UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL

ESCUELA DE FORMACIÓN PROFESIONAL DE INGENIERÍA DE SISTEMAS

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA EL JURADO ELECTORAL ESPECIAL LIMA OESTE 2014"

Tesis presentada por:

Bach. Javier LOPEZ JURADO

Para optar el Título Profesional de Ingeniero de Sistemas

AYACUCHO - PERÚ

2015

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA EL JURADO ELECTORAL ESPECIAL LIMA OESTE 2014".

RECOMENDADO : **29 DE DICIEMBRE DEL 2015**

APROBADO : **21 DE ABRIL DEL 2016**

MSc. Ing. CARLOS A. PRADO PRADO
PRESIDENTE

Ing. ELINAR CARRILLO RIVEROS
MIEMBRO

Ing. JUAN C. CARREÑO GAMARRA
MIEMBRO

Ing. JENNIFER PILLACA DE LA CRUZ
SECRETARIA DOCENTE (e)

Según el acuerdo constatado en el Acta, levantada el 21 de abril del 2016, en la Sustentación de Tesis presentado por el Bachiller en Ingeniería Informática Sr. Javier LÓPEZ JURADO, con la Tesis Titulado "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA EL JURADO ELECTORAL ESPECIAL LIMA OESTE 2014", fue calificado con la nota de QUINCE (15) por lo que se da la respectiva APROBACIÓN.

RECOMENDADO : 29 DE DICIEMBRE DEL 2015

APROBADO : 21 DE ABRIL DEL 2016

MSc. Ing. CARLOS A. PRADO PRADO
PRESIDENTE

Ing. ELINAR CARRILLO RIVEROS
MIEMBRO

Ing. JUAN C. CARREÑO GAMARRA
MIEMBRO

Ing. JENNIFER PILLACA DE LA CRUZ
SECRETARIA DOCENTE (e)

DEDICATORIA

A mis queridos padres y hermanos por ser ejemplos de perseverancia y constancia que lo caracterizan y que me ha infundado siempre, por el valor mostrado para salir adelante, por su constante apoyo para hacer realidad mis proyectos de vida.

AGRADECIMIENTOS:

En primer lugar agradecer a Dios por todas las bendiciones.

A la Universidad Nacional San Cristóbal de Huamanga.

A la Escuela Profesional Ingeniería Informática.

RESUMEN

El sistema de gestión de seguridad de información es un tema importante y urgente en las entidades públicas, existe la resolución donde aprueban el uso obligatorio de la norma técnica peruana NTP-ISO/IEC 27001:2008 esta norma cubre todo tipo de organizaciones, el cual permite la gestión adecuada de la seguridad de la información, el activo más importante para una organización es la información que enfrenta un enorme número de amenazas que podría provocar severas pérdidas para la institución, así como también daños a la reputación de la misma.

La presente investigación busca diseñar un sistema de gestión de seguridad de información según la NTP-ISO/IEC 27001:2008 en una entidad pública y que pueda servir en un futuro como referencia para la implementación de lo mismo.

En efecto se realizara reuniones con la alta dirección que permitirá definir el alcance y la política del SGSI en la institución, enfocado a los procesos críticos de dicha entidad, realizar entrevistas que permitan identificar los activos de información y identificar los activos críticos de la entidad, identificar las amenazas para cada activo de información. Luego se identificara y evaluara los riesgos a los cuales estaban sometidos y por último se elaborara el documento llamado Declaración de Aplicabilidad, considerando el ciclo de Deming que se constituye como una de las principales herramientas para lograr la mejora continua en las organizaciones o entidades.

INTRODUCCIÓN

La información es el principal activo de todas las organizaciones se pueden dar de muchas formas papeles impresos, almacenado electrónicamente, transmitida por correo, ilustrado por películas o hablada en películas.

En el ambiente competitivo de hoy, la información está constantemente bajo la amenaza de muchas fuentes que puede ser internas, externas, accidentales o maliciosas para la organización con el incremento de uso de nueva tecnología para almacenar, transmitir y recobrar información se han abierto canales para un gran número y variedad de amenazas.

En la actualidad en las entidades públicas, la información cobra también un valor importante, por la gran cantidad de información que gestiona es por eso que los órganos rectores del país demandan que las entidades públicas implementen un programa de gestión de seguridad de información. Por lo tanto tenemos al ONGEI (Oficina Nacional de Gobierno Electrónico e Informática) que es un organismo rector del sistema nacional de informática quien brinda información y asistencia técnica a las entidades Públicas para la implementación de un Sistema de Gestión de Seguridad de Información, responsable del desarrollo del Sistema Nacional de Informática y supervisar el cumplimiento de la normativa correspondiente.

El Jurado Electoral Especial como órgano administrativo-jurisdiccional es responsable de una gestión eficiente en cada proceso electoral, sea para elegir candidatos (presidente y vicepresidentes de la República, congresistas, alcaldes y regidores, entre otros), o elegir opciones a través de una consulta popular de revocatoria del mandato de autoridades o de referéndum (aprobación o no de un proyecto de ley). Dispone de información importante y valiosa para cada proceso electoral los cuales deben ser protegidos adecuadamente respetando su confidencialidad, integridad y disponibilidad el cual consta de los siguientes procesos operativos como son propaganda electoral, publicidad estatal, inscripción de listas, registrar actas digitalizadas y proclamar resultados.

INDICE

1.- CAPITULO I: GENERALIDADES

1.1.- INFORMACION GENERAL DE LA ORGANIZACIÓN

1.1.1.- HISTORIA.- Desde el nacimiento de la época republicana, no existió propiamente un verdadero órgano rector de las elecciones populares. Las normas de entonces señalaban la existencia de juntas o colegios electorales, inclusive se instituyó alguna vez un poder electoral, como órganos ejecutores de los procesos de elecciones. Pero, en la práctica, éstos fueron manejados principalmente por el Ejecutivo o el Legislativo.

No obstante, en esta etapa se dieron diversas normas electorales. Entre ellas, el Reglamento de Elecciones para el Congreso (1822), la Ley de Elecciones Municipales (1824), los Reglamentos de Elecciones de 1839 y 1849, la Ley de Elecciones de 1857 y 1861 y la Ley Orgánica de Elecciones (1892).

El siglo XX no trajo grandes cambios para los órganos electorales ni para el sistema de elecciones. El país afrontó varios procesos electorales con la misma tónica de antes, sin contar con un órgano electoral imparcial, independiente y autónomo, y con un electorado limitado únicamente al varón contribuyente al fisco.

Luego, se dictaron nuevas disposiciones como la Ley de Elecciones (1896), la *cual*, por primera vez, creó la Junta Electoral Nacional, organismo colegiado de 9 miembros, y las Juntas Electorales Departamentales, así como el Registro Electoral.

Otras leyes de esta etapa son la Ley N° 861 de Elecciones Políticas (1908), la Ley N° 1072 de Elecciones Municipales (1909), la Ley N° 1533 de Elecciones Políticas (1912) y la Ley Electoral (1912).Esta última norma determinó la directa participación de la Corte Suprema en la conducción de las elecciones, como las de 1913 y 1915.

En 1930, el comandante Luis Miguel Sánchez Cerro instauró una Junta de Gobierno Militar, en Lima. Pero los acontecimientos políticos de coyuntura hicieron que renunciara al cargo y posibilitara la instalación de una Junta Nacional de Gobierno presidida por David Samanez Ocampo y Sobrino, quien mediante Decreto Ley 7160, convocó a Elecciones Generales y creó el Jurado Nacional de Elecciones como máximo órgano rector de los procesos electorales, otorgándole una vida institucional autónoma, independiente y de naturaleza colegiada.

El primer Pleno del JNE, instalado el 22 de septiembre de 1931, estuvo presidido por el Dr. Ernesto Araujo Álvarez e integrado por los miembros Max González Olaechea, Leandro Pareja, Ricardo Rivadeneyra, Ernesto Flores, Humberto Garrido Lecca y Nicanor Hurtado. El primer Secretario General fue Eloy B. Espinoza.

La Constitución de 1993 fragmentó el Jurado en tres entes autónomos, separando de él al RENIEC y a la ONPE.

Hasta el año 2005, el JNE organizó, dirigió y fiscalizó treinta y uno (31) procesos electorales de carácter nacional, aparte de elecciones complementarias, consultas populares y revocatorias. Diecisiete (17) de ellos fueron elecciones políticas, que permitieron elegir doce (12) presidentes

constitucionales y otros tantos congresos nacionales. Diez (10) fueron comicios municipales, dos elecciones para congreso constituyente, un referéndum y un proceso de elecciones para gobiernos regionales.

El JNE cuenta con el primer museo a nivel mundial de temas electorales denominado Museo Electoral y de la Democracia creado en el año 2005 durante la presidencia de Enrique Javier Mendoza Ramírez siendo su primer director Miguel Arturo Seminario Ojeda bajo la curaduría del museólogo Juan Augusto Fernández en su edificio principal ubicado en Lima.

FUNCIONES:

Fiscaliza la legalidad del ejercicio del sufragio, de los procesos electorales, del referéndum y de otras consultas populares, garantizando así el respeto a la voluntad ciudadana, lo que en su momento le permite certificar los resultados electorales y otorgar las credenciales correspondientes al Presidente de la República, congresistas y autoridades regionales y locales.

1.1.2.- JURADO NACIONAL DE ELECCIONES EN LA ACTUALIDAD.-

El Jurado Nacional de Elecciones es un organismo constitucional autónomo del Estado Peruano. Tiene como finalidad fiscalizar la legalidad del ejercicio del sufragio, los procesos electorales y las consultas populares, garantizando el respeto a la voluntad ciudadana. En consecuencia es el órgano encargado de proclamar los resultados electorales y otorgar los reconocimientos o credenciales correspondientes a las autoridades electas. Así mismo tiene como función el dictar resoluciones de carácter general, para reglamentar y normar las disposiciones electorales.

Finalmente, el jurado revisa en grado de apelación las resoluciones expedidas en primera instancia por los Jurados Electorales Especiales y resuelve en definitiva las controversias sobre materia electoral. También decide en segunda y última instancia sobre los casos de vacancias declaradas por los Concejos Regionales y Municipales.

Es un órgano colegiado, cuyos cinco integrantes son elegidos por distintas entidades del Estado. El presidente es elegido por la Sala Plena de la Corte Suprema de Justicia, y los restante cuatro magistrados son designados por la Junta de Fiscales Supremos, por votación universal de los Abogados de Lima, y por los Decanos de Facultades de Derecho uno de las universidades públicas y otro de las privadas.

Dentro del Jurado Nacional de Elecciones se encuentra el Registro de Organizaciones Políticas, donde se mantienen inscritos los partidos políticos vigentes. Su sede se encuentra en la ciudad de Lima.

El actual presidente del Jurado Nacional de Elecciones es el Dr. Francisco Artemio Távara Córdova, Vocal y Ex Presidente de la Corte Suprema de Justicia de la República del Perú.

1.1.3.- JURADO ELECTORAL ESPECIAL.- Los Jurados Electorales especiales son órganos temporales creados para cada proceso electoral, conforme al artículo 13 de la Ley N.° 26859, Ley Orgánica de Elecciones, y al artículo 32 de la la Ley N.° 26486, Ley Orgánica del Jurado Nacional de Elecciones (LOJNE), y estos, para el cumplimiento de sus funciones, establecidas en el artículo 36 de la LOJNE, requieren de disposiciones conducentes a hacer más eficiente su gestión, en particular, y en general, para

mejorar la gestión de los procesos electorales.

El Jurado Electoral Especial es un órgano administrativo-jurisdiccional que se constituye por un tiempo determinado, con motivo de la convocatoria a un proceso electoral, sea para elegir candidatos (presidente y vicepresidentes de la República, congresistas, alcaldes y regidores, entre otros), o elegir opciones a través de una consulta popular de revocatoria del mandato de autoridades o de referéndum (aprobación o no de un proyecto de ley).

El Jurado Electoral Especial tiene las mismas atribuciones e impedimentos que los miembros del Pleno del Jurado Nacional de Elecciones, en la circunscripción para la cual se ha definido.

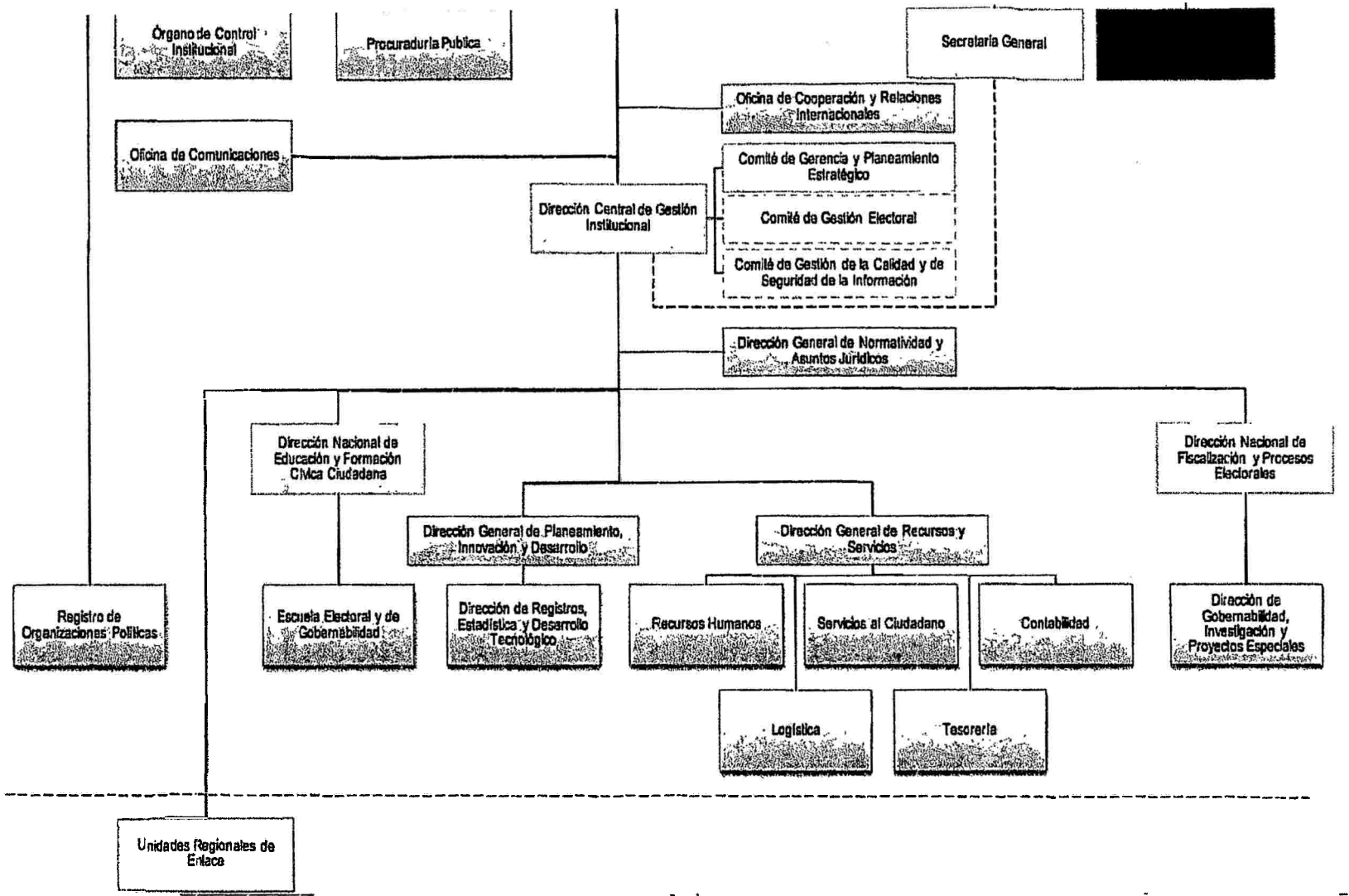

Grafico Nro. 1. Organigrama del JNE

1.1.4.- VISION, MISION Y VALORES

Visión

Ser el organismo rector del sistema democrático, reconocido en la región por su absoluta garantía de respeto de la voluntad popular.

Misión

Contribuir y garantizar la consolidación del sistema democrático y la gobernabilidad del país, a través de sus funciones constitucionales y legales.

Valores

- Identificación institucional.
- Integridad.
- Trabajo en equipo.
- Proactividad.
- Respeto.

Principios

- Imparcialidad.
- Confiabilidad.
- Transparencia.
- Calidad.
- Inclusión Social.

1.2.- IDENTIFICACION DEL PROBLEMA

Para identificar el problema nos basamos en la aplicación de las normas que indican una adecuada Gestión de la seguridad de la información, diseño e implementación de un sistema de gestión de seguridad de información y la importancia de la información dentro de las organizaciones en las empresas.

1.2.1.- IMPORTANCIA DE GESTION DE LA SEGURIDAD DE LA INFORMACION:

La necesidad de gestionar la seguridad de la información nace de un entorno cada vez más globalizado donde las empresas deben tomar decisiones rápidas y eficientes convirtiendo la información en uno de los activos más importantes dentro de las organizaciones llegando a tener una importancia estratégica para muchas de ellas ya que les permite mantener una ventaja competitiva frente a otras empresas.

Se confunde la seguridad de la información con la seguridad Informática podemos ver que la segunda está enmarcada por la primera ya que la seguridad informática ve aspectos de tecnologías de la información mientras que seguridad de información es un concepto más global, es un problema de negocios, no es un problema de tecnología.

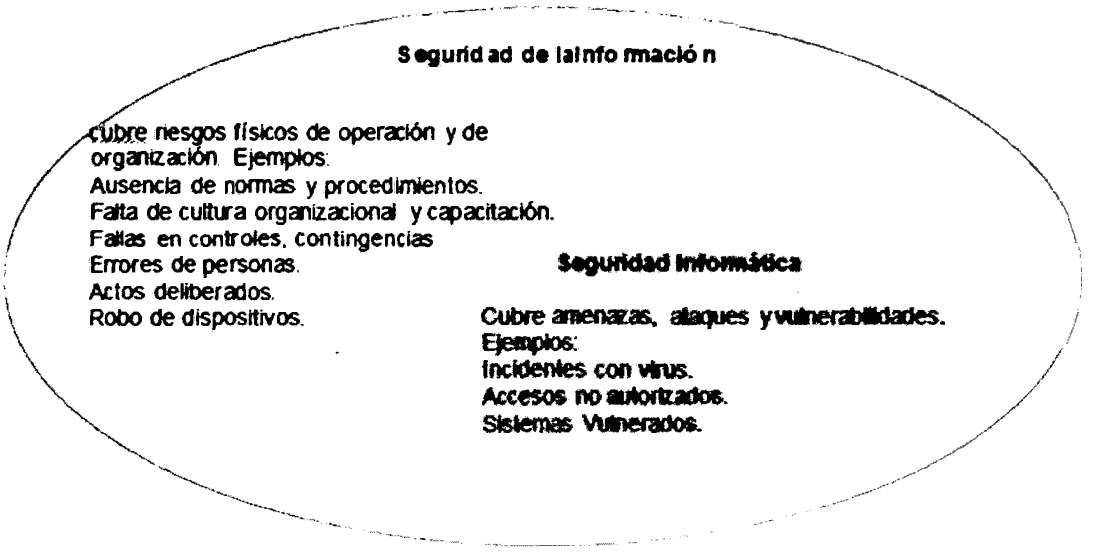

Grafico Nro. 2: Seguridad de Información y Seguridad Informática

Fuente: Elaboración Propia.

La seguridad de la información se encarga de la búsqueda de la preservación de la confidencialidad, integridad y disponibilidad de la información [NTP ISO/IEC 17799], es decir, buscar protegerla tanto de ataques físicos, tales como robos o incendios, como de ataques cibernéticos, tales como el aprovechar vulnerabilidades de los sistemas de información.

1.2.2.- NORMAS TECNICAS PERUANAS

En nuestro país, desde hace más de diez años, las políticas del gobierno han ido recomendando una adecuada gestión de la seguridad de la información con resoluciones ministeriales tales como la N° 224-2004-PCM en la que aprueban el uso obligatorio de la NTP ISO/IEC 17799:2004 en las entidades públicas referente a las buenas prácticas para gestionar la seguridad de la información [NTP ISO/IEC 17799].

Adicionalmente, el marco legal de nuestro país obliga a las entidades públicas, pertenecientes al Sistema Nacional de Informática, el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basándose en la norma técnica peruana (NTP) – ISO/IEC 27001:2008 mediante la resolución ministerial N° 129-2012-PCM emitida en mayo del 2012.

Ambas normas técnicas peruanas, la NTP ISO/IEC 27001 y la NTP ISO/IEC 17799, están basadas en la familia de normas ISO 27000 correspondiente a seguridad de la información. La primera, es el estándar principal de esta familia y menciona cuales son los requerimientos para desarrollar un sistema de gestión de seguridad de la información basándose en el ciclo de DEMING, o ciclo Plan – Do – Check - Act, una metodología cíclica muy usada en las normas ISO relacionadas a normas de gestión [NTP ISO/IEC 27001].

Como parte de esta norma, se presenta una lista de 133 controles, divididos en 11 módulos, para resguardar los activos de información de posibles riesgos que se encuentren en la organización. La explicación en detalle de cada uno de estos controles se puede ubicar en la NTP ISO/IEC 17799:2007, ya que es la hermana de la primera y está basada en la ISO/IEC 27002:2005.

Los sistemas de gestión, son estructuras probadas para la gestión y mejora continua de políticas, procedimientos y procesos [BSI, 2013]. Este sistema, en particular, busca establecer, implementar y mejorar la seguridad de la información en una determinada organización [NTP ISO/IEC 27001], y deberá ser implementado según un cronograma propuesto por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), organismo encargado de apoyar a las entidades públicas durante el proceso de implementación de la norma, el

cual, propone 5 fases para la implementación del SGSI, siendo muy similares a las fases propuestas en la norma técnica peruana, la cual a su vez se basa en el ciclo de DEMING.

La siguiente gráfica, véase Tabla N° 1 muestra un resumen del cronograma de implementación incremental de un SGSI en entidades públicas en comparación con el ciclo de DEMING, como se observa, las fases I y II de este cronograma están íntimamente relacionadas con la fase de Planeación de este ciclo, mientras que la fase III correspondiente al despliegue está ligada a la fase Do / Hacer, ya que se encarga de la implementación del SGSI en sí.

De igual forma, la fase de revisión, en ambos casos, hace referencia a la verificación de la correcta implementación y monitoreo del sistema, mientras que la fase de consolidación está ligada al último paso del ciclo de DEMING, ya que se encarga de implementar las mejoras y correcciones de lo detectado en la fase anterior.

IMPLEMENTACION NTP– ISO/IEC 27001:2008 RESOLUCION MINISTERIAL N° 129-2012-PCM			CICLO DEMING
FASE	NOMBRE	OBJETIVO	CICLO (PDCA)
I	ORGANIZACIÓN	Desarrollar las actividades principales para la dirección e inicio de la implementación del SGSI.	PLANEAR – PLAN
II	PLANIFICACION	Desarrollar las actividades de planificación requeridas por la norma de manera metodológica y en concordancia con la política y objetivos de SGSI dentro del alcance del mismo.	PLANEAR – PLAN
III	DESPLIEGUE	Desplazar las actividades de implementación del SGSI	HACER–DO
IV	REVISION	Realizar actividades de revisión del SGSI evidenciando el cumplimiento de los requisitos de la norma.	REVISAR – CHECK
V	CONSOLIDACION	Auditar e implementar las mejoras y correcciones del SGSI a fin de cumplir con los requisitos de la norma.	ACTUAR-ACT

Tabla Nro. 1: Comparación de la implementación incremental de la ONGEI y el ciclo de Deming

Fuente: Implementación Incremental de NTP ISO/IEC 27001:2008; Portal Oficial de la Oficina Nacional de Gobierno Electrónico e Informática. http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552

La resolución ministerial se publicó a finales de mayo del 2012 publicada en el diario "El Peruano" [RM-129-2012-PCM], en ella se mencionaban plazos máximos para cada fase además de empezar la primera Fase o Fase I a un plazo no mayor de 45 días de publicada la presente resolución tal como se puede observar en la tabla Nro. 2 los plazos máximos por fase.

Según este cronograma, las entidades públicas deben haber terminado la implementación de este sistema de gestión para el año 2014; sin embargo, se maneja muy poca información de los avances de las distintas entidades

públicas con respecto a estos temas, siendo la ONP e INDECOPI las únicas del sector público con una certificación internacional relacionada a seguridad de la información [INDECOPI; 2013; Noticias]. Una de las posibles causas de esta situación es que la norma indica que se debe hacer, más no, como se debe hacer.

Implementación incremental de NTP-ISO/IEC 27001:2008

Resolución Ministerial N° 129-2012-PCM

FASE	Nombre	Objetivo	Actividades Principales	Plazo máximo por fase
I	ORGANIZACIÓN	Desarrollar las actividades principales para la dirección e inicio de la implantación del SGSI.	• Obtener el apoyo institucional • Determinar el alcance del Sistema de Gestión de Seguridad de la Información • Determinar la declaración de Política de Seguridad de la Información y objetivos • Desarrollar documentos necesarios para la Fase II • Determinar criterios para la evaluación y aceptación de riesgos	Hasta 3 meses
II	PLANIFICACIÓN	Desarrollar las actividades de planificación requeridas por la norma de manera metodológica y en concordancia con la política y objetivos del SGSI dentro del alcance del mismo.	• Realizar evaluación de Riesgos • Conducir un análisis entre los riesgos identificados y las medidas correctivas existentes • Desarrollar un plan de tratamiento de riesgos • Desarrollar documentos necesarios para la Fase III • Desarrolla la declaración de Aplicabilidad	Hasta 4 meses
III	DESPLIEGUE	Desplegar las actividades de implementación del SGSI	• Elaborar el plan de trabajo priorizado • Desarrollar documentos y registros necesarios • Implementar los controles seleccionados	Hasta 12 meses
IV	REVISIÓN	Realizar actividades de revisión del SGSI evidenciando el cumplimiento de los requisitos de la norma	• Monitorear el desempeño del SGSI • Fortalecer la gestión de incidentes • Desarrollar documentos y registros necesarios • Desarrollar las actividades para evidenciar la mejora continua	Hasta 4 meses
V	CONSOLIDACIÓN	Auditar e implementar las mejoras y correcciones del SGSI a fin de cumplir con los requisitos de la norma.	• Auditar internamente el SGSI • Implementar las acciones correctivas • Implementar las acciones preventivas pertinentes • Desarrollar, corregir y mejorar documentación nueva o existente	Hasta 4 meses

FASE OPCIONAL:

VI	CERTIFICACIÓN		• Iniciar el proceso de certificación internacional en ISO/IEC 27001:2005 y obtener la certificación	No Aplica

Tabla Nro. 2: Plazos por fase para cumplir con la implementación del SGSI

Fuente: Portal Oficial de la Oficina Nacional de Gobierno Electrónico e Informática
http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552

1.2.3.- PROBLEMA GENERAL:

¿De qué manera el diseño de un Sistema de Gestión de Seguridad de Información en los Jurados Electorales Especiales mejora el servicio de calidad, incrementa la confianza de la población, transparencia y imagen en los procesos electorales?

