Jeffrey Badí Quinteros Basantes

C.I: 0102966546

1 Antecedentes

1.1 Normas de Calidad

La Organización Internacional de Estándares, ISO se fundó en el año de 1947 y nació de la unión de dos organizaciones la ISA (International Federation of the National Standardizing Associations) la cual fue creada en el año de 1926 en Nueva York y que era administrada por Suiza, y por la UNSCC (United Nations Standards Coordinating Committee) creada en 1944 y administrada en Londres. (International Organization for Standardization, 1997).

Ilustración 1 En la conferencia nacional de estándares que tuvo lugar en el Instituto de Ingenieros Civiles en Londres del 14 al 26 de octubre de 1946 se estableció la ISO. La reunión tuvo la presencia de veinte y cinco países con sesenta y cinco delegados.

Las actividades de la ISA estuvieron limitadas a Europa, en donde predomina el sistema que usa como base de sus medias el metro. En cambio Gran Bretaña y Estados Unidos usaban la pulgada como base en su sistema de medidas. Por lo que la nueva organización deseaba establecer normativas internacionales las cuales puedan ser aplicadas de tal forma de poder realizar análisis subsecuentes.

De manera directa, se puede indicar, que existen ventajas para la aplicación de estándares para cada uno de los elementos de la sociedad, tanto como para los negocios quienes al tener estándares, los cuales son herramientas estratégicas,

que muestran la manera como puede alinearse los negocios a los desafíos actuales, así como para los ciudadanos comunes y corrientes quienes utilizan los servicios que los negocios a nivel mundial ofrecen. Estos estándares ayudan a garantizar que los negocios mantengan operaciones eficientes, lo cual genera un aumento de productividad, lo que permite que el negocio pueda alcanzar nuevos nichos de mercado. Los beneficios para la industria pueden verse de forma tangible en ahorros financieros, mejora de la calidad con los clientes, ventajas competitivas y beneficios en el cuidado ambiental.

Para la sociedad, las normas internacionales, aportan aproximadamente 19000 estándares que abarcan todos los aspectos de la vida diaria. La aplicación de estándares, permite que los consumidores tengan la seguridad que los productos o servicios que reciben han sido elaborados siguiendo normativas que permiten que la calidad del producto sea la mejor que el fabricante puede brindar, y que se han considerado aspectos medio ambientales para el mejoramiento de la sostenibilidad (International Organization for Standardization, 2016).

Para las entidades gubernamentales, la aplicación de estándares permite que los ciudadanos a quienes sirven, puedan sentir que existe transparencia, mejora la confianza de los ciudadanos y ciudadanas en las instituciones gubernamentales, permite mejorar los niveles de satisfacción de los servicios y/o productos entregados, entre otros.

Dentro de las normas internacionales ISO se tienen entre otras las que se muestran en la Tabla 1. (Protti Quesada, 2014)

Tabla 1 Algunas normas ISO

Norma	Título
ISO 3166	Código de los países
ISO 4217	Código de monedas
ISO 7810	Documentos de identidad (Norma que regula características físicas y químicas de las tarjetas para carnet, tarjetas de crédito, documentos de identidad, entre otras)
ISO 9000	Sistemas de Gestión de la Calidad
ISO 14000	Sistemas de Gestión Ambiental
ISO 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 26000	Responsabilidad social
ISO 27000	Seguridad de la Información

FUENTE: (Protti Quesada, 2014)
ELABORACIÓN: BADÍ QUINTEROS

1.2 Norma Internacional ISO/IEC 27001:2013

La serie ISO 27000 es una serie de estándares que permiten el establecimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI) del cual se puede obtener una certificación. Los orígenes de las normativas ISO27001 y de la ISO27002 provienen de un trabajo previo realizado por la UK DTI y BSI (Guilles, 2011). Se puede determinar que se tiene la siguiente evolución de la normativa tal como se indica en la Tabla 2:

Tabla 2 Cronología Normas ISO 27000

Año	Descripción
1989	UK DTI se publica un código de buenas prácticas de seguridad de la información
1993	BS PD 003: un código de prácticas de manejo de seguridad de la información
1995	BS7799-1: un código de prácticas que evolucionó del BS PD 003
1998	BS7799-2: un estándar de certificación del manejo de seguridad de la información
1999	BS7799-1 y BS7799-2: las subsecuentes versiones de los estándares ISO17799 y ISO27002 son basados en la versión BS7799-1
2002	BS7799-2 es modificado para incluir el proceso cíclico Planear-Hacer-Chequear-Actuar alineado con la ISO9001. Esta versión es la que se usa de base para la normativa ISO27001 generada en el 2005.
2005	Se publica la normativa ISO para la gestión de seguridad de la información ISO17799 en junio
2005	Se publica la certificación de la normativa ISO de la gestión de sistema de seguridad de la información ISO27001 (octubre)
2007	La ISO17799 es renumerada como ISO27002.
2013	Se emite primera revisión la normativa ISO 27001.

FUENTE: IMPROVING THE QUALITY OF INFORMATION SECURITY MANAGEMENT SYSTEMS WITH ISO27000 (Guilles, 2011)
ELABORACIÓN: BADÍ QUINTEROS

La nueva versión de la normativa ISO/IEC 27001:2013 es muy diferente a la ISO/IEC 27001:2005, no existen requerimientos duplicados y principalmente dan la libertad a la empresa de la elección de los complementos necesarios para su implementación. Además se puede ver que la norma ISO/IEC 27001:2013 se alinea con otras normas ISO como: ISO 9001 (calidad), ISO 22301 (continuidad del negocio) e ISO 31000 (gestión de riesgos); permitiendo a las organizaciones poder tener iguales metodologías para diferentes normativas.

A continuación se presentan en la tabla 3 los dominios de la normativa ISO/IEC 27001:2013 (López Neira & Ruiz Spohr, 2016):

Tabla 3 Dominios y Controles de la normativa ISO 27001:2013

A.5 Políticas de Seguridad de la Información	
	A.5.1 Dirección Administrativa de la seguridad de la información
	Proveer dirección y soporte administrativo para la seguridad de la información de acuerdo con los requerimientos del negocio y leyes relevantes y regulaciones.
A.6 Aspectos de la Organización con respecto a la seguridad de la información	
	A.6.1 Organización Interna
	Establecer un marco de referencia de administración para iniciar y controlar la implementación y operación de la seguridad de la información con la organización
	A.6.2 Dispositivos móviles y teletrabajo
	Seguridad en teletrabajo y en el uso de dispositivos móviles
A.7 Seguridad Ligada a los recursos humanos	
	A.7.1 Antes de la contratación
	Asegurar que los empleados y contratistas entiendan sus responsabilidades que tienen con el perfil para lo que se les ha considerado
	A.7.2 Durante la contratación
	Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades con la seguridad de la información
	A.7.3 Terminación o cambio de contratación
	Proteger los interés de la organización en el proceso de cambio o de terminación del contrato
A.8 Gestión de Activos	
	A.8.1 Responsabilidad de activos
	Identificar los activos de la organización y definir las responsabilidades y apropiada protección de los mismos
	A.8.2 Clasificación de la Información
	Asegurarse que la información reciba un apropiado nivel de protección según la importancia que esta tenga para la organización
	A.8.2.3 Manejo de medios electrónicos
	Prevenir la divulgación no autorizada, modificación, eliminación o extracción de información almacenada en medios electrónicos
A.9 Control de Acceso	
	A.9.1 Requerimientos del negocio con respecto al control de acceso
	Limitar el acceso a la información y a las instalaciones donde se procesa la información
	A.9.2 Administración del acceso de los usuarios
	Asegurar que los usuarios tengan la autorización para el uso de los sistemas y servicios previniendo el acceso no autorizado
	A.9.3 Responsabilidad de los usuarios
	Responsabilidad de los usuarios de salvaguardar sus claves de acceso
	A.9.4 Control de acceso a sistemas y aplicaciones
	Prevenir el acceso no autorizado a las aplicaciones y los sistemas
A.10 Cifrado	
	A.10.1 Controles criptográficos
	Asegurar el propio y afectivo uso de métodos criptográficos para proteger la confidencialidad, autenticidad y/o integridad de la información
A.11 Seguridad física y de entorno	
	A.11.1 Áreas seguras
	Prevenir el acceso físico no autorizado, daño e interferencia en la información y las instalaciones donde se procesa la información de la organización
	A.11.2 Equipamiento
	Prevenir la perdida, el daño, el hurto o que los bienes estén comprometidos de tal forma que puedan interrumpir la operación de la organización
A.12 Seguridad en la Operación	
	A.12.1 Responsabilidades y procedimientos de operación
	Asegurar la operación correcta y segura de los medios de procesamiento de la información

	mediante el desarrollo de los procedimientos de operación apropiados.
	A.12.2 Protección contra código malicioso
	Asegurar que la información y los centros de procesamiento de información estén protegidos ante código malicioso
	A.12.3 Copias de seguridad
	Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.
	A.12.4 Monitoreo y registro de actividad
	Los sistemas deberían ser monitoreados y los eventos de la seguridad de información registrados.
	A.12.5 Control del software en producción
	Asegurar la integridad de los sistemas en operación
	A.12.6 Gestión de la vulnerabilidad técnica
	Prevenir los daños de vulnerabilidades técnicas
	A.12.7 Consideraciones de las auditorías de los sistemas de información
	Minimizar el impacto de actividades de auditoría en los sistemas en operación
A.13 Seguridad en las Comunicaciones	
	A.13.1 Gestión de la seguridad en las redes
	Asegurar la protección de la información en las redes de telecomunicaciones
	A.13.2 Intercambio de información con partes externas
	Mantener la seguridad de la información al ser transferida dentro de la organización y con entidades externas
A.14 Adquisición, desarrollo y Mantenimiento de los sistemas de información	
	A.14.1 Requisitos de seguridad de los sistemas de información
	El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información.
	A.14.2 Seguridad en los procesos de desarrollo y soporte
	Se deberían controlar estrictamente los entornos de desarrollo de proyectos y de soporte.
	A.14.3 Datos de Prueba
	Asegurar la protección de los datos reales en ambientes de prueba
A.15 Relación con proveedores	
	A.15.1 Seguridad de la información en las relaciones con proveedores
	La seguridad de la información de la organización y las instalaciones de procesamiento de la información no debería ser reducida por la introducción de un servicio o producto externo.
	A.15.2 Gestión de la prestación del servicio por proveedores
	La organización debería verificar la implementación de acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se ser prestan cumplen con todos los requerimientos acordados con los terceros.
A.16 Gestión de Incidentes	
	A.16.1 Gestión de incidentes de seguridad de la información y mejoras
	Deberían establecerse las responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información de una manera efectiva y una vez que hayan sido comunicados.
A.17 Aspectos de la Seguridad de la Información en la Gestión de la Continuidad de Negocio	
	A.17.1 Continuidad de la seguridad de la información
	Se deberían determinar los requisitos de seguridad de la información al planificar la continuidad de los procesos de negocio y la recuperación ante desastres.
	A.17.2 Redundancias
	Asegurar la disponibilidad de la infraestructura
A.18 Cumplimiento	
	18.1 Cumplimiento de los requisitos legales y contractuales
	El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales. Los requisitos legales específicos deberían ser advertidos por los asesores legales de la organización o por profesionales adecuadamente cualificados.
	A.18.2 Revisiones de la seguridad de la información

	Asegurar que la seguridad de la información esta implementada y operando de acuerdo con las políticas y procedimientos de la organización

FUENTE: ISO 27000.ES (López Neira & Ruiz Spohr, 2016)
ELABORACIÓN: BADÍ QUINTEROS

2 Estado del Arte

La responsabilidad de la ejecución de procesos eleccionarios recae sobre la administración electoral u organismos electorales que constituyen “la estructura institucional o el conjunto de instituciones públicas de carácter permanente, autónomo, independiente y especializado en materia electoral, encargadas de tutelar y **garantizar** el ejercicio de los derechos políticos de la ciudadanía y el principio de soberanía popular del Estado, **por medio de la correcta y eficaz gestión de los procesos electorales, el control y supervisión de las organizaciones políticas, la formación cívico-política de los ciudadanos y la administración de la justicia electoral.**” (Pozo Bahamonde, 2015). Los organismos electorales deberán ejercer control sobre cada una de las fases dentro del proceso electoral, que son: la pre-electoral, electoral y post-electoral.

Los Estados de Suramérica, dentro de sus procesos de integración muestran su deseo de consolidar la democracia como un sistema político, en el cual los gobernantes son elegidos mediante sufragio directo y secreto, en elecciones limpias, periódicas y competitivas (Pozo Bahamonde, 2015). En consecuencia, la implementación de normas internacionales es un paso decisivo para permitir a los ciudadanos y ciudadanas puedan contar con eventos eleccionarios más transparentes.

Dentro de este contexto, los países miembros de UNASUR[2] han conformado doce consejos sectoriales, siendo uno de ellos el Consejo Electoral cuyo objetivo es: “Propiciar la creación, uso y aplicación de tecnologías no dependientes para el desarrollo de los sistemas electorales, mediante la transferencia en materia de innovación y modernización tecnológica, así como las **buenas prácticas de sistemas** en los procesos electorales”. (Unión de Naciones Suramericanas, 2011)

Tal como indica el Dr. Juan Pablo Pozo: “...el trabajo del CEU[3] es **garantizar** en Suramérica la vigencia plena del derecho al voto universal, igual, directo, secreto y escrutado públicamente, como fundamento del poder público de cada Estado y a la vez del proceso de integración suramericano” (Pozo Bahamonde, 2015); la garantía de este derecho radica fundamentalmente en poder mantener, de manera íntegra, la confidencialidad, integridad y disponibilidad de la información que es parte de los procesos eleccionarios en cualquier nivel de gobierno. Estas mejores prácticas han sido plasmadas en normativas internacionales y su aplicación en los

[2] Unión de Naciones Suramericanas
[3] Consejo Electoral de UNASUR

organismos electorales propenderá a mejorar, visibilizar su transparencia y eficiencia en los procesos eleccionarios, aumentando la participación y mejorando la aceptación ciudadana.

