UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN GESTIÓN PÚBLICA

Seguridad de la información y gestión de riesgos del proceso servicio electoral, Reniec, Lima, 2020

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Gestión Pública

AUTOR:

Br. Luis Enrique Leon Alvarado (ORCID: 0000-0002-0458-6884)

ASESORA:

Dra. Francis Ibarguen Cueva (ORCID: 0000-0003-4630-6921)

LÍNEA DE INVESTIGACIÓN:

Gestión de Políticas Públicas

Lima – Perú

2020

Dedicatoria

A mis padres Enrique y Angélica, a ti mamá, por tu incondicional apoyo y ser mi ejemplo a seguir, por darme fuerzas cuando flaqueaba y desde el cielo por guiarme con tu luz, nunca estaré lo suficiente agradecido con Dios por haberme regalado una madre como tú.

A mí amada Karina, esposa y compañera inseparable, por ser mí apoyo y estar siempre a mi lado en los momentos más importantes y difíciles de mi vida.

A mis hijos Karicris y Zedrick, con sus increíbles sonrisas me alentaba y animaba a culminar este proyecto.

Agradecimientos

A Dios, mi madre y abuelita, quienes guían mis pasos. A la Universidad César Vallejo por haberme brindado la oportunidad en mi desarrollo profesional. A la Dra. Francis Ibarguen Cueva asesora del curso diseño y desarrollo del trabajo de investigación por las horas y conocimientos dedicados a la culminación de esta investigación. A mis amigos y compañeros de trabajo que participaron del presente.

PÁGINA DEL JURADO

DECLARATORIA DE AUTENTICIDAD

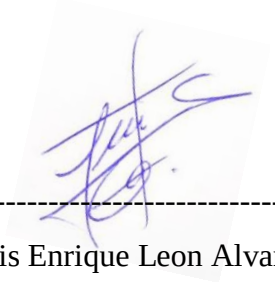
Yo, Luis Enrique Leon Alvarado, estudiante del programa de Maestría en Gestión Pública, de la Universidad César Vallejo, con la tesis titulada "Seguridad de la información y Gestión de riesgos del proceso servicio electoral, Reniec, Lima, 2020".

Declaro bajo juramento que:

- ✓ La tesis es de mi autoría
- ✓ He respetado las normas internacionales de citas y referencias para las fuentes consultadas. Por tanto, la tesis no ha sido plagiada ni total ni parcialmente.
- ✓ La tesis no ha sido auto plagiada; es decir, no ha sido publicada ni presentada anteriormente para obtener algún grado académico previo o título profesional.
- ✓ Los datos presentados en los resultados son reales, no han sido falseados, ni duplicados, ni copiados y por tanto los resultados que se presenten en la tesis se constituirán en aportes a la realidad e investigada.

De identificarse la falta de fraude (datos falsos), plagio (información sin citar a autores), auto plagio (presentar como nuevo algún trabajo de investigación propio que ya ha sido publicado), piratería (uso ilegal de información ajena) o falsificación (representar falsamente las ideas de otros), asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad César Vallejo.

Lima, agosto de 2020.



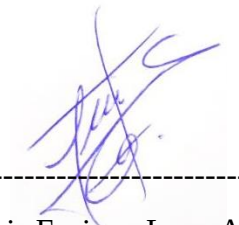
Br. Luis Enrique Leon Alvarado

DNI. 09742840

Presentación

Señores miembros del Jurado:

En cumplimiento del Reglamento de Grados y Títulos de la Universidad César Vallejo presento ante Ustedes la tesis titulada Seguridad de la información y gestión de riesgos del proceso servicio electoral, Reniec, Lima, 2020, la misma que someto a vuestra consideración y espero que cumpla con los requisitos de aprobación para obtener el grado académico de: Maestro en Gestión Pública.



Br. Luis Enrique Leon Alvarado

DNI. 09742840

Índice

Índice de tablas

Índice de figuras

Resumen

El estudio investigativo tiene el propósito de determinar la relación entre la seguridad de la información y gestión de riesgos del proceso del servicio electoral, Reniec, Lima, 2020. Estuvo regida bajo el enfoque cuantitativo, diseño no experimental correlacional, transversal. La muestra empleada fue de 64 colaboradores del proceso del servicio electoral de Reniec, Lima, 2020, con instrumentos validados por expertos y una alta fiabilidad. Los resultados nos indicaron la existente de una correlación fuerte entre las variables seguridad de la información y gestión de riesgos: Rho de Spearman de ,722** y una significación bilateral de ,000.