1.2.4.- PROBLEMAS ESPECIFICOS:

- ¿De qué manera el Sistema De Gestión De Seguridad De Información mejora la calidad de servicio a la ciudadanía?

- ¿De qué manera el Sistema de gestión de Seguridad de Información mejora la confianza de la población en los procesos electorales?

- ¿De qué manera el Sistema de gestión de Seguridad de Información ayuda con la transparencia en los procesos electorales?

- ¿Cómo un Sistema de gestión de Seguridad de Información mejora la imagen institucional?

1.3.- OBJETIVOS

1.3.1.- OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de información para el JURADO ELECTORAL ESPECIAL según lo indicado por la NTP ISO/IEC 27001:2008 y la NTP-ISO/IEC 17999:2007 de seguridad de información con la finalidad de brindar garantía y confianza a la población.

1.3.2.- OBJETIVOS ESPECIFICOS.-

a.- Desarrollar un Sistema de Gestión de seguridad de Información elaborando documentos exigidas por la NTP ISO/IEC 27001 que sirvan como marco de referencia de seguridad de la información para la organización, para mejorar la calidad de servicio a la ciudadanía.

b.-Desarrollar un Sistema de Gestión de Seguridad de Información obteniendo la valoración de activos de información para conocer aquellos activos que son importantes para la organización y puedan ser objetos de un análisis de riesgos mejorando la confianza a la población.

c.- Desarrollar un Sistema de Gestión de Seguridad de Información realizando la evaluación y tratamiento de riesgos en los activos valiosos para la organización, donde se realizara un estudio para conocer los riesgos que representan una amenaza a estos, brindando transparencia en el proceso electoral.

d.- Desarrollar un Sistema de Gestión de Seguridad de Información obteniendo el documento de declaración de aplicabilidad que es importante para una auditoria de un SGSI, mejorando la imagen institucional.

1.4.- HIPOTESIS Y VARIABLES DE LA INVESTIGACION

1.4.1.- DEFINICION DE LA HIPOTESIS

Si diseñamos un Sistema de Gestión de Seguridad de Información para el jurado electoral especial entonces cumplimos con las regulaciones vigentes, apoyamos al proceso electoral brindando y garantizando la voluntad popular.

1.4.2.- DEFINICION DE LAS VARIABLES

1.4.2.1.- VARIABLE INDEPENDIENTE

Sistema de Gestión de Seguridad de Información

Indicadores VI

- Documentos de SGSI.

- Inventarios de activos.

- Documentación de tratamiento de riesgos.

- Documento de Aplicabilidad del SGSI.

1.4.2.2.- VARIABLE DEPENDIENTE

JURADO ELECTORAL ESPECIAL

Indicadores VD

- Calidad en servicio.

- Confianza de la Población.

- Transparencia del proceso electoral.

- Imagen institucional.

1.5.-METOLOGIA DE LA INVESTIGACION:

1.5.1.- TIPO DE INVESTIGACIÓN

Tipo de Investigación:

Aplicada

Es la utilización de los conocimientos en la práctica, para aplicarlos, en la mayoría de los casos, en provecho de la sociedad.

Nivel de Investigación:

Descriptivo

Conocida como la investigación estadística, describen los datos y este debe tener un impacto en las vidas de la gente que le rodea. Por ejemplo, la búsqueda de la enfermedad más frecuente que afecta a los niños de una ciudad. El lector de la investigación sabrá qué hacer para prevenir esta enfermedad, por lo tanto, más personas vivirán una vida sana.

Diseño: Investigación por Objetivo conforme al esquema siguiente

$$OG \left\{ \begin{array}{l} oe1\text{----------}cp1 \\ oe2\text{----------}cp2 \\ oe3\text{----------}cp3 \\ oe4\text{----------}cp4 \end{array} \right\} CF$$

1.5.2.- TÉCNICAS E INSTRUMENTOS

Técnicas

a) Encuestas
b) Entrevistas
c) Observación
d) Análisis de la Organización

Instrumentos

a) Metodología gestión por procesos Ciclo de Deming PDCA
b) Normas ISO 27001, ISO 17799, ISO27003, ISO27005 Y ISO 31000

1.6.- DELIMITACION

1.6.1.- ESPACIAL

La investigación se realizara en el JURADO ELECTORAL ESPECIAL un órgano administrativo y jurisdiccional del JURADO NACIONAL DE ELECCIONES.

1.6.2.- CONCEPTUAL

Las soluciones tecnológicas para mantener y aprovechar el crecimiento empresarial de largo plazo en gestión, hacen que soluciones como la IMPLEMENTACION DE SGSI (Sistema de Gestión de Seguridad de Información) apoyen las condiciones, convirtiendo la gestión de seguridad de información en un técnica estratégica que permita generar y controlar cambios de manera confiable, segura y oportuna.

2.- CAPÍTULO II: MARCO TEÓRICO

2.1.- ANTECEDENTES Y TRABAJOS RELACIONADOS

En un mundo actual de constantes cambios tecnológicos, el manejo de la seguridad de información a todo nivel se convierte en un problema grave cuando no se le brinda el control y tratamiento apropiado.

Tomando como base lo expuesto surge la necesidad que toda institución pública o privada debe de contar con sistema de gestión de seguridad de información, el cual le permita administrar toda sus información garantizando los aspectos de confidencialidad, integridad, disponibilidad y auditabilidad que esta debe de cumplir.

En inicios del año 2014, se manejaba poca información sobre el análisis y diseño de un Sistema de Gestión de Seguridad de Información en entidades públicas del Perú, de las entidades certificadas con la ISO 27001 dos son entidades públicas de las 8.

Revisando proyectos de fin de carrera sobre el Sistema de Gestión de Seguridad de Información se obtuvieron los siguientes:

-Metodología de un Sistema de Gestión de Seguridad de Información Para el sector Financiero peruano.

(Aquije Quijandria Jorge Gilmer / Jave Bobadilla Liz Laura)

Universidad Nacional de Ingeniería.

La presente tesis brinda una propuesta metodológica para realizar una implementación exitosa SGSI cumpliendo las regulaciones de la SBS Superintendencia de Banca, Seguros y AFP publicada el 6 de abril del 2009 en

el diario el peruano, La circular G-140-2009 Gestión de Seguridad de Información, afecta a las siguientes organizaciones bancos, financieras, AFP y Cooperativas de ahorro y crédito que deberán establecer, mantener y documentar un SGSI..

-Diseño de Un sistema de Gestión de Seguridad de Información para el centro de Cómputo del Ministerio de Economía Basado en el cumplimiento NTP/ISO/IEC 17799:2007.

Universidad Nacional Mayor de San Marcos

La presente tesis presenta un diseño de un Sistema Gestión Seguridad Información para el centro de cómputo cumpliendo los mandatos regulatorios para las entidades públicas, donde la información cobra un valor importante, debido a este valor que se incrementa con el tiempo, es que los órganos rectores del país demandan que las entidades públicas que tratan información critica nacional implementan un programa de gestión de seguridad de información.

-Diseño de Un sistema de Gestión de Seguridad de Información para una compañía de Seguros.

(Ampuero Chang, Carlos Enrique)

Pontificia Universidad Católica del Perú

La presente tesis presento un proyecto de fin de año, donde se presentó los factores claves para la implementación de un SGSI En caso alguno de los factores no esté presente durante la implementación podrían actuar de forma

negativa para el proceso, aumentando el tiempo de proyecto y en algunos casos deteniéndolo indefinitivamente estos son:

Compromiso de la dirección

Consideraciones financieras

Organización dela seguridad de la información

Actividades especificas de seguridad

Gestión de riesgos

Involucrar a los Stakeholders

-Sistema de Gestión de Seguridad de Información Para el sector Financiero peruano.

(Moises Antonio Villena Aguilar)

Pontificia Universidad Católica del Perú

La presente tesis ha realizado una investigación de las normas y estándares que van difundiéndose con mayor énfasis en el mercado peruano, en especial en el sector financiero. Se rescataron los aspectos más saltantes de cada norma y estándar, a partir de los cuales se plantea un esquema de gestión de seguridad de información que puede ser empleado por una institución financiera en el Perú, lo cual permitirá que ésta cumpla con las normas de regulación vigentes en lo relacionado a la Seguridad de Información

2.2.- MARCO CONCEPTUAL

A continuación, se presenta la definición de algunos conceptos claves que deben estar claros para la comprensión del tema.

2.2.1. INFORMACIÓN

La información es un activo que brinda valor al negocio; por ello, se necesita tener una adecuada protección frente a la constante exposición a distintas amenazas y vulnerabilidades. Esta puede adoptar distintas formas, de ahí surge la importancia de conocerlas para poder protegerla adecuadamente, estas formas son:

- Impresa o escrita en papel
- Almacenada electrónicamente
- Transmitida vía correo o e-mail
- Mostrada en videos
- Hablada en conversaciones [NTP ISO/IEC 17799]

2.2.2.-SEGURIDAD DE INFORMACIÓN

Es la protección de la confidencialidad, integridad y disponibilidad de la información; es decir, es asegurarse que esta sea accesible solo a las personas autorizadas, sea exacta sin modificaciones no deseadas y que sea accesible a los usuarios cuando lo requieran [NTP ISO/IEC 17799].

2.2.3. OFICIAL DE SEGURIDAD DE INFORMACIÓN

El oficial de seguridad de la información, conocido como CISO por sus siglas en inglés (Chief Information Security Officer), es la persona encargada de

planificar, presupuestar y verificar el rendimiento de los componentes de la seguridad de la información. Así como de realizar una correcta gestión de riesgo para la toma de decisiones.

2.2.4. POLÍTICA DE SEGURIDAD DE INFORMACIÓN

Las políticas de seguridad de información son aquellas normas que se establecen para guiar a los miembros de la organización a resguardar correctamente la seguridad de la información.

Peltier, en su libro "Information Security Fundamentals", considera a las políticas de seguridad de información como la piedra angular de una efectiva arquitectura de seguridad de la información, ya que de ella nacen otros documentos importantes tales como directivas, estándares, procedimientos y guías y nos menciona que estas cumplen con 2 roles importantes, un rol interno y otro externo.

- Rol Interno: Ya que se menciona a cada uno de los miembros de la organización que se espera que realicen y como se evaluará el trabajo realizado.

- Rol Externo: Ya que sirve para mostrarle al mundo como es que se trabaja dentro de la organización, que somos conscientes de la necesidad de proteger nuestra información y la de los clientes y que estamos trabajando para realizarlo.

2.2.5. SISTEMA DE GESTIÓN

Un sistema de gestión es una estructura probada para la gestión y mejora continua de políticas, procedimientos y procesos de una organización.

La implementación de un sistema de gestión ayuda a mejorar la efectividad operativa, optimizar costos, lograr mejoras continuas, aumentar la satisfacción de las partes interesadas al negocio y renovar constantemente las estrategias de la organización.

2.2.6. SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

Conocido como SGSI o ISMS por sus siglas en inglés (Information System Management System) es un sistema de gestión para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información, de esta manera un SGSI lo que busca es poder mantener la confidencialidad, integridad y disponibilidad de la información mientras minimiza los riesgos de seguridad de la información. [NTP ISO/IEC 27001]

2.2.7. RIESGO

Un riesgo es cualquier tipo de evento o circunstancia que de ocurrir amenazarían los objetivos de una organización, estos riesgos tienen una posibilidad de ocurrencia por lo que se miden como la multiplicación de impacto por probabilidad. [NTP ISO/IEC 17799]

HALVORSON (2008, 71) explica tres (3) naturalezas del riesgo, estos son los riesgos estratégicos, tácticos y operacionales.

Los riesgos estratégicos son los que pueden estar ligados a la seguridad de la información; sin embargo, se encuentran más orientados a los riesgos de las

ganancias y reputación de la organización, ya que se derivan de decisiones estratégicas que han sido tomadas o serán tomadas en la organización.

Los riesgos tácticos son los asociados a los sistemas que vigilan la identificación, control y monitoreo de los riesgos que afectan a la información, son aquellos que afectan indirectamente a la información.

Los riesgos operacionales son los relacionados a aquellos activos que pueden afectar los objetivos de una empresa (tales como presupuestos, cronogramas y tecnologías).

Para poder identificar el potencial daño o perdida debido a un riesgo los dueños de los activos pueden responder estas cuatro preguntas:

- ¿Qué puede suceder? (¿Cuál es la amenaza?)
- ¿Qué tan malo puede ser? (¿Cuál es el impacto?)
- ¿Qué tan seguido puede suceder? (¿Cuál es la frecuencia?)
- ¿Qué tan ciertas son las respuestas de las tres primeras preguntas? (¿Cuál es el grado de confianza?) [OZIER, 2004]

2.2.8. ADMINISTRAR RIESGOS

Es el uso de la información para estimar el impacto de los riesgos e identificar sus causas, de esta manera se pueden tomar medidas anticipadas ante un incidente.

2.2.9.-CONTROL

Los controles son medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales. "Una de las clasificaciones más generalizadas es:

- Preventivos: Reducen las vulnerabilidades.
- Detectivos: Descubren amenazas o escenarios previos a ellas permitiendo activar otros controles.
- Correctivos: Contrarrestan el impacto de la ocurrencia de una amenaza.
- Disuasivos: Reducen la probabilidad de ocurrencia de las amenazas." [TUPIA, 2009]

En el NTP ISO/IEC 17799 también se utiliza el control como un sinónimo de contramedida.

2.2.10.- ISO/IEC 27000

Es una norma internacional que busca dar información general sobre los sistemas de gestión de seguridad de información, así como definir algunos términos que son usados por todos los estándares de la familia 27000.

A diferencia de las otras normas de esta familia, esta es de libre distribución y se caracteriza por brindar un listado de las normas mencionadas (véase el grafico Nro. 3) junto con una pequeña descripción [ISO/IEC 27000, 2012]:

- ISO/IEC 27001: El estándar principal de la familia, brinda los requerimientos para el desarrollo y operación de SGSI incluyendo una lista de controles para el manejo y mitigación de los riesgos asociados a los activos de

información. Se puede confirmar la eficacia de la implementación del SGSI mediante una auditoria o certificación

- ISO/IEC 27002: Este estándar brinda la guía de implementación de la lista de las mejores prácticas y los más aceptados objetivos de control presentados como anexo en la ISO/IEC 27001, con el objetivo de facilitar la elección de controles para asegurar la seguridad de los activos de información.

- ISO/IEC 27003: Este estándar brinda información y una guía práctica para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI según lo establecido por la ISO/IEC 27001.

- ISO/IEC 27004: Este estándar provee guías prácticas para el uso de métricas que evalúen la efectividad, objetivos de control y controles usados en un SGSI.

- ISO/IEC 27005: Este estándar provee una guía para la gestión de los riesgos de seguridad de información según los requerimientos establecidos por la ISO/IEC 27001.

- ISO/IEC 27006: Este estándar se complementa con el ISO/IEC 17021 y brinda los requerimientos necesarios para la acreditación de la certificación de una organización que certifique los SGSI según la ISO/IEC 27001.

- ISO/IEC 27007: Provee una guía para conducir una auditoria de un SGSI así como las competencias necesarias de los auditores de sistemas de gestión de seguridad complementando la ISO/IEC 19011

- ISO/IEC TR 27008: Es un reporte técnico que brinda una guía para la revisión de la implementación de los controles del SGSI.

- ISO/IEC 27010: Provee una guía para gestionar la seguridad de la información en caso la organización intercambie o comparta información importante, ya sea que pertenezca al sector público o privado, que lo haga nacional o internacionalmente, o en el mismo sector u otros sectores del mercado en el que opera.

- ISO/IEC 27011: Provee una guía para apoyar la implementación de un SGSI en una empresa de telecomunicaciones.

- ISO/IEC 27013: Brinda una guía para la implementación integrada del ISO/IEC 27001 y el ISO/IEC 20000 (gestión de servicios de TI), ya sea implementándolos al mismo tiempo o uno después de otro.

- ISO/IEC 27014: Brinda una guía para conocer los principios y procesos del gobierno de la seguridad de la información, que busca que las organizaciones puedan evaluar, dirigir y monitorear la gestión de la seguridad de la información.

- ISO/IEC TR 27015: Sirve como complemento a las normas de la familia ISO/IEC 27000 para la implementación, mantenimiento y mejora del SGSI en empresas que provean servicios financieros.

- ISO/IEC TR 27016: Es un reporte técnico que brinda una metodología que permite a las organizaciones saber cómo valorar adecuadamente los activos de información identificados, los riesgos potenciales a los activos, apreciar el valor de los controles que protegen a estos activos y determinar el nivel óptimo de recursos que deben ser usados para asegurarlos.

- ISO/IEC 27799:2008: Brinda una guía para apoyar la implementación de un SGSI en las empresas de salud con la adaptación del ISO/IEC 27002 según los requerimientos de este sector.

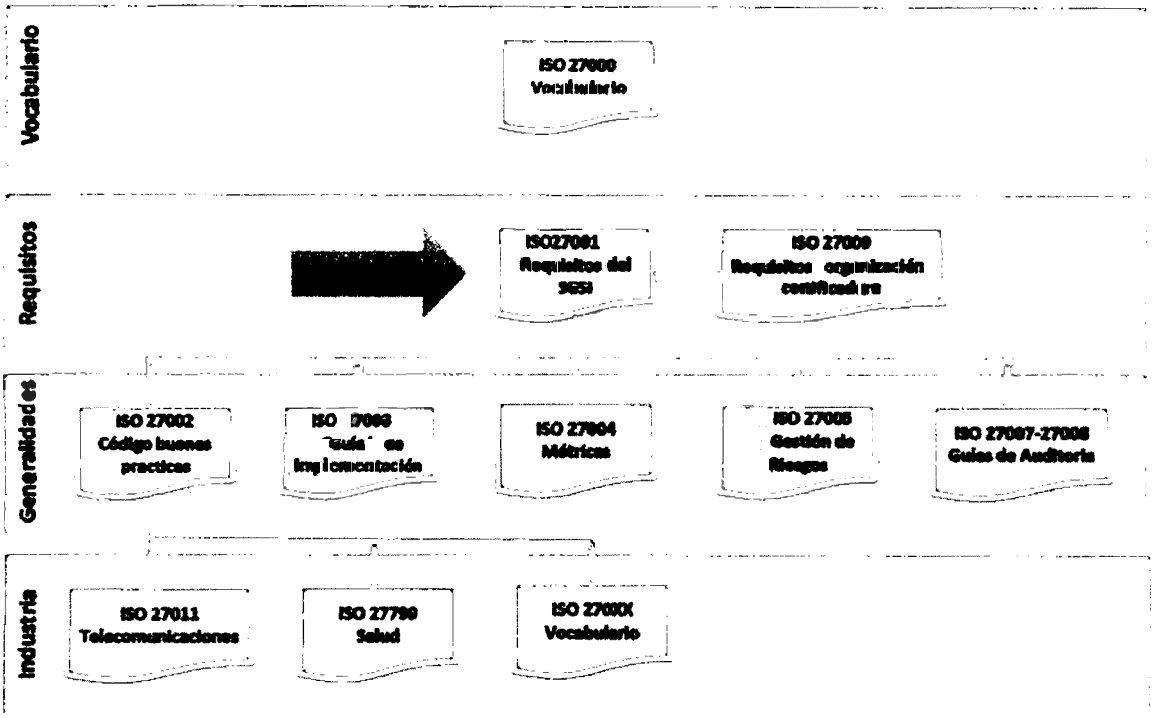

Grafico 3 - Relación de los estándares de la familia del SGSI

Fuente: ISO/IEC 27000–Tecnologías de información –Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Información general y vocabulario

2.2.11.- CICLO DE DEMING - CICLO PDCA

La presente metodología posee los 4 pasos iterativos que pueden ser adaptados fácilmente a los sistemas de gestión siendo muy utilizado por las normas ISO de sistemas de gestión, incluyendo la de gestión de seguridad de información.

Conocido como círculo, rueda o ciclo de Deming o círculo o ciclo PDCA, por sus siglas en ingles Plan, Do, Check y Act. Se llama así debido a que nace a

raíz de una conferencia que dio el Dr. W. Edwards Deming en Japón el año 1950.

La rueda de Deming se caracteriza por tener cinco (5) puntos clave, estos son:

1. Diseñar el producto con las pruebas apropiadas

2. Realizarlo probándolo en la línea de producción y en el laboratorio

3. Ponerlo en el mercado

4. Probar su utilidad y ver que piensa los usuarios de nuestro producto

5. Rediseñar el producto siguiendo los 4 pasos anteriores considerando la opinión de los usuarios.

Poco tiempo después esta rueda evolucionaria en el ciclo PDCA de la siguiente manera:

1. Diseñar – Planear (Plan): Diseñar el producto corresponde, en gestión, a la fase de planeamiento.

2. Producción – Hacer (Do): Este punto corresponde a la realización de lo que se ha planeado.

3. Venta – Verificar (Check): Ponerlo en el mercado corresponde a la fase de revisar que es lo que opinan los usuarios sobre lo que hemos realizado y si satisface sus necesidades.

4. Investigación – Actuar (Act): En caso de encontrar alguna queja debe ser incorporada en la fase de planificación y tomar medidas correctivas la próxima vez que se inicie este ciclo.

El uso del circulo de Deming es una práctica muy común en las normas ISO relacionadas a sistema de gestión, para el caso de un SGSI se puede adaptar según lo indicado en el Grafico Nro. 4.

Por ejemplo, Carlsom en el capítulo 2 del libro "Information Security Management Handbook, 6th edition" nos muestra los pasos para implementar el SGSI según el círculo de Deming.

1. Planear: Establecer el SGSI

Entender el contexto de la organización Evaluar los riesgos de la empresa

Trazar programa de seguridad de información Evaluar los riesgos del programa

2. Hacer: Implementar y operar el SGSI

Crear un plan base de seguridad de información Crear implementaciones específicas por cada dominio

3. Verificar: Monitorear y revisar el SGSI Evaluar el riesgo operacional

4. Actuar: Mantener y mejorar el SGSI Medir y monitorear

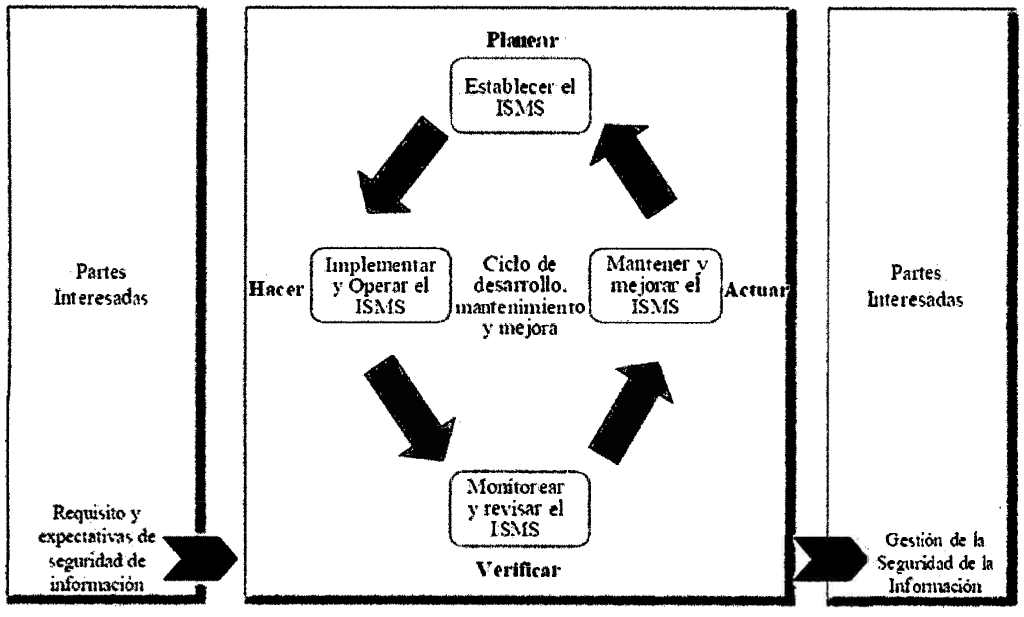

Grafico Nro. 4 Modelo PDCA aplicado al SGSI

Fuente: Sacado de la NTP ISO/IEC 27001:2008 – Tecnologías de información – Técnicas de seguridad – Sistemas de seguridad de la información - Requerimientos

De esta metodología solo se realizará el primer paso de "Planear" ya que el alcance del proyecto cubre el diseño más no la implementación, revisión ni mejora de un SGSI.

2.2.12. MAGERIT3.0

El Consejo Superior de Administración Electrónica de España elaboró MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) para gestionar los riesgos de las TIC debido al creciente uso y dependencia de estas para alcanzar los objetivos que cada individuo u organización desea. En esta metodología la gestión de riesgos se divide en 2 subprocesos, estos son:

- Análisis de Riesgos:

Permite determinar lo que posee la organización y que le podría suceder.

- Tratamiento de Riesgos:

Organiza una defensa prudente para sobrevivir a los incidentes y seguir operando en las mejores condiciones, al no poder controlar se maneja un riesgo residual que es asumido por la alta dirección.

De esta manera MAGERIT busca no solo concientizar a los responsables del gobierno de TI dé la existencia de riesgos sino que ayuda a descubrir y planificar un tratamiento oportuno para mantener a estos riesgos bajo control.