Los países de la Región Andina han mostrado su interés en modernizar y llevar adelante procesos de mejoramiento de los sistemas de los procesos electorales. La Comunidad Andina en la XIV Reunión del Consejo Presidencial Andino, en el documento 551 indica:

"Proponer la **modernización** y automatización de los sistemas de los procesos electorales de la región y de cada uno de los Países Miembros" (Secretaría General de la Comunidad Andina, 2003).

Por su parte, la Organización de Estados Americanos ha iniciado un proceso de promoción y búsqueda de la implementación de Sistemas de Gestión de la Calidad en el ámbito electoral. Para esto sugirió la idea de impulsar la creación de una norma ISO Electoral, bajo la cual los entes electorales de las Américas y del resto del mundo puedan certificarse (Organización de los Estados Americanos, 2016). En conjunto con la ISO, se creó una nueva Norma Internacional Electoral, ISO/TS 17582:2014, la cual fue publicada en febrero del 2014. Esta Norma Electoral define requisitos específicos para procesos fundamentales que deben existir en cualquier elección como son: registro de los votantes, registro de las organizaciones políticas y de los candidatos, logística electoral, emisión del voto, recuento de votos y publicación de resultados, capacitación electoral, fiscalización del financiamiento de campañas y resolución de disputas electorales (International Organization for Standardization, 2014). Además esta normativa tiende al mejoramiento de los procesos, promoviendo una gestión más transparente, eficiente y alineada con los objetivos que el organismo electoral posee. En consecuencia, la ciudadanía tiene más confianza en: los resultados emitidos, los órganos involucrados en la elección como los partidos y movimientos políticos y la transparencia de las entidades electorales de los países (International Organization for Standardization, 2014).

La normativa ISO/TS 17582:2014 utiliza dentro de sus especificidades, a otras normativas para su aplicación, siendo una de ellas la norma ISO/IEC 27000, que hace referencia a la seguridad de la información. Al ser una sugerencia de la Organización de los Estados Americanos, algunos países han obtenido la certificación ISO/TS 17582:2014, entre los que están a la Oficina Nacional de Procesos Electorales del Perú, el Consejo Nacional Electoral del Ecuador y la Junta Central Electoral de la República Dominicana (Organización de los Estados Americanos, 2016).

El Consejo Nacional Electoral ha obtenido la certificación ISO/TS 17582:2014, sin embargo la elaboración de las Políticas de Seguridad de la Información que son parte de este trabajo no forman parte, ni de forma parcial, de la certificación ISO/TS17582:2014. En conjunto las normativas ISO/TS17582:2014 y la ISO/IEC 27001:2013 apuntalan y se alinean para el cumplimiento de las responsabilidades constitucionales del Consejo Nacional Electoral.

Hoy en día las tecnologías de la información y comunicación ofrecen accesibilidad, rapidez, flexibilidad, seguridad, solidez y automatización a los Organismo Electorales, lo que permite que se lleven a cabo los procesos electorales de manera más exitosa.

3 Justificación del Proyecto

En la actualidad la información de cualquier organización, más aún de los organismos electorales, ha sido reconocida como un activo valioso y a medida que los sistemas de información apoyan cada vez más a los procesos de misión crítica se requiere contar con estrategias de alto nivel, que permitan el control y administración efectiva de los datos. Las instituciones, los sistemas y red de información enfrentan amenazas de seguridad que incluyen entre otras: el fraude por computador, espionaje, sabotaje, vandalismo, robo, etc. Las posibilidades de daño y pérdida de información por código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes, ya sean estos ataques de origen externo así como de origen interno de las instituciones. Por lo que se hace imperiosa la necesidad de alinear los procesos de seguridad a normas internacionales que permitan la mitigación de estas amenazas.

El Consejo Nacional Electoral del Ecuador, se encuentra en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) el cual servirá para ayudar al cumplimiento de las atribuciones constitucionales que posee dicha función del Estado Ecuatoriano. Por lo que es indispensable la creación de Políticas de Seguridad de la Información que permitan ser la base del establecimiento del SGSI. La falta de estas políticas hace que no exista un control coordinado, seguimiento y administración del uso, acceso y/o modificación de la información que administra el Consejo Nacional Electoral.

4 Objetivos

4.1 Objetivos Generales

Elaborar las Políticas de Seguridad de la Información para el Consejo Nacional Electoral del Ecuador

4.2 Objetivos Específicos

- Evaluar el estado actual de controles y procesos de gestión de seguridad de la Información en base al estándar ISO/IEC 27001:2013.
- Identificar y evaluar los riesgos a los que estaría expuesta la información institucional como resultado de las brechas observadas en la evaluación de controles y procesos de gestión de seguridad, en base al estándar internacional ISO/IEC 27001:2013.
- Elaborar las Políticas de Seguridad de la Información previas a su aprobación por parte del Consejo Nacional Electoral del Ecuador.

4.3 Alcance

Generar las Políticas de Seguridad de la Información para el Consejo Nacional Electoral utilizando el método científico, las cuales estarán basadas en el estándar internacional ISO/IEC 27001:2013. Estas políticas se convierten en la base para la implantación de los controles, procedimientos y estándares para la elaboración de procesos y procedimientos para labores electorales y no electorales. Este trabajo no incluye la aprobación, puesta en operación y evaluación posterior a la puesta en ejecución de las Políticas de Seguridad de la Información en el Consejo Nacional Electoral del Ecuador.

5 Implementación de sistemas de Seguridad de la Información en organismos electorales.

La gestión de entidades electorales a través de un sistema de Seguridad de la Información, permitirá que se tenga una mejor percepción de la ciudadanía de transparencia y confianza. Los sistemas de gestión de la Seguridad de la Información no son de exclusivo uso de la industria ni de las iniciativas privadas, en la siguiente tabla se muestran los países que han obtenido una certificación ISO/IEC 27001 así como los entes electorales de los países se encuentran en un proceso de implementación de la normativa ISO/TS 17582:2014 *"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"*, estos dos sistemas de calidad presentan una oportunidad de incluir en los procesos de elección popular los niveles de calidad que la ciudadanía requiere.

Según el estudio de implementación de sistemas de calidad realizado por José Magdiel Martínez Quiroga (Martínez Quiroga, 2015) y por lo indicado por la Organización de Estados Americanos (Organización de los Estados Americanos, 2016) se muestran en la Tabla 4 los siguientes avances de implementación:

Tabla 4 Organismos electorales con certificaciones o en proceso de certificar ISO 9001:2008 y en ISO/TS 17582:2014

País	Organismo Certificado	Norma	Fecha Original de Certificación	Organismo de Certificación	Alcance Certificado
México	Comisión Estatal Electoral Nuevo León	ISO 9001:2008	29 nov 2004	ABS Quality Evualuations, inc	• Planeación, dirección, organización y vigilancia para la ejecución de las elecciones en el Estado de Nuevo León. • Contribución a la cultura democrática en el Estado de Nuevo León. • Sistema de prerrogativas y fiscalización a los partidos políticos en el Estado de Nuevo León
Panamá	Tribunal Electoral de Panamá	ISO 9001:2008	Año 2010	ABS Quality Evaluations, Inc.	• Dirección de Informática: Diseño y Gestión de Soporte a Tecnología Informática • Dirección Nacional de Registro Civil: Provisión de Servicios de Registro Civil • Dirección Nacional de Cedulación: Servicios de Cedulación • Dirección Nacional de Organización Electoral: Provisión de Servicios Administrativos Electorales, incluyendo: Control de Registros de Adherentes a Partidos Políticos, Actualización de Residencia Electoral, Elaboración de Mapas Electorales y Distribución de Centros de Votación
México	Tribunal Electoral del Poder Judicial de la Federación	ISO 9001:2008	6 octubre 2010	ABS Quality Evaluations, Inc.	• Administración en la Recepción, Atención y Trámite de los Medios de Impugnación en la Sala Regional Monterrey y sus servicios de Soporte.
México	Tribunal Electoral del Poder Judicial de	ISO 9001:2008	Año 2012	American Trust Register, S.C.	• Administración en la Recepción Atención y Tramite de los Medios de Impugnación en la Sala

País	Organismo Certificado	Norma	Fecha Original de Certificación	Organismo de Certificación	Alcance Certificado
	la Federación				Superior
Perú	Jurado Nacional de Elecciones de Perú	ISO 9001:2008 ISO 27001:2013	Año 2011 y 2013		• Procesos de fiscalización, atención al ciudadano, educación cívica y formación cívica ciudadana y registro de organizaciones políticas y normatividad. • Proceso de apoyo de logística, recursos humanos y registros, estadística y desarrollo tecnológico.
Costa Rica	Tribunal Supremo de Elecciones	ISO 9001:2008	25 octubre 2013		• Procesos registrales civiles de inscripción de hechos vitales y actos jurídicos • Expedición de documentos de identidad. • Trámite de opción y naturalización y la emisión de padrón nacional electoral de acuerdo con estándares internacionales.
República Dominicana	Junta Central Electoral de la República Dominicana	ISO 9001:2008 e ISO/TS 17582:2014	Entre septiembre del 2013 y febrero del 2014		Registro Electoral y Cedulación; Reconocimiento de Partidos Políticos; Logística Electoral; Proceso de Votación; Escrutinio y Emisión de Boletines; Educación Electoral; Entrega de los Recursos Económicos del Estado a los Partidos – Recepción de Informes de Gastos de los Partidos y, Escuela nacional de Formación Electoral y Estado Civil (EFEC)
Ecuador	Consejo Nacional Electoral	ISO/TS 17582:2014 ISO 9001:2008	7 de julio del 2016		Registro electoral; registro de organizaciones políticas y candidatos; logística electoral; sufragio; votaciones y escrutinio, adjudicación de puestos; capacitación electoral; fiscalización y gasto electoral; Y derecho a la oposición (resolución de disputas.)

FUENTE: J. M. MARTÍNEZ QUIROGA, «IMPORTANCIA DE UN SISTEMA DE GESTIÓN DE LA CALIDAD EN UN ORGANISMO JUDICIAL ELECTORAL BASADO EN LA NORMA ISO9001:2008: ESTUDIO DE CASO,» (Martínez Quiroga, 2015) Y ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, «SECRETARÍA PARA EL FORTALECIMIENTO DE LA DEMOCRACIA (SFD),» (Organización de los Estados Americanos, 2016).
ELABORACIÓN: BADÍ QUINTEROS

Como se puede apreciar únicamente Perú ha obtenido la certificación ISO/IEC 27001 adicional a la normativa ISO/TS 17582.

6 Evaluar el estado actual de controles y procesos de gestión de seguridad de la Información en base al estándar ISO/IEC 27001:2013

Hoy en día la accesibilidad, rapidez, flexibilidad, seguridad, robustez y automatización que deben ofrecer la aplicación de las tecnologías de la información y comunicaciones en los Organismos Electorales, permiten que se lleven a cabo procesos electorales exitosos. En el caso del Consejo Nacional Electoral del Ecuador, la implantación de las nuevas tecnologías es una prioridad debido a su vital importancia para el cabal cumplimiento de sus funciones y objetivos estratégicos recopilados en los siguientes documentos:

Visión:

“Para el 2021, ser la institución Electoral referente a nivel regional por su autonomía, innovación en automatización del voto, transparencia, eficacia e inclusión en la organización y gestión de los procesos electorales, fortalecimiento del sistema político y la democracia en el Ecuador.” (Consejo Nacional Electoral, 2014)

Misión:

“Fortalecer la democracia en el Ecuador, garantizando los derechos políticos y la organización política de la ciudadanía, promoviendo el ejercicio de la democracia comunitaria y ejerciendo rectoría, planificación, regulación y control de los mecanismos de democracia directa y representativa.” (Consejo Nacional Electoral, 2014)

Pilares (extracto):

- Procesos transparentes.
- Soberanía electoral.
- Fortalecimiento institucional.