Palabras clave: Seguridad, información, Gestión, Riesgos, Colaboradores

Abstract

The research study aims to determine the relationship between information security and risk management of the electoral service process, Reniec, Lima, 2020. It was governed under the quantitative approach, non-experimental correlational, cross-sectional design. The sample used was 64 collaborators from the Reniec electoral service process, Lima, 2020, with instruments validated by experts and high reliability. The results indicated the existence of a strong correlation between the variables information security and risk management: Spearman's rho of .722 ** and a bilateral significance of .000.

Keywords: Security, information, Management, Risks, Collaborators

I. Introducción

Estudios internacionales sirvieron para entender la problemática en las organizaciones, en la actualidad existe una gran preocupación en la valoración y protección de los activos de la información, nos referimos a los datos, sistemas, procesos, tecnología, hardware, software, redes, soportes, servicios, productos, infraestructura, recursos y las personas, esto a consecuencia del descuido y falta de preocupación en proteger la información del personal no autorizado y exponiéndolas a las amenazas o ataques, así mismo el mal uso de las medidas preventivas no ayudaran a protegerlas, afectando el funcionamiento de una organización y teniendo como consecuencia el riesgo de la perdida de información sin distinción al tipo de organización o empresa, así como señala Isaca (2012) indica que dentro de una organización la información siempre debe estar protegida de la divulgación de personas que no estén autorizados.

Como indica Moreno y Camacho (2011) menciona que el riesgo de la perdida de información afecta a todos sin distinción de clase social tanto a los países ricos y pobres, así mismo Tabango y Guerrero (2014) indica que toda organización pone en riesgo los activos de información exponiéndolas a las vulnerabilidades, amenazas o ataques y que es necesario detectarlos a tiempo. También Barrantes y Hugo (2012) mencionan que no debe de existir descuido en disminuir los peligros que pueden llevar a la organización a perder no solo la información, sino también en el aspecto económico, por ultimo según Godoy (2014) indica que el daño que pueda afectar el funcionamiento de una organización están vinculados y dependen del buen uso de medidas preventivas que permiten proteger la información.

Revisaron también estudios de Medina y Rico (2008) donde indican que el aspecto cultural debe ser parte de este tipo de gestión seguridad de información, esto gracias a la implementación de lineamientos y estrategias del negocio, según Aenor (2015) señala que este tipo de gestión está relacionada a la seguridad de información, el cual tiene establecido cimientos primordiales en función a gestión de riesgos el cual enfrenta la organización, al respecto Romero, Figueroa, Vera, Álava, Parrales, Álava, Murillo y Castillo. (2018) definen la necesidad de la disponibilidad, confidencialidad e integridad siendo estas los 3 pilares, si uno de ellos es débil perderá su esencia o queda expuesta a

ataques reflejándose el peligro de ser dañada y no contar en el momento oportuno con la información.

Como sustenta Tarazona y César (2007) señala que la información es considerado un activo esencial para la organización y debe ser protegida de forma adecuada, además, Magerit (2012) menciona que las dimensiones confidencialidad, así como la integridad y disponibilidad está muy relacionada en mantener y proteger la información tales como la base de datos, servicios, listas de clientes, claves firmadas digitalmente, registros de actividades, , por ultimo Fernández y Piattini (2003) argumenta que una amenaza es un problema potencial a raíz de un incidente, hacia todos los activos que una organización custodia, nos refiere que si se haría efectiva la amenaza esta pone en peligro los pilares de la información.

A nivel nacional no se aplica la implementación ordenada por el gobierno en casi todas las instituciones del estado, así mismo existe gran resistencia al cambio y falta de compromiso por parte de los trabajadores siendo los riesgos más frecuentes el descuido de protección contra amenazas externas e interna, mal uso de las carpetas compartidas, perdida de archivos, registro de información errónea, dejar la PC prendida sin bloquear la pantalla, mal uso de los correos electrónicos institucionales, escritorios desordenados, documentos expuestos y sin utilizar, exponer contraseñas en lugares visibles, falta de cuidado al usar el internet y dispositivos como el USB, dejar documentos en la impresora expuesta a terceros, etc. es decir, los evento no deseados ponen en peligro a la confidencialidad, disponibilidad así como la integridad de los activos de información.