El método de análisis de riesgos que proporciona MAGERIT consiste en cinco (5) pasos [MAGERIT, 2012]:

1. Determinar los activos relevantes para la organización, sus relaciones entre si y el valor que tienen (según el coste que supondría su degradación)

2. Determinar las amenazas a las que se exponen los activos

3. Determinar las salvaguardas disponibles y que tan eficaces son frente al riesgo

4. Estimar el impacto que tendría una amenaza al dañar un activo

5. Estimar el riesgo

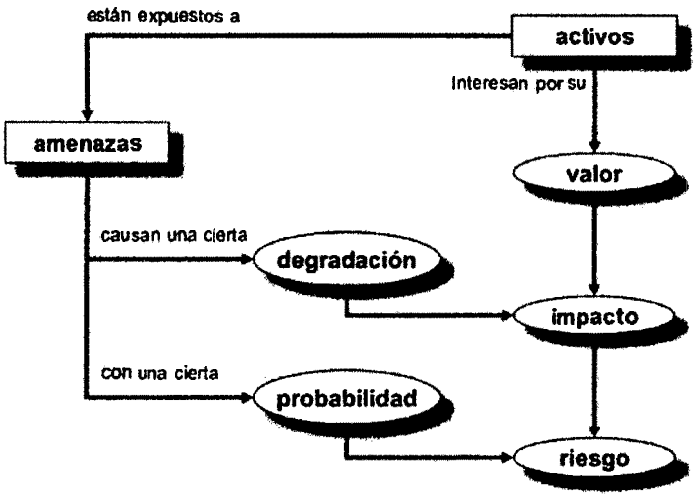

Grafico Nro. 5 – Elementos del Análisis de riesgos potenciales

Fuente: Concejo Superior de Administración Electrónica de España – MAGERIT – Libro I - Método

2.3.-MARCO NORMATIVO

Las siguientes normas son importantes y claves para el desarrollo del proyecto, estas son:

2.3.1.- NTP ISO/IEC 27001:2008

Es la norma técnica peruana basada en el estándar internacional principal de la familia ISO 27000, correspondiente a las normas sobre seguridad de información [ISO/IEC 27000, 2012], y contiene, como su nombre lo indica, los requerimientos para desarrollar un Sistema de Gestión de Seguridad de Información.

Esta norma fue certificable hasta el año 2013; sin embargo, fue sustituida por la nueva versión de esta norma la ISO/IEC 27001:2013.

Entre los puntos que cubre esta norma internacional encontramos [ISO/IEC 27001:2005]:

- Sistema de Gestión de Seguridad de Información

En este punto se busca es definir el alcance y las políticas del SGSI según las necesidades de la organización. De la misma manera, indica los pasos a seguir para identificar, analizar y evaluar los riesgos y sus posibles tratamientos.

Obsérvese que este punto se enfoca en la planificación no solo del análisis, diseño e implementación del SGSI, sino también del mantenimiento y mejora del SGSI.

- Responsabilidad de la gerencia

En esta norma se busca la participación activa de la alta dirección, ya que ellos son los dueños del negocio, la norma busca que ellos estén conscientes de las políticas de seguridad y de los planes del SGSI aprobándolos y dándoles a conocer ante toda la organización. De la misma manera, en caso se necesite más recursos son ellos los que lo proporcionaran.

- Auditorías internas

La auditoría interna busca conocer si es que los puntos tratados con anterioridad por el SGSI siguen están operativos y actualizados y no se quedaron. Mediante este punto se busca comprometer a los gerentes de las diversas áreas de la empresa a asegurarse que las acciones se ejecuten según como fueron documentadas.

- Revisión Gerencial del SGSI

Como se indicó, el SGSI busca la participación activa de la alta dirección, este punto se busca que el SGSI sea revisado al menos una vez al año por la alta

dirección y así asegurar el correcto funcionamiento del mismo y mejorarlo en caso se detecten algunas oportunidades para hacerlo.

- Mejora

El punto final contemplado por la norma, este se asegura de usar cada uno de los puntos anteriormente descritos para mejorar la efectividad del SGSI.

La identificación de no conformidades en el SGSI, es decir, situaciones que no están acordes a nuestros planes o lo deseado por la organización terminaran en correcciones que permitirán mejorar nuestro SGSI.

Carlson en el capítulo 2 del libro "Information Security Management Handbook, 6th edition" nos muestra 4 beneficios que posee la implementación de su norma hermana, la ISO/IEC 27001:2005, para mejorar la organización

1. Seguridad:

La estructura propia de un SGSI muestra una clara dirección, las políticas son dadas por la alta dirección, los gerentes se encarga del cumplimiento y los detalles son sacados de la documentación generada. De esta manera se puede monitorear y evaluar los resultados de una forma más ordenada. El SGSI proporciona mayor seguridad si es que ha sido validado por un auditor externo brindando ventajas ya sea si somos consumidores o proveedores de información, después de todo trabajar con alguien que ha pasado exitosamente por esta auditoria asegura que no darán problemas de seguridad a la organización.

2. Diferencia:

Un SGSI puede servir como un diferenciador de mercado mejorando la imagen que se proyecta. Muchos sectores demandan un cierto grado de confidencialidad al trabajar. Tener una certificación nos hace un socio estratégico para estas empresas.

3. Permite negocios:

Al implementar un SGSI se busca cubrir el marco legal que afecta a la empresa y resguardar la información que se posea con ayuda de controles, sin embargo; este hecho también posibilita, a la empresa, el ingreso a otros mercados que exijan la gestión de seguridad de información tales como entidades financieras o que alberguen datos personales.

4. Estructura:

Un SGSI brinda una estructura a la empresa, con una dirección y roles definidos, funciones y servicios delegados y métricas que pueden ser analizadas brinda una mejora continua a la empresa. En muchos casos, la implementación de un SGSI inspira a las organizaciones a tener un sistema gestión en otras áreas como recursos humanos, seguridad física continuidad de negocio, etc.

Justificación: El presente proyecto busca desarrollar un sistema gestión de seguridad de la información para una empresa pública y el presente ISO fue desarrollado para "proporcionar un modelo para implementar, operar, monitorear, revisar y mejorar un sistema de gestión de la seguridad de la información (SGSI)" [ISO/IEC 27001:2005].

Es por eso que se puede afirmar que esta es la norma base para el desarrollo del presente proyecto de fin de carrera, ya que en ella se encuentran los lineamientos necesarios para el diseño de un SGSI y así cumplir con lo solicitado con el primer y segundo resultado esperado.

2.3.2.- NTP ISO/IEC 17799:2007

La norma técnica peruana ISO/IEC 17799:2007 fue elaborada por el Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos (EDI) utilizando como base la norma ISO/IEC 17799:2005 y solo cambiando terminologías propias del idioma español. [NTP ISO/IEC 17799:2007]

Sin embargo, desde el 1 de julio de 2007 la norma ISO/IEC 17799:2005 cambio de nombre a ISO/IEC 27002:2005, manteniendo su año de edición y sin alterar su contenido.

En esta norma ISO se explican de una forma más detallada cada uno de los controles y objetivos que se mostraron en el anexo A de la NTP ISO/IEC 27001.

Estos controles se pueden dividir en 11 dominios, 39 objetivos de control y 133 controles.

Los dominios se pueden observar en la figura 1.5.1 y son los siguientes [ISO/IEC 27002:2005]:

- Políticas de seguridad

En este dominio se busca que la alta dirección demuestre su compromiso con el SGSI publicando y distribuyendo las políticas del SGSI previamente alineadas con los requisitos de la organización legales y operativos.

- Aspectos organizativos para la seguridad

Busca gestionar la seguridad de la información dentro de la organización, de ser necesario se debería buscar el apoyo de consultores expertos en la seguridad de información, así mismo se busca asignar responsabilidades de seguridad en la organización y gestionar la seguridad de la información que es manejada por terceros o grupos externos.

- Clasificación y control de activos

En este dominio se busca mantener una protección adecuada sobre cada activo de la organización, se recomienda asignar el custodio de los activos a sus dueños para que ellos sean responsables de sus confidencialidad, integridad y disponibilidad y clasificarlos para indicar el grado de protección que necesitan.

- Seguridad en recursos humanos

Se busca asegurar que los empleados, contratistas y terceros que trabajan con la organización entiendan las responsabilidades que tienen al formar parte del SGSI y que estén capacitados para responder ante un evento o incidencia según sus roles.

- Seguridad física y del entorno

En este dominio se trata de evitar cualquier tipo de acceso no autorizado a la organización o a sus distintas sub áreas, así como controlar el correcto funcionamiento de los equipos que envíen o reciban datos.

- Gestión de comunicaciones y operaciones

Trata de gestionar el correcto uso de los equipo de comunicación así como de evitar cualquier tipo de ataque o malfuncionamiento de estos equipos que deriven en una pérdida o modificación de la información.

- Control de accesos

Busca evitar que la información sea accedida o compartida por personal no autorizado en la organización y detectar actividades no autorizadas.

- Adquisición, desarrollo y mantenimiento de sistemas

En este dominio se busca asegurar que los sistemas de información son seguros y cumplen con los requisitos de seguridad para evitar la pérdida, modificación o mal uso de los datos a través de los sistemas de información.

- Gestión de incidentes en la seguridad de información

Busca asegurar que los eventos o incidencias relacionados a la seguridad de información sean comunicados de una manera eficiente para poder tomar acciones correctivas contra ellos a tiempo. Asimismo se busca tener claro que pasos seguir una vez se reciba la alerta de haber encontrado algún incidente.

- Gestión de continuidad de negocio

Busca reaccionar con medidas correctivas frente a algún evento o incidencia que pueda detener parcial o completamente los procesos críticos del negocio contemplando la seguridad de la información. De esta forma se busca mitigar el efecto negativo que pueda tener este acontecimiento sobre la organización.

- Cumplimiento

Este dominio busca evitar que se incumplan las normas o el marco legal bajo el cual se rige la organización. Este marco legal contempla las leyes que afectan a la empresa y al negocio, las obligaciones contractuales, requisitos reglamentarios y requisitos de seguridad. Pero también busca que los sistemas de información de la organización cumplan con las políticas de seguridad.

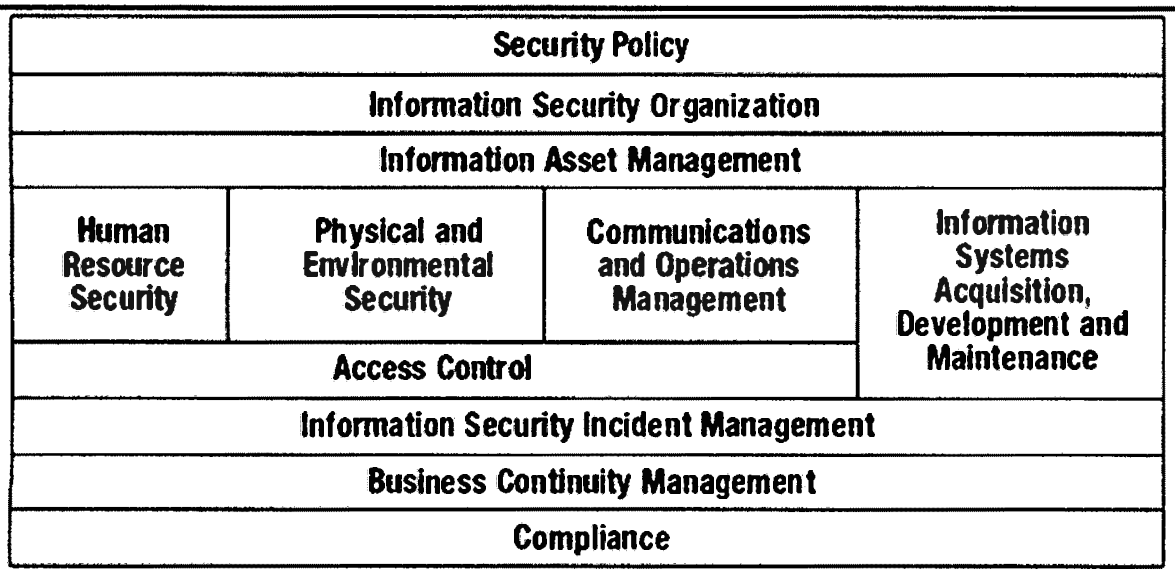

Grafico Nro. 5 - Los dominios de la ISO/IEC 27002:2005

Fuente: Sacado del libro CISM Review Manual 2013

~~Justificación Al estar basada en el anexo A de la NTP ISO/IEC 27001, contiene~~ lineamientos prácticos para la implementación de los controles en la organización lo cual es de utilidad para el desarrollo del octavo resultado esperado que es la declaración de aplicabilidad.

2.3.3.-ISO/IEC 27003:2010

El presente estándar brinda información y una guía práctica para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el diseño de un SGSI según lo establecido por la ISO/IEC 27001:2005.

La importancia del uso de este radica en que no cubre actividades propias del SGSI, solo muestra conceptos relacionados al diseño del plan del SGSI y lo que se debe realizar hasta antes de ejecutar el plan de implementación del sistema de gestión, lo cual está fuertemente vinculado al alcance del presente plan del proyecto.

Entre los puntos que aclara podemos encontrar los siguientes:

- Como preparar un plan de implementación de un SGSI para una organización
- Las actividades criticas del proyecto de un SGSI
- Ejemplos de cómo alcanzar los requerimientos de la ISO 27001

Como se mencionó, la presente norma ISO indica cómo debe realizarse el diseño del SGSI desde su inicio hasta el desarrollo de los planes de implementación, desde el proceso para obtener la aprobación de la alta dirección y la definición de un proyecto para la implementación del sistema de gestión, hasta la elaboración del plan final de implementación del SGSI.

Por último, como se menciona dentro del estándar, la ISO/IEC 27003 es aplicable a todas las organizaciones de todos los tamaños y tipos, considerando la complejidad y riesgos únicos de cada una de ellas. [ISO/IEC 27003:2010]

Justificación: Se decidió establecer como resultado esperado parte de la documentación propuesta por la presente norma, como es el caso del Business Case, debido a que brinda orientación para el desarrollo de un plan de implementación de un sistema de gestión de seguridad de la información cumpliendo con el alcance del presente proyecto al contemplar toda la documentación necesaria para el diseño de un SGSI; sin embargo, también se incluye la ISO/IEC 27001 ya que esta es la norma base para el desarrollo del proyecto.

2.3.4.-. ISO/IEC 27005:2011

Hace uso del modelo de ciclo de Deming (PDCA) para gestionar los riesgos, es un estándar especializado que complementa a la norma internacional ISO/IEC 31000, la cual se especializa en la gestión de riesgos, indicando las mejores prácticas para gestionar los riesgos relacionados a la seguridad de la información. Se puede observar su proceso de gestión de riesgos en el Grafico Nro. 7.

Existen varias metodologías para el análisis de riesgos, por ejemplo, tenemos a MAGERIT, una metodología de riesgos desarrollada en España que ayuda a identificar y planear un tratamiento de riesgos de las organizaciones [MAGERIT, 2012]. También existe OCTAVE, un conjunto de herramientas, técnicas y métodos para la valoración y planeamiento de la seguridad de la información basada en riesgos [OCTAVE].

Sin embargo, estas metodologías son más usadas en los contextos en las que fueron creadas. Por otro lado, la norma ISO/IEC 27005 es una norma internacional que complementa a la ISO/IEC 31000 y al ser parte de la familia

ISO 27000 busca apoyar la tarea de análisis y gestión de riesgos a la hora de implementar el SGSI con el ISO/IEC 27001, es por este motivo que se adoptarán algunos aspectos de esta norma para el tratamiento de riesgos durante el proyecto.

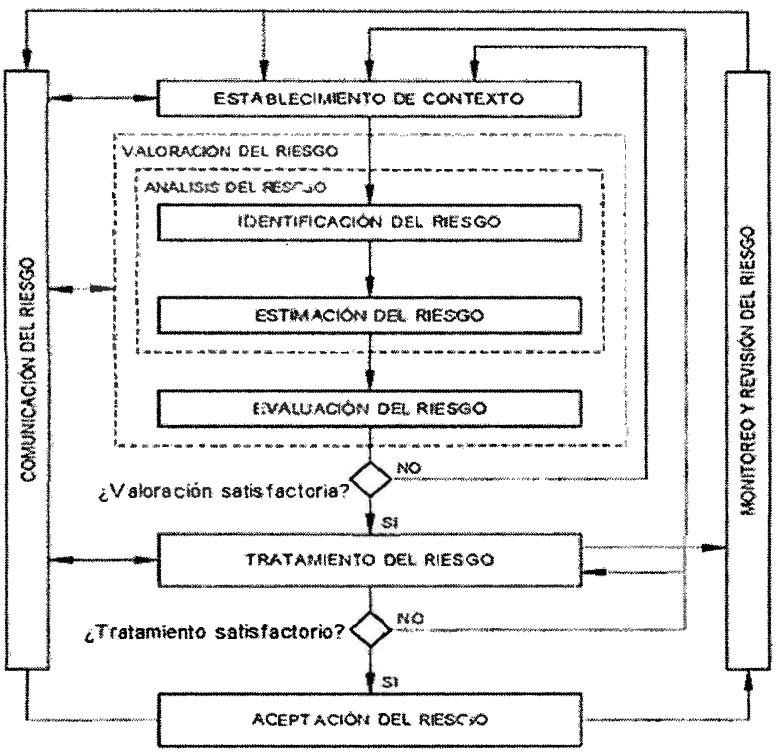

Grafico Nro. 7 – Proceso de Gestión de riesgos de Seguridad de Informacion.

Fuente: Ilustración basado en el ISO/IEC 27005:2011

2.3.5.-. NTP ISO 31000:2011

Esta norma técnica peruana está basada en la ISO 31000:2009, la cual forma parte de la familia de estándares que gestionan el riesgo. Esto debido a la existencia de factores, internos o externos, que añaden incertidumbre en el logro de los objetivos de las organizaciones.

Esta norma busca establecer principios para tener una gestión eficaz del riesgo mediante la implementación y mejora continua de un marco de trabajo para la

integración del proceso de gestión de riesgos en la planificación, estrategia, gestión, procesos de información, políticas, valores y cultura de la organización.

La gestión de riesgo se debe basar en:

- Crear valor
- Tratar la incertidumbre
- Formar parte de las decisiones
- Estar hecha a la medida
- Considerar factores humanos y culturales
- Facilitar la mejora continua de la organización

El proceso de gestión del riesgo lo podemos observar en el Grafico Nro. 8

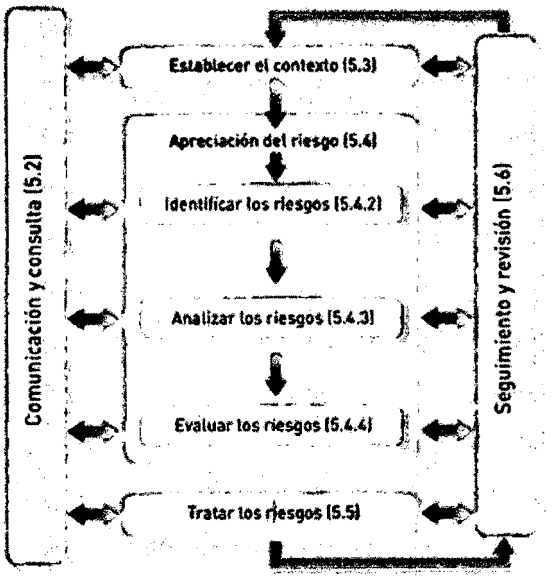

Grafico Nro. 8 – Proceso de gestión de riesgos

Fuente: ESCORIAL, Ángel. 2012 "La Gestión de riesgos impulsa la credibilidad y la transparencia", Gerencia de riesgos y seguros. España, No 112, p51

2.4.- MARCO REGULATORIO / LEGAL

Las siguientes resoluciones ministeriales fueron autorizadas por la Presidencia del Consejo de Ministros, las cuales afectan directamente al proyecto de fin de carrera, estas son:

2.4.1.- RM-246-2007-PCM

Mediante esta resolución se aprueba el uso obligatorio de la "NTP-ISO/IEC 17799:2007 Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información" en todas las entidades públicas que pertenecen al Sistema Nacional de Informática. Esto significaba el reemplazo de la NTP-ISO/IEC 17799:2004 que en ese tiempo era de uso obligatorio.

2.4.2.- RM-197-2011-PCM

Mediante esta resolución se establece como fecha límite para la implementación de la "NTP-ISO/IEC 17799:2007 Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información" el día 31 de diciembre del 2012 para todas aquellas empresas que pertenecen al Sistema Nacional de Informática.

2.4.3.- RM-129-2012-PCM

La emisión de esta resolución deja sin efecto la RM-197-2011-PCM, debido a que la norma "NTP-ISO/IEC 17799:2007" que debía ser implementada establece recomendaciones y buenas prácticas de seguridad de información pero no definía una forma exacta de verificar la efectividad y eficiencia de lo que había sido implementado, por lo que la fecha limite dada por esta resolución ya no tenía valor.

Además se define que se debe implementar de manera obligatoria la "NTP ISO/IEC 27001:2008" y da nuevas fechas límites para desarrollar la implementación para todas las empresas públicas (véase figura 1.1.2).

La norma fue emitida el 23 de mayo del 2012, y da 45 días para el inicio de la primera fase por lo que a la primera semana de julio del 2012 debió haberse empezado la misma.

3.- CAPITULO III: DESARROLLO DE LA INVESTIGACION

3.1.- MODELO DE NEGOCIO DEL JEE LIMA OESTE

Para obtener el total apoyo de la alta dirección es crucial en el desarrollo del proyecto. Además sabemos que la NTP ISO/IEC 27001 indica que se debe buscar obtener este compromiso dentro de la fase inicial del proceso de implementación. Ante esta situación, se desarrolló un documento que permita evidenciar ante la gerencia cual es la situación actual de la organización, la problemática que enfrentan y que opciones se posee para atender estas nuevas necesidades.

3.1.1.- REVISIÓN DEL NEGOCIO: ESTRATEGIA DEL NEGOCIO

3.1.1.1.- LA EMPRESA

Los Jurados Electorales especiales son órganos temporales creados para cada proceso electoral, conforme al artículo 13 de la Ley N.° 26859, Ley Orgánica de Elecciones, y al artículo 32 de la la Ley N.° 26486, Ley Orgánica del Jurado Nacional de Elecciones (LOJNE), y estos, para el cumplimiento de sus funciones, establecidas en el artículo 36 de la LOJNE, requieren de disposiciones conducentes a hacer más eficiente su gestión, en particular, y en general, para mejorar la gestión de los procesos electorales.

El Jurado Electoral Especial es un órgano administrativo-jurisdiccional que se constituye por un tiempo determinado, con motivo de la convocatoria a un proceso electoral, sea para elegir candidatos (presidente y vicepresidentes de la República, congresistas, alcaldes y regidores, entre otros), o elegir opciones a través de una consulta popular de revocatoria del mandato de autoridades o de referéndum (aprobación o no de un proyecto de ley).

El Jurado Electoral Especial tiene las mismas atribuciones e impedimentos que los miembros del Pleno del Jurado Nacional de Elecciones, en la circunscripción para la cual se ha definido.

FUNCIONES Y ATRIBUCIONES DE LOS JEE

Los JEE tendrán, de acuerdo a su competencia territorial y tipo de proceso electoral, las siguientes funciones:

a) Administrar justicia electoral en primera instancia, con arreglo a la Constitución Política del Perú, las leyes, las normas emitidas por el Pleno del JNE y los principios generales del derecho.

b) Calificar y conceder, de ser el caso, los recursos de apelación que se interpongan contra sus pronunciamientos, elevando los actuados al JNE.

c) Acreditar a los personeros de las organizaciones políticas, de los promotores de las consultas populares y de las autoridades sometidas a consulta popular, que participen en los procesos electorales, de acuerdo a la reglamentación expedida por el JNE.

d) Inscribir las listas de los candidatos en cada tipo de proceso electoral.

e) Resolver las tachas formuladas contra la inscripción de candidatos y listas de candidatos.

f) Resolver las tachas formuladas contra los postulantes a los cargos de jefe de ODPE, administrador de ODPE y coordinador de local de votación de ODPE.

g) Resolver las tachas formuladas contra los ciudadanos sorteados para conformar las mesas de sufragio, así como excluir de oficio a los ciudadanos sorteados que tengan comprobado impedimento para asumir la función de miembro de mesa.

h) Fiscalizar la legalidad del ejercicio del sufragio.

i) Fiscalizar la legalidad de la realización de los procesos electorales, del referéndum u otras consultas populares. Esta fiscalización incluye actos previos a la realización de los procesos electorales, en coordinación con la DNFPE.

j) Velar por el cumplimiento obligatorio de las resoluciones, directivas y otras normas del JNE, y cualquier otra norma sobre el desarrollo de los procesos electorales y de consulta popular, así como las demás disposiciones referidas a la administración de justicia electoral.

k) Elevar al JNE las quejas que se presenten contra el JEE.

l) Expedir las credenciales correspondientes a los candidatos elegidos y a los Accesitarios en caso de consultas de revocatoria.

m) Declarar la nulidad de un proceso electoral, del referéndum u otras consultas Populares en primera instancia, conforme a ley.

n) Poner en conocimiento del JNE y de la autoridad competente, las infracciones o delitos cometidos por las personas, autoridades, funcionarios o trabajadores públicos, en aplicación de las normas electorales, registrando tales infracciones o delitos en el reporte de incidencias establecido por la DNFPE.

o) Resolver las impugnaciones de las decisiones de los miembros de mesa hechas durante la votación y el escrutinio en las mesas de sufragio.

p) Resolver en primera instancia las observaciones de las actas electorales.

q) Proclamar los resultados del referéndum o de otro tipo de consulta popular llevados a cabo en su ámbito.

r) Proclamar los resultados de las elecciones y a los candidatos elegidos.

s) Remitir al JNE los resultados electorales obtenidos.

t) Administrar los fondos que se le asignen, de acuerdo a Ley y sujetándose a las normas y procedimientos de los sistemas de Contabilidad y de Tesorería, así como a las directivas emitidas por el JNE.

u) Designar a su personal administrativo de acuerdo a su presupuesto, aplicando la normativa existente sobre procesos de selección y contratación e Incompatibilidades previstas en la Ley, así como las directivas emitidas por el JNE.

v) Rendir cuentas del presupuesto asignado dentro de los plazos establecidos en la Ley.

w) Presentar un informe final al JNE, antes de su cese, de acuerdo a ley.

x) Otras funciones relacionadas con su competencia.

CONSTITUCIÓN DE LOS JEE

El JEE está constituido por tres (3) miembros:

a) Un (1) juez superior en ejercicio de la Corte Superior bajo cuya circunscripción se encuentra la sede del JEE, quien lo preside.

b) Un (1) miembro designado por el Ministerio Público, elegido entre sus fiscales superiores en actividad y jubilados.

c) Un (1) miembro designado por el JNE mediante sorteo en acto público de una lista de veinticinco (25) ciudadanos que residan en la sede del JEE y que se encuentren inscritos en el RENIEC.