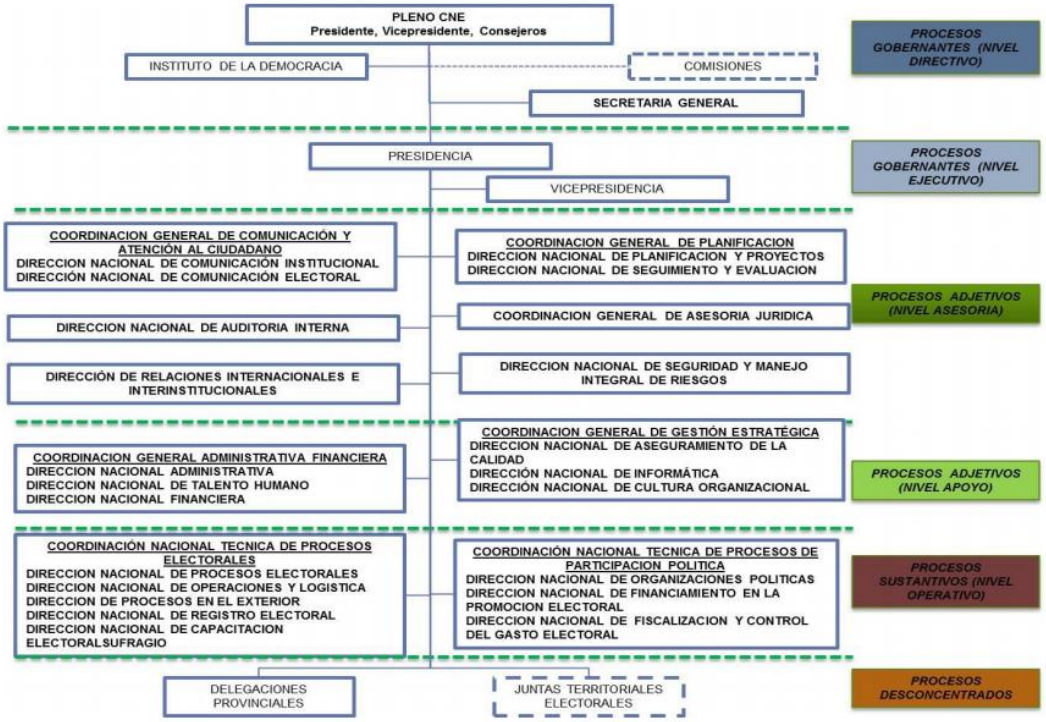
Objetivos Estratégicos (extracto) (Consejo Nacional Electoral, 2014):

- Incrementar la transparencia, eficiencia, confianza ciudadana.
- Incrementar la participación y organización política de la ciudadanía.
- Incrementar el ejercicio de los derechos de participación política.
- Incrementar la eficacia y eficiencia institucional.

El Consejo Nacional Electoral en el año 2014 elaboró el Plan Estratégico Institucional 2014-2017 (Consejo Nacional Electoral, 2014), en el cual se detallan los objetivos, políticas y estratégicas para poder alcanzar los Objetivos Estratégicos. En este documento el objetivo estratégico 4 indica: "Incrementar la eficacia y eficiencia institucional para brindar servicios de calidad", teniendo como política 4.2 "Brindar servicios de calidad y calidez a los usuarios internos externos", con la estrategia "i) Implementar un sistema de gestión integral de riesgos, para los procesos electorales, institucionales y de seguridad de la información." Por lo que la elaboración de las políticas de seguridad se alinea con los objetivos institucionales.

De los datos presentados anteriormente el Consejo Nacional Electoral identifica a la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que la institución establezca un marco que asegure que la información sea protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Estructura orgánica funcional:



6.1.1 Entendimiento

La fase de entendimiento permitió Identificar tres objetivos críticos de negocio de Consejo Nacional Electoral. Para cada uno de estos objetivos, se evaluó su nivel de dependencia respecto a la tecnología de información en aspectos como procesamiento de información, automatización de procesos e innovación del negocio. Los resultados de esta evaluación de dependencia se presentan en la Tabla 5:

Tabla 5 Dependencia de los Objetivos Críticos del Negocio en la Tecnología de Información

Objetivos críticos de negocio	Nivel de dependencia de Tecnología de Información
A. Organizar procesos electorales	**Alta**
B. Garantizar derechos democráticos	**Media**
C. Transparentar información confiable	**Alta**

FUENTE: BADÍ QUINTEROS
ELABORACIÓN: BADÍ QUINTEROS

Como se puede evidenciar el Consejo Nacional Electoral tiene una alta dependencia de las Tecnologías de Información para poder cumplir con sus responsabilidades.

6.1.2 Levantamiento

Con base en el estándar ISO 27001:2013 definido para el trabajo, se realizan entrevistas y sesiones de levantamiento de información con los principales responsables de las siguientes áreas:

- Tecnología de Información
- Seguridad Informática
- Infraestructura
- Desarrollo de aplicaciones
- Recursos Humanos
- Seguridad Física
- Verificación de Firmas (proceso de negocio)

6.1.3 Brechas observadas y análisis de principales riesgos

Con cada uno de los involucrados se confirma la existencia de políticas, controles o procesos de gestión relacionados a los Objetivos de Control de la norma ISO 27001:2013 para las siguientes Áreas y Dominios:

- Gobiernos de Seguridad
- Política de seguridad de la información
- Organización de la seguridad de la información
- Cumplimiento
- Seguridad de Datos
- Gestión de Activos
- Control de Accesos
- Criptografía
- Seguridad de procesos
- Seguridad ligada a Recursos Humanos
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Relaciones con proveedores
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio
- Seguridad operativa
- Seguridad en operaciones
- Seguridad en las telecomunicaciones
- Seguridad física y ambiental
- Gestión de incidentes de seguridad de la información

De acuerdo a la información recibida en las sesiones de levantamiento, determinamos la existencia o no de brechas totales o parciales respecto a los requisitos de la norma ISO 27001:2013 en el Consejo Nacional Electoral.

7 Identificación y evaluación de los riesgos a los que estaría expuesta la información institucional como resultado de las brechas observadas en la evaluación de controles y procesos de gestión de seguridad, en base al estándar internacional ISO/IEC 27001:2013

Se resumen las principales observaciones obtenidas durante el proceso de levantamiento de la situación actual. Asimismo se incluye el análisis de las principales consecuencias (impactos) que potencialmente podrían afectar al Consejo Nacional Electoral en caso de materializarse los riesgos a través de las debilidades de control observadas.

La evaluación de riesgos se realizó utilizando una escala cualitativa de tres niveles (alto, medio, bajo) para las dimensiones de impacto y probabilidad del riesgo, considerando la efectividad de los controles y procesos existentes observados (riesgos residuales a la fecha de evaluación), los cuales se muestran en la Tabla 6:

Tabla 6 Brechas e Impactos Potenciales

Áreas y Dominios de Gestión de Seguridad de la Información	Principales brechas observadas	Impactos potenciales
Gobierno de Seguridad		
Política de seguridad de la información	• No existe una Política de Seguridad de la información aprobada formalmente • Se observan versiones preliminares de políticas de uso de tecnología, aún pendientes de aprobación • No se observa una estructura aprobada de políticas alineada a las necesidades y objetivos de negocio	• Inconsistencia en aplicación de controles. • Costos elevados en medidas de seguridad ineficientes. • Falta de conciencia de seguridad institucional. • Elevada exposición a ataques internos y externos • Niveles de protección mínimos desconocidos • Escasa percepción del riesgo en la Alta Dirección • Impacto indirecto en confidencialidad e integridad **Impacto =** Medio **Probabilidad =** Media
Organización de la seguridad de la	• No se han definido formalmente los roles y responsabilidades de	• Dilución de responsabilidades

Áreas y Dominios de Gestión de Seguridad de la Información	Principales brechas observadas	Impactos potenciales
información	Seguridad de la Información • No se ha designado un CISO (Gerente de Seguridad de la Información) y actualmente algunas de estas funciones sólo recaen en un delegado del área de TI. • No existen actividades de contacto con grupos o entidades de investigación en temas de seguridad	• Retraso en toma de decisiones • Ejecución de actividades no autorizadas • Alta dependencia de personal específico • Costos elevados en medidas de seguridad ineficientes • Falta de conciencia de seguridad institucional. • Reactividad como única estrategia ante amenazas **Impacto =** Alto **Probabilidad =** Media
Cumplimiento	• No se han establecido mecanismos para la protección de propiedad intelectual.	• Exposición ante organismos reguladores • Multas y daño a la imagen institucional • Nivel real de efectividad de seguridad desconocido **Impacto =** Medio **Probabilidad =** Baja
Seguridad de Datos		
Gestión de Activos	• No se han llevado a cabo esfuerzos de clasificación de información. • No existen procedimientos seguros para la gestión, eliminación y retiro de medios removibles que podrían contener información confidencial	• Costos elevados en medidas de seguridad ineficientes. **Impacto =** Medio **Probabilidad =** Media
Control de Accesos	• Existen mecanismos de control para las cuentas con acceso privilegiado tanto en áreas de negocio como en Tecnología, pero requieren alinearse y juntarse en una sola política.	• Elevada exposición a ataques internos y externos • Impacto directo en confidencialidad, integridad, disponibilidad • Deterioro significativo de la imagen institucional **Impacto =** Alto **Probabilidad =** Alta

Áreas y Dominios de Gestión de Seguridad de la Información	Principales brechas observadas	Impactos potenciales
Criptografía	• No se observan procesos ni herramientas de encriptación de información sensible.	• Exposición ante organismos reguladores • Multas y daño a la imagen institucional • Impacto indirecto en confidencialidad • Fuga de información **Impacto =** Alto **Probabilidad =** Alta
Seguridad de procesos		
Seguridad ligada a Recursos Humanos	• Si bien existen procesos formales para las fase de contratación y retiro de empleados y su respectiva relación con la asignación y revocación de accesos, no se observa una estructura de perfiles, funciones y responsabilidades que permita asegurar la adecuada asignación de niveles de acceso al personal.	• Elevada exposición a ataques internos • Ejecución de actividades no autorizadas • Impacto indirecto en confidencialidad, integridad **Impacto =** Bajo **Probabilidad =** Baja
Adquisición, desarrollo y mantenimiento de los sistemas de información	• Los requerimientos para desarrollo de aplicaciones incluyen una sección explícita y formal de seguridad de la información, pero que necesita alinearse a las Políticas de Seguridad de la Información. • En general, los objetivos de control de este dominio son cubiertos a través de esfuerzos específicos del área, aunque no se logran observar mecanismos formales que aseguren su aplicación homogénea y alineada a los objetivos de negocio.	• Exposición moderada a ataques internos • Inyección de programas no autorizados • Impacto indirecto en integridad, disponibilidad • Exposición moderada a fuga de información, alteración no autorizada de datos, colusión y fraude • Deterioro significativo de la imagen institucional **Impacto =** Alto **Probabilidad =** Baja
Relaciones con proveedores	• Se poseen controles de requerimientos de seguridad para proveedores de servicios críticos (ISP, Telecom), pero necesitan estar	• Exposición moderada a ataques externos • Sobrecostos e ineficiencia de

Áreas y Dominios de Gestión de Seguridad de la Información	Principales brechas observadas	Impactos potenciales
	alineados a las Políticas de Seguridad de la Información	contratos • Impacto indirecto en disponibilidad **Impacto** = Bajo **Probabilidad** = Baja
Aspectos de seguridad de la información en la gestión de la continuidad del negocio	• Si bien los procesos electorales cuentan con un plan de seguridad específico que incluye aspectos como redundancia y alta disponibilidad, La operación diaria fuera de los procesos electorales no cuenta con las mismas estrategias de continuidad que aseguren la disponibilidad de otros procesos críticos de negocio.	• Impacto directo en integridad, disponibilidad • Elevada exposición a pérdida de información e interrupción de actividades de negocio • Deterioro significativo de la imagen institucional **Impacto** = Alto **Probabilidad** = Baja
Seguridad operativa		
Seguridad física y ambiental	• Quedan pendientes de definición e implementación las políticas y controles de equipo desatendido y escritorios limpios. • En general, se observa un nivel intermedio o superior de cumplimiento de los objetivos de control de este dominio, debido principalmente a las políticas de seguridad física impulsadas por la Dirección de Seguridad Integral.	• Impacto directo en integridad, disponibilidad • Exposición moderada a pérdida de información e interrupción de actividades de negocio • Deterioro significativo de la imagen institucional **Impacto** = Alto **Probabilidad** = Baja
Seguridad en operaciones	• Se observa que existen procesos operativos documentados y formales. • Existen procesos formales y consistentes de control de software malicioso, respaldo de información, registro de eventos, protección del registro de eventos, registro de actividades de cuentas privilegiadas, instalación de software no autorizado y gestión de vulnerabilidades técnicas. • Estas normas deberán estas alineadas a las Políticas de	• Ejecución de actividades no autorizadas • Costos elevados en medidas de seguridad ineficientes • Impacto directo en integridad, disponibilidad • Deterioro significativo de la imagen institucional **Impacto** = Alto **Probabilidad** = Alta

Áreas y Dominios de Gestión de Seguridad de la Información	Principales brechas observadas	Impactos potenciales
	Seguridad de la Información	
Seguridad en las telecomunicaciones	• Existen mecanismos de separación de redes de telecomunicaciones, se observa una aplicación media de controles de seguridad en redes.	• Impacto directo en confidencialidad, integridad, disponibilidad • Elevada exposición a fuga y robo de información, alteración no autorizada de datos, interrupción de servicios • Deterioro de la imagen institucional **Impacto =** Medio **Probabilidad =** Alta
Gestión de incidentes de seguridad de la información	• Se observan procesos de identificación, reporte y gestión de incidentes de seguridad. Las responsabilidades sobre la gestión de incidentes no están definidas ni asignadas formalmente.	• Impacto indirecto en integridad, disponibilidad • Exposición ante organismos reguladores, multas • Deterioro de la imagen institucional **Impacto =** Medio **Probabilidad =** Alta

FUENTE: BADÍ QUINTEROS
ELABORACIÓN: BADÍ QUINTEROS

8 Ventajas de aplicación de la normativa ISO 27001 en procesos electorales

Para poder tener una aplicación más coherente de la normativa ISO27001:2013 a organismos electorales es necesario realizar una comparación con la normativa ISO17582 y evidenciar las ventajas existentes las cuales se muestran en la tabla 7:

Tabla 7 Ventajas al combinar las normativas ISO 17582 e ISO 27001

Dominio/Control	Procesos Electorales según ISO/TS 17582:2014	Beneficio

ISO/IEC 27001:2013	Registro Electoral	Registro de organizaciones políticas y de candidatos	Logística Electoral	Emisión del voto	Recuento de votos y declaración de resultados	Capacitación electoral	Fiscalización del financiamiento de campañas electorales	Resolución de conflictos electorales	
A.5 Políticas de seguridad de la Información / A.5.1 Dirección Administrativa de la seguridad de la información	X	X	X	X	X	X	X	X	La aplicación de PSI[4] dentro de organismos electorales permite tener un marco de referencia para la gestión de los Activos de Información además de mostrar dirección y soporte administrativo para la gestión de la seguridad de la información
A.6 Aspectos organizativos de la información de seguridad / A.6.1.5 Seguridad de la Información en la Gestión de Proyectos.	X	X	X	X	X	X	X	X	Al tener en cuenta las PSI en la gestión de los proyectos que los organismos electorales se plantean se asegurarán que el manejo de la seguridad de la información será en función a las directrices planteadas.
A.7 Seguridad ligada a los recursos humanos / A.7.1.2 Términos y condiciones de contratación.	X	X	X	X	X	X	X	X	Todos los actores de manipulación, acceso, custodia, entre otros, de la información de los organismos electorales deben tener conocimiento de las PSI de tal forma que tengan un compromiso de cumplimiento. Además se debe asegurar que todos los actores hayan firmado los acuerdos de confidencialidad necesarios para el manejo de la información.
A.8 Gestión de Activos / A.8.2.1 Directrices de Clasificación.	X	X			X		X	X	La clasificación de la información permite tratar a los medios de transporte de esta información en función a su categorización y criticidad, en algunos casos esta categorización y criticidad puede estar delimitada por legislación existen, tal como en el caso del Ecuador con la LOTAIP[5]
A.8 Gestión de Activos / A.8.2.2 Etiquetado y manipulado de la Información.	X	X	X		X		X	X	Este control permite que los activos de información tengan el tratamiento necesario durante los procesos eleccionarios. Definiendo los responsables, custodios, propietarios, entre otros. También define los procesos de cadena de custodia de la información.
A.8 Gestión de Activos / A.8.3.1 Gestión de medios removibles.	X	X	X	X	X	X	X	X	Esta política evita que los activos de información almacenados en medios digitales sean extraídos de

[4] Políticas de Seguridad de la Información
[5] Ley Orgánica de Transparencia y Acceso a la Información Pública

Dominio/Control ISO/IEC 27001:2013	Procesos Electorales según ISO/TS 17582:2014								Beneficio
	Registro Electoral	Registro de organizaciones políticas y de candidatos	Logística Electoral	Emisión del voto	Recuento de votos y declaración de resultados	Capacitación electoral	Fiscalización del financiamiento de campañas electorales	Resolución de conflictos electorales	
									los organismos electorales de forma inapropiada o por personal no autorizado, evitando de esta forma fuga de información categorizada.
A.9 Control de Acceso / A.9.1 Requerimientos del negocio con respecto al control de acceso	X	X	X	X	X	X	X	X	Los organismos electorales deben definir de manera clara cuales van a ser las políticas de gestión de usuarios, de tal forma que puedan tenerse las herramientas para tener la trazabilidad de las autorizaciones para dicha gestión. De tal forma que los usuarios y usuarios tengan acceso a la red y a los servicios para los que expresamente han sido autorizados a utilizar.
A.9 Control de Acceso / A.9.2 Administración de acceso de los usuarios.	X	X	X	X	X	X	X	X	Estos procesos permiten tener una gestión eficiente y oportuna de los usuarios de tal forma que se eviten acceso no autorizados. Esto incluye el control de los sistemas de administradores de base de datos, registros, entre otros.
A.9 Control de Acceso / A.9.4 Control de acceso a sistemas y aplicaciones.	X	X	X	X	X	X	X	X	Los procesos de control de acceso a sistemas y aplicaciones permiten tener las evidencias necesarias para generar la trazabilidad de acceso y uso de las herramientas informáticas
A.10 Cifrado / A.10.1.1 Política en el uso de controles criptográficos	X	X	X	X	X	X	X	X	Según la clasificación de la información se definirán cuáles son los elementos que deberán tener sistemas de encriptación dentro de su ciclo de vida documental.
A.11 Seguridad física y de entorno / A.11.1 Áreas seguras	X	X	X	X	X	X	X	X	Las definición de áreas seguras permite evitar que exista personal no autorizado tenga acceso de manera física a los activos de la información.
A.12 Seguridad en la Operación / A.12.3 Copias de seguridad de la información	X	X	X	X	X		X	X	Permite tener una forma de almacenar y recuperar información en caso de una falla casual o provocada

Dominio/Control ISO/IEC 27001:2013	Procesos Electorales según ISO/TS 17582:2014								Beneficio
	Registro Electoral	Registro de organizaciones políticas y de candidatos	Logística Electoral	Emisión del voto	Recuento de votos y declaración de resultados	Capacitación electoral	Fiscalización del financiamiento de campañas electorales	Resolución de conflictos electorales	
A.13 Seguridad en las Comunicaciones / A.13.1 Gestión de la seguridad en las redes	X	X	X	X	X	X	X	X	Permite evitar que existan intromisiones a la red desde donde se puedan vulnerar la confiabilidad, disponibilidad y integridad de la información que atraviesan las redes de comunicaciones.
A.13 Seguridad en las Comunicaciones / A.13.2 Intercambio de información con partes externas	X	X			X		X	X	Permite establecer parámetros claros y definidos sobre la distribución de información y las responsabilidades que las partes externas obligadas a tener sobre el manejo de dicha información.
A.14 Adquisición, desarrollo y Mantenimiento de los sistemas de información / A.14.1 Requisitos de seguridad de los sistemas de información	X	X	X	X	X	X	X	X	Evitará que se produzca fuga de información de los sistemas que gestionarán los procesos electorales de tal forma de evitar el bloqueo e intromisión a los sistemas.
A.15 Relación con proveedores / A.15.1 Seguridad de la Información en las relaciones con proveedores					X				Todos los proveedores de servicios deberán conocer las PSI y entender su rol en el manejo y/o uso de la información a la cual acceden.
A.16 Gestión de Incidentes / A.16.1 Gestión de incidentes de seguridad de la información y mejoras	X	X	X	X	X	X	X	X	Tener procedimientos autorizados los cuales permitan tener una gestión eficiente de los incidentes de seguridad de la información.
A.17 Aspectos de la Seguridad de la Información en la Gestión de la Continuidad del Negocio / A.17.2 Redundancias	X	X	X	X	X	X	X	X	Proveer a los organismos electorales los mecanismos de aseguramiento de los servicios de tal manera de mantener la continuidad sobre todo en todas las fases de los procesos eleccionarios.[6]

FUENTE: BADÍ QUINTEROS

ELABORACIÓN: BADÍ QUINTEROS

[6] Las fases son: Pre-electoral, electoral y post-electoral

9 Políticas de Seguridad de la Información para el Consejo Nacional Electoral del Ecuador

A continuación se transcribe las Políticas de Seguridad de la Información elaboradas por el Ing. Badí Quinteros, las cuales fueron presentadas al Comité de Seguridad de la Información para su aprobación.

9.1 Introducción

Este documento recopila las Políticas de Seguridad de la Información definidas para el Consejo Nacional Electoral.

Las políticas expresadas en este documento son base para la generación de normas y procedimientos de cada una de las Coordinaciones Nacionales, Direcciones y Delegaciones Nacionales, para de tal forma garantizar la seguridad de la Información en el Consejo Nacional Electoral.

La implementación de nuevos proyectos, compra o elaboración de herramientas de software y/o hardware que involucre gestión de información deben cumplir con las políticas definidas en este documento, con el objeto de proteger la información.

El Consejo Nacional Electoral define que para la gestión de seguridad de la información utilizará las normas internacionales ISO/IEC de la serie 27000, la presente Política de Seguridad de la información fue elaborada con base en la norma internacional ISO/IEC 27001:2013, el Consejo Nacional Electoral formaliza su compromiso con el proceso de gestión de la información, que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de la información generada.

Con la divulgación de este documento se busca que todos los servidores, servidoras y el personal externo a la institución que prestan servicios en el Consejo Nacional Electoral, conozcan el marco normativo para que de forma individual y colectiva, brinden apoyo para la administración, utilización, cuidado, protección y disponibilidad de la información con niveles adecuados de seguridad.

Este documento permite establecer políticas sobre las cuales se debe direccionar el desarrollo de la seguridad de la información del Consejo Nacional Electoral y los principios de actuación de todo el personal que tenga acceso o responsabilidades sobre la información en esta entidad.

9.2 Objetivo General

Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información institucional relevante, con el objeto de asegurar continuidad

operacional de los procesos y servicios que desarrolla en el Consejo Nacional Electoral, mediante el resguardo de los activos de información asociados a los procesos críticos del negocio y su soporte.

9.3 Objetivo Específico

Establecer un marco de referencia para la generación e implementación de las normas y procedimientos referidos a los derechos, responsabilidades y obligaciones aplicables a todas las personas que laboran o ejecutan tareas en el Consejo Nacional Electoral en relación con los activos de información a los cuales tienen acceso con ocasión de su quehacer en el Consejo.

9.4 Alcance

Este documento se aplica a todos los servidores, servidoras y personal externo que preste servicios en el Consejo Nacional Electoral tanto en la matriz como en las Delegaciones Provinciales, Instituto de la Democracia, Organismos Electorales Desconcentrados y todos los demás usuarios que tengan acceso a los activos de información que posee el Consejo Nacional Electoral.

Cada Coordinación Nacional y/o Dirección deberá elaborar normativas según el ámbito de sus competencias para el cumplimiento de las Políticas de Seguridad de la Información, las cuales deberán ser revisadas y validadas por el Comité de Seguridad de la Información o su Delegado.

Las Políticas de Seguridad de la Información serán revisadas y/o actualizadas en períodos cíclicos de un año a menos que las circunstancias o eventos de seguridad requieran lo contrario.

El Oficial de Seguridad de la Información será el responsable de elaborar auditorías de cumplimiento de las Políticas de Seguridad de la Información en donde se definirán las brechas existentes, y en conjunto con cada una de las Coordinaciones Nacionales y/o Delegaciones Provinciales establecerán los cronogramas correspondientes de tal forma de solventar las no conformidades encontradas.

9.5 Roles y Responsabilidades

Comité de Seguridad de la Información: El Rol del Comité de Seguridad de la Información fue determinado en la resolución No. 130-P-JPPB-CNE-2015 del 26 de octubre del 2015 entre las cuales se mencionan:

a) Definir y mantener la política y normas institucionales particulares en materia de seguridad de la información y gestionar su aprobación
b) Monitorear cambios significativos de los riesgos que afecten a los recursos de información frente a las amenazas más importantes

c) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad
d) Aprobar las principales iniciativas para incrementar la seguridad de la información de acuerdo a las competencias y responsabilidades asignadas a cada área
e) Aprobar y acordar metodologías y procesos específicos, relativos a la seguridad de la información
f) Evaluar y coordinar la implementación de controles específicos de la información
g) Promover la difusión y apoyo a la seguridad de la información dentro de la Institución
h) Gestionar la provisión permanente de recursos económicos, tecnológicos y humanos para la gestión de la seguridad de la información
i) Velar por la aplicación de las normas de seguridad de la información

Oficial de Seguridad de la Información: El Rol del Oficial de Seguridad de la Información fue determinado en la resolución No. 130-P-JPPB-CNE-2015 del 26 de octubre del 2015 entre las cuales se mencionan:

a) Definir procedimientos para el control de cambios a los procesos operativos, sistemas e instalaciones, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
b) Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
c) Controlar los mecanismos de distribución y difusión de información dentro y fuera de la Institución.
d) Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso, garantizar la seguridad de los datos y los servicios conectados a las redes de la Institución.
e) Desarrollar procedimientos adecuados de concienciación de usuarios en materia de seguridad, controles de acceso a los sistemas y administración de cambios.
f) Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos.

Coordinaciones Nacionales/Direcciones: Es responsabilidad de las Coordinaciones Nacionales/Direcciones con respecto a la Seguridad de la Información:

a) Elaborar las normativas, procesos y/o procedimientos necesarios para la aplicabilidad de las Políticas de Seguridad de la Información en función de

sus competencias, las cuales serán revisadas por el Comité de Seguridad de la Información o su delegado.

b) Velar por el cumplimiento de las Políticas de la Seguridad de la Información dentro de sus competencias
c) Asegurarse que los servidores, servidoras y el personal externo de la Institución que brinda sus servicios en el Consejo Nacional Electoral que laboran dentro de su Coordinación/Dirección han sido capacitados y entienden sus responsabilidades del cumplimiento de las Políticas de Seguridad de la Información.

Dirección Nacional de Tecnologías de la Información y Comunicación: Es responsabilidad de la Dirección Nacional de Tecnologías de la Información y Comunicación con respecto a la Seguridad de la Información además de las ya establecidas en Coordinaciones Nacionales/Direcciones las siguientes:

a) Ser el custodio de toda la información digital generada por el Consejo Nacional Electoral, las excepciones a esta responsabilidad las determinará el Consejo de Seguridad de la Información.
b) Coordinar con los responsables de la información los procesos de mantenimiento preventivo y correctivo que impliquen una afectación al servicio.

Dirección Nacional de Talento Humano: Es responsabilidad de la Dirección Nacional de Talento Humano con respecto a la Seguridad de la Información además de las ya establecidas en Coordinaciones Nacionales/Direcciones las siguientes:

a) Capacitar a los servidores, servidoras y al personal externo de la Institución que brinda sus servicios en el Consejo Nacional Electoral en las Políticas de Seguridad de la Información.