Como indica Condori y Mauricio (2012) en el Perú el sector público tuvo como solución la implementación de normas de seguridad de información, permitió tomar decisiones y evaluar riesgos que determinaron implementarlas, Así también refiere Baca (2016) indica que no hay interés en estas actividades, además se observó falta de normativas, políticas, así como supervisión de seguridad, como indica la ISO 17799 (2007) buscar proteger de ataques físicos, robos e incendios, de ataques cibernéticos, así como aprovechar las debilidades del sistema de información. También Alvarado (2016) menciona que en nuestro país, existe una institución encargada de implantar el ISO/IEC 27001:2014, que expone requisitos de implantar sistemas de gestión relacionado a la primera variable en mención, asimismo Reniec (2014) custodia documentos históricos

cuyas medidas de seguridad son controladas de manera estricta con el objetivo de conservar el activo de información y pueda estar disponible al servicio de los ciudadanos que necesiten acceder a ella en salvaguarda de sus derechos, Además Reniec (2019) indica que el registro de la identidad nacional y el padrón electoral es el activo de información que se encuentra centralizada y cuya custodia está soportada por el ISO de seguridad de información.

A nivel local los gestores operativos de Seguridad de la Información de la Gerencia de Registro Electoral, cumplen las funciones de integrar el equipo de riesgos y ejecutar las actividades que demande la gestión de la seguridad de la información, sin embargo se observó que los colaboradores, no toman el interés y se resisten a la adaptación del cambio, así como el mantener buenas prácticas respecto a al estudio en mención, además que la sensibilización implementada no están dando resultados, sin embargo la finalidad de capacitar, orientar y sensibilizar es con el objetivo de establecer la protección de los mismos y gestionar los riesgos que puedan ocasionarse en el transcurso del desarrollo de las actividades, así mismo Bernaldo (2018) indica que, al estar involucrado la información que la organización custodia, es de gran interés generar concientización en la protección de la información y sensibilizar al personal sobre estos temas.

Siguiendo el procedimiento se ha tomado en cuenta los antecedentes de estudios internacionales como: Arévalo, Bayona y Rico (2015) en su artículo de investigación permitieron establecer las debilidades del sistema de gestión de seguridad de la información de acuerdo con los retos de competitividad, concluye que los logros dependen del compromiso de adaptación al cambio de las organizaciones, se necesita un nivel de concientización, de esta manera la capacitación es un instrumento de sensibilización para lograr los resultados de compromiso al cambio, otros estudios realizados por Javier, Enriquez y Benavides (2015) en su artículo de investigación refiere que la ISO/IEC 27001 establecen requerimientos, tales como revisar, monitorear, así como mantener y sobre todo mejorar la seguridad de información, concluye argumentando que no existe un compromiso en los responsables de las organizaciones y que no son conscientes los trabajadores. Asimismo, Aguilar (2020) en su tesis de maestría tiene como propósito el estudio de un modelo relacionado a la variable en investigación que permitirá un control efectivo en sus procesos, se comparan los estándares o la existencia de buenas prácticas.

Cano y Almanza (2020). En su artículo tuvo como finalidad estudiar y entender el funcionamiento de seguridad de información en el contexto colombiano, busco comprender los factores o fenómenos relevantes de la realidad de este país, en este sentido, concordamos con los autores que el activo de información más importante son las personas el cual es el sustento principal de la presente investigación, en cambio Secaira, Ocampo, Mera y Kovalenko (2020) en su artículo tuvo como objetivo describir una metodología bajo la norma ISO 27001, se identificaron los procesos claves, se clasificaron activos de información y se permitieron controles de gestión. Finalmente, se contempló una serie de políticas y procedimientos de la organización, un plan de concientización, capacitación y políticas específicas de continuidad del negocio, al respecto Genesis y Romero (2019) Esta investigación tiene como finalidad analizar las vulnerabilidades que pueden presentarse en las actividades de seguridad para la preservación de la información, permite proteger el activo de la organización, además de mitigar cualquier riesgo al que se encuentre expuesta. Se contrasto que son propensas a recibir ataques por agentes maliciosos externos y agentes internos, esta última por la falta de conocimiento o inexperiencia del mismo personal que no saben cómo actuar ante esta situación. Esto conlleva a la necesidad de tomar medidas que garanticen la integridad, así como confidencialidad y por último la disponibilidad relacionados a la información.

Espinosa, García y Giraldo (2016) Esta investigación propone sentar una base para la correcta gestión relacionado a la seguridad de información en una institución, es importante la información de fortalezas y vulnerabilidades a las que pueden estar expuestos sus activos de información y cómo cualquier fallo puede violar su confidencialidad, como integridad y disponibilidad de información que custodian, se pretendió, apoyarse en las normas de la ISO 27001 e ISO 27002, así como implementar una política de SGSI acorde a la institución, identificar claramente los riesgos que están sometidos los activos, el cual están identificando amenazas y vulnerabilidades, así como analizar, evaluar y manejar los riesgos. Esto dará como resultado el cumplimiento de la metodología PHVA que corresponde a Planear, hacer, verificar y actuar, siendo propuestas por la norma ISO 27001 así como la ISO 27002.