ORGANIGRAMA

El Organigrama del JEE LIMA OESTE se muestra en la Figura 1. En él se aprecia la estructura organizacional basada en las funciones de cada integrante de esta organización.

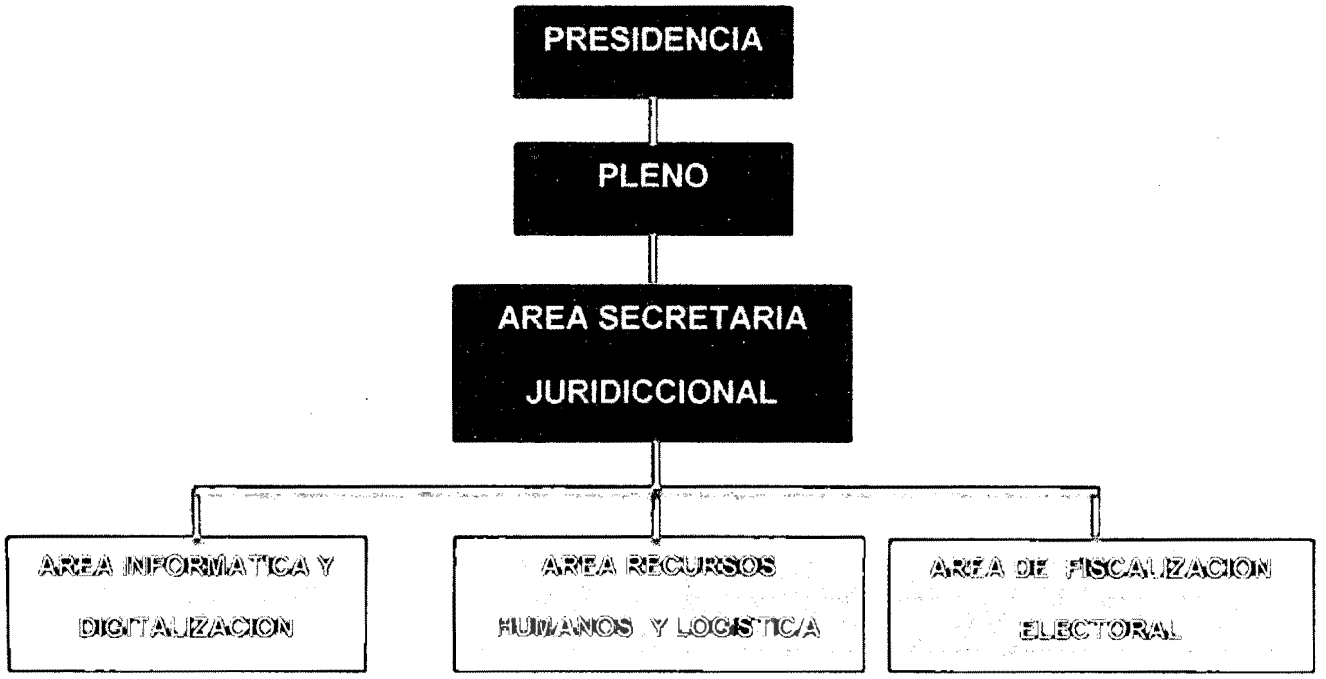

Grafico Nro. 9. Organigrama del JEE LIMA OESTE, setiembre 2014.

Fuente: Elaboración Propia a partir de resoluciones del Jurado Nacional de Elecciones

Visión

Ser el organismo rector del sistema democrático, reconocido en la región por su absoluta garantía de respeto de la voluntad popular.

Misión

Contribuir y garantizar la consolidación del sistema democrático y la gobernabilidad del país, a través de sus funciones constitucionales y legales.

Valores

- Identificación institucional.
- Integridad.
- Trabajo en equipo.
- Proactividad.
- Respeto.

Principios

- Imparcialidad.
- Confiabilidad.
- Transparencia.
- Calidad.
- Inclusión Social.

3.1.1.2.- ANÁLISIS FODA DEL JEE LIMA OESTE

Síntesis del diagnóstico externo:

Oportunidades

- Impulso al proceso de descentralización y desconcentración de las funciones del estado.
- Restitución de las otras funciones electorales: organización de procesos electorales.

- Cooperación técnica internacional de organismos vinculados a temas de fortalecimiento de la democracia a través de la participación ciudadano.

- Incremento de la confianza ciudadana en el JEE, respecto de su derecho a elegir y ser elegido.

Amenazas

- Imprecisiones, vacíos y contradicciones en la legislación electoral vigente.

- Modificación constitucional de los organismos electorales.

- Reforma constitucional que restringe al JEE funciones de registros de organizaciones políticas.

- Falta de conciencia política ciudadana al elegir a sus representantes.

Síntesis del diagnóstico interno:

Fortalezas

- Imagen y prestigio Institucional.

- Eficacia en el logro de sus objetivos.

- Interés del personal por capacitación y participar en actividades de educación y fiscalización.

- Facultad de iniciativa legislativa en materia electoral otorgada constitucionalmente.

- Personal profesional y técnico calificado, innovador y comprometido: con principios y valores éticos y democráticos.

Debilidades

- Alta rotación de personal durante épocas electorales.
- Inadecuada distribución del personal administrativo y de línea.
- Falta de innovación de servicios institucionales.
- Inadecuados niveles de comunicación.
- Centralización de las funciones del JNE en épocas no electorales.

	FORTALEZAS	DEBILIDADES
	1. Imagen y prestigio Institucional. 2. Eficacia en el logro de sus objetivos. 3. Interés del personal por capacitación y participar en actividades de educación y fiscalización. 4. Facultad de iniciativa legislativa en materia electoral otorgada constitucionalmente. 5. Personal profesional y técnico calificado, innovador y comprometido: con principios y valores éticos y democráticos. 6. Aplicación de la norma ISO 27001(seguridad de información) 7. Directivos comprometidos con la innovación y tecnologías.	1. Alta rotación de personal durante épocas electorales. 2. Inadecuada distribución del personal administrativo y de línea. 3. Falta de innovación de servicios institucionales. 4. Inadecuados niveles de comunicación. 5. Centralización de las funciones del JNE en épocas no electorales. 6. Mínimo conocimiento de la importancia de seguridad de información.
OPORTUNIDADES 1. Impulso al proceso de descentralización y desconcentración de las funciones del estado. 2. Restitución de las otras funciones electorales: organización de procesos electorales. 3. Cooperación técnica internacional de organismos vinculados a temas de fortalecimiento de la democracia a través de la participación ciudadano. 4. Incremento de la confianza ciudadana en el JEE, respecto de su derecho a elegir y ser elegido. 5. Desarrollo acelerado de las tecnologías de información y comunicación,	F1O1.- Aprovechar la imagen y el prestigio institucional para el impulso al proceso de descentralización y desconcentración de las funciones del estado. FIO4.-Aprovechar la imagen y prestigio para el incremento de la confianza ce la ciudadanía en los proceso electorales. F5O5.-Aprovechar personal profesional y técnico calificado para la mejora de procesos de negocio aplicando tecnologías de información. F2O4.-Aprovechar la eficacia en el logro de sus objetivos para el incremento de confianza ciudadana en procesos electorales. F6O5.- Concientizar al personal a trabajar según las normas ISO 27001 usando herramientas tecnológicas. F7O5.-El compromiso de los directivos en la implementacion de Tics y mejora de procesos,	D3O1.- Mejora en la innovación de servicios institucionales en una gestión descentralizada. D2O1.-Mejora de la distribución de personal para el impulso de descentralización y desconcentración de las funciones del estado. D5O3.- Disminuir la centralización de las funciones del JNE en épocas no electorales con la descentralización y desconcentración de las funciones del estado. D3O5.-Mejora de servicios institucionales aplicando tecnologías de información y comunicaciones. D6O5.-Realizar capacitación y concientización usando tecnologías
AMENAZAS 1. Imprecisiones, vacíos y contradicciones en la legislación electoral vigente. 2. Modificación constitucional de los organismos electorales. 3. Reforma constitucional que restringe al JEE funciones de registros de organizaciones políticas. 4. Falta de conciencia política ciudadana al elegir a sus representantes.	F4A1.-Minimizar las imprecisiones, vacíos y contradicciones en la legislación mediante la facultad de iniciativa legislativa otorgada constitucionalmente. F1A4.-Concientizacion ciudadana para elegir a los políticos mediante el prestigio institucional que tenemos. F5A4.-Capacitacion y conocimiento de la importancia de elegir a los políticos mediante el personal calificado con principios valores éticos y democráticos.	D1A4.-Mantener personal sobresaliente para la concientización, capacitación y conocimiento para elegir representantes calificados con valores éticos y democráticos. D2A4.-Adecuada distribución de personal administrativo para la concientización ciudadana de elegir a su representante. D1A4.- Concientizar al personal que hay más ciudadanos para capacitar en las responsabilidades de elegir a su representantes.

Tabla Nro. 3

Fuente: Elaboración Propia

3.1.2.- MODELO DE NEGOCIO: ANÁLISIS FUNCIONAL

Luego del análisis realizado, se prosigue con la descripción de la descomposición funcional de la Institución, donde se encuentra el proceso de Registro de actas digitalizadas.

3.1.2.1.- IDENTIFICACIÓN DE PROCESO

En el JEE LIMA OESTE se puede identificar procesos, los cuales son:

a) PROCESO ESTRATEGICOS

- Gestión del presidente
- Gestión del pleno JURADO ELECTORAL ESPECIAL
- Gestión de la calidad
- Imagen institucional

b) PROCESOS MISIONALES O OPERATIVOS

- Propaganda electoral
- Publicidad estatal
- Inscripción de listas
- registrar actas digitalizadas
- proclamar resultados

c) PROCESOS DE APOYO

- Gestión administrativa
- Gestión de bienes y servicios
- Gestión de talento humano
- Fiscalización electoral
- Gestión de TICs
- Atención al ciudadano

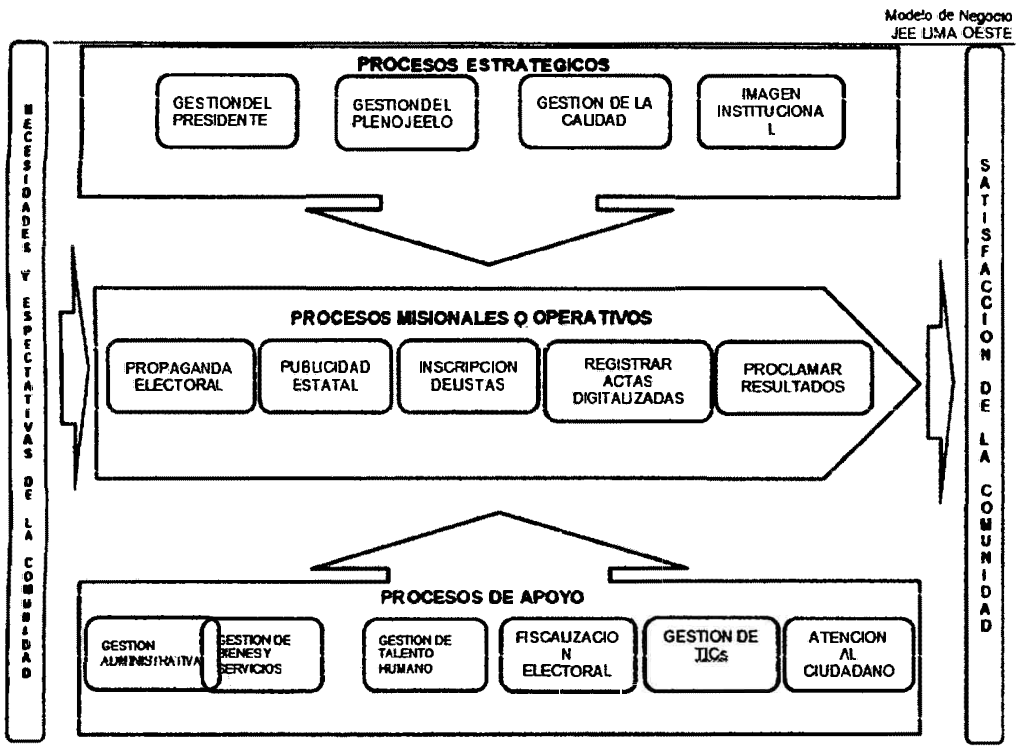

Grafico Nro. 10

Fuente: Elaboración Propia

3.1.2.2.- METODOLOGIA DE LA ELIPSES EN EL PROCESO DE REGISTRAR ACTAS DIGITALIZADAS

a).- REGISTRAR ACTAS DIGITALIZADAS

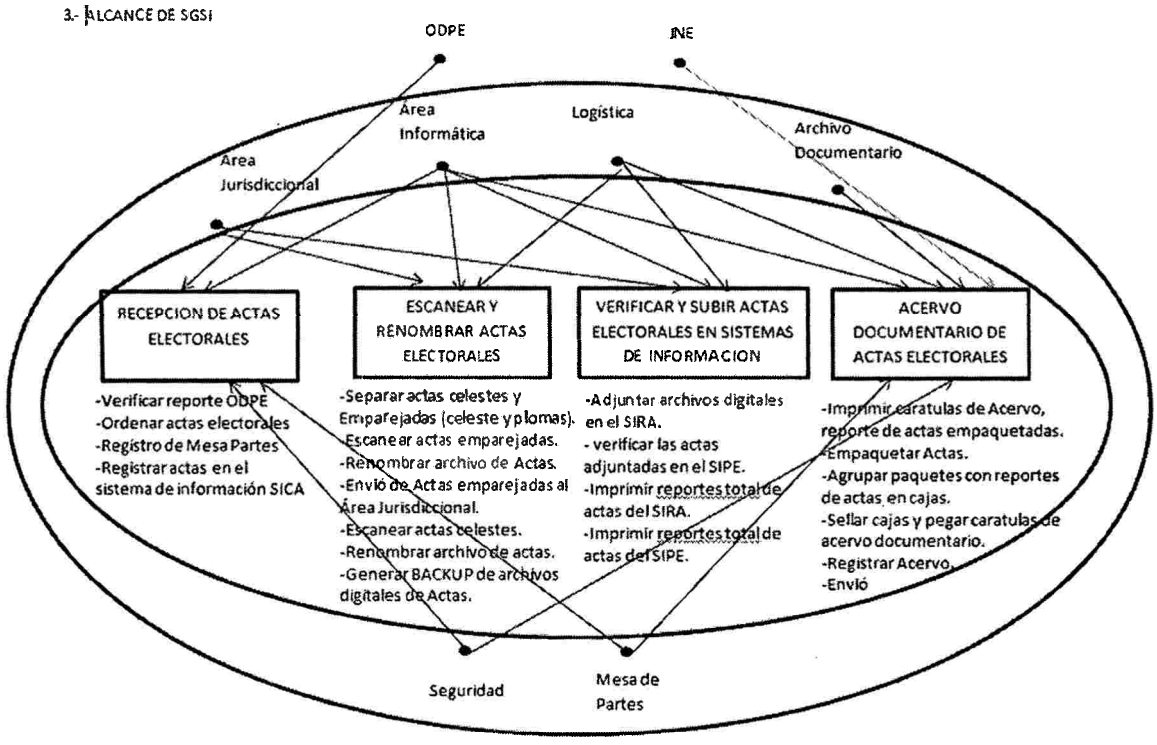

Grafico Nro. 11

Fuente: Elaboración Propia

3.2.- ALCANCE DEL SISTEMA DE GESTION DE SEGURIDAD DE INFORMACION (SGSI):

El presente proyecto busca diseñar un sistema de gestión de seguridad de información para resguardar la confidencialidad, disponibilidad e integridad de los activos de información involucrados en los procesos institucionales críticos de una entidad pública. Debido a ello debemos considerar que el alcance del proyecto de

fin de carrera estará claramente ligado al alcance que sea definido por la alta dirección de la empresa, siendo una base para definir el documento de alcance del presente proyecto.

3.2.1.- DESCRIPCION DE ESTE DOCUMENTO DE ALCANCE SGSI

3.2.1.1.- OBJETIVO

Seguridad en el registro de actas digitalizadas de acuerdo a los controles del estándar ISO/IEC 27001-2008 relevantes y aplicables para la organización.

3.2.1.2.- AUDIENCIA

- Presidente de JEE Lima Oeste
- Miembros del pleno.
- Jefes de áreas.
- Representante del JNE

3.2.1.3.- CONTENIDO

- Documentos de referencia.
- Normativa Legal.
- Definición del alcance del SGSI.
- Justificación.
- Límites de la organización.

- Límites físicos.

- Alcance abreviado.

- Exclusiones del alcance.

3.2.2.- DOCUMENTOS DE REFERENCIA

- Constitución Política del Perú.

- Ley N.° 26859, Ley Orgánica de Elecciones.

- Ley N.° 26486, Ley Orgánica del Jurado Nacional de Elecciones.

- Ley N.° 29688, Ley que modifica la Ley 26859, Ley Orgánica de Elecciones, y la Ley N° 26486, Ley Orgánica del Jurado Nacional de Elecciones.

- Ley N.° 30194, Ley que modifica el artículo 33 de la Ley N.° 26486, Ley Orgánica de Elecciones.

- Ley Anual de Presupuesto del Sector Público.

- Ley N.° 28693, Ley General del Sistema Nacional de Tesorería y sus modificatorias.

- Ley N.° 28411, Ley General del Sistema Nacional de Presupuesto y sus modificatorias.

- Ley N.° 27815, Ley del Código de Ética de la Función Pública.

- Decreto Legislativo N.° 1017, Ley de Contrataciones del Estado.

- Decreto Legislativo N.° 276, Ley de Bases de la Carrera Administrativa y de Remuneraciones del Sector Público.

- Decreto Supremo N.° 184-2008-EF, Reglamento de la Ley de Contrataciones del Estado.

- Resolución Directoral N.° 002-2007-EF/77.15, que aprueba la Directiva de Tesorería N° 001-2007-EF/77.15.

- Resolución N.° 601-2010-JNE, que aprueba el Texto Único Ordenado del Reglamento de Organización y Funciones del Jurado Nacional de Elecciones.

- Resolución N.° 738-2011-JNE, que aprueba la actualización del Reglamento de Organización y Funciones del Jurado Nacional de Elecciones.

- Resolución N.° 461-2013-JNE que precisan aspectos referidos al ámbito territorial sobre el que el RENIEC debe seleccionar a ciudadanos designados como miembros integrantes de un Jurado Electoral Especial.

- Acuerdo del Pleno del Jurado Nacional de Elecciones, de fecha 4 de julio de 2013, que precisa la edad límite de los miembros de los Jurados Electorales Especiales.

- Acuerdo del Pleno del Jurado Nacional de Elecciones, de fecha 28 de noviembre de 2013, que aprueba el formato de informe final para los Jurados Electorales Especiales.

- Resolución de Superintendencia N.° 007-99/SUNAT, Reglamento de Comprobantes de Pago.

3.2.3.- NORMATIVIDAD LEGAL

RM-246-2007-PCM

RM-197-2011-PCM

RM-129-2012-PCM

Norma Técnica Peruana NTP-ISO/IEC 27001:2008.

Norma Técnica Peruana NTP-ISO/IEC 17799:2007.

3.2.4.- DEFINICIÓN DEL ALCANCE DEL SGSI

La implementación del SGSI será la capacitación y concientización de personal de sistemas, logística, área jurisdiccional, archivo documentario, seguridad y mesa de partes para que el proceso de registro de actas digitalizadas sea integro, disponible y confidencial aplicado en el JURADO ELECTORAL ESPECIAL LIMA OESTE la cual se desarrollara solo en los JEE de la Provincia de Lima en el proceso de registro de actas digitalizadas.

3.2.4.1.- JUSTIFICACIÓN

- Proceso relevante de la organización.
- Reducir riesgos asociados y garantizar la continuidad del servicio.

3.2.4.2.- LÍMITES DE LA ORGANIZACIÓN

Área comprendida por el Radio Urbano del Jurado Electoral Especial Lima Oeste.

3.2.4.3.- LÍMITES FÍSICOS

Local del Jurado Electoral Especial ubicado en el distrito de Santiago de Surco entre las Av. Benavides y Tomas Marsano.

Las dirección es Av. Ayacucho N° 1316 Urbanización Liguria distrito de Santiago de Surco

3.2.4.4.- ALCANCE ABREVIADO

Proceso: Registro de actas Digitalizadas.

3.2.4.5.- EXCLUSIONES DEL ALCANCE

- JEE de otras provincias.
- JEE de otros departamentos.

3.3.- POLÍTICA DE SEGURIDAD DE INFORMACIÓN

3.3.1.- ROLES Y RESPONSABILIDADES

3.3.1.1.- REPRESENTANTE DEL PLENO

1.- Conocer y difundir la política de seguridad de la información a todos los trabajadores de la organización.

2.- Estar comprometidos con el sistema de gestión de la seguridad de información.

3.3.1.2.- COMITÉ DE SEGURIDAD DE INFORMACION

1.- Comunicar la importancia de los objetivos de la seguridad de la información y la necesidad de mantener una mejora continua.

2.- Estar informados de las necesidades actuales del negocio y de los cambios dados en los procesos pertenecientes al alcance del SGSI.

3.- Facilitar y dar seguimiento a la asignación de recursos relacionados al SGSI.

3.3.1.3.- OFICIAL DE SEGURIDAD DE INFORMACION

1.- Diseñar, implementar, monitorear y mejorar el sistema de gestión de seguridad de la información en la empresa.

2.- Elaborar y ejecutar planes de capacitación para el personal involucrado con el alcance del SGSI.

3.- Seleccionar y capacitar al personal adecuado para la auditoria interna del SGSI.

3.3.1.4.- PERSONAL DE LA ORGANIZACION

1.- Conocer e identificar aquellos activos de información de los cuales son dueños.

2.- Asegurar que los activos de información que poseen son manejados y administrados correctamente.

3.- Reportar al Oficial de Seguridad de información sobre cualquier vulnerabilidad detectada que afecte sus activos de información.

3.3.2.- POLITICA

Asegurar los activos de información jurado electoral especial Lima Oeste en su confidencialidad, integridad y disponibilidad contra amenazas internas o externas, deliberadas o accidentales mediante la capacitación y concientización de seguridad de información al personal del JEELO con el compromiso del Presidente

y el Pleno para la prevención de incidentes que afecten la continuidad de las operaciones en el JEELO.

3.4.- IDENTIFICACION Y VALORACION DE LOS ACTIVOS DE INFORMACION:

3.4.1.- IDENTIFICACION DE LOS ACTIVOS DE INFORMACION

Una vez mapeado cada uno de los procesos que forman parte del alcance del proyecto, se debe realizar una serie de entrevistas para identificar cada uno de los activos de información que están involucrados en los procesos, luego se procederá a valorarlos y asegurar cada uno de los activos más importantes para la organización.

Para la identificación de estos activos se utilizó el mapa de procesos durante cada una de las entrevistas, ya que permitió asociar los activos con una actividad del proceso.

De acuerdo a la ISO 27001 un activo de la información es todo aquello que de valor a la organización y pueden distinguirse según su naturaleza. Tomando como referencia la mitología Magerit para agrupar los activos y consideraremos los siguientes tipos:

- Actividades y procesos de negocio.- Actividades o procesos de negocio internos (aquellos que una parte de la organización suministra a otra) y externos (aquellos que son suministrados por un tercero a la organización).

- Información (Física o Lógica).- Aquellos datos en cualquier formato que se generen, recopilen, gestionen, transmiten y destruyen la organización.

- Hardware.- Equipos utilizados para gestionar la información (servidores, PCs, impresoras, ups, escáner, fotocopiadoras, router, switches etc.).

- Software.- Aplicaciones informáticas que se utilizan para gestionar la información.

- Redes.- Equipos utilizados para gestionar las comunicaciones que dan soporte a la organización para el movimiento de la información. Pueden ser redes propias o redes contratadas como por ejemplo LAN, DMZ, VLANs yVPN.

- Personal.- Personal propio de la organización, personal subcontratado, clientes, usuarios y en general todos aquellos que tengan acceso de un manera u otra a los activos de información de la organización.

- Sitio.- Lugares en los que se alojan los sistemas de información (Oficinas, Edificios, Agencias, Áreas restringidas, etc.).

- Estructura de la Organización.- Una de sus características de este tipo de activo es que son intangibles como la imagen y la reputación de la organización.

El objetivo de esta parte del proyecto es obtener un inventario de los activos de información involucrados en el alcance del SGSI, para ello se desarrolló una metodología de valoración de activos, basada en lo propuesto por la ISO/IEC 27005:2008, en la cual se detalla cual es el procedimiento para la identificación de los mismos, esta metodología puede ser consultada en el "Anexo 5 – Metodología de Valoración de Activos" del documento.

Para la realización del inventario de activos se tomó en cuenta los siguientes datos:

- Correlativo: Identificador de activo es el numero consecutivo para ordenar los activos.
- Unidad Operativa/Función: Es el área o dpto. donde se encuentra el activo de información.
- Proceso/Subproceso: El proceso en el que se encuentra el activo de información.
- Dueño del proceso/subproceso: Es el responsable del proceso y el dueño del activo de la información.
- Código: Es el nombre o identificador que se ha asignado por el cual se conoce a cada activo listado.
- Nombre Activo: El nombre por el cual se conoce a cada activo listado.
- Descripción: Es una breve descripción del activo o bien puede ser el nombre con el cual es conocido dentro de la empresa.

- Tipo de Activo: Según nuestra metodología que se tiene tomando como referencia la metodología magerit se agrupa a los activos en varios tipos de acuerdo a la función que ejercen el tratamiento de información.

- Clasificación: Para realizar la valoración de activos se clasifican en activos primarios y activos de soporte.

- Propietario: Persona que determina las acciones que se realizan con le activo.

- Usuario: Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de datos personales por encargo del titular de banco personales.

- Dato personal: Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que puedan ser razonablemente utilizadas.

- Datos sensibles: Datos personales constituidos por los datos biométricos que por si mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

- Datos sensibles de los clientes: Datos personales sensibles relacionados al cliente o ciudadano.

- Ubicación Física: Ubicación física del activo de información (oficinas, edificios, agencias, áreas, departamentos, etc.).

- Ubicación Electrónica: Ubicación lógica del activo de información como por ejemplo un numero IP de un servidor.