Servidores, servidoras y personal externo a la Institución: Es responsabilidad de los servidores, servidoras y del personal externo de la Institución que brinde servicios en el Consejo Nacional Electoral las siguientes:

a) Conocer y aplicar las Políticas de la Seguridad de la Información en función a sus competencias.

9.6 Políticas de Seguridad de la Información

Tabla 8 Políticas de Seguridad de la Información

#	**Descripción**
A.5 Políticas de Seguridad de la Información	

#	Descripción
Las Políticas de Seguridad de la información son el marco de referencia de generación de normativas, procesos y/o procedimientos de cada una de las coordinaciones adjetivas y sustantivas, Direcciones y Delegaciones Nacionales del Consejo Nacional Electoral.	
A.5.1 Políticas de la Dirección Administrativa de la seguridad de la información Las Políticas de Seguridad de la Información tienen como objetivo principal establecer de forma clara las líneas de actuación y manifiestan tanto su apoyo como compromiso a la seguridad de la información, esta política deberá estar dentro de un proceso de mejoramiento continuo.	
1	El Comité de Seguridad de la Información debe demostrar su compromiso con la seguridad por medio de la aprobación de las políticas, normas y demás lineamientos que desee establecer la institución. Las Políticas de Seguridad de la información serán revisadas y/o actualizadas en períodos cíclicos de un año, a menos que las circunstancias o eventos de seguridad requieran lo contrario.
2	Bajo ninguna circunstancia los servidores y servidoras de la Institución, utilizarán los recursos informáticos para realizar actividades contrarias a la normativa interna de la Institución o legislación aplicable para el efecto.
3	Los equipos informáticos, equipos de comunicaciones de propiedad del Consejo Nacional Electoral, se utilizarán únicamente para actividades laborales que estén relacionadas con las funciones que cada servidor o servidora desempeña.
4	La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.
5	El Oficial de Seguridad de la Información tiene la responsabilidad de incluir dentro del plan anual de auditorías la verificación del cumplimiento de las políticas de Seguridad de la Información y normativas generadas por las diferentes Coordinaciones Nacionales y/o Direcciones que usen como base las Políticas de Seguridad de la Información y que se encuentren aprobadas.
6	El Consejo Nacional Electoral es el propietario de toda la información que se genere, modifique, actualice, adquiera, entre otros. El Comité de Seguridad de la Información designará a los custodios o responsables de la Información de las diferentes áreas de la entidad.
A.6 Políticas de los aspectos Organizacionales de la información de seguridad El Consejo Nacional Electoral por intermedio del Comité de Seguridad de la Información establecerá de forma clara la administración de la Seguridad de la Información, como parte fundamental de los objetivos y actividades.	
A.6.1 Políticas de la Organización Interna de la Seguridad de la Información El Consejo Nacional Electoral por intermedio del Comité de Seguridad de la Información deberá definir las responsabilidades de los diferentes actores con respecto a la Seguridad de la Información.	
7	El Comité de Seguridad de la información es el responsable de la definición del marco de referencia de la administración de la gestión de la seguridad, de tal forma que controle la implementación y la operación de la seguridad de la información del Consejo Nacional Electoral.
8	El Comité de Seguridad de la Información deberá distribuir tareas a las áreas de responsabilidad ante posibles conflictos de interés de manejo de la Información, con el fin de reducir las oportunidades de una modificación no autorizada y/o no intencionada, o el de un mal uso de los activos que manejen información de la organización.

#	Descripción
9	El Oficial de Seguridad de la Información deberá mantener una comunicación apropiada con grupos o foros de seguridad especializados, asociaciones profesionales y entes externos cuando los eventos de seguridad de la Información así lo requieran, según las directrices del Comité de Seguridad de la Información.
10	Todos los proyectos nuevos o mejoras en los proyectos existentes deberán cumplir las políticas y normativas de la Seguridad de la Información. Se deberá incluir en todos los proyectos nuevos o mejoras a proyectos existentes que afecten directamente a los activos que manejan información, una sección en la que se definan de forma explícita el o los mecanismos por el cual se cumplen las políticas de Seguridad de la Información.
11	Todos los servidores y servidoras del Consejo Nacional Electoral deben cumplir y velar por el cumplimiento de las Políticas de Seguridad de la Información en el ámbito de sus competencias.
A.6.2 Políticas de Dispositivos móviles y teletrabajo El Consejo Nacional Electoral deberá definir los procesos y procedimientos necesarios para el uso de dispositivos móviles y de teletrabajo de los servidores y servidoras que laboran para la institución.	
12	La Dirección Nacional de Tecnologías de la Información y Comunicación proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos inteligentes y tabletas, entre otros) institucionales. Así mismo, velará porque los servidores y servidoras hagan un uso responsable de los servicios y equipos proporcionados por la entidad.
13	Los Dispositivos móviles entregados por el Consejo Nacional Electoral son expresamente para facilitar el desarrollo de actividades laborales. Su uso estará sujeto a monitoreo y debe estar relacionado con las actividades del área a la cual ha sido asignado.
14	Se autoriza el uso de dispositivos móviles personales para el acceso a sitios públicos o de acceso público del Consejo Nacional Electoral. Se prohíbe el uso de dispositivos móviles y/o fijos de propiedad de los servidores para acceder a información crítica del Consejo Nacional Electoral, cualquier excepción a esta normativa la deberá aprobar el Comité de Seguridad de la Información o su delegado.
15	El Comité de Seguridad de la Información establecerá las circunstancias y requisitos para el uso de conexiones remotas a la plataforma tecnológica de la institución; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura. Se deberá delimitar el acceso de los usuarios, de acuerdo con las labores desempeñadas. La Dirección Nacional de Tecnologías de la Información y Comunicación determinará los mecanismos de seguridad, periodicidad, procesos de gestión de usuarios, entre otros de los usuarios remotos.
16	Si por necesidad laboral un servidor o servidora debe recibir el correo institucional en su dispositivo móvil personal, deberá hacerlo siguiendo un estricto control en la información que mantiene, toda información crítica que le llegue por este medio deberá ser almacenada usando métodos de encriptación y al menos una clave de desbloqueo en el dispositivo; o, en su defecto la información crítica deberá ser borrada. Será responsabilidad del servidor si se produce fuga de información por este medio.
A.7Políticas de seguridad ligada a los recursos humanos El Consejo Nacional Electoral deberá elaborar la normativa, procesos y/o procedimientos necesarios para que todos los servidores, servidoras y personal externo que preste servicios en el Consejo Nacional Electoral tanto en la matriz como en las Delegaciones Provinciales, Instituto de la Democracia, los Organismos Electorales Desconcentrados y todos los demás usuarios que	

#	Descripción
tengan acceso a los activos de información que posee el Consejo Nacional Electoral sean capacitados desde su ingreso y en forma continua, cualquiera que sea su actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.	
A.7.1 Políticas antes de la contratación El Consejo Nacional Electoral deberá contemplar medidas para seleccionar adecuadamente el personal necesario, especialmente para los trabajos sensibles.	
17	La Dirección Nacional de Talento Humano debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en Consejo Nacional Electoral, antes de su vinculación definitiva.
18	Cada Coordinador, Director y Jefe de Oficina debe verificar la existencia de "Acuerdos y/o Cláusulas de Confidencialidad" y de la documentación de "Aceptación de Políticas de Seguridad de la Información" para el personal externo a la Institución, que esté prestando sus servicios al Consejo Nacional Electoral, antes de otorgar acceso a la información del Consejo Nacional Electoral.
19	Los servidores, servidoras y el personal externo a la Institución que realice labores en o para el Consejo Nacional Electoral, debe firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información, antes de que se le otorgue acceso a las instalaciones y a la plataforma tecnológica.
A.7.2 Políticas durante el tiempo de contratación El Consejo Nacional Electoral deberá tomar las medidas necesarias para que existan procesos permanentes de capacitación y de seguimiento de aplicabilidad de las Políticas de Seguridad de la Información al personal que tiene acceso a los activos de información, tales como documentos, archivos, entre otros.	
20	El Comité de Seguridad de la Información debe promover la importancia de la seguridad de la información entre los servidores y servidoras del Consejo Nacional Electoral y el personal externo a la Institución que esté prestando sus servicios al Consejo Nacional Electoral, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.
21	La Dirección Nacional de Talento Humano será la responsable de realizar las inducciones necesarias y llevar un registro de capacitación a todos los servidores, servidoras y personal externo que preste servicios Consejo Nacional Electoral en cuanto a las Políticas de Seguridad de la Información.
22	El Comité de Seguridad de la Información debe enmarcar en el proceso disciplinario existente, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.
A.7.3 Políticas de terminación o cambio de contratación El Comité de Seguridad de la Información o su delegado deberán elaborar las políticas que sean necesarias para evitar que exista pérdida, destrucción y/o manipulación intencionada o no de los activos de la información durante la desvinculación de personal.	
A.8 Políticas de gestión de activos El Comité de Seguridad de la Información o su delegado deberán elaborar la normativa necesaria para que pueda tener un conocimiento preciso sobre los activos que posee como parte importante de la gestión de riesgos. Los activos a considerar son: Recursos de información, tales como bases de datos, archivos, documentación de sistemas, manuales de usuario, licencias de uso, entre otros. Activos físicos, tales como equipos informáticos, equipos de comunicaciones, medios magnéticos de almacenamiento, entre otros.	

#	Descripción
A.8.1 Políticas de responsabilidad de activos El Comité de Seguridad de la Información o su delegado deberán definir la responsabilidad que tiene el personal que utiliza los activos de información con respecto a los activos que posee y la normativa de la gestión que brinda con respecto a los activos que tiene.	
23	La Dirección Nacional de Tecnologías de la Información y Comunicación es quien custodia los activos de información correspondientes a la plataforma tecnológica del Consejo Nacional Electoral y, en consecuencia, debe asegurar su apropiada operación y administración.
24	La Dirección Nacional de Tecnologías de la Información y Comunicación es el área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, está prohibido a los servidores de la Institución emitir cualquier disposición respecto a los recursos tecnológicos de la Institución.
25	Los custodios de los activos de información deben ser conscientes que los recursos de procesamiento de información de la institución, se encuentran sujetos a auditorías por parte del Oficial de Seguridad y a revisiones de cumplimiento por parte de la Dirección Nacional de Seguridad y Manejo Integral de Riesgos.
26	Todos los derechos de autor de un software, hojas de cálculo, archivos PDF o tipo de documentos, macros, base de datos, entre otros, junto con su respectiva documentación, creados por los servidores y/o servidoras en ejercicio de sus actividades laborales, son de absoluta exclusividad del Consejo Nacional Electoral.
27	Todos los servidores y servidoras del Consejo Nacional Electoral que tengan asignado un equipo informático, estarán conscientes que los datos que se crean y/o modifican en todos los sistemas, aplicaciones y cualquier otro medio de procesamiento electrónico sea disco duro interno o externo, memoria flash, entre otros durante el desarrollo normal de sus actividades laborales, son propiedad de la Institución. Todos los servidores y servidoras del Consejo Nacional Electoral a quienes se haya entregado claves de acceso de sitios externos o que sean administradores de estos sitios tales como redes sociales institucionales, sitios de proveedores, entre otros y que hayan realizado cambios en las credenciales de acceso deberán notificar de estos cambios en las 48 horas posteriores al cambio a las Direcciones Nacionales, coordinaciones o Direcciones nacionales correspondientes quienes son los custodios de esta información. Ningún servidor o servidora podrá hacer uso inadecuado de las claves de acceso de sitios externos.
28	La Dirección Nacional de Tecnologías de la Información y Comunicación debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones del Consejo Nacional Electoral.
A.8.2 Políticas de clasificación de la Información El Consejo Nacional Electoral definirá una clasificación de la información a fin de indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento.	
29	El Comité de Seguridad de la Información debe recomendar al señor Presidente del Consejo Nacional Electoral los niveles de clasificación de la información para su aprobación y aplicación.
30	El Comité de Seguridad de la Información deberá desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización.
31	El Comité de Seguridad de la Información o su delegado deberán desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.