Estudios nacionales como: Calderón (2019) en su tesis de maestría tuvo como finalidad distinguir la relación de las variables correspondiente de seguridad de

información, así como gestión de riesgos teniendo como resultado una relación alta. Concordando con el autor en tomar en cuenta el establecer acertadas decisiones que ayuden a desarrollar el proceso de información en la organización. Al respecto Huayllani (2020) en su tesis de maestría, tuvo como finalidad la aplicación de seguridad de información relacionado a gestionar los riesgos, se observó un nivel alto existiendo relación positiva y significativa entre la variable de investigación. También Bernaldo (2018) en su investigación tiene como resultado altamente significativa, así mismo es de gran interés, puesto que planteo mejorar e implantar un conjunto de acciones que permitirá reducir riesgos en los activos de información.

Así mismo Jara (2018) en su tesis de maestría tuvo el objetivo de medir la gestión en función a las variables en estudio. Se evidenciaron en los resultados la existencia de mejora al aplicar un sistema enfocado en la seguridad de información sobre procedimientos de gestión de los riesgos de un gobierno local. Seclén (2016) en su artículo de investigación cuyo problema fue identificar los elementos que producen la gestión relacionado a la seguridad de información en las Instituciones públicas del Perú, y su objetivo al investigar fue analizar las limitaciones y dificultades que enfrentan las instituciones del sector público a la implementación de dicho sistema. Teniendo como conclusión la relación entre las variables establecidas en el presente estudio.

A continuación, se detalla las teorías relacionadas a la variable 1 seguridad de la información, están conceptuadas de la siguiente manera: al respecto, Soriano (2014) menciona que son los medios preventivos aplicados a salvaguardar así como proteger la información en un marco de la confidencialidad, como la disponibilidad y también con la integridad, sin embargo, Aenor (2015) estableció esta variable como un procesos de implementación, así como mantener y mejorar continuamente la seguridad activos que correspondan a la información, teniendo como base los riesgos a los que la organización se enfrenta, en cambio ISO 27001 (2014) señala que las normativas establecen e implementan sistemas establecidos en una determinada organización para utilizar los procesos en ellas mismas.

Se fundamenta en la teoría según Areito (2008) como una disciplina en constante evolución, el cual permite que una organización cumpla objetivos estableciendo cuidados con los riesgos, así también la ISO 17799 (2007) menciona en las normativas

internacionales tienen como preservación importante a la integridad, confidencialidad así como la disponibilidad de información, además Merino y Cañizares (2014) indica que la implantación de un sistema en una organización debe estar sustentado en la mejora continua, la organización es quien decide proponer un enfoque para sus procesos. Por ultimo De Freitas (2012) plantea que se debe identificar, así como analizar, evaluar y sobre todo gestionar los riesgos de una organización relacionados a sus activos de información, con el fin de reducir y eliminar una posible ocurrencia basada en la Norma ISO 27001.

Para una mejor comprensión de la familia de las normas UNE de seguridad de la información se conoce las siguientes: ISO 27000:2014 (2014) quien define en la aplicación la utilización de esta norma es necesaria un vocabulario bien definido para evitar diferentes interpretaciones de los conceptos. 27001:2014 (2014) Se establecen requisitos para implementar, documentar y evaluar un sistema. 27002:2017 (2017) establece recomendaciones para iniciar una práctica eficaz. 27003:2010 (2010) guía de implementación e información del modelo PDCA y requisitos. 27004:2010 (2010) establece técnicas de medida para determinar la eficacia y controles. ISO 27005 (2011) guía para la gestión del riesgo y de apoyo a la ISO 27001. ISO 27006 (2011) requisitos de acreditación y certificación de entidades para auditorías. ISO 27032 (2012) guía de recomendaciones para mejorar la ciberseguridad, redes e internet. ISO 31000 (2010) orientar en cómo se debe de gestionar el riesgo de manera efectiva.