3.4.2.- VALORACION DE ACTIVOS DE INFORMACION

Una vez identificados cada uno de los activos involucrados en el alcance del SGSI, se debe valorar cada uno de ellos para seleccionar aquellos que pasarán al análisis de riesgo, para ello, se realizaron entrevistas con los dueños de los procesos para responder a la siguiente pregunta ¿De qué manera la pérdida del activo impacta a la confidencialidad/integridad/disponibilidad de la información?

Durante las entrevistas, se utilizó la siguiente tabla de valoración:

		CLASIFICACION DE ACTIVOS	
		PRIMARIO	SOPORTE
CONFIDENCIALIDAD	BAJA = 1	Puede darse a conocer a externos y no ocasionaría perjuicios a la entidad.	La información que es almacenada, transportada y manejada puede darse a conocer a externos
	MEDIA = 5	Solo uso interno en la entidad, todos lo trabajadores de la empresa lo pueden conocer.	La información almacenada, transportada y manejada es de uso interno en la entidad, solo lo pueden conocer los trabajadores.
	ALTA = 10	Accesible solo para algunas personas dentro de la entidad es muy sensible y ocasionaría serios daños si se hace pública.	La información almacenada, transportada y manejada es de confidencialidad alta para el proceso ocasionaría danos si se hace público.

Tabla Nro. 4

Fuente: Elaboración Propia

		CLASIFICACION DE ACTIVOS	
		PRIMARIO	SOPORTE
INTEGRIDAD	BAJA = 1	El impacto es mínimo si la exactitud de esta información se degrada.	El proceso no depende del correcto funcionamiento de este activo la información que procesa, almacena o transporta tiene una integridad baja.
	MEDIA= 5	Si la exactitud de esta información se degrada ocasionaría un impacto significativo en el proceso de negocio.	Fallas en este activo ocasionaría daños considerables en la información de integridad media que procesa, almacena o transporta.
	ALTA= 10	La degradación de la integridad de esta información es inaceptable porque originaria una interrupción del proceso.	Fallas en este activo ocasionaría serios daños en la información de integridad alta que procesa, almacena o transporta. Originando interrupción en el proceso.

Tabla Nro. 5

Fuente: Elaboración Propia

		CLASIFICACION DE ACTIVOS	
		PRIMARIO	SOPORTE
DISPONIBILIDAD	BAJA = 1	La no disponibilidad de esta información por varios días originaria un impacto mínimo en la entidad.	La no disponibilidad de este activo por varios días originaria un impacto mínimo en la entidad y no ocasionaría problemas en la ejecución del proceso.
	MEDIA= 5	Se puede tolerar	Fallas en este activo ocasionaría daños considerables en la información de integridad media que procesa, almacena o transporta.
	ALTA= 10	La degradación de la integridad de esta información es inaceptable porque originaria una interrupción del proceso.	Fallas en este activo ocasionaría serios daños en la información de integridad alta que procesa, almacena o transporta. Originando interrupción en el proceso.

Tabla Nro. 6

Fuente: Elaboración Propia

Una vez valorados todos los activos previamente identificados se escogerán aquellos cuyo valor promedio de confidencialidad, integridad y disponibilidad sea mayor a 5

En el "Anexo 001 – Inventario y Valoración de Activos" se puede encontrar el inventariado de los activos relacionados al alcance del SGSI y valorados por los usuarios.

ORGANIZACIÓN				
Correlativo	Unidad Operativa/Función	Proceso/Subproceso	Dueño del Proceso/Subproceso	
1	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	I
2	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	I
3	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	I
4	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	I
5	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	I
6	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	I
7	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	I
8	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	I
9	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	I
10	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	I

Tabla Nro. 7

Fuente: Elaboración Propia

ACTIVO DE INFORMACIÓN					
Código	Nombre Activo	Descripción	Tipo	Clasificación	
DIGJEE_001	SISTEMA INFORMATICO SIPE	Sistema de Informacion de Proceso Electoral	Software	Activo de Soporte	G
DIGJEE_002	SISTEMA INFORMATICO SICA	Sistema de Informacion de control de actas	Software	Activo de Soporte	G
DIGJEE_003	SISTEMA INFORMATICO SIRA	Sistema de informacion de registro de Acervo	Software	Activo de Soporte	G
DIGJEE_005	SERVIDOR DE BASE DE DATOS	Software gestor de base de datos	Software	Activo de Soporte	G
DIGJEE_008	CARPETA COMPARTIDA	Carpeta compartida para el proceso de digitalizacion	Información	Activo Primario	A
DIGJEE_016	WINDOWS 7 PROFESIONAL	Sistema Operativo usado en las computadoras personales	Software	Activo de Soporte	A
DIGJEE_022	ESPECIALISTA INFORMATICO	Responsable de la digitalizacion de las Actas y manejo de software.	Personal	Activo de Soporte	
DIGJEE_023	ASISTENTE JURIDICCIONAL	Responsable de generar resoluciones a cada Acta y responsable del manejo del SIPE	Personal	Activo de Soporte	
DIGJEE_029	ACTAS ELECTORALES CELESTES	Actas de color celestes con informacion del proceso electoral - recepcionada y resguardadas en el JEE	Información	Activo Primario	P
DIGJEE_030	ACTAS ELECTORALES PLOMAS	Actas de color ploma con informacion del proceso electoral - enviadas por la ODPE para verificar	Información	Activo Primario	A C

Tabla Nro. 8

Fuente: Elaboración Propia

	LEY PROTECCIÓN DATOS PERSONALES				UBICACIÓN	
Propietario (No se requiere en la nueva NTP ISO/IEC 27001:2014)	Usuario	¿Es un dato personal? ' (S/N)	¿Es un dato personal sensible? (S/N)	¿Es un dato sensible de los clientes? (S/N)	Ubicación Física	Ubicación Electrónica
Gerencia TI	Asist. Juridiccional	S	S	S	Lima	192.168.15.121
Gerencia TI	Esp. Informatico	S	S	S	Lima	192.168.15.122
Gerencia TI	Asist. Administrativo	S	S	S	Lima	192.168.15.123
Gerencia TI	DBA	N	N	N	Lima	192.168.15.121
Area Informatica	Esp. Informatico	S	S	S	Lima	192.168.25.150
Area Informatica	Esp. Informatico	N	N	N	Lima	192.168.25.101
		N	N	N	Lima	
		N	N	N	Lima	
Presidenta del JEE	Esp. Informatico	S	S	S	Lima	
Adminitrador de ODPE	Esp. Informatico	S	S	S	Lima	

Tabla Nro. 9

Fuente: Elaboración Propia

NIZ	ACTIVO DE INFORMACIÓN					VALORACIÓN			
Correlativo	Código	Nombre Activo	Descripción	Tipo	Clasificación	Confidencialidad	Integridad	Disponibilidad	Valor del Activo
1	DIGJEE_001	SISTEMA INFORMATICO SIPE	Sistema de Informacion de Proceso Electoral	Software	Activo de Soporte	5	5	5	7
2	DIGJEE_002	SISTEMA INFORMATICO SICA	Sistema de Informacion de control de actas	Software	Activo de Soporte	5	5	5	7
3	DIGJEE_003	SISTEMA INFORMATICO SIRA	Sistema de Informacion de registro de Acervo	Software	Activo de Soporte	1	5	5	4
4	DIGJEE_005	SERVIDOR DE BASE DE DATOS	Software gestor de base de datos	Software	Activo de Soporte	5	5	5	7
5	DIGJEE_008	CARPETA COMPARTIDA	Carpeta compartida para el proceso de digitalizacion	Información	Activo Primario	5	5	1	4
6	DIGJEE_016	WINDOWS 7 PROFESIONAL	Sistema Operativo usado en las computadoras personales	Software	Activo de Soporte	1	5	5	4
7	DIGJEE_022	ESPECIALISTA INFORMATICO	Responsable de la digitalizacion de las Actas y manejo de software.	Personal	Activo de Soporte	5	5	5	7
8	DIGJEE_023	ASISTENTE JURIDICCIONAL	Responsable de generar resoluciones a cada Acta y responsable del manejo del SIPE	Personal	Activo de Soporte	5	5	5	5
9	DIGJEE_029	ACTAS ELECTORALES CELESTES	Actas de color celestes con informacion del proceso electoral - recepcionada y resguardadas en el JEE	Información	Activo Primario	5	5	5	7
10	DIGJEE_030	ACTAS ELECTORALES PLOMAS	Actas de color ploma con informacion del proceso electoral - enviadas por la ODPE para verificar	Información	Activo Primario	5	5	5	7

Tabla Nro. 10

Fuente: Elaboración Propia

3.5.- METODOLOGIA DE ANALISIS DE RIESGOS

En el presente capítulo se elabora la Matriz de Riesgos de la organización, para ello se tendrá que definir una metodología de evaluación de riesgos, existen numerosas metodologías estandarizadas de riesgos, aunque es perfectamente aceptable definir una propia en la cual se describía cual era el apetito de riesgo de la organización, el procedimiento para la identificación de riesgos y el criterio para la evaluación de los mismos.

Para el desarrollo de esta metodología se utilizó la norma ISO/IEC 27005:2008, la cual brinda una guía sobre la gestión de riesgos en la seguridad de la información, y se adaptó según las necesidades de la organización, por lo tanto tenemos lo siguiente:

3.5.1.-METODOLOGÍA DE EVALUACION DE RIESGOS:

3.5.1.1.- IDENTIFICACION DE AMENAZAS:

Una amenaza tiene el potencial de dañar activos como sistemas, procesos o información, por ello es muy importante identificar cuáles son las amenazas principales a los que los activos de información son expuestos.

El oficial de seguridad de información y personal debidamente capacitados deberán realizar entrevistas a los dueños de los procesos con la intención de identificar las amenazas a lo que los activos se encuentran expuestos, para ello podrá hacer uso de un alista de amenazas.

Lista de amenazas:

SISTEMAS OPERATIVOS	Avería de origen físico o lógico
	Errores de Usuarios
	Errores de Administrador
	Difusión de software dañino
	Destrucción de información
	Fugas de información
	Vulnerabilidad de los programas
	Errores de mantenimiento/actualización de software
	Suplantación de identidad de usuario
	Abuso de privilegios de acceso

SERVIDOR BASE DE DATOS	Fuego
	Daños por Agua
	Desastre natural
	Contaminación electromagnética
	Alteración
	Avería de origen físico o lógico
	Corte de suministro eléctrico
	Condiciones inadecuadas de temperatura o humedad
	Errores del Administrador
	Errores de mantenimiento/ actualización de equipos
	Caída del sistema por agotamiento de recursos
	Perdida de equipos
	Abuso de privilegios de acceso
	Acceso no autorizado
	Denegación de servicio
	Robo

ASISTENTE JURIDICCIONAL	Indisponibilidad del personal
	extorsión
	Ingeniería Social(exceso de confianza)
	Fuga de Información
	Deficiencia en la Organización

SISTEMA SIPE	Avería de origen físico o lógico
	Errores de Usuarios
	Errores de Administrador
	Difusión de software dañino
	Destrucción de información
	Fugas de información
	Vulnerabilidad de los programas
	Errores de mantenimiento/actualización de software
	Suplantación de identidad de usuario
	Abuso de privilegios de acceso
	Acceso no autorizado
	Denegación de servicio
	Robo

SISTEMA SICA	Avería de origen físico o lógico
	Errores de Usuarios
	Errores de Administrador
	Difusión de software dañino
	Destrucción de información
	Fugas de información
	Vulnerabilidad de los programas
	Errores de mantenimiento/actualización de software
	Suplantación de identidad de usuario
	Abuso de privilegios de acceso
	Acceso no autorizado
	Denegación de servicio
	Robo

SISTEMA SIRA	Avería de origen físico o lógico
	Errores de Usuarios
	Errores de Administrador
	Difusión de software dañino
	Destrucción de información
	Fugas de información
	Vulnerabilidad de los programas
	Errores de mantenimiento/actualización de software
	Suplantación de identidad de usuario
	Abuso de privilegios de acceso
	Acceso no autorizado
	Denegación de servicio
	Robo

ACTAS ELECTORALES CELESTES	Robo
	Indisponibilidad del personal
	Fuga de Información
	Fuego
	Denegación de servicio

ACTAS ELECTORALES PLOMAS	Robo
	Indisponibilidad del personal
	Fuga de Información
	Fuego
	Denegación de servicio

CARPETA COMPARTIDA	Abuso de privilegios de acceso
	Acceso no autorizado
	Denegación de servicio

ESPECIALISTA INFORMATICO	Difusión de software dañino
	Destrucción de información
	Fugas de información
	Manipulación de Registros de actividad (LOG)
	Manipulación de la configuración
	Suplantación de identidad de usuario
	Abuso de privilegios de acceso
	Intercepción de información(escucha)
	Destrucción de información
	Indisponibilidad del personal
	extorsión
	Difusión de software dañino
	Destrucción de información
	Fugas de información
	Manipulación de Registros de actividad (LOG)
	Manipulación de la configuración

3.5.1.2.- IDENTIFICACION EVALUACION DE RIESGOS

Una vez realizada la identificación de amenazas se podrá identificar fácilmente cuales son los riesgos que amenazan la información y se podrá tomar medidas que ayuden a protegerla.

3.5.1.2.1.- IDENTIFICACION DE RIESGOS:

El riesgo se definirá como la probabilidad que una amenaza explote una vulnerabilidad de un activo haciéndole perder alguna propiedad relacionada a la seguridad de la información (confidencialidad, disponibilidad, integridad, auditabilidad, etc.).

3.5.1.2.2.-DETERMINACION DE PROBABILIDAD E IMPACTO:

Indicar desde la lista desplegable de la celda la Probabilidad del suceso del riesgo; es decir la probabilidad de ocurrencia de un suceso que origina un riesgo que atente contra la confidencialidad, integridad y disponibilidad de la información. Se toma como referencia la descripción de cada nivel de probabilidad presentado en la siguiente tabla:

LISTA DE PROBABILIDADES		
NIVEL	**DESCRIPCION**	**PROBABILIDAD PARA PROCESOS ELECTORALES**
1	**MUY BAJO**	Puede ocurrir en circunstancias excepcionales; como 2 veces cada 4 procesos electorales.
2	**BAJO**	Puede ocurrir en algún momento; al menos una vez cada 2 procesos electorales.
3	**MODERADO**	Puede ocurrir en algún momento; al menos una vez en un proceso electoral.
4	**ALTO**	Probablemente ocurrirá en la mayoría de las circunstancias; al menos una vez al mes
5	**MUY ALTO**	Ocurrirá en la mayoría de las circunstancias; todos los días o varias veces al mes.

Indicar desde la lista despiegable de la celda el nivel de impacto que atentan contra la institución según la siguiente tabla:

LISTA DE NIVELES DE IMPACTO		
NIVEL	**DESCRIPCION**	**PROBABILIDAD PARA PROCESOS ELECTORALES**
1	**INSIGNIFICANTE**	No hay impacto directo sobre la organización, no hay daño a la reputación, no existen sanciones legales ni impacto financiero o operacional no es percibida por los clientes pero si por los colaboradores.
2	**MENOR**	Riesgo aceptable en el sector, no hay daño a la reputación, no hay sanciones legales, poro si observaciones por parte de los reguladores, el impacto operacional o mínimo es financiero.
3	**MODERADO**	El impacto sobre la compañía es directo y medio, se podría incurrir en gastos operativos controlados, existen sanciones por falta leve, se expone la imagen de la organización con un impacto medio..
4	**MAYOR**	Daño sobre la empresa es mayor, riesgo inusual o inaceptable en el sector; cobertura a nivel nacional; investigación del regulador y sanciones por falta grave; involucramiento de la alta gerencia, gastos operativos de consideración; pérdidas financieras mayores.
5	**CATASTROFICA**	Pérdida o daño catastrófico a la reputación de la organización, pérdidas financieras Importantes, cobertura a nivel nacional y de forma prolongada; intervención regulatoria con sanciones por faltas muy graves; pérdida de clientes a gran escala; involucramiento directo de la alta gerencia o directorio.

3.5.1.2.3.-EVALUACION DEL NIVEL Y VALOR DE RIESGO:

El nivel de los riesgos se obtendrá de la multiplicación de la probabilidad y el impacto previamente definido por los dueños de los procesos lo cual permitirá ubicar al riesgo en uno de las siguientes celdas:

		Impacto				
	Escala	1	2	3	4	5
Probabilidad	5	5	10	15	**20**	**25**
	4	4	8	12	16	**20**
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Tabla Nro. 11

Fuente: Elaboración Propia

Una vez se obtenga el nivel de los riesgos, estos deberán ser clasificados según los siguientes niveles de riesgo mostrados en la siguiente tabla.

Nivel de Seguridad	
BAJO	
MEDIO	
ALTO	

Tabla Nro. 12

Fuente: Elaboración Propia

3.5.1.2.4.-PLAN DE TRATAMIENTO DE RIESGO:

Seleccionar desde la lista desplegable de la celda la opción de tratamiento del riesgo, la cual debe ser validado por el propietario del riesgo. Entre las opciones tenemos:

Tratamiento	Descripción
EVITAR	Cese de la actividad que lo origina.
ACEPTAR	No realizar nada.
TRANFERIR	Consiste en trasladar el impacto de un riesgo a un tercero, junto con la responsabilidad de la respuesta. El trasladar o compartir el riesgo no implica que se deje de ser propietario del riesgo.
MITIGAR	- Identificar controles - Desarrollar el SOA (Declaración de Aplicabilidad)

Tabla Nro. 13

Fuente: Elaboración Propia

3.5.1.2.5.-CONTROLES:

Una vez identificados y evaluados cada uno de los riesgos que amenazan a los activos claves de la organización, el oficial de seguridad de información, con la ayuda de la NTP ISO/IEC 17799, deberá identificar que controles ha de implementar para reducir el impacto o la probabilidad de los mismos hasta llevarlos a un nivel aceptable e introducir esta información dentro de la matriz de riesgo, a fin de mantener un registro de estos datos.

5 Política de seguridad

5.1 Política de seguridad de la información

5.1.1 Documento de la política de seguridad de la información

5.1.2 Revisión de la política de seguridad de la información

6 Organización de la seguridad de la información

6.1 Organización interna

6.1.1 Compromiso de la gerencia con la seguridad de la información

6.1.2 Coordinación de la seguridad de la información

6.1.3 Asignación de las responsabilidades de la seguridad de la información

6.1.4 Autorización de proceso para facilidades procesadoras de información.

6.1.6 Contacto con las autoridades

6.1.7 Contacto con grupos de interés especial

6.1.8 Revisión independiente de la seguridad de la información

6.2 Grupos o personas externas

6.2.1 Identificación de los riesgos relacionados con los grupos externos

6.2.2 Tratamiento de la seguridad cuando se lidia con clientes

6.2.3 Tratamiento de la seguridad en acuerdos con terceros

7 Gestión de activos

7.1 Responsabilidad por los activos

7.1.1 Inventario de los activos

7.1.2 Propiedad de los activos

7.1.3 Uso aceptable de los activos

7.2 Clasificación de la información

7.2.1 Lineamientos de clasificación

7.2.2 Etiquetado y manejo de la información

8 Seguridad de recursos humanos

8.1 Antes del empleo

8.1.1 Roles y responsabilidades

8.1.2 Investigación de antecedentes

8.1.3 Términos y condiciones del empleo

8.2 Durante el empleo

8.2.1 Responsabilidades de la gerencia

8.2.2 Conocimiento, educación y capacitación en seguridad de la información

8.2.3 Proceso disciplinario

8.3 Terminación o cambio de empleo

8.3.1 Responsabilidades de terminación

8.3.2 Devolución de los activos

8.3.3 Retiro de los derechos de acceso

9 Seguridad física y ambiental

9.1 Áreas seguras

9.1.1 Perímetro de seguridad física

9.1.2 Controles de ingreso físico

9.1.3 Asegurar las oficinas, habitaciones y medios

9.1.4 Protección contra amenazas externas e internas

9.1.5 Trabajo en áreas aseguradas

9.1.6 Áreas de acceso público, entrega y carga

9.2 Equipo de seguridad

9.2.1 Ubicación y protección del equipo

9.2.2 Servicios públicos de soporte

9.2.3 Seguridad del cableado

9.2.4 Mantenimiento de equipo

9.2.5 Seguridad del equipo fuera del local

9.2.6 Seguridad de la eliminación o re-uso del equipo

9.2.7 Retiro de propiedad

10 Gestión de las comunicaciones y operaciones

10.1 Procedimientos y responsabilidades operacionales

10.1.1 Procedimientos de operación documentados

10.1.2 Gestión del cambio

10.1.3 Segregación de los deberes

10.1.4 Separación de los medios de desarrollo, prueba y operación

10.2 Gestión de la entrega del servicio de terceros

10.2.1 Entrega del servicio

10.2.2 Monitoreo y revisión de los servicios de terceros

10.2.3 Manejo de cambios en los servicios de terceros

10.3 Planeación y aceptación del sistema

10.3.1 Gestión de la capacidad

10.3.2 Aceptación del sistema

10.4 Protección contra el código malicioso y móvil

10.4.1 Controles contra códigos maliciosos

10.4.2 Controles contra códigos móviles

10.5 Respaldo o Back-Up

10.6 Gestión de seguridad de la red

10.6.1 Controles de redes

10.6.2 Seguridad de los servicios de la red

10.7 Gestión de medios

10.7.1 Gestión de medios removibles

10.7.3 Procedimientos para el manejo de información

10.7.4 Seguridad de la documentación del sistema

10.8 Intercambio de información

10.8.1 Políticas y procedimientos de intercambio de información

10.8.2 Acuerdos de intercambio

10.8.3 Medios físicos en tránsito

10.8.4 Mensajes electrónicos

10.8.5 Sistemas de información comercial

10. 9 Servicios de comercio electrónico

10.9.1 Comercio electrónico

10.9.2 Transacciones en-línea

10.9.3 Información públicamente disponible

10.10 Monitoreo

10.10.1 Registro de auditoría

10.10.2 Uso del sistema de monitoreo

10.10.3 Protección del registro de información

10.10 4 Registros del administrador y operador

10.10.5 Registro de fallas

10.10.6 Sincronización de relojes

11 Control del acceso

11.1 Requerimiento del negocio para el control del acceso

11.1.1 Poiítica de control del acceso

11.2 Gestión de acceso del usuario

11.2.1 Registro del usuario

11.2.2 Gestión de privilegios

11.2.3 Gestión de las claves secretas de los usuarios

11.2.4 Revisión de los derechos de acceso del usuario

11.3 Responsabilidades del usuario

11.3.1 Uso de claves secretas

11.3.2 Equipo del usuario desatendido

11.3.3 Política de escritorio y pantalla limpios

11.4 Control de acceso a la red

11.4.1 Política sobre el uso de los servicios de la red

11.4.2 Autenticación del usuario para las conexiones externas

11.4.3 Identificación del equipo en las redes

11.4. Protección del puerto de diagnóstico y configuración remoto

11.4.5 Segregación en redes

11.4.6 Control de conexión a la red

11.4.7 Control de routing de la red

11.5 Control del acceso al sistema operativo

11.5.1 Procedimientos para un registro seguro

11.5.2 Identificación y autenticación del usuario

11.5.3 Sistema de gestión de claves secretas

11.5.4 Uso de las utilidades del sistema

11.5.5Cierre de una sesión por inactividad

11.5.6 Limitación del tiempo de conexión

11.6 Control de acceso a la aplicación y la información

11.6.1 Restricción del acceso a la información

11.6.2 Aislar el sistema confidencial

11.7 Computación y tele-trabajo móvil

11.7.1 Computación y comunicaciones móviles

11.7.2 Tele-trabajo

12 Adquisición, desarrollo y mantenimiento de los sistemas de información

12.1 Requerimientos de seguridad de los sistemas de información

12.1.1 Análisis y especificación de los requerimientos de seguridad

12.2 Procesamiento correcto en las aplicaciones

12.2.1 Validación de la input data

12.2.2 Control del procesamiento interno

12.2.3 Integridad del mensaje

12.2.4 Validación de la output data

12.3 Controles criptográficos

12.3.1 Política sobre el uso de controles criptográficos .

12.3.2 Gestión de claves

12.4 Seguridad de los archivos del sistema

12.4.1 Control del software operacional

12.4.2 Protección de la data del sistema

12.4 3 Control de acceso al código fuente del programa

12.5 Seguridad en los procesos de desarrollo y soporte

12.5.1 Procedimientos del control del cambio

12.5.2 Revisión técnica de la aplicación después de cambios en el sistema

12.5.3 Restricciones sobre los cambios en los paquetes de software

12.5.4 Filtración de información

12.5.5 Desarrollo de software abastecido externamente

12.6 Gestión de la Vulnerabilidad Técnica

12.6.1 Control de las vulnerabilidades técnicas

13 Gestión de un incidente en la seguridad de la información

13.1 Reporte de los eventos y debilidades de la seguridad de la información

13.1.1 Reporte de eventos en la seguridad de la información

13.1.2 Reporte de las debilidades en la seguridad

13.2 Gestión de los incidentes y mejoras en la seguridad de la información

13.2.1 Responsabilidades y procedimientos

13.2.2 Aprender de los incidentes en la seguridad de la información

13.2.3 Recolección de evidencia

14 Gestión de la continuidad del negocio

14.1 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio

14.1.1 Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio

14.1.2 Continuidad del negocio y evaluación del riesgo

14.1.3 Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información

14.1.4 Marco Referencial de la planeación de la continuidad del negocio

14.1.5 Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio.

15 Cumplimiento

15.1 Cumplimiento de los requerimientos legales

15.1.1 Identificación de la legislación aplicable

15.1.2 Derechos de propiedad intelectual (IPR)

15.1.3 Protección de registros organizacionales

15.1.4 Protección de la data y privacidad de la información personal

15.1.5 Prevención del mal uso de los medios de procesamiento de la información.

15.1.6 Regulación de controles criptográficos

15.2 Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico

15.2.1 Cumplimiento con las políticas y estándares de seguridad

15.2.2 Chequeo del cumplimiento técnico

15.3 Consideraciones de auditoria de los sistemas de información

15.3.1 Controles de auditoría de los sistemas de información

15.3.2 Protección de las herramientas de auditoría de los sistemas de información

3.5.1.2.6.-RIESGO RESIDUAL:

El oficial de seguridad de información debe realizar un seguimiento en el tiempo y revisar cada uno de los controles implementados para asegurar que exista una verdadera reducción de la probabilidad o impacto del riesgo.

IDENTIFICACION Y EVALUACION DE RIESGOS DEL ACTIVO DE INFORMACION SICA (SISTEMA DE INFORMACION DE CONTROL DE ACTAS.