#	Descripción
A.8.3 Política de manejo de medios electrónicos El Consejo Nacional Electoral deberá emitir normativas que precautelen el buen uso de medios electrónicos de almacenamiento de información.	
32	El Comité de Seguridad de la Información deberá emitir políticas para proteger los medios electrónicos que contienen información contra acceso no autorizado, mal uso o destrucción durante el transporte fuera de los límites físicos de la organización.
33	La Dirección Nacional de Tecnologías de la Información y Comunicación debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la institución, de acuerdo con los lineamientos y condiciones establecidas.
34	La Dirección Nacional de Tecnologías de la Información y Comunicación debe elaborar políticas para la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.
35	Todos los documentos que sean publicados y/o entregados de forma electrónica deberán ser en formatos de no edición y en el caso de entrega se adjuntará información adicional que permita reconocer la alteración posterior del documento, además toda publicación y/o entrega de información deberá cumplir las normativas de imagen institucional y legales vigentes. Las excepciones a esta política las tomará el Comité de Seguridad de la Información.
A.9 Políticas de Control de Acceso El Comité de Seguridad de la Información deberá implementar las normativas, procesos y procedimientos necesarios para el control, gestión, seguimiento y trazabilidad del uso de los activos de información asignados a los usuarios.	
A.9.1 Políticas de Requerimientos del negocio con respecto al control de acceso El Comité de Seguridad de la Información deberá controlar los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades.	
36	La Dirección Nacional de Tecnologías de la Información y Comunicación deberá establecer, documentar y revisar una política de control de accesos a recursos tecnológicos de su competencia en base a las necesidades de seguridad del Consejo Nacional Electoral.
37	La Dirección Nacional de Tecnologías de la Información y Comunicación debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la institución, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.
38	La Dirección Nacional de Tecnologías de la Información y Comunicación debe asegurar que las redes de la institución cuenten con métodos de autenticación que eviten accesos no autorizados, y que mantengan un control de accesos al contenido en Internet. Las Direcciones Nacionales, Coordinaciones o Direcciones Nacionales a quienes se ha delegado la responsabilidad de la creación de cuentas institucionales en sitios externos que no sean gestionados por el Consejo Nacional Electoral (ejemplo: redes sociales, sitios de proveedores de servicios entre otros) son las responsables de la custodia de los datos de acceso a estos sitios y entregará las credenciales de acceso, según un procedimiento establecido por ellos, a los servidores o servidoras que administrará estos sitios. En el caso de que este sitio externo maneje doble autenticación estas funcionalidades deben ser utilizadas de forma obligatoria. El uso de estos sitios externos es de total responsabilidad de los servidores y servidoras a quienes se han entregado las claves de acceso mediante el procedimiento establecido. La Dirección Nacional de Tecnologías de la Información y Comunicación elaborará un documento en el cual se realizarán sugerencias para la gestión de este tipo de credenciales de acceso a sitios externos.
39	No se podrán utilizar los recursos tecnológicos del Consejo Nacional Electoral, como un medio de participación, acceso y distribución de actividades o materiales que vayan en

#	Descripción
	contra de la ley o pongan en riesgo la confidencialidad e integridad de la información de la Institución.
40	Los servidores y servidoras del CNE son los únicos responsables de todas las actividades realizadas desde sus cuentas de acceso y buzones en relación al “Reglamento de uso de correo electrónico”.
A.9.2 Políticas de Administración del acceso de los usuarios El Comité de Seguridad de la Información deberá establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información. Los procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información. Se debería prestar especial atención a la necesidad de controlar la asignación de permisos de acceso con privilegios que se salten y anulen la eficacia de los controles del sistema.	
41	La Dirección Nacional de Tecnologías de la Información y Comunicación debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los servidores se desvinculan, tomen licencia, vacaciones, sean trasladados o cambian de cargo.
42	El Comité de Seguridad de la Información o su delegado será el encargado de elaborar procesos y/o procedimientos para la entrega de credenciales de acceso a terceros a la información del Consejo Nacional Electoral.
43	Cada servidor y servidora es responsable de la información y contenidos a los que accede y de aquella información que copia en los equipos del Consejo Nacional Electoral. Los usuarios del servicio de Internet del Consejo Nacional Electoral deben hacer uso del mismo en relación con las actividades laborales que así lo requieran de la Institución.
44	La Dirección Nacional de Tecnologías de la Información y Comunicación debe establecer los procedimientos para la gestión cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.
45	El Comité de Seguridad de la Información o su delegado será el encargado de elaborar procesos y/o procedimientos para las auditorias de los accesos de terceros a la información del Consejo Nacional Electoral.
A.9.3 Políticas de Responsabilidad de los usuarios El Consejo Nacional Electoral deberá implementar las medidas necesarias para el uso responsable de las contraseñas de acceso, la cooperación de los usuarios autorizados es esencial para una seguridad efectiva. Los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición.	
46	Las contraseñas de los servidores y servidoras no deben compartirse o revelarse a ninguna otra persona aparte del usuario autorizado, así que, si los usuarios necesitan compartir datos que se encuentran en el computador, entonces deben usar el correo electrónico, los directorios públicos en los servidores de red de área local y otros mecanismos. Se prohíbe el uso de sistemas de almacenamiento externos que no sean los aprobados por la Dirección Nacional de Tecnologías de la Información y Comunicación
A.9.4 Políticas de Control de acceso a sistemas y aplicaciones El Comité de Seguridad de la Información deberá elaborar las normas necesarias para que todos los medios de acceso a los activos de información sean controlados y físicamente protegidos. Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos, datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retiro o destrucción de activos no autorizadas.	

#	Descripción
47	La Dirección Nacional de Tecnologías de la Información y Comunicación deberá generar procedimientos para restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.
48	La Dirección Nacional de Tecnologías de la Información y Comunicación definirá cuando sea pertinente el acceso a los sistemas la utilización de procedimientos seguros de log-on (doble autenticación)
49	La Dirección Nacional de Tecnologías de la Información y Comunicación debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.
50	La Dirección Nacional de Tecnologías de la Información y Comunicación deberá elaborar procesos y procedimientos que restrinjan el acceso al código fuente de las aplicaciones software.
A.10 Políticas de Cifrado de la Información El Consejo Nacional Electoral deberá establecer normas, procesos y/o procedimiento para el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.	
A.10.1 Políticas de Controles criptográficos El Consejo Nacional Electoral deberá elaborar la normativa necesaria con el objetivo de proteger la confidencialidad, autenticidad o integridad de la información mediante la ayuda de técnicas criptográficas. Se deberán usar controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización o aquella información definida por el Comité de Seguridad de la Información o por los responsables de la información.	
51	La Dirección Nacional de Tecnologías de la Información y Comunicación deberá implementar de forma progresiva el uso de firmas digitales de tal forma de proporcionar un medio de protección de la autenticidad e integridad de los documentos electrónicos según la normativa legal vigente.
52	La Dirección de Informática, debe desarrollar y establecer estándares para la aplicación de controles criptográficos.
53	La Dirección Nacional de Tecnologías de la Información y Comunicación debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.
A.11 Políticas de Seguridad física y de entorno El Consejo Nacional Electoral debe elaborar normas, procesos y/o procedimientos que permitan minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización.	
A.11.1 Políticas de Áreas seguras El Consejo Nacional Electoral mediante el área que corresponda deberán elaborar las normas que eviten el acceso físico no autorizado, daño e interferencia con la información y las dependencias de la Institución.	
54	La Dirección Nacional de Tecnologías de la Información y Comunicación en coordinación con la Dirección Nacional de Seguridad Integral y Gestión de Riesgos, debe desarrollar y establecer un procedimiento para la protección de los equipos de áreas sensibles, para proteger su acceso de los demás servidores de la red de la empresa.

#	Descripción
55	La Dirección Nacional de Tecnologías de la Información y Comunicación debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas, entre otros. Estos sistemas se deben monitorear de manera permanente.
56	La Dirección Nacional de Seguridad y Manejo Integral de Riesgos debe identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos y/o controles, con el fin de proveer la seguridad física de las instalaciones de la institución.
57	La Dirección Nacional de Seguridad y Manejo Integral de Riesgos deberá elaborar los procesos necesarios para el control de acceso a áreas restringidas y debe certificar la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo y demás áreas de procesamiento de información. Deberá elaborar procesos y procedimientos que permitan diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.
58	La Dirección Nacional de Seguridad y Manejo Integral de Riesgos deberá elaborar procesos y procedimientos que permitan diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.
59	La Dirección Nacional de Tecnologías de la Información y Comunicación, en conjunto con la Dirección Nacional de Seguridad y manejo integral de riesgos debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.
A.11.2 Políticas de Equipamiento El Comité de la Seguridad de la Información o su delegado deben elaborar las normas, procesos y procedimientos para proteger los equipos, elementos de comunicación, elementos de transmisión, entre otros contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo.	
60	La Dirección Nacional de Tecnologías de la Información y Comunicación debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la institución.
61	Si por necesidad institucional algún equipo informático requiere ser movilizado fuera de la entidad, el servidor o servidora responsable del bien deberá tener autorización de su inmediato superior esta documentación deberá ser validada por el personal de la Dirección Nacional de Seguridad Integral. La emisión de esta autorización deberá tener un periodo de vigencia conforme la necesidad.
62	La Dirección Nacional de Seguridad y Manejo Integral de Riesgos debe elaborar procesos y/o procedimientos para velar la seguridad e integridad de los equipos informáticosdel Consejo Nacional Electoral fuera de las instalaciones.
63	La Dirección Nacional de Tecnologías de la Información y Comunicación debe autorizar el uso de periféricos o medios de almacenamiento en la plataforma tecnológica de la institución de acuerdo con el perfil del cargo del servidor solicitante.
64	La Dirección Nacional de Tecnologías de la Información y Comunicación deberá elaborar los procesos y procedimientos para asegurar de que los equipos no supervisados cuenten con la protección adecuada.
65	Los servidores, servidoras de la institución y el personal externo a la Institución, que esté prestando sus servicios al Consejo Nacional Electoral deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.

#	Descripción
A.12 Políticas de seguridad en la operación El Consejo Nacional Electoral debe implantar mecanismos de control y gestión del cuidado de los activos de la información durante los procesos operativos.	
A.12.1 Políticas de responsabilidades y procedimientos de operación El Consejo Nacional Electoral debe asegurar la operación correcta y segura de los medios de procesamiento de la información, mediante el desarrollo de los procedimientos de operación. Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información.	
66	La Dirección Nacional de Tecnologías de la Información y Comunicación a través de sus servidores y servidoras, debe generar, la documentación necesaria y la actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la institución, la cual incluye la gestión de cambios, entre otros.
67	La Dirección Nacional de Tecnologías de la Información y Comunicación debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y se haga un uso adecuado de ellos.
68	La Dirección Nacional de Tecnologías de la Información y Comunicación debe generar estándares de configuración segura para los equipos de cómputo de los servidores de la institución y configurar dichos equipos aplicando los estándares generados.
69	La Dirección Nacional de Tecnologías de la Información y Comunicación deberá mantener actualizado el catálogo de servicios tecnológicos de la Institución.
70	La Dirección Nacional de Tecnologías de la Información y Comunicación debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica.
71	La Dirección Nacional de Tecnologías de la Información y Comunicación debe establecer procesos, procedimientos y controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
A.12.2 Políticas de protección contra código malicioso El Comité de Seguridad de la Información debe elaborar normas, procesos y/o procedimientos para la protección del software y los medios de procesamiento de la información ya que estos son vulnerables a la introducción de códigos maliciosos y se requiere tomar precauciones para evitar y detectar la introducción de códigos de programación maliciosos y códigos con capacidad de reproducción y distribución automática no autorizados para la protección de la integridad del software y de la información que sustentan.	
72	La Dirección Nacional de Tecnologías de la Información y Comunicación debe generar procesos y/o procedimientos a fin de asegurar que el Consejo Nacional Electoral cuente con un sistema antivirus, antispam, anti malware, firewall, entre otros, los cuales sean eficaces y eficientes para la protección de sus activos de información ante las amenazas existentes tanto en los equipos de core del Consejo Nacional Electoral así como en los terminales de usuario según el caso.
A.12.3 Política de respaldos El Comité de Seguridad de la Información debe establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo para realizar copias de seguridad y probar su puntual recuperación.	
73	La Dirección Nacional de Tecnologías de la Información y Comunicación debe elaborar procesos y procedimientos para garantizar las estrategias de generación, retención y rotación de las copias de respaldo de los activos información de la institución según la clasificación de documentos existente.
A.12.4 Políticas de monitoreo y registro de actividad	

#	Descripción
El Comité de Seguridad de la Información o su delegado deben monitorizar todos los sistemas que usan los activos de la información y los eventos de la seguridad de información registrados.	
74	El Oficial de Seguridad de la Información debe revisar periódicamente los registros de auditoria de la plataforma tecnológica y los sistemas de información con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo.
75	La Dirección Nacional de Tecnologías de la Información y Comunicación debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.
76	La Dirección Nacional de Tecnologías de la Información y Comunicación y/o el Oficial de Seguridad de la Información deben determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información del Consejo Nacional Electoral.
77	La Dirección Nacional de Tecnologías de la Información y Comunicación debe certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información del Consejo Nacional Electoral. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.
78	La Dirección Nacional de Tecnologías de la Información y Comunicación debe elaborar procesos y procedimientos para registrar las actividades del administrador y del operador del sistema y los registros asociados se deberán proteger y revisar de manera regular.
79	La Dirección Nacional de Tecnologías de la Información y Comunicación deberá sincronizar los relojes de todos los sistemas de procesamiento de información pertinentes dentro del Consejo Nacional Electoral en relación a una fuente de sincronización única de referencia.
A.12.5 Políticas de control del software en producción El Comité de Seguridad de la Información debe de minimizar los riesgos de alteración de los sistemas de información mediante controles de implementación de cambios, imponiendo el cumplimiento de procedimientos formales que garanticen que se cumplan los procedimientos de seguridad y control, respetando la división de funciones. Se deben verificar que los cambios sean gestionados por personal autorizado y en atención a los términos y condiciones que surjan de la licencia de uso. Se deberá efectuar un análisis de riesgos previo a los cambios en atención al posible impacto por situaciones adversas. Se deberá actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.	
80	La Dirección Nacional de Tecnologías de la Información y Comunicación debe establecer los procesos y/o procedimientos que indiquen las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la institución.
A.12.6 Políticas de gestión de la vulnerabilidad técnica El Comité de Seguridad de la Información o su delegado debe mantener sus sistemas informáticos dentro de la rutina de actualización de versiones, para que sus sistemas no queden fuera de soporte por el fabricante. Además debe implementar la forma de realizar auditorías o pruebas de sus sistemas de seguridad según las necesidades que se definan.	
81	La Dirección Nacional de Tecnologías de la Información y Comunicación debe establecer los procesos y/o procedimientos para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, estas pruebas deberán ser realizadas por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.
82	La Dirección Nacional de Tecnologías de la Información y Comunicación y/o el Oficial de Seguridad de la Información deben generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.
83	La Dirección Nacional de Tecnologías de la Información y Comunicación y/o el Oficial de Seguridad de la Información debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y