Esta investigación presenta varias características de la primera variable, según Medina y Rico (2008) menciona: a) Experiencia sobre procesos del negocio desarrollados, donde podemos asegurar las mejores prácticas en servicios, b) Involucrar una Base de Conocimiento para un buen manejo de la información de valor, c) El mejoramiento continuo de todos los procesos, así como de los servicios prestados, d) Mayor empoderamiento de las demás dependencias sobre sus funciones y mejor gestión de los requerimientos del cliente evidenciado en la práctica del trabajo realizado, de este modo Secaira, Ocampo, Mera, y Kovalenko (2020) fundamenta la implementación en mención, el cual se encuentra establecida por la estructura organizacional de las organizaciones, así como sus características: a) tipo, b) tamaño, c) objetivos, d) servicios, e) procesos, f) personal y g) seguridad el cual está basado en la ISO/IEC-27001

Las dimensiones de la primera variable seguridad de la información definidas también como los 3 pilares establecidas por Soriano (2014) son: 1) La confidencialidad, nos indica la referencia de cómo se debe proteger la información a una posible divulgación de parte de entidades o individuos que no están autorizados, 2) La integridad, protección de datos en una posible modificación parcial o total por parte de entidades que no están autorizadas, 3) La disponibilidad, tener acceso a la información en el momento adecuado y cuando se requiera, igualmente en la ISO 17799 (2007) menciona que se considerada como la protección de la información siendo estas las dimensiones: 1) Confidencialidad, es garantizar que esta sea accesible solo para el personal autorizado, 2) integridad, sea exacta sin cambios ni modificaciones no voluntarias y disponibilidad que sea accesible al personal cuando lo soliciten o requieran. Finalmente, como indica Aenor (2015) 1) Confidencialidad, quien da garantía de acceso autorizados para tal fin, 2) Integridad, quien da preservación de la información completa y exacta y 3) Disponibilidad, quien es da garantía de que el usuario accede a la información que necesita en ese preciso momento.

La importancia de la primera variable de estudio según Areito (2008) radica en la preservación de la información o datos clasificados sin importar el tipo de organización, siendo imprescindible la necesidad de seguridad teniendo en cuenta la aplicación que se debe de determinar, es un proceso continuo el cual debe tener en cuenta la gestión en la organización, asi mismo en la ISO 27001 (2014) sustenta la importancia de gestion un sistema de seguridad de informacion por estar integrado en los procesos de una organización, ademas estructurado en su gestion y se debe de considerar en los diseños de los procesos a la seguridad de informacion, asi como en los sistemas y sobre todo en los controles de informacion, finalmente Lorenzo (2014) ayuda identificar y medir los riesgos y permitiendo la toma de decisiones del tratamiento de determinados riesgos.

La teoría de la variable gestión de riesgos según Westerman (2006) indica que una organización están en la capacidad de gestionar riesgos que dan como beneficio una gestión de forma efectiva, considerando que influyen en los riesgos técnicos así como riesgos de tecnología de información, además, aunando a esto Gerber y Von (2005) adopta un enfoque al análisis de riesgos tradicional, con el cual se analizar los riesgos de los activos tangibles como los intangibles, al respecto Alexander (2007) indica que analizar riesgos es identificar sus amenazas vulnerabilidades basados en los activos,

Peltier (2014) define el presente proceso en identificar los riesgos, evaluar la probabilidad de que sucedan y tener medidas para reducirlas.

Las dimensiones de gestión de riesgos planteadas por Westerman (2006) indican que se debe de construir la variable en mención según la capacidad de una organización en poder gestionar riesgos, es una combinación coherente de tres disciplinas centrales siendo estas sus dimensiones: 1) Cultura consciente sobre riesgos, personas capacitadas que saben cómo identificar y evaluar amenazas e implementar una mitigación de riesgos efectiva. 2) Proceso de gobernanza del riesgo, políticas completas y efectivas relacionadas con el riesgo, combinadas con un proceso maduro y consistente para identificar, evaluar, priorizar y monitorear los riesgos a lo largo del tiempo. 3) Implantación eficaz de riesgos: Infraestructura de TI y aplicaciones que tienen un riesgo inherentemente menor porque están bien diseñadas y bien administradas.

Se formuló la interrogante: ¿Cómo se relaciona la seguridad de la información y la gestión de riesgos del proceso servicio electoral, Reniec, Lima, 2020? (Ver anexo 1). El estudio de la problemática se justificó en el aspecto teórico porque se comparó con las teorías de la variable 1 seguridad de la información y variable 2 gestión de riesgos, el cual servirán para la investigación correspondiente. Podrán emplearse para reforzar los conocimientos sobre la seguridad de información en las organizaciones e institución pública con la finalidad de que los colaboradores gocen de mayor profundidad teórica e incrementen sus conocimientos. También se justificó en la parte práctica porque ayudara en el aspecto de dotar de una serie de recomendaciones que servirán para que los colaboradores de la Gerencia de Registro Electoral mejoren sus desempeños y trabajen en equipo y muestren mayor predisposición en el momento de emitir juicios de valor sobre la seguridad de información de su organización o institución y así poder elevar el nivel de gestión de riesgo y por ende responder a las demandas sociales. Se justificó metodológicamente porque se ha realizado un proceso metodológico científico. Se investigó la apreciación de los colaboradores a través de los cuestionarios el cual han sido confiables que servirán para a la institución además que han sido adaptados y evaluados por especialistas, que dan fe a que puedan ser utilizados en otros estudios bajo la metodología cuantitativa.