ACTIVO						
Código	Descripción	Valoración	Amenaza	Probabilidad	Impacto	Riesgo
DIGJEE_001	SISTEMA INFORMATICO SIPE	10	Avería de origen físico o lógico	4	5	
			Errores de Usuarios	4	4	
			Errores de Administrador	3	4	12
			Difusión de software dañino	2	3	6
			Destrucción de información	1	2	2
			Fugas de información	2	3	6
			Vulnerabilidad de los programas	3	3	9
			Errores de mantenimiento/actualización de software	2	3	6
			Suplantación de identidad de usuario	2	3	6
			Abuso de privilegios de acceso	2	3	6
			Acceso no autorizado	2	3	6
			Denegación de servicio	4	5	
			Robo	1	3	3

		Impacto				
	Escala	1	2	3	4	5
Probabilidad	5	5	10	15		
	4	4	8	12	16	
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Tabla Nro. 14

Fuente: Elaboración Propia

		TRATAMIENTO DEL RIESGO			
Codigo Riesgo	Propietario Riesgo	Control	Responsable Control	Plan de Accion	Fecha(de ejec
RGOJEE_001	Usuario de equipo informatico	A.9.1.4, A.9.2.4	Especialista Informatico	Mantenimiento preventivo	sep-16
RGOJEE_002	Usuario de equipo informatico	A.8.2.2,A.11.2.3,A.11.5.2	Asistente Jurisdiccional, Mesa de Partes	Concientizar y capacitar a los usuarios.	sep-16
RGOJEE_003	Especilsita Informatico				sep-16
RGOJEE_004	Usuario de equipo informatico				sep-16
RGOJEE_005	Especilsita Informatico				sep-16
RGOJEE_006	Usuario de equipo informatico				sep-16
RGOJEE_007	Usuario de equipo informatico				sep-16
RGOJEE_008	Usuario de equipo informatico				sep-16
RGOJEE_009	Usuario de equipo informatico				sep-16
RGOJEE_010	Usuario de equipo informatico				sep-16
RGOJEE_011	Usuario de equipo informatico				sep-16
RGOJEE_012	Gerente de TI	A.10.3.1,A.10.3.2,A.10.8.1,A.10.8.5,A.10.10.5,A.13.1.2,A.13.2.1	Gerente de TI, Especilista Informatico	Establecer responsabilidades y procedimientos en las comunicaciones y operaciones del sistema.	sep-16
RGOJEE_013	Usuario de equipo informatico				sep-16

Tabla Nro. 15

Fuente: Elaboración Propia

		RIESGO RESIDUAL		
Codigo Riesgo	Propietario Riesgo	Probabilidad	Impacto	Riesgo
RGOJEE_001	Usuario de equipo Informatico	3	3	9
RGOJEE_002	Usuario de equipo Informatico	3	3	9
RGOJEE_003	Especilsita Informatico	2	3	6
RGOJEE_004	Usuario de equipo Informatico	1	2	2
RGOJEE_005	Especilsita Informatico	1	2	2
RGOJEE_006	Usuario de equipo informatico	1	2	2
RGOJEE_007	Usuario de equipo informatico	2	2	4
RGOJEE_008	Usuario de equipo informatico	2	2	4
RGOJEE_009	Usuario de equipo informatico	2	2	4
RGOJEE_010	Usuario de equipo informatico	2	2	4
RGOJEE_011	Usuario de equipo informatico	2	2	4
RGOJEE_012	Gerente de TI	3	4	12
RGOJEE_013	Usuario de equipo informatico	1	2	2

Tabla Nro. 16

Fuente: Elaboración Propia

3.6.- DECLARACION DE APLICABILIDAD

La norma NTP ISO/IEC 27001:2008, exige como parte del establecimiento del SGSI, la preparación de la declaración de aplicabilidad incluyendo cuales son los objetivos de control y los controles seleccionados justificando su elección.

En este documento se analizara cada uno de los controles propuestos por estas normas y se indicara si son aplicables a la realidad de la empresa o si no lo son justificando en ambos casos el porqué de esta decisión.

Este documento puede ser revisado como anexo del presente proyecto con nombre Anexo 2 – Declaración de Aplicabilidad que muestra la siguiente información:

- Nro. de control: El identificador de cada uno de los controles propuestos por la norma.

- Control: El nombre de control, se hace referencia a un tema específico al que riesgo puede estar asociado.

- Objetivo de control: Es la descripción del control, en el se indica exactamente a que se refiere cada uno de los controles de la norma.

- Aplicable a la Organización: Se indica si el control en mención es aplicable a la organización o si no lo es.

- Justificación: La justificación de la aplicabilidad o no aplicabilidad del control en mención.

4.- CAPITULO IV: CONCLUSIONES Y RECOMENDACIONES

4.1.- CONCLUSIONES:

- La obtención del diseño de un sistema de gestión de seguridad de información adecuado cumpliendo las NTP ISO\IEC 27001 es indispensable para toda entidad pública cumpliendo la confidencialidad, integridad y disponibilidad de la información brindando calidad y confianza en los procesos electorales.

- Se logró elaborar documentos exigidos por la NTP ISO\IEC 27001 como el modelo del negocio (business case), alcance del JEE y la política de seguridad de información.

- Se identificó los activos de información y se logró elaborar una metodología para valorar los activos de información.

- Se logró elaborar una metodología de análisis de riesgos propia para el JEE donde se evaluó los riesgos que amenazan a activos críticos de información.

- Se logró elaborar del listado de controles de acuerdo a la norma NTP ISO\IEC 17799 y obtuvo el documento de aplicabilidad es importante para las auditorias que se tenga en la institución.

4.2.- RECOMENDACIONES:

- Es importante el apoyo y compromiso de los directivos para el diseño del SGSI debido a que fue necesario su intervención y colaboración para la elaboración de la documentación exigida por la norma, concientizar al personal.

- Es importante el apoyo de los jefes de área o personal clave para la identificación de los activos de información y desarrollo de una metodología para valorar los activos de información identificando los activos claves para el JEE.

- Es necesario implementar talleres de capacitación y concientización para mejorar la cultura en seguridad de información del personal del JEE.

- Es necesario que la organización asigne un presupuesto orientado a la implementación de los controles del SGSI, así como las capacitaciones, charlas de concientización, servicios de consultoría.

- Se propone como trabajo futuro el diseño e implementación de un sistema de gestión de continuidad de negocio.

REFERENCIA BIBLIOGRAFICA

1. MAGERIT – versión 3.0. **Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método** Ministerio de Hacienda y Administraciones Públicas, España 2012

2. ESCORIAL, Ángel **La gestión de riesgos impulse la credibilidad y la transparencia** Gerencia de Riesgos y Seguros. España, 2012

3. Alberto G. Alexander. **Diseño de un Sistema de Gestión de Seguridad de información** Editorial Hispano americana Marcombo 2007

4. Harold F. Tipton, CISSP – Micki Krause CISSP **Information Security Management Handbook, 6th edition** Editorial Aurbach Publications 2006

5. By John A. Blackley - **Information Security Fundamentals 1st (first) Edition** Editorial Paperback 2005

6. http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552

7. http://www.acis.org.co/fileadmin/Base_de_Conocimiento/XIV_JornadaSeguridad/ELSI_2014.pdf

8. http://tesisdeinvestig.blogspot.pe/2011/05/tipos-de-investigacion.html

9. http://www.iso27000.es/sgsi.html

10. http://www.seinhe.com/gestion-de-activos-ti/

11. http://www.iso27000.es/download/doc_sgsi_all.pdf

12. http://www.indecopi.gob.pe/0/modulos/NOT/NOT_DetallarNoticia.aspx?PFL=0&NOT=6 12 INDECOPI 2013. "INDECOPI garantiza la seguridad de la información al obtener la Certificación ISO 27001". Noticia en página web. Consulta

13. Ley Orgánica de la Oficina Nacional de Procesos Electorales Ley Nº 26487

14. Ley Orgánica del Jurado Nacional de Elecciones Ley Nº 26486

GLOSARIO

- **JURADO NACIONAL DE ELECCIONES.-** Organismo autónomo que cuenta con personería jurídica de derecho público encargado de administrar justicia en materia electoral; de fiscalizar la legalidad del ejercicio del sufragio, de la realización de los procesos electorales, del referéndum y de otras consultas populares y de la elaboración de los padrones electorales; de mantener y custodiar el registro de organizaciones políticas; y demás atribuciones a que se refieren la Constitución y las leyes.

- **JURADO ELECTORAL ESPECIAL.-** Órgano de carácter temporal, creado para un determinado proceso electoral o consulta popular. Las funciones y atribuciones del JEE están establecidas en la Ley Orgánica del JNE, la LOE y demás normas pertinentes.

- **PRESIDENTE DEL JEE.-** Es el juez superior designado por la Corte Superior de Justicia bajo cuya circunscripción se encuentra la sede del JEE.

- **CIRCUNSCRIPCIÓN ELECTORAL O DISTRITO ELECTORAL.-** Conjunto de electores asentados en un determinado territorio, que conforma la base para que sus votos se repartan entre un número determinado de escaños o cargos. En ella se asignan éstos a los ganadores de las elecciones. La circunscripción, dependiendo de cada proceso electoral, puede ser distrital, provincial, departamental o nacional.

- **RADIO URBANO**.- Esto es señalar el ámbito territorial dentro del cual las organizaciones políticas deben señalar su domicilio procesal, para ser notificados de las resoluciones emitidas por el Jurado Electoral Especial. Debe definirse con indicación precisa -denominación vigente- de la plaza, avenida, jirón o calle, las intersecciones e indicación de los puntos de inicio y fin. La determinación del radio urbano debe efectuarse a través de una resolución, a la cual debe anexarse un plano para mejor orientación a los interesados.

- **DIFUSIÓN DE INFORMACIÓN EN CONTRA**.- Es toda aquella noticia que tiene por objeto desacreditar o denigrar a una organización política que participa en un proceso electoral, incluyendo a sus candidatos, personeros, militantes y simpatizantes.

- **FRANJA ELECTORAL REGIONAL**.- Es el espacio publicitario emitido en canales de televisión de señal abierta y estaciones de radio, públicos y privados, de cobertura nacional y regional, puesto a disposición de las organizaciones políticas participantes en el Proceso de Elecciones Regionales, para que sin costo alguno puedan difundir propaganda electoral.

- **LAS LISTAS DE CANDIDATOS**.- Es aquel cuerpo que representa, respetando un orden de prelación, aquel menú de candidaturas presentadas por una determinada organización política dentro de una determinada circunscripción electoral. La Lista de Candidatos está compuesta por miembros titulares y suplentes, los primeros constituyen la primera opción mientras que los segundos

constituyen una reserva sólo recurrible en caso que la candidatura de los primeros resulte fallida por algún factor exógeno.

- **LISTA CERRADA Y BLOQUEADA**.- Permite al votante dar su voto a una lista en bloque. El elector tiene que ceñirse al orden de aparición de los candidatos en la lista tal y como fue dispuesto por el partido; y no puede alterarlo.

- **MEDIOS DE COMUNICACIÓN SOCIAL**.- Son las instituciones públicas y privadas que brindan información a través de la prensa, la radio, la televisión, así como las redes sociales y demás servicios existentes en Internet.

- **ORGANIZACIÓN POLÍTICA**.- Asociación de ciudadanos que adquiere personería jurídica con su inscripción en el Registro de Organizaciones Políticas, cuya finalidad es ejercer sus actividades dentro y fuera de periodos electorales, formulando propuestas o programas de gobierno y contribuyendo a la formación de la voluntad cívico-ciudadana. El término organización política comprende a los partidos con alcance nacional, a los movimientos de alcance regional o departamental, a las alianzas electorales y a las organizaciones políticas locales, provinciales y distritales.

- **OFICINAS DESCENTRALIZADAS DE PROCESOS ELECTORALES**.- Son órganos electorales de carácter temporal, constituidos para un proceso específico, de acuerdo con las circunscripciones electorales que determine el Jurado Nacional de Elecciones.

- **PROPAGANDA POLÍTICA**.- Toda acción o efecto en aras de conocer la ejecución de los planes y programas que desarrollan las entidades estatales y sus

dependencias, con el propósito de conseguir adhesión o apoyo hacia una determinada organización, programa, ideología u orientación política, sujeta a prohibiciones cuando se trata de procesos electorales en trámite.

- **PROPAGANDA ELECTORAL**.- Propaganda política que se realiza en un período electoral, orientada a persuadir a los ciudadanos 5 para obtener resultados electorales a través de la captación de sus votos y con ello aspirar a cargos políticos por elección popular

- **PUBLICIDAD ESTATAL**.- Toda divulgación de información que tenga por finalidad promover conductas de relevancia social o que coadyuven a la ejecución de los planes y programas a cargo de las entidades y sus dependencias, a través de cualquier medio de difusión.

- **PUBLICIDAD ESTATAL POR EXCEPCIÓN**.- Toda divulgación de información realizada por las entidades y sus dependencias, en época de elecciones regionales y municipales, justificada por razones de necesidad y utilidad públicas

- **TACHA**.- Es la oposición que pueden formular los ciudadanos contra candidaturas, listas de candidatos, miembros de Jurados Electorales Especiales, personal de las Oficinas Descentralizadas de Procesos Electorales y organizaciones políticas en proceso de inscripción.

- **TOTAL DE VOTOS EMITIDOS**.- Es el resultado de la suma de los votos a favor de las organizaciones políticas, más los votos en blanco, nulos e impugnados, correspondiente a cada tipo de elección en el acta electoral.

- **AUDITOR**.- (Inglés: Auditor). Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.

- **AUDITORÍA**.- (Inglés: Audit). Proceso sistemático, independiente y documentado para obtener evidencias de auditoriía y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

- A**UTENTICACIÓN**.- (Inglés: Authentication). Provisión de una garantía de que una característica afirmada por una entidad es correcta.

- **AUTENTICIDAD**.- (Inglés: Authenticity). Propiedad de que una entidad es lo que afirma ser.

- **CONFIDENCIALIDAD**.- (Inglés: Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **CONTROL**.- Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **DESASTRE**.- (Inglés: Disaster). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

- **DISPONIBILIDAD**.- (Inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **ISACA**.- Information **S**ystems Audit and Control Association. Publica CobiT y gestiona diversas acreditaciones personales en el ámbito de la auditoría de sistemas y la seguridad de la información.

- **ISSA**.- Information Systems **S**ecurity Association.

- **PROCESO**.- (Inglés: Process). Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

- .**TRAZABILIDAD**.- (Inglés: Accountability). Según [CESID:1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

- **VULNERABILIDAD**.- (Inglés: **V**ulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas.

GLOSARIO DE ABREVIACIONES

JNE.- Jurado Nacional de Elecciones.

JEE.- Jurado Electoral Especial.

LOE.- Ley Orgánica de Elecciones

ODPE.- Oficina Descentralizada de Procesos Electorales.

RENIEC.- Registro Nacional de Identificación y Estado Civil.

DNFPE.- Dirección Nacional de Fiscalización y Procesos Electorales.

DRET.- Dirección de Registros, Estadística y Desarrollo Tecnológico

DGRS.- Dirección General de Recursos y Servicios

SIPE-SG.-: Sistema de Información de Procesos Electorales de la Secretaría General.

SIRC.- Sistema Integrado de Rendición de Cuentas.

URE.- Unidad Regional de Enlace

Formato: SSI-022

INVENTARIO DE ACTIVOS DE INFORMACIÓN

Preparado por: Javier Lopez Jurado

ORGANIZACIÓN		ACTIVO DE INFORMACIÓN							LEY PROTECCIÓN DE DATOS PERSONALES				UBICACIÓN	VALORACIÓN			
Unidad Operativa/Función	Proceso/Subproceso	Dueño del Proceso/Subproceso	Código	Nombre Activo	Descripción	Tipo	Clasificación	Propietario (No se requiere en la nueva NTP ISO/IEC 27001:2014)	Usuario	¿Es un dato personal? (S/N)	¿Es un dato personal sensible? (S/N)	¿Es un dato sensible de los clientes? (S/N)	Ubicación Física	Ubicación Electrónica	Confidencialidad	Integridad	Disponibilidad	Valor del Activo
1 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_001	SISTEMA INFORMATICO SIPE	Sistema de información de Proceso electoral	Software	Activo de Soporte	Gerencia TI	Asist. Jurisdiccional	S	S	S	Lima	192.168.15.121				
2 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_002	SISTEMA INFORMATICO SICA	Sistema de información de control de actas	Software	Activo de Soporte	Gerencia TI	Esp. Informatico	S	S	S	Lima	192.168.15.122				
3 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_003	SISTEMA INFORMATICO SIRA	Sistema de información de registro de Acopio	Software	Activo de Soporte	Gerencia TI	Asist. Administrativo	S	S	S	Lima	192.168.15.123	S			
4 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_004	WINDOWS 2008 SERVER	Sistema operativo usado para el servidor de Base de Datos	Software	Activo de Soporte	Gerencia TI	Esp. Plataforma TICs	N	N	N	Lima	192.168.15.121	S			
5 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_005	SQL SERVER 2008	Software gestor de base de datos	Software	Activo de Soporte	Gerencia TI	DBA	N	N	N	Lima	192.168.15.121	S			
6 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_006	NOD 32 CORPORATIVO	Software de protección de servidor	Software	Activo de Soporte	Gerencia TI	Esp. Seg. Informatica	N	N	N	Lima		S		S	7
7 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_007	ENDIAN FIREWALL	Software Distribucion Linux Cortafuegos	Software	Activo de Soporte	Gerencia TI	Esp. Seg. Informatica	N	N	N	Lima		S			
8 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_008	CARPETA COMPARTIDA	Carpeta compartida para el proceso de digitalizacion	Información	Activo Primario	Area de digitalizacion	Esp. Informatico	S	S	S	Lima			S	S	7
9 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_009	CARPETA DE ACTAS DIGITALIZADAS	Carpeta contenida de actas electorales digitalizadas	Información	Activo Primario	Area de digitalizacion	Esp. Informatico	S	S	S	Lima					
10 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_010	KODAK ALARIS	Software de escaneo Documentos.	Software	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		1	S		6
11 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_011	ADVANCED RENAMER	Software de renombra de archivos	Software	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		1	S		6
12 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_012	PDF SAM INSTALLER	Software de Edicion archivos corregir unir y rotar	Software	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		1	S		6
13 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_013	AOSTOSOFT PDF TO DOCUMENT IMAGE	Software de Edicion archivos PDF convertir pdf a Image	Software	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		1	S		6
14 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_014	ACTAS DIGITALES	Actas en formato digital en jpeg - jpg	Información	Activo Primario	Area de digitalizacion	Esp. Informatico	S	S	S	Lima					
15 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_015	BACKUP CARPETA DIGITALIZADAS	Copia de respaldo de las actas digitales.	Información	Activo Primario	Area de digitalizacion	Esp. Informatico	S	S	S	Lima					
16 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_016	WINDOWS 7 PROFESIONAL	Sistema operativo usado en las computadoras personales	Software	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		1	S	S	6
17 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_017	OFFICE 2010	Software ofimatico word,excel, etc	Software	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		1	S	S	6
18 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_018	ANTIVIRUS AVG	Software de protección usuarios contra virus	Software	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		1	S	S	6
19 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_019	INTERNET EXPLORER 9	Software navegador de internet	Software	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		1	S	S	6
20 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_020	ADOBE ACROBAT	Software editor de archivos PDF	Software	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		1	S	S	6
21 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_021	MESA DE PARTES	Responsable de la recepcion de documentos y responsable del manejo del SIRA	Personal	Activo de Soporte						Lima		1	S	S	6
22 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_022	ESPECIALISTA INFORMATICO	Responsable de la digitalizacion de las Actas y manejo de software.	Personal	Activo de Soporte						Lima					
23 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_023	ASISTENTE JURIDICCIONAL	Responsable de generar resoluciones a cada Acta y responsable del manejo del SIRA	Personal	Activo de Soporte						Lima			S	S	7
24 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_024	TECNICO DE ARCHIVO DOCUMENTARIO	Personal de apoyo del JEE para la digitalizacion de Actas electorales y manejo documentario.	Personal	Activo de Soporte						Lima			S	S	7
25 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_025	ASISTENTE ADMINISTRATIVO	Personal de apoyo del JEE para la digitalizacion de Actas electorales	Personal	Activo de Soporte						Lima					
26 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_026	ESPECIALISTA EN RECURSOS	Personal encargado de brindar todos lo recursos al proceso de digitalizacion.	Personal	Activo de Soporte						Lima			S	S	6
27 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_027	PERSONAL DE SEGURIDAD	Personal de apoyo en la recepcion de actas y envio de acervo documentario.	Personal	Activo de Soporte						Lima		S	S	S	6
28 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_028	SECRETARIA JURIDICCIONAL	Personal raponsable de recepcionar Actas y dar conformidad.	Personal	Activo de Soporte						Lima			S	S	7
29 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_029	ACTAS ELECTORALES CELESTES	Actas de color celestes con Informacion del proceso electoral - recepcionada y resguardadas en el JEE	Información	Activo Primario	Presidenta del JEE	Esp. Informatico	S	S	S	Lima					
30 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_030	ACTAS ELECTORALES PLOMAS	Actas de color ploma con informacion del proceso electoral - enviadas por la ODPE para verificar	Información	Activo Primario	Administrador de ODPE	Esp. Informatico	S	S	S	Lima					
31 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_031	REPORTE DE ACTAS - ODPE	Informacion del Total de actas enviadas al JEE junto al documento de entrega de actas	Información	Activo Primario	Administrador de ODPE	Esp. Informatico	S	S	S	Lima					
32 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_032	REPORTE DE ACTAS - JEE	Reporte generado por el SICA una vez registrada todas las actas.	Información	Activo Primario	Area de digitalizacion	Esp. Informatico	S	S	S	Lima					
33 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_033	DOCUMENTO DE ENTREGA ACTAS	Documento relacionado al envio de las actas con fecha de envio , cantidad y otras caracteristicas.	Información	Activo Primario	Area de digitalizacion	Mesa de Partes	N	N	N	Lima		S	S	S	6
34 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_034	CRONOGRAMA ELECTORAL	Cronograma del proceso electoral	Actividades y Proceso de negocio	Activo Primario	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		1	S	1	6
35 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_035	CUADERNO DE CONTROL	Cuaderno escrito por le personal de seguridad registre todo los eventos de ingreso y salida del JEE	Información	Activo Primario	R.R.H.H.	Seguridad	N	N	N	Lima		S	S	S	6
36 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_036	FILE DE REGLAMENTO	File contenida de Reglamentos para el buen funcionamiento del JEE	Información	Activo Primario	R.R.H.H.	Jefa de R.R.H.H.	N	N	N	Lima		S	S	S	6
37 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_037	FILE DE REPORTES	File contenida de Reportes generados por los sistemas y reportes de actas de entrega de la ODPE.	Información	Activo Primario	Gerencia de Archivos	Mesa de Partes	N	N	N	Lima		S	S	1	6
38 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_038	FILE DE CARGOS	File contenida de cargos de envio de documentos, requerimientos y informes.	Información	Activo Primario	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		1	S	1	3
39 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_039	FILE DE GUIAS	File contenida de las guias recibidas de los equipo y dispositivos informaticos, recepcion de materiales y suministros administrativos y informaticos.	Información	Activo Primario	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		1	S	1	3
40 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_040	REPORTE DE EXPEDIENTES ACTAS OBSERVADAS	Reporte de expedientes generados por el area jurisdiccional relacionadas a proceso de actas observadas.	Información	Activo Primario	Area Jurisdiccional	Asistenta Jurisdiccional	N	N	N	Lima			S	S	7
41 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_041	REPORTE TOTAL EXPEDIENTES DEL SIPE	Reporte total de expedientes generados por el sistema de Información de procesos electorales.	Información	Activo Primario	Area Jurisdiccional	Asistenta Jurisdiccional	N	N	N	Lima		S	S	S	6
42 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_042	REPORTE TOTAL DE ACTAS OBSERVADAS	Reporte total de actas observadas ingresadas en el sica.	Información	Activo Primario	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		S	S	S	6
43 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_043	REPORTE ACTAS CELESTES	Reporte de control de actas ingresadas y digitalizadas.	Información	Activo Primario	Area de digitalizacion	Esp. Informatico	N	N	N	Lima			S	S	7
44 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_044	REPORTE DE DISTRITOS	Reporte de los distritos con la cantida de actas que le corresponden.	Información	Activo Primario	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		1	S	S	6
45 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_045	REPORTE DE ACERVO	Informacion de Documentos enviados al JNE	Información	Activo Primario	Gerencia de Archivos	Mesa de Partes	N	N	N	Lima		S	S	S	6
46 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_046	CARGOS DE RECEPCION	Cargos de documentos y informes recepcionados	Información	Activo Primario	Gerencia de Archivos	Mesa de Partes	N	N	N	Lima		S	S	1	6
47 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_047	CARGOS DE EMISION	Copias de documentos y informes enviados	Información	Activo Primario	Gerencia de Archivos	Mesa de Partes	N	N	N	Lima		S	S	1	6
48 SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_048	REGLAMENTO DE DIGITALIZACION DE ACTAS	Reglamento del proceso de digitalizacion tipo de formato, tamaño de archivo y otras caracteristicas.	Información	Activo Primario	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		S	S	S	6

						Por															
50	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_050	CD BACKUP	CD contenida información de expedientes y archivos digitalizados del JEE.	Información	Activo Primario	Area de digitalizacion	Esp. Informatico	S	S	S	Lima				5		
51	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_051	EQUIPO MULTIFUNCIONAL XEROX	Dispositivo informatico de impresión, copia y scaneo tamaño A3 y A4	Hardware	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima	192.168.25.10	1		5	6	
52	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_052	SCANER	Dispositivo informatico de scaneo recomendado para el proceso de digitalizacion de actas electorales	Hardware	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		5				
53	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_053	UPS	Dispositivo utilizado para mantener la unidad operativa de los distintos dispositivos informaticos.	Hardware	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		5		5	7	
54	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_054	IBM PSEUDOSERVIDOR	Equipo usado como un servidor donde se guarda expedientes, actas digitalizadas, programas y otros.	Hardware	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima	192.168.25.20	5		5	7	
55	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_055	CABLEADO	Red de cableado del JURADO ELECTORAL ESPECIAL LIMA OESTE.	Redes	Activo de Soporte	Area de digitalizacion	Esp. Cable Estructurado	N	N	N	Lima		1		5	6	
56	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_056	ROUTER	Dispositivo informatico encargado del funcionamiento del internet.	Redes	Activo de Soporte	Gerencia de TI	Esp.Informatico	N	N	N	Lima	192.168.48.46	5		5	7	
57	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_057	SWICH	Dispositivo informatico encargado de funcionamiento de una red local.	Redes	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		5		5	7	
58	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_058	TELEFONO	Dispositivo de comunicación mediante voz.	Redes	Activo de Soporte	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		5	5	5	5	
59	SISTEMAS	DIGITALIZACION DE ACTAS	PRESIDENTA JEE	DIGJEE_059	LECTOR DE CODIGO DE BARRAS	Lectora usada para agilizar el ingreso de actas al sistema.	Información	Activo Primario	Area de digitalizacion	Esp. Informatico	N	N	N	Lima		5				