#	Descripción
	los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.
84	La Dirección Nacional de Tecnologías de la Información y Comunicación debe establecer los procesos y/o procedimientos para la instalación de aplicativos que no consten en el catálogo de servicios en los equipos del Consejo Nacional Electoral.
A.12.7 Políticas de consideraciones de las auditorías de los sistemas de información El Comité de Seguridad de la Información o su delegado deben maximizar la efectividad del proceso de auditoría de los sistemas de información y minimizar las intromisiones desde éste proceso. Durante las auditorías de los sistemas de información deben existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría.	
85	La Dirección Nacional de Tecnologías de la Información y Comunicación deberá planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.
A.13 Política de seguridad en las comunicaciones El Comité de Seguridad de la Información o su delegado deben asegurar la protección de la información que se comunica por redes de telecomunicaciones y la protección de la infraestructura de soporte.	
A.13.1 Políticas de gestión de la seguridad en las redes El Comité de Seguridad de la Información o su delegado deben controlar los accesos a servicios internos y externos conectados en red.	
86	La Dirección Nacional de Tecnologías de la Información y Comunicación debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red del Consejo Nacional Electoral.
87	La Dirección Nacional de Tecnologías de la Información y Comunicación debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la institución, acogiendo buenas prácticas de configuración segura.
88	La Dirección Nacional de Tecnologías de la Información y Comunicación debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
89	La Dirección Nacional de Tecnologías de la Información y Comunicación debe instalar protección entre las redes internas del Consejo Nacional Electoral y cualquier red externa, que esté fuera de la capacidad de control y administración de la institución.
A.13.2 Políticas de intercambio de información con partes externas El Consejo Nacional Electoral debe realizar los intercambios de información sobre la base de una política formal de intercambio, según los acuerdos de intercambio y cumplir con la legislación correspondiente. Se deberían establecer procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito.	
90	La Coordinación General de Asesoría Jurídica, debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre el Consejo Nacional Electoral y terceras partes incluyendo los compromisos adquiridos y las penalidades que se aplicarán por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por el Consejo Nacional Electoral a terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez que cumpla su cometido.
91	La Secretaría General de la Institución y las Áreas que correspondan deben certificar que todo envío de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por el Consejo Nacional Electoral, y que estos permitan ejecutar rastreo de las entregas.
92	Los custodios de los activos de información deben asegurar que los datos requeridos de

#	Descripción
	los beneficiarios sólo puedan ser entregado a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.
93	Los custodios de los activos de información deben asegurarse que el intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de Intercambio de Información del Consejo Nacional Electoral, así como del procedimiento de intercambio de información.
94	Los custodios o responsables de los activos de información deben velar porque la información del Consejo Nacional Electoral o de sus beneficiarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las clausulas relacionadas en los contratos, acuerdos de confidencialidad o acuerdos de intercambio establecidos.
95	La Dirección Nacional de Tecnologías de la Información y Comunicación debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
96	Los servidores y servidoras no deben utilizar el correo electrónico como medio para enviar o recibir información sensible de la institución o de sus beneficiarios.
97	El Comité de Seguridad de la Información y/o el Oficial de Seguridad de la Información bajo dirección del Comité, debe autorizar el establecimiento del vínculo de transmisión de información a terceros, para que posteriormente las áreas funcionales realicen las actividades de transmisión requeridas en cada caso.
98	Los terceros con quienes se intercambia información del Consejo Nacional Electoral deben dar manejo adecuado a la información recibida, en cumplimiento de las políticas de seguridad de la institución, de las condiciones contractuales establecidas y del procedimiento de intercambio de información.
99	No está permitido el intercambio no autorizado de información de propiedad del Consejo Nacional Electoral, de sus clientes y/o de sus servidores, con terceros.
100	El Comité de Seguridad de la Información debe establecer el procedimiento de intercambio de información con los diferentes terceros que hacen parte de la operación del Consejo Nacional Electoral, los cuales reciben o envían información de los beneficiarios de la institución, que contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de la misma.
101	La Dirección Nacional de Tecnologías de la Información y Comunicación debe diseñar y socializar las directrices técnicas para el uso de los servicios de correo electrónico.
102	La Dirección Nacional de Tecnologías de la Información y Comunicación debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.
103	La Secretaría General de la Institución debe acoger el procedimiento para el intercambio, de información (medios de almacenamiento y documentos) con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.
A.14 Políticas de adquisición, desarrollo y mantenimiento de los sistemas de información El Comité de Seguridad de la Información o su delegado deben asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información. Además debe definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan. Debe definir los métodos de protección de la información crítica o sensible.	

#	Descripción
A.14.1 Políticas de requisitos de seguridad de los sistemas de información El Comité de Seguridad de la Información o su delegado velarán que los requisitos de seguridad deben ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información.	
104	Es responsabilidad de los servidores y servidoras la conexión a redes que no presten la seguridad de acceso y autenticación adecuados.
105	La Dirección Nacional de Tecnologías de la Información y Comunicación deberá elaborar procesos y procedimientos que protejan la trasmisión de información por redes de telecomunicaciones de tal manera de proteger la información para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.
A.14.2 Políticas de seguridad en los procesos de desarrollo y soporte El Comité de Seguridad de la Información o su delegado elaborarán normativas, procesos y/o procedimientos para controlar estrictamente los entornos de desarrollo de proyectos y de soporte.	
106	La Dirección Nacional de Tecnologías de la Información y Comunicación debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.
107	La Dirección Nacional de Tecnologías de la Información y Comunicación debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información del Consejo Nacional Electoral.
108	La Dirección Nacional de Tecnologías de la Información y Comunicación deberá supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado.
109	Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.
110	La Dirección Nacional de Tecnologías de la Información y Comunicación debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
A.14.3 Política de datos de prueba El Comité de Seguridad de la Información o su delegado deben implementar normativas, procesos y/o procedimientos para evitar la exposición de datos sensibles en entornos de prueba.	
111	Es responsabilidad de la Dirección Nacional de Tecnologías de la Información y Comunicación desarrollar procesos y/o procedimientos para evitar la exposición de datos sensibles en entornos de prueba.
A.15 Políticas de relación con proveedores El Comité de Seguridad de la Información o su delegado deben implementar y mantener el nivel apropiado de seguridad de la información con los acuerdos de entrega de servicios de terceros. Se debe validar la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceros.	
A.15.1 Seguridad de la información en las relaciones con proveedores El Comité de Seguridad de la Información o su delegado velarán que la seguridad de la información del Consejo Nacional Electoral y las instalaciones de procesamiento de la información no sea reducida por la introducción de un servicio o producto externo.	
112	Los administradores de contratos deben divulgar las políticas, normas y procedimientos de

#	Descripción
	seguridad de la información del Consejo Nacional Electoral a la otra parte contractual, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de terceros se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.
113	El Oficial de Seguridad de la Información y la Coordinación General de Asesoría Jurídica deben generar un modelo base para los acuerdos de niveles de servicio y requisitos de seguridad de la información, con los que deben cumplir contratistas o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.
114	La Dirección Nacional de Tecnologías de la Información y Comunicación debe establecer procesos y procedimientos que garanticen condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los proveedores de servicios.
115	La coordinación de correspondencia debe evaluar y aprobar los accesos a la información de la institución requeridos por terceros.
116	La Dirección Nacional de Tecnologías de la Información y Comunicación será la responsable de que los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.
A.1.2 Políticas de gestión de la prestación del servicio por proveedores El Comité de Seguridad de la Información o su delegado deben verificar la implementación de acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se prestan cumplen con todos los requerimientos acordados con los terceros.	
117	La Dirección Nacional de Tecnologías de la Información y Comunicación y los Administradores de contratos, deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los proveedores de servicios.
118	Los Administradores de contrato, con el apoyo de la Dirección Nacional de Tecnologías de la Información y Comunicación, deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad estipulados en el contrato y monitoreando la aparición de nuevos riesgos.
A.16 Políticas de gestión de incidentes El Comité de Seguridad de la Información o su delegado deben garantizar que los eventos de seguridad de la información y las debilidades asociadas a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.	
A.16.1 Políticas de gestión de incidentes de seguridad de la información y mejoras El Comité de Seguridad de la Información o su delegado deben establecerse las responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información de una manera efectiva y una vez que hayan sido comunicados. Se debe aplicar un proceso de mejora continua en respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes en la seguridad de información.	
119	El Comité de Seguridad de la Información debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
120	Los servidores y servidoras tienen la responsabilidad de que en caso de conocer la pérdida o divulgación no autorizada de información, debe notificar al Oficial de Seguridad de la Información y a su jefe inmediato, para que se registre y se le dé el trámite necesario.
121	Los custodios de los activos de información deben informar al Oficial de Seguridad de la Información y a su jefe inmediato los incidentes de seguridad que identifiquen o que reconozcan su intento de materialización.

#	Descripción
122	El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
123	Es responsabilidad de los servidores y servidoras del Consejo Nacional Electoral reportar en el término de 48 horas, evento o incidente relacionado con la información y/o los recursos tecnológicos.
124	El Oficial de Seguridad de la información debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su recurrencia.
125	La Dirección Nacional de Tecnologías de la Información y Comunicación, con el apoyo del Oficial de Seguridad, deberá crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.
126	El Comité de Seguridad de la Información deberá definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.
A.17 Políticas de aspectos de la seguridad de la información en la gestión de la continuidad de negocio El Comité de Seguridad de la Información o su delegado deben preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.	
A.17.1 Políticas de continuidad de la seguridad de la información El Comité de Seguridad de la Información o su delegado deben determinar los requisitos de seguridad de la información al planificar la continuidad de los procesos de negocio y la recuperación ante desastres.	
127	La Dirección Nacional de Tecnologías de la Información y Comunicación, deben elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados. Se deberán elaborar planes de prueba de los procedimientos de contingencia, recuperación y retorno a la normalidad.
128	La Dirección Nacional de Tecnologías de la Información y Comunicación debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
129	La Dirección Nacional de Tecnologías de la Información y Comunicación y el Oficial de Seguridad de la Información deberán verificar regularmente los controles de continuidad de seguridad de la información establecida e implementada para poder garantizar su validez y eficacia ante situaciones adversas.
A.17.2 Políticas de redundancias El Comité de Seguridad de la Información o su delegado deben establecer las normativas que indiquen cuales son los activos de información que deben poseer redundancias según las necesidades y el momento.	
130	La Dirección Nacional de Tecnologías de la Información y Comunicación debe analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para la institución y la plataforma tecnológica que los apoya. Además se debe elaborar los procedimientos de prueba de las redundancias a fin de que la conmutación funcione de forma adecuada.
A.18 Políticas de cumplimiento El Comité de Seguridad de la Información o su delegado debe velar que se cumplan con todos los requisitos y normativas existentes en el diseño, operación y uso de los activos de la información.	
A.18.1 Políticas de cumplimiento de los requisitos legales y contractuales	

#	Descripción
El Comité de Seguridad de la Información o su delegado debe velar que el diseño, operación, uso y gestión de los sistemas de información cumplan con las normas legales y contractuales existentes.	
131	La Coordinación General de Asesoría Jurídica debe identificar, documentar y mantener actualizados los requisitos legales, o reglamentarios aplicables al Consejo Nacional Electoral y relacionados con seguridad de la información.
132	La Dirección Nacional de Tecnologías de la Información y Comunicación debe certificar que todo el software que se ejecuta en el Consejo Nacional Electoral y que está protegido por derechos de autor, se posea la licencia de uso o en su lugar sea software de libre distribución y uso.
133	La Dirección Nacional de Control de Calidad debe elaborar procesos y procedimientos para la protección contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales, de los documentos físicos.
134	La Dirección Nacional de Tecnologías de la Información y Comunicación debe elaborar procesos y procedimientos para la protección contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales, de los documentos digitales.
135	La Dirección Nacional de Tecnologías de la Información y Comunicación debe implantar los controles necesarios para proteger la información personal de los beneficiarios, servidores, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.
136	La Dirección Nacional de Tecnologías de la Información y Comunicación deberá utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.
A.18.2 Políticas de revisiones de la seguridad de la información El Comité de Seguridad de la Información o su delegado deben realizar revisiones regulares de la seguridad de los sistemas de información.	
137	Los Coordinadores y Directores deberán revisar regularmente el cumplimiento de las Políticas de Seguridad de la información dentro de su área de responsabilidad.
138	El Oficial de Seguridad deberá revisar regularmente los sistemas de información para verificar su cumplimiento con las políticas y normas de seguridad dispuestas.

FUENTE: CONSEJO NACIONAL ELECTORAL
ELABORACIÓN: BADÍ QUINTEROS

10 Resultados, Conclusiones y Recomendaciones

10.1 Resultados

El Consejo Nacional Electoral del Ecuador mediante resolución 019-P-JPPB-CNE-2016 del 4 de abril del 2016, indica que: “Autoriza la ejecución y aplicación en el Consejo Nacional Electoral y en las Delegaciones Provinciales Electorales las POLITICAS DE SEGURIDAD DE LA INFORMACIÓN expedidas y aprobadas por el Comité de Seguridad de la Información” (Presidencia del Consejo Nacional Electoral, 2016).