Se determinó la relación entre la seguridad de la información y la gestión de riesgos del proceso servicio electoral, Reniec, Lima, 2020. Así como se probó la hipótesis: Seguridad de la información se relaciona con la Gestión de riesgos del proceso del servicio electoral, Reniec, Lima, 2020. (Ver anexo 1)

II. Método

2.1 Tipo y diseño de investigación

El análisis se definió como una investigación Básica, para Cabezas, Andrade y Torres (2018), que es generación del conocimiento nuevo, encaminado a incrementar en la ciencia postulados teóricos (p. 34). El diseño es no experimental. Cabezas, Andrade y Torres (2018), explicaron que la variable no se manipula en forma intencional. El enfoque fue cuantitativo, según Cabezas, Andrade y Torres (2018), emplea el recojo de cifras respaldado en el análisis de la estadística y medición de números, para probar teorías y establecer patrones de comportamiento (p. 19). Fue de método hipotético deductivo. Hernández, et. ál. (2018) dicen que es un método teórico de función epistemológica para construir y desarrollar teorías científicas, basadas a partir de principios, teorías o leyes que concluyen en respuestas que argumentan el fenómeno confirmadas luego en la práctica (pp. 94-95).

2.2 Operacionalización de variables

Operacionalización de la variable 1: Seguridad de la información, según Soriano (2014) lo definió como medios preventivos aplicados a salvaguardar así como proteger la información en un marco de la confidencialidad, integridad y disponibilidad. Seguridad de la información se operacionalizó con el cuestionario de calderón (2019) que fue adaptado por el investigador, compuesta por 22 preguntas dividas en tres dimensiones con escala de Liket. (Ver anexos 2): confidencialidad, integridad y disponibilidad.

Operacionalizacion de la variable 2: Gestión de riesgos, según Westerman (2006) indica que las organizaciones están en la capacidad de gestionar riesgos que dan como beneficio una gestión de forma efectiva, considerando que influyen en los riesgos técnicos así como riesgos de tecnología de información. Gestión de riesgos se operacionalizó con el cuestionario de calderón (2019) que fue adaptado por el investigador, compuesta por 20 preguntas dividas en tres dimensiones con escala de Liket. (Ver anexos 2): Proceso de gobernanza del riesgo, Cultura consciente sobre riesgos e Implantación eficaz de riesgo.

2.3 Población, muestra

Levin y Rubín (2004) afirmaron que es el grupo infinito o finito de objetos o personas. La población censal estuvo conformada por 64 colaboradores de la Gerencia de Registro Electoral del Reniec.

2.4 Técnicas e instrumentos de recolección de datos, validez y confiabilidad

La técnica empleada fue la encuesta, al respecto, Gallardo (2017) señaló tiene como objetivo recolectar información de un grupo o parte de la población de interés utilizando procedimientos estandarizados, y estos pueden ser de dos tipos: encuesta oral y encuesta escrita. El cuestionario. Según, Gallardo (2017) señaló: es una lista de preguntas que se propone con cualquier fin. La validez se realizó por expertos, según Hernández et. ál. (2018, p. 80) indicaron que es la competencia que tienen los datos conseguidos para reproducir el aspecto de la realidad estudiada. Se ejecutó a través de opinión de expertos. (Ver anexo 3). Se halló la fiabilidad con 64 trabajadores, se recolectó datos y luego se halló la confiabilidad cuyos resultados el alfa de Cronbach de 0,823 y el de 0,821 ambos altamente fiables. (Ver anexo 5)

2.5 Procedimiento

Se procedió a las autorizaciones respectivas para la ejecución de la investigación, luego se realizó la recolección de información de los informantes (colaboradores) previa sensibilización y finalidad del estudio. Los datos obtenidos se procesaron estadísticamente en Excel y SSPS 23.

2.6 Método de análisis de datos

La metodología empleada para el análisis fue la organización y descripción de datos en tablas y figuras (análisis-descriptivo). Luego se utilizó el índice de Spearman para establecer las correlaciones entre variables.

2.7 Aspectos éticos

La investigación realizada se trabajó con mucho respeto hacia los colaboradores, protegiendo su anonimato y confidencialidad. Igualmente, el respeto a los protocolos de redacción de tesis de la universidad césar vallejo y al respeto a las normas APA.