Política de seguridad	A.5.1				
	A.5.1.1	Documentos de política de seguridad de la información	La gerencia deberá aprobar, publicar y comunicar a todos los empleados y terceras partes que lo requieran.	SI	Es importante establecer y publicar las políticas de seguridad de información para el proceso de registro de actas digitalizadas aprobadas por la presidenta y lo miembros del pleno.
	A.5.1.2	Revisión de la política de seguridad de la información	La política será revisada en intervalos planificados, y en caso de cambios que la afecten, asegurar que siga siendo apropiada, conveniente y efectiva	SI	Es necesario especificar de que tiempo revisar la política de la seguridad de información para que pueda ser actualizados y de acuerdo a los cambios internos y externos sobre la institucion.
	A.6.1				
	A.6.1.1	Comité de gestión de seguridad de la información	La gerencia debe respaldar activamente la seguridad dentro de la organización a través de una dirección clara, un compromiso apropiado, recursos adecuados y conocimiento de responsabilidades de la seguridad de información	SI	Es necesario que la presidenta, los miembros del pleno y le comité de seguridad de informacion se comprometan con la seguridad de información mediante reuniones de manera periodica para la aprobacion de documentos y revision de avances.
	A.6.1.2	Coordinación de la seguridad de la información	Las actividades en la seguridad de la información deben ser coordinados por representantes de diferentes partes de la organización que tengan roles relevantes y funciones de trabajo	SI	Es necesario la coordinacion de las personas que han sido asignados para cumplir distintos roles relevantes con el personal involucrado en la seguridad de informacion y esta comprendido por un un miembro del pleno, secretaria jurisdiccional, jefa de RR.HH. y el especialista informatico siendo personales claves de un proceso electoral.
	A.6.1.3	Asignación de responsabilidades sobre seguridad de la información	Todas las responsabilidades sobre la seguridad de información deben ser claramente definidas.	SI	Es neceario la asginacion de responsabilidades en el personal que ha sido asignado para la seguridad de informacion y deben de ser bien definidas.
	A.6.1.4	Proceso de autorización para las nuevas instalaciones de procesamiento de información	Debe establecerse y definirse un proceso de gestión de autorización para facilitar los nuevos procesamientos de información	SI	Es necesario definir un nuevo procedimiento donde indique cual es la gestion adecuada para adquirir o recibir nuevos recursos para el tratamiento de la informacion.
	A.6.1.5	Acuerdos de confidencialidad	Se debe identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejen las necesidad de la organización para la protección de información	SI	Es necesario emitir normativas adecuadas en la cual se indique cada cuanto se debe revisar y actualizar los acuerdos de confidencialidad en los contratos con los proveedores, trabajadores y locadores de la organización para evitar la divulgación de información.
Aspectos organizativos para la seguridad	A.6.1.6	Contacto con autoridades	Deben mantenerse contactos apropiados con autoridades relevantes	SI	Es necesario un procedimiento de contacto con las autoridades pertinentes ante incidentes, sabemos que la entidad encargada de ver estos temas a nivel nacional es la ONGEI.
	A.6.1.7	Contacto con grupos de interés especial	Se debe mantener contactos con grupos de interés especial u otros foros de especialistas en seguridad así como de asociaciones profesionales	SI	Es necesario establecer contacto con personal especializado relacionado a seguridad de la información, actualmente se tiene contacto conla ONGEI, encargada de supervisar la implementación del SGSI a nivel nacional.
	A.6.1.8	Revisión independiente de la seguridad de la información	El alcance de la organización para manejar la seguridad de la información, así como su implementación (como por ejemplo: los objetivos de control, los controles, las políticas, procesos y procedimientos) deben ser revisados independientemente durante intervalos planificados o cuando ocurran cambios significativos en la implementación.	SI	Es necesario de una auditoria interna que se realice revisiones periodicas del alcance del sistema y su implementacion por parte dela presidencia y miembros del pleno del jurado electoral especial.
	A.6.2	Seguridad en los accesos de terceros			
	A.6.2.1	Identificación de riesgos por el acceso de terceros	Se evaluará los riesgos asociados con el acceso a las instalaciones de procesamiento de la información organizacional por parte de terceros, y se implementarán controles de seguridad adecuados antes de permitir su acceso	SI	Es necesario establecer controles adecuados para gestionar e identificar los posibles riesgos de accesos de terceros a la organización, el personal de la organización ha logrado identificar algunos posibles riesgos por los partidos politicos y los proveedores.
	A.6.2.2	Requisitos de seguridad cuando se trata con clientes	Se deben identificar todos los requisitos de seguridad antes de dar acceso a clientes a los activos o la información de la organización	SI	Es importante identificar todos los requisitos de seguridad antes brindar un acceso a la ciudadania a los activos de la informacion.
	A.6.2.3	Requisitos de seguridad en contratos de outsourcing	Los acuerdos que involucran el acceso, procesamiento ,comunicación o manejo de terceros de las instalaciones de procesamiento de información organizacional o la adición de productos o servicios a dichas instalaciones, deben cubrir todos los requisitos de seguridad necesarios.	SI	Es importante establecer una serie de controles para asegurar la seguridad de la información para trabajar con terceros, ya que los repsonsables de realizar contratos de outsorcing son los de la sede central del JNE y solo se ha contemplado acuerdos de confidencialidad.
	A.7.1	Responsabilidad por los activos			
	A.7.1.1	Inventario de activos	Se elaborará y mantendrá un inventario de todos los activos importantes que sean claramente identificados	SI	Es importante elaborar un inventario de todos los activos de informacion asi como tambien su documentacion de importancia involucrados en el alcance.
	A.7.1.2	Propiedad de los activos	Toda la información y los activos asociados con las instalaciones de procesamiento de información deben ser propiedad de una parte designada de la organización	SI	Es necesario definir los propietarios de los activos de información.
sificación ntrol de tivos	A.7.1.3	Uso aceptable de los activos	Se debe identificar, documentar e implementar las reglas para el uso aceptable de los activos de información asociados con las instalaciones del procesamiento de la información.	SI	Es importante concientizar en el cumplimiento del reglamento internode trabajo en el cual hace mencion de la correcta utilizacion de los activos de la empresa donde se ha podido verificar que no lo ponen en practica ademas de difundir la cultura de seguridad informacion.
	A.7.2	Clasificación de la información			
	A.7.2.1	Guías de clasificación	La información debe ser clasificada en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización	SI	Es necesario clasificar en funcion de su valor, requisitos legales y criticidad para la institucion.

	A.7.2.2	Etiquetado y tratamiento de la información	Se definirá e implementará un conjunto de procedimientos apropiados para etiquetar y manejar información, de conformidad, con el esquema de clasificación adoptado por la organización	SI	Se debe realizar la identificacion de los activos y ser roturados.
	A.8.1	Seguridad antes del empleo			
	A.8.1.1	Roles y Responsabilidades	Se definirán y documentarán los roles de seguridad y las responsabilidades de los empleados, contratistas y usuarios externos en concordancia con la política de seguridad de la información de la organización	SI	Se debe de establecer en los contratos de los trabajadores del Jurado electoral especial, los roles y responsabilidades que poseerán dependiendo de los cargos a los que sean asignados.
	A.8.1.2	Investigación	Se debe hacer un chequeo y verificación de informaciones anteriores de todos los candidatos para empleo, contratistas y personal externo, en concordancia con las leyes, regulaciones y ética; y proporcional a los requisitos del negocio, la clasificación de la información a ser accedida y a los riesgos percibidos	SI	Es necesario revisar los antecendentes penales y policiales de cada uno de los candidatos a un puesto laboral, como tambien una verificacion de la informacion que indica en su hoja de vida del postulante es verdadero.
	A.8.1.3	Términos y condiciones de la relación laboral	Los empleados, contratistas y terceros suscribirán un acuerdo de confidencialidad como como parte de los términos y condiciones iniciales de su empleo en donde se señalará la responsabilidad del empleado en cuanto a la seguridad de la información.	SI	Dentro del contrato debe contemplarse las responsabilidad de cada trabajador nuevo con la seguridad de informacion.
	A.8.2	Durante el empleo			
	A.8.2.1	Responsabilidades de la gerencia	La gerencia debe requerir a sus empleados, contratistas y a los usuarios externos aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización	SI	La institución deberá hacer publica, dentro de la organización, cada uno de las politicas y procedimientos relacionados a la seguridad de la información.
Seguridad Recursos umanos	A.8.2.2	Concientización, educación y entrenamiento en la seguridad de la información	Todos los empleados de la organización, y donde sea relevante, contratistas y usuarios externos deben recibir una adecuada concientización, entrenamiento y actualizaciones regulares en los procesos y políticas organizacionales, como acciones relevantes de su función laboral.	SI	Los trabajadores de la institucion tanto internos como externos deberan tener conciencia de su papel sobre la seguridad de informacion.
	A.8.2.3	Proceso disciplinario	Debe existir un proceso disciplinario para los empleados que hayan cometido una violación de seguridad	SI	Dentro de la política de Seguridad de la información se definio las sanciones que aplicarán al personal que no cumpla con la misma.
	A.8.3	Finalización o cambio del empleo			
	A.8.3.1	Responsabilidades de finalización	Debe informarse sobre los incidentes de seguridad a través de canales administrativos adecuados, tan pronto como sea posible.	SI	Es necesario establecer procedimientos adecuados para el caso que un empleado deja dela borar.
	A.8.3.2	Devolución de activos	Todos los empleados, contratistas y usuarios externos deben realizar la devolución de los activos de la organización que están en su posesión cuando termine su empleo, contrato o acuerdo	SI	Es necesario establecer un procedimiento formal para la devolucion de activos.
	A.8.3.3	Retiro de los derechos de acceso	El derechos de acceso a la información y a las instalaciones de procesamiento de información, que se le otroga a los empleados, contratistas y usuarios externos, debe ser removido cuando termine su empleo, contrato o acuerdo; o modificado ante cambios	SI	Es necesario eliminar los accesos al empleado interno y extero, contratistas a la informacion y a las instalaciones de procesamiento de la informacion al termino de sus relaciones laborales con la institucion, verificando informacion de no tener ninguna deuda con las areas o la institucion.
	A.9.1	Áreas seguras			
	A.9.1.1	Seguridad física perimetral	Las organizaciones usarán perímetros de seguridad (como paredes, puertas con control de entrada por tarjeta o recepciones) para proteger áreas que contienen información e instalaciones de procesamiento de información	SI	Se debe de implementar puertas de control de entrada por tarjeta para las areas que contiene informacion que es importante para el proceso electoral.
	A.9.1.2	Controles físicos de entradas	Las áreas seguras estarán protegidas mediante controles de acceso adecuados para garantizar que unicamente personal autorizado pueda ingresar	SI	Se debe establecer un procedimiento para que todo el personal del JURADO ELECTORAL ESPECIAL identifique las areas restringidas o lugares con informacion confidencial ademas implementar un control de seguridad para el area de digitalizacion que contiene informacion confidencial.
	A.9.1.3	Seguridad de oficinas, despachos y recursos	Se deben designar y mantener áreas seguras con el fin de proteger las oficinas, despachos e instalaciones.	SI	Es necesario mejorar y establecer controles de acceso a las areas donde se encuentran los procesos mas relevantes
	A.9.1.4	Protección contra amenazas externas y ambientales	Se deben designar y mantener protección física contra daños por fuego, inundación, terremoto, explosión, manifestación civil y otras formas de desastre natural o realizado por el hombre.	SI	Es importante establecer mecanismos de proteccion contra amenzas externas y ambientales.
	A.9.1.5	El trabajo en las áreas seguras	Se debe designar y mantener protección física y pautas para trabajar en áreas seguras	SI	Es necesario mejorar los controles las areas del lugar de trabajo.
	A.9.1.6	Áreas de carga, descarga y acceso público	Las áreas de carga, descarga y acceso público y otras áreas donde las personas tengan acceso, deben controlarse y, cuando sea posible, aislarse de las instalaciones de procesamiento de información para evitar un acceso no autorizado	SI	Existen controles para dar acceso a personal externo a la organización; sin embargo, estos controles poseen varias deficiencias por lo que deben ser mejorados y monitoreados. Para los dias de votacion ya que se tiene la presencia masiva de mas trabajadores contratados por el JEE y lo partidos politicos.

Seguridad ica y del ntorno	A.9.2	Seguridad de los equipos			
	A.9.2.1	Ubicación y protección de equipos	El equipamiento será ubicado o protegido para reducir los riesgos de amenazas, peligros ambientales y oportunidad de acceso no autorizado.	SI	Se debe establecer normas para evitar comer o beber cerca de los equipos. También, se debe establecer controles de acceso a las áreas operativas involucradas en el alcance del SGSI.
	A.9.2.2	Suministro eléctrico	El equipamiento se protegerá de fallas de energía y otras anomalías eléctricas causadas por fallo en el suministro eléctrico.	SI	Es necesario disponer de un equipo electrogeno en caso de cortes de luz en dias de procesos electorales.
	A.9.2.3	Seguridad del cableado	Se protegerá el cableado de energía y telecomunicaciones que transporten datos o respalden servicios de información frente a interceptaciones o daños.	SI	Es necesario implementar un proyecto para realizar un correcto cableado estructural dentro de la organización.
	A.9.2.4	Mantenimiento de equipos	El equipamiento recibirá un adecuado mantenimiento para garantizar su continua disponibilidad e integridad	SI	Es importante tener un cronograma de mantenimiento de equipos y aplicar todas las practicas de Gestion de servicios TI.
	A.9.2.5	Seguridad de equipos fuera de los locales de la organización	Se debe aplicar seguridad al utilizar equipamiento para procesar información fuera de los locales de la organización tomando en cuenta los diferentes riesgos en los que se incurre.	SI	Es necesario desarrollar procedimientos para entrega equipos fuera de los locales de la organizacion a personal autorizado, se debe implementar controles para proteger la información que se maneja dentro de los equipos debido a que, en caso de pérdida o robo, solo se realiza una denuncia policial y un pago equivalente al costo del activo físico , más no existe forma de proteger la información que esta llevaba.
	A.9.2.6	Seguridad en el re-uso o eliminación de equipos	Todos los equipos que contienen almacenamiento de datos deben ser revisados con el fin de asegurar que los datos sensibles y los software con licencia han sido removido o sobrescritos antes de desecharlos o reutilizarlos.	SI	Se deberá realizar un procedimiento formal para la eliminación y re-uso de los equipos electrónicos.
	A.9.2.7	Retiro de la propiedad	Los equipos, información y software no deben ser retirados fuera de la organización sin una autorización previa.	SI	Es necesario mejorar el procedimiento para entrega equipos al personal autorizado, así como un formato para autorizar la salida de las laptops fuera de la organización; sin embargo, se sabe que en muchos casos este formato no es utilizado.
	A.10.1	Procedimientos y responsabilidades de operación			
	A.10.1.1	Documentación de procedimientos operativos	Los procedimientos operativos deberán estar documentados, mantenidos y estar disponibles a todos los usuarios que lo requieran.	SI	Esím portante que la documentacion de los procesos operativos de la organizacion se hagan conocer y sea de facil acceso y esten disponibles ya que en algunos casos se desarrolla mediante los conocimientos de los usuarios.
	A.10.1.2	Gestión de cambios	Se controlarán los cambios en las instalaciones y sistemas de procesamiento de la información.	SI	Es necesario que se controlen los cambios para los recursos y sistemas de tratamiento de informacion.
	A.10.1.3	Segregación de tareas	Se segregarán las obligaciones y las áreas de responsabilidad con el fin de reducir las oportunidades de modificaciones no autorizadas o mal uso de los activos de la organización	SI	Se deben definir las tareas para restringir modificaciones no autorizadas.
	A.10.1.4	Separación de las instalaciones de desarrollo, prueba y operación	Se separarán las instalaciones de desarrollo, prueba y operación con el fin de reducir el riesgos de acceso no autorizado o cambios en el sistema operacional	SI	En la organización se manejan los tres ambientes solicitados, pero se debe documentar un procedimiento oficial especificando quienes tienen permisos para acceder a dichos entornos y bajo que circunstancias se puede trabajar con cada uno de ellos.
	A.10.2	Gestión de servicios externos			
	A.10.2.1	Entrega de servicios	Debemos asegurarnos que los controles de seguridad, las definiciones de servicio y los niveles de entrega incluidos en el acuerdo de servicios externos sean implementados, esten operativos y sean mantenidos por el personal externo	SI	La organización debe entregar acuerdos de seguridad conjuntamente con los servicios que llegan a entidades externas.
	A.10.2.2	Monitoreo y revisión de los servicios externos	Los servicios, reportes y registros provistos por terceras partes deben ser monitoreados y revisados regularmente. Igualmente, se deben llevar a cabo auditorías con regularidad	SI	La organización debe establecer métricas adecuadas para una adecuado monitoreo de los servicios entregados por los proveedores.
	A.10.2.3	Gestión de cambios de los servicios externos	Se debe manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejore de la política de seguridad de información, procedimientos y controles, tomando en cuenta la criticidad de los sistemas de negocio y procesos envueltos en la reevaluación de riesgos.	SI	La organización debe realizar un procedimiento adecuado, en el cual se indique como se debe gestionar los cambios en los servicios prestados por los terceros, tanto para modificaciones de políticas de la organización o implementación de nuevos controles para los proveedores, como para la solicitud del uso de nuevas tecnologías como parte del servicio
	A.10.3	Planificación y aceptación del sistema			
	A.10.3.1	Gestión de la capacidad	Se monitorearán las demandas de capacidad y se harán las proyecciones de futuros requisitos de capacidad para asegurar el desarrollo requerido por el sistema	SI	Dentro de la organización existe un procedimiento formal de como se debe realizar la planificación de nuevos proyectos y el analisis de los requerimientos de nuevos sistemas. Sin embargo, se debe evidenciar el correcto cumplimiento de este procedimiento dentro de la organización a través de los años.
	A.10.3.2	Aceptación del sistema	Se establecerán los criterios de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones y se llevarán a cabo pruebas adecuadas del sistema antes de su aceptación	SI	Dentro de la organización existe un procedimiento formal para la aceptación de los nuevos sistemas; sin embargo, se debe evidenciar el correcto cumplimiento de estos procedimientos, en muchos casos, no existen manuales de usuario utilizados para cada uno de los sistemas desarrollados por la empresa.
	A.10.4	Protección contra software malicioso			

	A.10.4.1	Controles contra software malicioso	Para ofrecer protección frente a software malicioso ,se implementarán controles de detección, prevención y procedimientos adecuados de toma de conciencia con los usuarios.	SI	Se debe capacitar al personal para saber que hacer en caso se detecte algún softwa re malicioso dentro de algu no de los activos que manejen y del buen uso de dispositivos de almacenamiento externos.
	A.10.4.2	Controles contra software móvil	Donde sea autorizado el uso de software móvil, la configuración debe asegurar que este opere de acuerdo a una política de seguridad clara y definida igualmente, se debe pre venir la ejecución de código movil no autorizado.	NO	El presente control no aplica ya que no esta contemplado en el á lca nce.
	A.10.5	***Gestión interna de respaldo y recuperación***	**Mantener la integridad y la disponibilidad del procesamiento de información y servicios de comunicación**		
	A.10.5.1	Recuperación de la información	Se obtendrán y probarán las copias de recuperación y respaldo de información y software regularmente en concordancia con la política acordada	SI	Es necesario que le especialista de TI real ize respaldos de la inform ación almacenada en cada equipo de com puto con una frecuencia det erminada; De igual forma, los respaldos realizados deben de almacenarse dentro del area de sistemas y definir lugares apropiados para el almacenamiento de estos respaldos.
	A.10.6	***Gestión de seguridad de redes***	**Asegurar la salvaguarda de información en las redes y la protección de su infraestructura de soporte.**		
	A.10.6.1	Controles de red	Se implementará un conjunto de controles para lograr y mantener la seguridad en las redes, y mantener la segurida de los sistemas y aplicaciones usuarios de la red, incluyendo la información en tránsito.	SI	Se debe normar la implementación de controles para resguardar la información que viaja a través de las redes, que permitan el trabajo eficiemnte de la red.
	A.10.6.2	Seguridad de los servicios de redes	Se deben identificare incluir en cualquier acuer do de servicio de red los aspectos de seguridad , niveles de servicio de red los aspectos de seguridad , niveles de servicio y requisitos de gestión, así estos servicios sea provistos interna o externamente.	SI	A través del directorio activo se ha estab lecido perfiles de acceso a las distintas carpetas compartidas y redes de la organización; sin embargo, se debe establecer procedimientos formales para monitorear y audit ar la correcta gestión de accesos a la red. Se debe normar la revisión de los acuerdos de servicio con los proveedores de telecomunicaciones, debido aque este tipo de fallas se están volviendo muy comunes en la organización.
	A.10.7	***Utilización y seguridad de los medios de información***	**Prevenir daños, modificaciones o destrucciones a los act ivos e interrupciones de las actividades del negocio.**		
Gestión de unicaciones eraciones	A.10.7.1	Gestión de med ios remov ibles	Deben de existir procedimientos para la gestión de med ios remov ibles	SI	Se ha implementado una política para restringir el uso de los puertos USB dentro de la organización; sin embargo, no esta normado el correcto uso de estos medios para el almacenamiento de respaldos de información crítica para el negocio.
	A.10.7.2	Eliminación de medios	Se elimin arán los med ios de forma segura cuando ya no se necesiten, utiliz ando procedimientos formales	SI	Se debe establecer procedimientos formales para la elimin ación de medios de almacenamiento de la información, tanto digital como física, por el momento, solo se realiza con medios digitales en el área de TI.
	A.10.7.3	Procedimientos de manipulación de la información	Se establecerán procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información de divulgaciones no autorizadas o su mal uso	SI	Es necesario el manejo de procedimientos para la manipulacion y almacenamiento de la infor mación.
	A.10.7.4	Seguridad de la documentación de sistemas	La documentación de los sistemas se protegerá de accesos no aut orizados	SI	No existe una adecuada difusión de la documentacion, por lo que primero se debe actualizar esta docu mentación para luego establecer pr ocedimientos formales para su correcta d istribución.
	A.10.8	***Intercambio de información***	**Mantener la seguridad de información y el intercambio de software dentro de la organización y con entidades externas**		
	A.10.8.1	Políticas y procedimientos para el intercambio de información	Se deben establecer políticas, pr ocedimientos y controles formales de intercambio para proteger el intercambio de información durante el uso de todo tipo de recursos de comunicación	SI	En la organización no existen políticas o controles que permitan asegurar el intercambio de organización, por ello se deberá establecer una serie de charlas de capacitación explicando a cada uno de los usuarios el cuidado que debe tener con la información sensible enviada a traves de los correos. se debe implementar controles para proteger los correos enviados y recibidos por el personal operativo.
	A.10.8.2	Acuerdos de Intercambio	Se deben de establecer acuerdos para el intercambio de l nformación y software entre la organización y entidades externas	SI	Al ser una organización publica responsable de fiscalizar los procesos electorales,es necesario desarrollar clausulas en las cuales se afirma que la información enviada por otras organizaciones deben ser tratadas como confidencial, en caso se pierda algún cargo o envío, se deberá presentar una denuncia policial para informar de este suceso a la organizacion.
	A.10.8.3	Seguridad de medios físicos en tránsito	Los medios a ser transportados deberán ser protegidos de acceso no autorizado, mal uso o corrupción durante su transporte fuera de los límites físicos de la organización	SI	El transporte de información de los procesos electorales es realizado por el personal de la organización . Se debe mejorar los controles para asegura rla mientras se encuentre en transito y asegurar el correcto traslado de esta información.
	A.10.8.4	Seguridad del correo electrónico	La inf ormación contenida en los correos electrón icos debe ser pr otegida apropiadamente	SI	Se deberá sensibilizar a los usuarios para evitar que dejen des bloqueada su computadora ya que posee acceso a los correos de cada usuario, adicionalmente, se deberá implementar una serie de controles para asegurar la información ante código malicioso que pueda afectar la información.
	A.10.8.5	Seguridad en los sistemas de información de negocios	Se deben desarrolla r e implementar políticas y procedim ientos para proteger la información asociada con la I nterconexión de los sistemas de información del negocio	NO	El presente control no aplica ya que no esta contemplado en el alcance.
	A.10.9	***Servicios de comercio electrónico***	**Mantener la seguridad en los servicios de comercio electrónico y la seguridad en su uso**		
	A.10.9.1	Seguridad en el Comercio Electrónico	El comercio electrónico pasando será protegido frente a actividades fraudulentas, controversias contractua les y divulgación o modificación de información.	NO	El presente control no aplica a la organización debido a que no brinda un servicio de comer cioelectrónico