10.2 Conclusiones

Al alinearse el Consejo Nacional Electoral a normas internacionales de gestión de la seguridad de la Información como la ISO/IEC 27001:2013 genera impactos sustanciales respecto al aumento de la confianza en los procesos eleccionarios. La alineación de las normas ISO/TS 17582:2014 y de la ISO/IEC 27001:2013 de seguridad de la información, permitirá tener soluciones que cumplan con las exigencias actuales de la ciudadanía para los procesos electorales y las normas de seguridad de la información. Así mismo los procesos más transparentes permitirán mostrar a la ciudadanía que se ha guardado la confidencialidad, integridad y disponibilidad de la información como parte de los procesos eleccionarios, por lo cual la implementación de estas dos normativas debería ser analizada por los entes electorales para su aplicación.

Las normativas que establece la ISO/IEC 27001:2013 al control y acceso de los usuarios a la información, permiten realizar la trazabilidad de las acciones realizadas por parte de cualquier usuario, a fin de controlar, de manera adecuada, la manipulación de la información. Además permite evitar accesos no autorizados, tomando acciones necesarias para un seguimiento y gestión sobre los eventos de seguridad de la información. Una de las principales formas de seguimiento es la existencia de controles y documentos, que certifican la integridad de la información generada durante todas las fases del proceso electoral. La confidencialidad de la información se manifiesta cuando los organismos tienen la capacidad de clasificar su información y ponerla a disposición de los ciudadanos en el momento adecuado y requerido. Uno de los parámetros indispensables en todo proceso electoral es garantizar la disponibilidad de la información, considerando que en la actualidad casi la mayoría de la información se encuentra en medios digitales, los departamentos o áreas de tecnologías de la información deberán establecer planes de continuidad y de recuperación de desastres[7].

Con todo este conjunto de elementos los ciudadanos del Ecuador podrán incrementar, de manera significativa su percepción de confianza en los procesos eleccionarios, en donde se ha respetado su voluntad al elegir a sus mandatarios.

10.3 Recomendaciones para trabajos futuros

Como pasos posteriores a la aprobación de las Políticas de Seguridad de la Información en un organismo electoral, se tiene la inclusión de un Sistema de

[7] Este término hacer relación a la recuperación de servicios informáticos de una organización luego de haber ocurrido algún desastre.

Gestión de la Seguridad de la Información[8]. La implementación de un SGSI permitirá continuar con los pasos necesarios para que los organismos electorales puedan alcanzar los parámetros necesarios para obtener la certificación ISO 27001. Este es un proceso en el cual la normativa de gestión de la calidad ISO 17582, obtenida por el Consejo Nacional del Ecuador, es fundamental para que todos los procesos incluidos en las tareas electorales y no electorales puedan estar dentro de un marco de referencia internacional utilizando buenas prácticas en su operación.

Otro de las recomendaciones es la consideración por parte del Consejo Nacional Electoral de la normativa ISO/DIS 37001 Sistema de Gestión Anti Sobornos (International Organization for Standardization, 2016). Esta normativa ayudaría al Consejo Nacional Electoral a prevenir, detectar y abordar los posibles sobornos con lo que mejoraría aún más la transparencia que tendría ante la ciudadanía.

11 Referencias

Asamblea General de las Naciones Unidas. (10 de diciembre de 1948). *Naciones Unidas Derechos Humanos.* Recuperado el 7 de abril de 2016, de http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

Asamblea Nacional. (17 de octubre de 2012). *cne.gob.ec.* Recuperado el 09 de jun de 2016, de https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwj_9syZ1pvNAhWEtxQKHfaHDBYQFggaMAA&url=http%3A%2F%2Fcne.gob.ec%2Fes%2Fcomponent%2Ftags%2Ftag%2F76-codigo-de-la-democracia&usg=AFQjCNGYPRG9vJZGq44oE0qZmszV63WEAQ&sig2=klPc2k9IjoEy

Congreso de la Nación Paraguaya. (2001). *www.oas.org.* Recuperado el 09 de junio de 2016, de https://www.oas.org/es/sap/deco/moe/Paraguay2013/docs/CODIGO_ELECTORAL.pdf

Consejo Nacional Electoral. (22 de julio de 2010). *www.cne.gob.ve.* Recuperado el 10 de junio de 2016, de http://www.cne.gob.ve/web/normativa_electoral/elecciones/2010/parlamentarias/documentos/REGLAMENTO_4.pdf

Consejo Nacional Electoral. (2013). Reglamento Voto Electrónico. Quito: Consejo Nacional Electoral.

Consejo Nacional Electoral. (2014). *Plan Estratégico Institucional 2014-2017.* Quito, Pichincha, Ecusdor: Don Bosco Quito. doi:978-9942-07-796-7

Consejo Nacional Electoral. (s.f.). *http://www.cne.gob.ve/*. (Consejo Nacional Electoral) Recuperado el 10 de jun de 2016, de http://www.cne.gob.ve/web/ normativa_electoral/ley_organica_procesos_electorales/indice.php

Corte Electoral. (2 de abril de 2014). *aceproject.org.* Recuperado el 10 de junio de 2016, de https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwibuYy4kZ7NAhWJGR4KHTywBcoQFggmMAI&url=https%3A%2F%2Faceproject.org%2Fer

[8] Sistema SGSI

o-en%2Fregions%2Famericas%2FUY%2Furuguay-normativa-electoral-2012%2Fat_download%2Ffile&usg=AFQjCNEpLJ6AVjq

Decidamos. (Octubre de 2007). Recuperado el 10 de junio de 2016, de https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0ahUKEwi317PFgZ7NAhWJ1h4KHfnIDX8QFgg1MAQ&url=http%3A%2F%2Fwww.decidamos.org.py%2Fwww%2Fcomponent%2Fk2%2Fitem%2Fdownload%2F43_fafebb7618207d35333a4cc964e7ad43&usg=AFQjCNGi1AheO5NQe_abqq

Direccion Nacional Electoral. (2013). *www.electoral.gov.ar.* Recuperado el 9 de jun de 2016, de http://www.electoral.gov.ar/publicaciones/2015/folleto_residentes_en_el_exterior_BAJA.pdf

Dirección Nacional Electoral. (2013). *www.electoral.gov.ar.* Recuperado el 9 de jun de 2016, de http://www.electoral.gov.ar/pdf/manual_autoridades_paso_2013.pdf

EL PRESIDENTE DE LA REPUBLICA DE COLOMBIA. (23 de mayo de 2016). *www.secretariasenado.gov.co.* Recuperado el 09 de junio de 2016, de http://www.secretariasenado.gov.co/senado/basedoc/decreto_2241_1986.html

El Senado y la Cámara de Representantes de la República Oriental del Uruguay. (18 de junio de 1999). *www.corteelectoral.gub.uy.* Recuperado el 10 de junio de 2016, de https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwi3gu7TkJ7NAhWLKB4KHfOFC1oQFgggMAE&url=http%3A%2F%2Fwww.corteelectoral.gub.uy%2Fgxpsites%2Fagxppdwn.aspx%3F1%2C26%2C266%2CO%2CS%2C0%2C1040%253BS%253B1%253B42%2C&usg=AFQjCNH9AV1z7

Gobernador de la Provincia de Buenos Aires. (21 de agosto de 2003). *americo.usal.es.* Recuperado el 9 de junio de 2016, de http://americo.usal.es/oir/legislatina/leyesestados/Argentina/leyes_electorales_a/Buenos_Aires/1443_reglamen_voto_electronico.pdf

Guilles, A. (2011). Improving the quality of information security management systems with ISO27000. *The TQM Journal, 23*(4), 367-276. doi:10.1108/17542731111139455

International Organization for Standardization. (1997). *Friendship Among Equals.* Geneve, Switzerland: ISO. Recuperado el 1 de abril de 2016, de International Organization for Standardization: http://www.iso.org/iso/2012_friendship_among_equals.pdf

International Organization for Standardization. (2013). *ISO 27001:2013 Information technology - Security techniques - Information security management systems - Requirements.*

International Organization for Standardization. (20 de noviembre de 2014). ISO/TS 17852 Sistema 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.

International Organization for Standardization. (2016). *The Benefits of International Standards - ISO*. Recuperado el 07 de 04 de 2016, de http://www.iso.org/iso/home/standards/benefitsofstandards.htm

International Organization for Standardization. (04 de julio de 2016). *www.iso.org*. Obtenido de http://www.iso.org/iso/catalogue_detail?csnumber=65034

LA ASAMBLEA LEGISLATIVA PLURINACIONAL. (30 de junio de 2010). *pdba.georgetown.edu.* Recuperado el 9 de junio de 2016, de http://pdba.georgetown.edu/Electoral/Bolivia/Ley26-2010.pdf

López Neira, A., & Ruiz Spohr, J. (2016). *ISO 27000.ES*. Recuperado el 8 de abril de 2016, de http://www.iso27000.es/

Martínez Quiroga, J. (junio de 2015). Importancia de un Sistema de Gestión de la Calidad en un Organismo Judicial Electoral Basado en la norma ISO9001:2008: Estudio de Caso. *VinculaTegica*(1), 915-939. doi:ISSN: 2448-5101

Ministerio de Justicia. (7 de noviembre de 2012). *ar.vlex.com.* Recuperado el 9 de junio de 2016, de http://ar.vlex.com/vid/decreto-405902082

MINISTERIO DEL INTERIOR. (14 de abril de 1988). *www.leychile.cl.* Recuperado el 09 de junio de 2016, de https://www.leychile.cl/Navegar?idNorma=30082&idParte=0

MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA. (14 de diciembre de 2011). *www.leychile.cl.* Recuperado el 09 de junio de 2016, de https://www.leychile.cl/Navegar?idNorma=1034145&idParte=0

MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA. (31 de enero de 2012). Recuperado el 9 de junio de 2016, de https://www.leychile.cl/Navegar?idNorma=1035420&idParte=0

Oficina Nacional de Procesos Electorales. (17 de diciembre de 2010). *onpe.gob.pe.* Recuperado el 10 de junio de 2016, de https://www.web.onpe.gob.pe/modCompendio/html/procesos_electorales/reglamento_del_voto_electronico.html

Oficina Nacional de Procesos Electorales. (2016). *onpe.gob.pe.* Recuperado el 10 de jun de 2016, de https://www.web.onpe.gob.pe/nosotros/gestion-calidad/

Oficina Nacional de Procesos Electorales del Perú. (s.f.). *Observatorio del Voto-E en Latinoamérica.* Recuperado el 08 de junio de 2016, de www.voto-electronico.org: http://www.voto-electronico.org/

Organización de los Estados Americanos. (1 de abril de 2016). *Secretaría para el Fortalecimiento de la Democracia (SFD)*. (OEA, Editor) Recuperado el 1 de abril de 2016, de Organización de los Estados Americanos: http://www.oas.org/es/sap/deco/NormasISO.asp

Pozo Bahamonde, J. P. (2015). *Democracia en el Contexto Suramericano.* Quito, Pichincha, Ecuador: Instituto de la Democracia. doi:978-9942-20-573-5

Presidencia del Consejo Nacional Electoral. (04 de abril de 2016). Resolución No. 019-P-JPPB-CNE-2016. Quito, Pichincha, Ecuador. Recuperado el 13 de junio de 2016

Presidente de la República. (2013). *onpe.gob.pe.* Recuperado el 10 de junio de 2016, de https://www.web.onpe.gob.pe/modCompendio/html/procesos_electorales/ley_organica_titulo3.html

Protti Quesada, M. A. (junio de 2014). Sistema de gestión electoral: en busca de la mejora continua. *Revista Derecho Electoral*(17), 113-137. Recuperado el 1 de abril de 2016, de http://www.tse.go.cr/revista/art/17/protti_quesada.pdf

Secretaría General de la Comunidad Andina. (28 de junio de 2003). *Comunidad Andina.* doi:9972-787-08-7

Secretaría General de la Comunidad Andina. (2003 de junio de 28). *Comunidad Andina.* doi:9972-787-08-7

Tribunal Regional Eleitoral. (2016). *www.tre-pb.jus.br*. Recuperado el 09 de junio de 2016, de http://www.tre-pb.jus.br/eleicoes/seguranca/seguranca-do-processo-eleitoral

Tribunal Superior Eleitoral. (2016). *www.justicaeleitoral.jus.br.* Recuperado el 09 de jun de 2016, de http://www.justicaeleitoral.jus.br/arquivos/tse-resolucao-23-453-instrucao-53-935

Tribunal Superior Eleitoral. (2016). *www.tse.jus.br.* Recuperado el 9 de jun de 2016, de http://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/codigo_eleitoral/codigo-eleitoral-anotado-e-legislacao-complementar-12-edicao-atualizado.pdf

Tribunal Supremo Electoral. (2011). *tse.oep.org.bo.* Recuperado el 9 de junio de 2016, de https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwj57_KHx5vNAhUBmx4KHXh1CpEQFggaMAA&url=http%3A%2F%2Ftse.oep.org.bo%2Findex.php%2Fmarco-normativo%2Freglamentos%3Fdownload%3D71%3AREGLAMENTO%2520GENERAL%2520MUNICIPAL&usg=AFQjCNEJ

Unión de Naciones Suramericanas. (junio de 2011). *http://www.unasursg.org/.* Recuperado el 15 de abril de 2016, de http://www.unasursg.org/images/descargas/ESTATUTOS%20CONSEJOS%20MINISTERIALES%20SECTORIALES/ESTATUTO%20CONSEJO%20ELECTORAL%20UNASUR.pdf