III. Resultados

3.1. Resultados descriptivos

Tabla 1.
Niveles de la variable seguridad de la información y dimensiones

Niveles	Seguridad de la información		Confidencialidad		Integridad		Disponibilidad	
	f	%	f	%	f	%	f	%
Bajo	4	6.3	21	32.8	10	15.6	11	17.2
Medio	51	79.7	36	56.3	51	79.7	42	65.6
Alto	9	14.1	7	10.9	3	4.7	11	17.2
Total	64	100,0	64	100,0	64	100,0	64	100,0

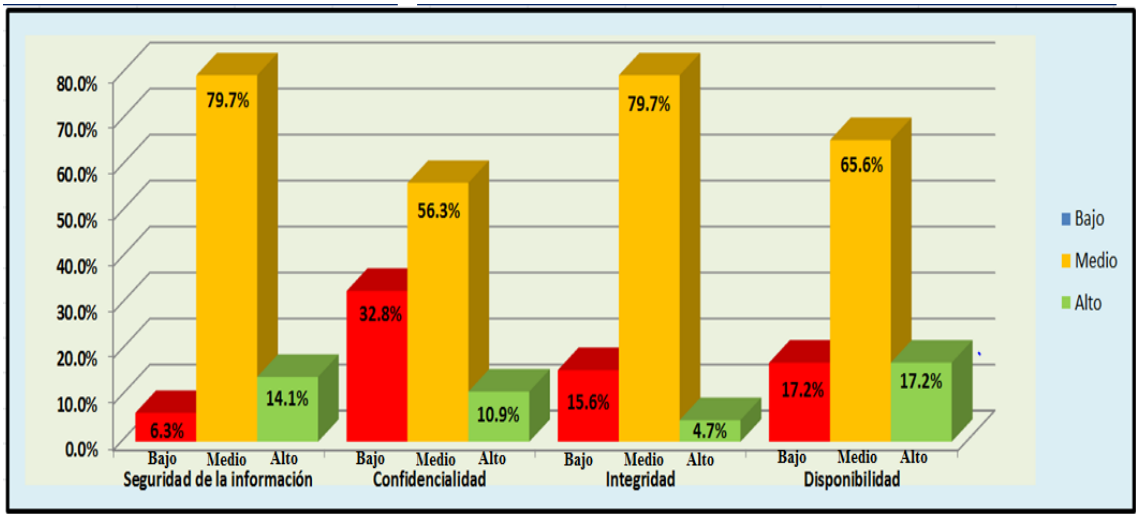


Figura 1. Niveles de percepción de la variable seguridad de la información y dimensiones

Los resultados descriptivos de la variable seguridad de la información de los trabajadores arrojaron que el 6.3% lo considera baja, el 79.7% lo consideran regular y el 14.1% es considerado como alta; en la dimensión Confidencialidad el 32.8% lo considera baja, el 56.3% lo considera regular y el 10.9% es considerado como alta; en la dimensión Integridad el 15.6% lo considera baja, el 79.7% lo considera regular y el 4.7% es considerado como alta; en la dimensión Disponibilidad el 17.2% lo considera baja, el 65.6% lo considera regular y el 17.2% lo considera como alta.

Tabla 2.
Niveles de la variable Gestión de riesgos y dimensiones

Niveles	Gestión de riesgos		Cultura consciente sobre riesgos		Proceso de gobernanza del riesgo		Implantación eficaz de riesgos	
	f	%	f	%	f	%	f	%
Bajo	13	20.3	9	14.1	22	34.3	12	18.7
Medio	44	68.8	48	75.0	30	46.9	44	68.8
Alto	7	10.9	7	10.9	12	18.8	8	12.5
Total	64	100,0	64	100,0	65	100,0	64	100,0