A.10.9.2	Seguridad en las Transacciones en Línea	La información contenida en línea debe ser protegida para prevenir transmisiones incompletas, ruta incorrectas, alteración no autorizada de mensajes o duplicación no autorizado de mensajes.	NO	El presente control no aplica a la organización debido a que no brinda transacciones en línea
A.10.9.3	Información disponible públicamente	Se protegerá la integridad de la información pública mente disponible para prevenir modificaciones no autorizadas	SI	Se debe desarrollar una serie de procedimientos y responsabilidades para asegurar que la información mostrada dentro de la pagina web sea correcta y actualizada aplicando normatividad informatica.
A.10.10	***Monitoreo***	**Detectar actividades de procesamiento de información no autorizadas**		
A.10.10.1	Registro de auditoria	Se deben producir y guardar, por un periodo acordado, los registros de auditoria que registran las actividades de los usuarios, excepciones y eventos de seguridad, con el fin de asistir a investigaciones futuras y al monitoreo del control de acceso	SI	Es importante el almacenamiento de las informacion de los procesos electorales en distintos medios ya que son importantes en el tiempo de 5 años para procesos de auditoria de procesos electorales.
A.10.10.2	Uso del sistema de monitoreo	Se deben establecer procedimientos para monitorear las instalaciones de procesamiento de información y los resultados del monitoreo de actividades deben ser revisados regularmente	NO	El presente control no aplica ya que no esta contemplado en el alcance.
A.10.10.3	*Protección de la información de registro*	Las instalaciones e información de registro debe ser registradas	NO	El presente control no aplica ya que no esta contemplado en el alcance.
A.10.10.4	Registro de administrador y operador	Las actividades del administrador y de los operadores del sistema deben ser registradas	SI	Es necesario establecer un procedimiento para la realización de registros de las actividades de los operadores de sistemas.
A.10.10.5	Registros con faltas	Las faltas deben ser registradas, analizadas y se deben tomar acciones apropiadas	SI	De las entrevistas realizadas con los usuarios, se detecto que los sistemas SIPE, SICA, SIRA y PECAO E poseen fallas que son reportadas en su momento al departamento de sistemas de información; sin embargo, no existe un registro oficial donde se almacene cuales han sido estos errores, los motivos por los cuales sucedieron ni cuales fueron las soluciones, se recomienda su inmediata documentación.
A.10.10.6	Sincronización de reloj	Los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad deben ser sincronizados con una fuente acordada y exacta de tiempo	SI	Se debe establecer una documentación formal para la sincronización y/o ajuste del reloj.
A.11.1	***Requisitos de negocio para el control de accesos***	**Controlar los accesos a la información**		
A.11.1.1	Política de control de accesos	Se debe establecer, documentar y revisar una política de control de accesos, basado en requisitos de acceso de seguridad y del negocio.	SI	Dentro de la organización existen perfiles tanto para los correos, como para el acceso a internet y a los sistemas; sin embargo, se debe documentar los requisitos de seguridad de manera independiente por cada sistema y documentar los perfiles estandar para cada puesto de trabajo dentro de la organización.
A.11.2	***Gestión de acceso de usuarios***	**Asegurar que el acceso de usuarios es autorizado y prevenir accesos no autorizados a los sistemas de información**		
A.11.2.1	Registro de usuarios	Habrá un procedimiento de registro y anulación formal de usuarios para otorgar y eliminar el acceso a todos los servicios y sistemas de información	SI	Es necesario desarrollar un procedimiento formal para dar de alta o de baja a los nuevos usuarios, esta labor se ha ido realizando por el especialista de Thy según lo solicitado por las diversas áreas del JEE; sin embargo, se debe documentar formalmente estos procedimientos.
A.11.2.2	Gestión de privilegios	Se restringirá y controlará la asignación y uso de privilegios	SI	Se debe generar un procedimiento adecuado, en el cual se indique que cada jefe de área o departamento, debe solicitar los permisos adecuados para cada personal que trabaje bajo su supervisión y establecer roles y responsabilidades para la adecuada gestión de privilegios.
A.11.2.3	Gestión de contraseñas de usuario	Se controlará la asignación de contraseñas a través de un proceso de gestión formal	SI	Se debe establecer una documentación formal en la cual se indique cuales son los pasos para la generación de contraseñas a nuevos usuarios, adicionalmente se deberá solicitar a los usuarios que firmen un compromiso para no compartir su contraseña con otros usuarios y realizar charlas de concientización para explicar les el porque no deben hacerlo.
A.11.2.4	Revisión de los derechos de acceso de los usuarios	La gerencia conducirá un proceso formal y de manera periódica para revisar los derechos de acceso de los usuarios	NO	El presente control no aplica ya que no esta contemplado en el alcance.
A.11.3	***Responsabilidad de los usuarios***	**Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento**		
A.11.3.1	Uso de contraseñas	Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas	SI	Existe un procedimiento formal con las reglas para la creación y cambio de contraseñas de los usuarios; sin embargo, se debe realizar una serie de charlas de concientización con los usuarios para evitar que se compartan contraseñas de manera no autorizada y para forzar el cambio de contraseña una vez se entregado por primera vez las credenciales al usuario.
A.11.3.2	Equipo informático de usuario desatendido	Se exige al usuario que asegure protección adecuada a un equipo desatendido	SI	No existe una normativa formal que exija a los usuarios el bloqueo de las computadoras al momento de ausentarse; sin embargo, se debe realizar charlas de concientización con los usuarios para que adopten esta costumbre, adicionalmente, se debe forzar que las computadoras se bloqueen automaticamente luego de un tiempo de estar desatendidas
A.11.3.3	Política de pantalla y escritorio limpio	Se debe adoptar una política de escritorio limpio para papeles y dispositivos de almacenamiento removibles. Igualmente, se debe adoptar una política para instalaciones de procesamiento de información	SI	No existe una política formal para mantener la pantalla y los escritorios de trabajo limpios, se debe establecer una política junto con una adecuada clasificación de la información, para asegurar aquellos activos que son importantes para la organización, adicionalmente, se debe de proveer a las áreas de lugares o equipamiento adecuado para que puedan asegurar este tipo de información.
A.11.4	***Control de acceso a la red***	**Prevenir el acceso no autorizado de los servicios de la red**		

-Controles acceso	A.11.4.1	Política de uso de los servicios de la red	Los usuarios deben tener acceso directo única mente a los servicios cuyo uso está específicamente autorizado	SI	La configuracion de usuario limitado restringe el acceso únicamente a los servicios a los que se le ha permitido; sin embargo, se debe realizar una documentación formal de estas acciones.
	A.11.4.2	Autenticación de usuario para conexiones externas	Deben usarse apropiados métodos de autenticación para contr olar el acceso de usuarios r emotos	SI	Existe la necesidad de implementar controles de autentificacion.
	A.11.4.3	Autenticación de equipos en la red	Se debería considerar equ ipos con identificación a utomática para autentificar conexiones desde ubicaciones y equipos específicos	NO	El presente control no aplica ya que no esta contemplado en el a lcance.
	A.11.4.4	Protección para la configuración de puertos y diagnóstico remoto	Debe controlarse la seguridad en el acceso físico y lógico para el diagnostico y configuración de puertos	NO	El presente control no aplica ya que no esta contemplado en el alcance.
	A.11.4.5	Segregación en las redes	Los grupos de servicios, usuarios y sistemas de información deben ser segregados en las redes	NO	El presente control no aplica ya que no esta contemplado en el alcance.
	A.11.4.6	Control de conexión a las redes	La capacidad de conexión de los usuarios de redes compartidas, especialmente aquellas que se extienden fuera de las fronteras de la organización, debe restringirse de conformidad con la política de control de acceso y los requisitos de las aplicaciones de negocio (vease 11.1)	SI	Se debe establecer una serie de controles para restringir el acceso a las redes compartidas de la organización a ciertos horarios que coincidan con el horario de trabajo.
	A.11.4.7	Control de enrutamiento en la red	Se debe implementar controles de ruteo para asegurar que las conexiones de com putadores y los flujos de i nformación no violen la política de control de acceso de las aplicaciones de negocios	NO	El presente control no aplica ya que no esta contemplado en el alcance.
	A.11.5	*Control de acceso al sistema operativo*	Prevenir accesos no autorizados a los sistemas operativos		
	A.11.5.1	Procedimientos seguros de conexión	Se usará un proceso de registro de conexión (log in) segur o pa ra acceder a los servicios de información	SI	Se encuentra normado que para acceder a todos las computadoras, se necesita poseer credenciales autorizadas brindadas por el departamento de TI.
	A.11.5.2	Identificación y autenticación del usuario	Todos los usuarios tienen un identificador único para su uso propio y exclusivo para sus actividades y debe elegirse una t écnica de autenticación adecuada para sustentar la identidad del usuario	SI	Todos los usuarios poseen un identificador único para acceder a las computadoras de la organización; sin embargo, se ha detectado, que en muchos casos, los usuarios comparten contraseñas para iniciar sesión en distintas computadoras, por lo que se debe realizar charlas de concientización a los usuarios para evitar estas practicas.
	A.11.5.3	Sistema de gestión de contraseñas	Sistemas de gestión de contraseñas proveerá n medios efectivos e interactivos, cuyo objetivo es asegurar contraselas de calidad	SI	Existen normas y restricciones para la creación de contraseñas de acceso a las computadoras, solicitudes forzadas para el cambio de contraseña cada cierto tiempo y cifrado de las mismas; sin embargo, no existe un procedimiento apropiado para la gestión de creación de usuarios nuevos, lo cual causa que los usuarios compartan contraseñas de manera no autorizada, por lo que se debe realizar charlas de concientización y establecer un procedimiento adecuado para la alta de usua rios
	A.11.5.4	Uso de los programas utilitarios del sistema	Se debe registrar y controlar firmemente el uso de programas util itarios que puedan ser capaces de forzar el sistema y los controles de aplicación	SI	La organización posee una serie de perfiles que restringen la ejecución de ciertos pr ogra mas que puedan vulnerar los permisos ot orgados a cada usuario; sin embargo , no existe un programa de análisis de software malicioso actualizado capaz de proteger los sistemas frentea este tipo de amenazas.
	A.11.5.5	Desconexión automática de terminales	Las sesiones inactivas deben cerrarse luego de un período definido de inactividad	SI	Es necesario desarrollar una documentación adecuada para delimitar los tiempos máximos de duración de las sesiones inactivas conectadas a los distintos sistemas a través de terminales.
	A.11.5.6	Limitación del tiempo de conexión	Se usará restricciones de t iem pos de conexión para ofrecen seguridad adicional para las aplicaciones de alto riesgo	SI	Se debe implementar una política que indique claramente bajo que horarios se puede iniciar sesión o no, esta política debe contemplar aquellos casos en los que se requiera una ampliación de hora rios y solicitudes para habilita r las sesiones en un horario que no pertenezca al horario normal de trabajo
	A.11.6	*Control de acceso a las aplicaciones e información*	Evitar el acceso no autorizado a la información contenida en los sistemas		
	A.11.6.1	Restricción de acceso a la información	El acceso a las funciones de información y de aplicación por usuarios y personal de soporte serán restringidos con la política de control de acceso	SI	Los usuarios autorizados para el manejo de los sist emas poseen los permisos y restricciones adecuados para la realización de su trabajo; sin embargo, estas autorizaciones no estan debidamente documentadas, por lo que se debe realizar procedimientos formales indicando cuales son los perfiles necesarios por sistema y cuales son los permisos que estos deben tener .
	A.11.6.2	Aislamiento de sistemas sensibles	Los sistemas sensibles tendran un ambiente de computo aislado	SI	Dentro de la organización se manejan 2 sistemas y varios módulos separados para la atención de los clientes empresariales; sin embargo, todos los sistemas son albergados dentro de un mismo servidor y tam poco existe documentación formal que indique que un sistema sea sensible.
	A.11.7	*Informática móvil y teletrabajo*	Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y facilidades de t eletrabajo		
	A.11.7.1	Informática y comunicaciones móviles	Se pondrá en práctica una política formal y se adoptarán los controles adecuados para prot egerse frente a los riesgos de trabajar con puntos de computadores móviles y medios de comunicación	SI	Se debe documentar las políticas forma les para proteger la información almacenada en las computadoras móviles, establecer una serie de controles de encriptación para asegurar que la información almacenada en ese dispositivo no pierda su confidencialidad.
	A.11.7.2	Teletrabajo	Se desarrollarán e implementarán políticas, procedimient os y está nda res para las actividades de teletra bajo	NO	El presente control no aplica a la organización debido a que no se ha implementado el teletr abajo.
	A.12.1	*Requisitos de seguridad de los sistemas de información*	Garantizar que la seguridad está incluida dentro de los sistemas de información		
	A.12.1.1	Análisis y especificación de los requisitos de seguridad	Los requisitos de negocio para nuevos sistemas, o ampl iaciones de los sistemas existentes, especificarán los requisitos de control	NO	El presente control no aplica ya que no esta contemplado en el alcance.

	A.12.2	***Proceso correcto de aplicaciones***	**Prevenir errores, pérdidas, modificaciones no autorizadas o mal uso de los datos del usuario en las aplicaciones**		
	A.12.2.1	Validación de los datos de entrada	Se validará el ingreso de datos a los sistemas de aplicacion para asegurar que sean correctos	SI	Los sistemas desarrollados poseen una validación de los datos ingresados en muchas funcionalidades; sinembargo, se debe elaborar la documentación faltante que evidencie cuales son todos los casos de prueba utilizados para la validación de los datos de entrada.
	A.12.2.2	Control del proceso interno	Se incorporarán verificaciones y validaciones para detectar cualquier corrupción de los datos procesados	SI	Durante el desarrollo de los sistema, seha implementado el manejo de excepciones para evitar que el sistema continue en caso se detecte algún error y se valida la información que se transmite internamente para asegurarse la integridad de datos; sinembargo, no hay una documentación formal de los controles implementados.
	A.12.2.3	Integridad de mensajes	Se deben identificar requisitos para la autenticación y protección de la integridad de mensajes. igualmente, se deben implementar e identificar controles apropiados	SI	Se debe realizar una metodología para identificar aquellos mensajes que deben ser protegidos para implementar controles y asegurar la confidencialidad, integridad y disponibilidad delosmismos.
	A.12.2.4	Validación de los datos de salida	Los datos de salida de una aplicación se validarán para garantizar que el procesamiento de la información almacenada sea correcto y adecuado a las circunstancias	SI	Se tiene conocimiento que en los ambientes de prueba y desarrollo se realiza una serie de casos de prueba para asegurar el correcto funcionamiento de los sistemas; sin embargo, nose posee una documentación formal de estas pruebas.
	A.12.3	***Controles criptográficos***	**Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos**		
	A.12.3.1	Política de uso de los controles criptográficos	Debe desarrollarse e implementrase una política sobre el uso de controles criptográficos para proteger la información	SI	La organización debe realizar una política de encriptación integral para asegurar la información sensible que esta maneja. Se tiene conocimiento que las contraseñas en los sistemas estan encriptadas.
	A.12.3.2	Gestión de claves	Se usará un sistema de gestión de claves con el fin de apoyar el uso de técnicas criptográficas dentro de la organización	SI	La organización debe realizar una política adecuada para una correcta entrega, revocatoria y eliminación de claves a los usuarios que así lo requieran
	A.12.4	***Seguridad de los archivos del sistema***	**Asegurar la seguridad de los archivos del sistema**		
	A.12.4.1	Control del software en producción	Se pondrá en práctica procedimientos para controlar la implementación del software en sistemas operacionales	NO	El presente control no aplica ya que no esta contemplado en el alcance.
	A.12.4.2	Protección de los datos de prueba del sistema	Se protegerán y controlarán los datos de prueba los cuales deben ser seleccionados cuidadosamente	NO	El presente control no aplica ya que no esta contemplado en el alcance.
	A.12.4.3	Control de acceso a la librería de programas fuente	El acceso a las librerías de programas fuente debe ser restringido	NO	El presente control no aplica ya que no esta contemplado en el alcance.
	A.12.5	***Seguridad en los procesos de desarrollo y soporte***	**Mantener la seguridad del software de aplicación y la información**		
	A.12.5.1	Procedimientos de control de cambios	La implementación de cambios se controlará estrictamente mediante el uso de procedimientos formales de control de cambios	NO	El presente control no aplica ya que no esta contemplado en el alcance.
	A.12.5.2	Revisión técnica de los cambios en el sistema operativo	Cuando los sistemas operativos son cambiados, se deben de revisar y probar las aplicaciones críticas de negocio con el fin de asegurar que no existan impactos adversos en las operaciones o seguridad de la organización.	NO	El presente control no aplica ya que no esta contemplado en el alcance.
	A.12.5.3	Restricciones en los cambios a los paquetes de software	No se debe fomentar las modificaciones en los paquetes. Se deberia limitar a cambios necesarios y todos estos cambios deben ser estrictamentecontrolados	NO	El presente control no aplica ya que no esta contemplado en el alcance.
	A.12.5.4	Fuga de la información	Se deben de prevenir las oportunidades de fuga del nformación	SI	Se deberá elaborar un procedimiento para implementar controles que ayuden a evitar la fuga de información a través de los distintos sistemas. Adicionalmente, se cuenta con las clausula de confidencialidad firmadas por cada uno de los trabajadores del local; sin embargo. se debe hacer difusión de la política de seguridad de la empresa ya que en ella se muestra cuales son las sanciones en caso no se cumpla con lo normado referente a seguridad de la información.
	A.12.5.5	Desarrollo externo del software	La organización debe supervisar y monitorear eldesarrollo externo de software	NO	El presente control no aplica, debido a que la organización posee un área que se encarga del desarrollo de software para la empresa.
	A.12.6	***Gestión de la vulnerabilidad técnica***	**Reducir los riesgos que son el resultado de la explotación de vulnerabilidades técnicas publicadas**		
	A.12.6.1	Control de las vulnerabilidadestécnicas	Se debe obtener información a tiempo sobre las vulnerabilidades técnicas de los sistemas de información que se utilizan. La exposición de la organización a tales vulnerabilidades debe ser evaluada y se debe tomar medidas apropiadas asociadas el riesgo.		La organización debe generar un procedimiento adecuado para crear un registro de errores reportados por los usuarios, en los cuales se deje conocer cual fue el problema, cual fue el impacto, cuando se reporto, cual fue la causa y como se solucionó. Adicionalmente, se debe indicar como es que se gestionará las nuevas vulnerabilidades detectadas o reportadas por los usuarios.
	A.13.1	***Reportando eventos y debilidades en la seguridad de la información***	**Asegurar que los eventos y debilidades en la seguridad de información asociados con los sistemas de información sean comunicados de una manera que permita tomar una acción correctiva a tiempo**		
	A.13.1.1	Reportando eventos de la seguridad de información	Los eventos en la seguridad dela información deben serr eportados lo más rápido posible a través de canales apropiados	SI	La organización debe generar un procedimiento para gestionar adecuadamente cada uno de los eventos de seguridad de la información reportados por el personal o detectados por cada uno de los controles implementados, además se debe realizar charlas de capacitación con el personal para explicar les cuales son sus roles y responsabilidades dentro del sistema de gestión.

12.-
isición de
temas,
rrollo y
nimiento

Gestión de ntes en la ridad de la rmación	A.13.1.2	Reportando debilidades de seguridad de información	Todos los empleados, contratistas o personal externo usuarios de los sistemas y servicios de información deben estar obligados de notar y reportar cualquier debilidad en la seguridad de los sistemas y servicios	SI	La organización debe capacitar adecuadamente a todo el personal de la organización para que sea capaz de detectar debilidades en el sistema de gestión de seguridad de información y puedan reportarlas adecuadamente, asimismo, se debe recalcar las sanciones que podrían recibir si es que deciden probar las debilidades encontradas.
	A.13.2	Gestión de los incidentes y mejoras en la seguridad de información	Asegurar que un alcance consistente y efectivo sea aplicado en la gestión de incidentes de la seguridad de información		
	A.13.2.1	Responsabilidades y procedimientos	Se deben establecer responsabilidades y procedimientos de gestión con el fin de asegurar una respuesta rápida, efectiva y ordenada ante incidentes en la seguridad de información	SI	Deben estar definidos las responsabilidades en el manejo de incidentes con el fin de obtener una respuesta rapida.
	A.13.2.2	Aprendiendo de los incidentes en la seguridad de información	Debe existir mecanismos que habiliten que los tipos, volúmenes y costos de los incidentes en la seguridad de información sean cuantificados y monitoreados	SI	Es necesario sentar precedentes luego de cada incidente con el fin de que en el futuro el tratamieno sea mas efectivo.
	A.13.2.3	Recolección de evidencia	Cuando exista una acción de seguimiento contra una persona u organización, luego de que un incidente en el sistema de información involucre una acción legal (civil o criminal) , se debe recolectar, retener y presentar evidencia conforme con las reglas dentro de la jurisdicción	SI	Es necesario la existencia de un procedimiento para registros evindesiables.
	A.14.1	Aspectos de la gestión de continuidad del negocio en la seguridad de la información	Neutralizar las interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas severas o desastres en los sistemas de información y asegurar su reanudación oportuna		
	A.14.1.1	Incluyendo la seguridad de información en la gestión de la continuidad del negocio	Se deben establecer procedimientos y responsabilidades de gestión con el fin de asegurar una respuesta rápida, efectiva y ordenada ante incidentes en la seguridad de la información	SI	Se debe establecer procedimientos y responsabilidades para gestionar adecuadamente la cotinuidad del negocio, en estos procedimientos se debe colocar explicitamente cuales son los activos relacionados con los procesos críticos del negocio , asegurar la seguridad del personal, establecer planes de continuidad y realizar las pruebas de los mismos.
Gestión de ntinuidad Negocio	A.14.1.2	Continuidad del negocio y evaluación de riesgos	Los eventos que pueden causar interrupciones en los procesos de negocio deben ser identificados así como las probabilidades e impacto de dichas interrupciones y sus consecuencias para la seguridad de información.	SI	Se debe realizar un analisis de impacto del negocio adecuado según el alcance del SGSI identificando posibles escenarios y evaluando los riesgos tras la materialización de cada uno de ellos.
	A.14.1.3	Desarrollando e implantando de planes de continuidad que incluyen la seguridad de información	Se deben desarrollar e implementar planes para mantener o reparar operaciones y asegurar la disponibilidad de información al nivel y tiempo requerido, siguiendo las interrupciones o fallas a los procesos críticos del negocio.	SI	Se debe realizar planes de continuidad de negocio que permitan establecer cuales son los tiempos máximos para la recuperación de los servicios, que tipo de información se debe resguardar y cual se puede perder y las fechas de actualización de los planes
	A.14.1.4	Marco de planificación de la continuidad del negocio	Un simple marco de los planes de continuidad del negocio debe ser mantenido para asegurar que todos los planes sean consistentes, que anexen consistentemente los requisitos de seguridad de la información, para identificar prioridades de prueba y mantenimiento	SI	Se debe establecer un estandar único para la elaboración de los planes de contiuidad del negocio, de tal forma que se pueda recolectar toda la información necesaria sobre la planificación de la continuidad del negocio en cada uno de los planes desarrollados.
	A.14.1.5	Probando, manteniendo y reevaluando los planes de continuidad del negocio	Los planes de continuidad del negocio deben ser probados y actualizados regularmente con el fin de asegurar que se encuentren actuales y que sean efectivos	SI	Se debe establecar una metodología de pruebas para verificar los planes de continuidad del negocio, en ella debe indicarse textualmente la frecuencia con la cual se harán las pruebas de continuidad en la organización, las simulaciones que se deberán hacer, como regresara la operatividad luego de las pruebas y como deberán realizarse los ensayos completos ante interrupciones
	A.15.1	Cumplimiento de los requisitos legales	Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad		
	A.15.1.1	Identificación de la legislación aplicable	Se definirán y documentarán explícitamente todos los requisitos legales, regulatorios y contractuales relevantes y se deben mantener actualizados cada sistema de información y la organización	SI	Se debe definir planes y procedimientos para verificar el correcto cumplimiento de la legislación aplicable tales como la implementación del SGSI.
	A.15.1.2	Derechos de propiedad intelectual (DPI)	Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales en el uso de material con respecto a derechos de propiedad intelectual y uso de productos de software propietario	SI	Se debe respetar los derechos intelectuales y de propiedad.
	A.15.1.3	Salvaguarda de los registros de la organización	Se protegerán los registros importantes de la organización frente a pérdidas, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio	SI	Se debe establecer guías y procedimiento que especifiquen por cuanto tiempo la organización está dispuesta a almacenar la información, cabe aclarar que como parte del proyecto se realizó un inventario de activos de información los cuales fueron valorados según la metodología de svalorización de activos.
	A.15.1.4	Protección de los datos y de la privacidad de la información personal	Se aplicarán controles para proteger información personal en conformidad con la legislación correspondiente y si es aplicable, con las cláusulas contractuales	SI	Se debe establecer un procedimiento para el adecuado manejo de la información personal almacenada dentro de la organización , en conformidad con la ley de protección de datos personales.
	A.15.1.5	Prevención en el mal uso de las instalaciones de procesamiento de la información	Los usuarios deben ser disuadidos de utilizar las instalaciones del procesamiento de información para propósitos no autorizados	SI	En la organización está normado, dentro del reglamento interno de trabajo, el prestamo de computadoras autorizadas para uso personal, siempre y cuando, se solicite con anticipación y de forma escrita ; sin embargo, se debe difundir mejor esta normatividad.
.15.- limiento	A.15.1.6	Regulación de los controles criptográficos	Se implementarán controles para permitir el cumplimiento de los acuerdos nacionales, leyes y reglamentos	NO	No es relevante.

A.15.2	***Cumplimiento con las políticas y estándares de seguridad y del cumplimiento técnico***	**Asegurar el cumplimiento de los sistemas** con las políticas y normas de seguridad **organizacionales**		
A.15.2.1	Cumplimiento con los estándares y la política de seguridad	Los gerentes deben tomar acciones para garantizar que todos los procedimientos de seguridad dentro de su área de responsabilidad se lleven a cabo correctamente con el fin de garantizar el cumplimiento de las políticas y estándares de seguridad	SI	Se debe implementar un procedimiento que permita a los gerentes evaluar el cumplimiento de los controles de seguridad de información que se desean implementar, de tal forma que pueda darle un tratamiento adecuado a las no conformidades detectadas.
A.15.2.2	Comprobación del cumplimiento técnico	Debe verificarse regularmente el cumplimiento de la implementación de normas de seguridad en los sistemas de información	SI	Se debe establecer una metodología de trabajo que permita verificar el correcto cumplimiento de la implementación de normas de seguridad en la organización, adicionalmente, se puede incluir un procedimiento para realizar un análisis de vulnerabilidades de los distintos sistemas incluidos en el alcance del SGSI.
A.15.3	***Consideraciones sobre la auditoría de sistemas***	**Maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema**		
A.15.3.1	Controles de auditoría de sistemas	Se planificarán cuidadosamene las auditorías de los sistemas operacionales a fin de minimizar el riesgo de interrupciones a los procesos del negocio	SI	Se debe establecer un procedimiento para el desarrollo de auditorías planificadas e inopinadas de los sistemas involucrados en el alcance del SGSI ya que hasta el momento no existe rastro alguno de una auditoría a estos sistemas.
A.15.3.2	Protección de las herramientas de auditoría de sistemas	Se protegerá el acceso a las herramientas de auditoría del sistema para prevenir cualquier posible mal uso o daño	SI	Se debe proteger todas las herramientas que componen una auditoría.