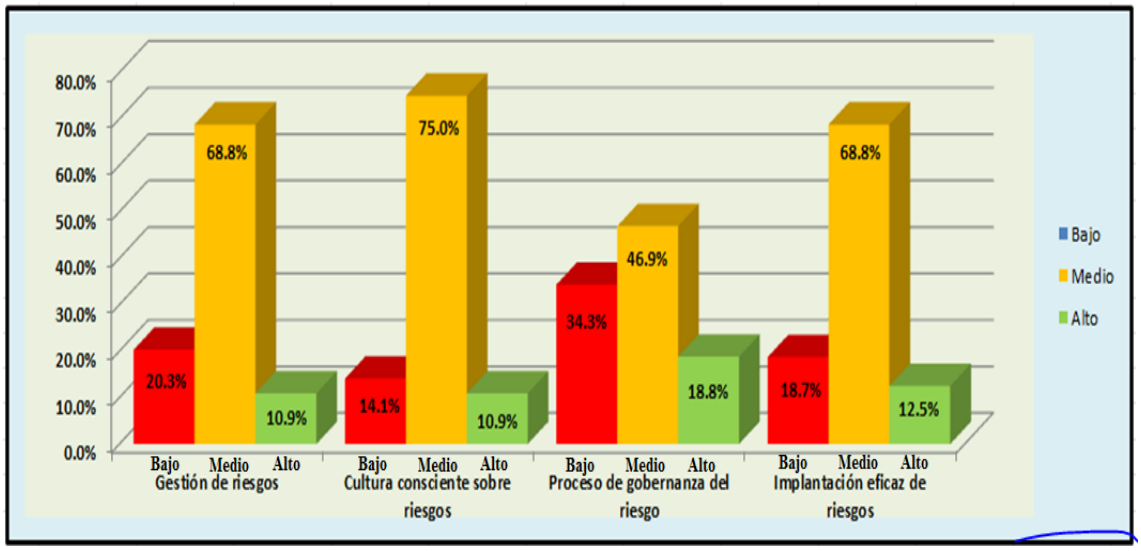


Figura 2. Figura 1. Niveles de percepción de la variable gestión de riesgos y dimensiones

Los resultados descriptivos de la variable gestión de riesgos de los trabajadores arrojan que el 20.3% lo consideran baja, el 68.8% lo consideran regular y el 10.9% es considerado como alta; en la dimensión Cultura consiente sobre riesgos el 14.1% lo consideran baja, el 75% lo considera regular y el 10.9% lo considera como alta; en la dimensión Proceso de gobernanza del riesgo el 34.3% lo considera bajo, el 46.9% lo consideran regular y el 18.8% lo considera como alta; en la dimensión implementación eficaz de riesgo el 18.7% lo considera bajo, el 68.8% lo considera regular y el 12.5% lo considera como bueno.

3.2. Resultados correlacionales

Se probó las hipótesis para ello se establecieron hipótesis nulas y la hipótesis alterna de las variables y de variable – dimensión, se utilizó el Rho de Sperman que indicó en la hipótesis general (Seguridad de la información y gestión de riesgos) el nivel de correlación es fuerte (Rho 0,722 y p-valor 0,000); la hipótesis específica – 1 (Confidencialidad y gestión de riesgos) el nivel de correlación es moderado (Rho 0,585 y p-valor 0,000); la hipótesis específica – 2 (Integridad y gestión de riesgos) el nivel de correlación es moderado (Rho 0,628 y p-valor 0,000); la hipótesis específica – 3 (Disponibilidad y gestión de riesgos) el nivel de correlación es moderado (Rho 0,488 y p-valor 0,000), en todo los casos el nivel es de 0,01.

Tabla 3.
Sistema de hipótesis de la investigación

Hipótesis	Variables*Correlación	Rho-Spearman	Significatividad-Bilateral	N	Nivel
Hipótesis general	Seguridad de la información*Gestión de riesgos	,722**	,000	64	Fuerte
Hipótesis específica-1	Confidencialidad*Gestión de riesgos	,585**	,000	64	Moderado
Hipótesis específica -2	Integridad*Gestión de riesgos	,628**	,000	64	Moderado
Hipótesis específica -3	Disponibilidad*Gestión de riesgos	,488*	,000	64	Moderado

**. La correlación es significativa en el nivel 0,01 (bilateral).

IV. Discusión

La presente investigación permitió alcanzar los objetivos planteados, sobre la Seguridad de la información y gestión de riesgos del proceso servicio electoral, Reniec, Lima, 2020, Se ha obtenido trabajos que permitieron responder sobre las variables estudiadas, así mismo se tiene la discusión dentro de una teoría, lo que garantiza un apoyo en ciertos enfoques de la presente investigación el cual se comparara con los antecedentes de las variables de investigación, confirmando la hipótesis planteada y pudiendo determinar que de acuerdo a mi hipótesis general las variables seguridad de la información se relaciona con la gestión de riesgos, las pruebas estadísticas utilizadas nos indican que existe una correlación no paramétrica de spearman fuerte (Rho 0.722 y p-valor 0,000); estos resultados fueron avalados por Calderón (2019) quien señala en su investigación una relación fuerte y concluyendo que existe una relación directa entre sus variables, recomendando que sus resultados sean tomados en cuenta al establecer acertadas decisiones que ayuden a desarrollar el proceso de seguridad de la información en la organización, así como seguir implementando un sistema de gestión y conformar un comité de gestión. Huayllani (2020) indica en su investigación que después de aplicar los instrumentos y el estudio estadístico concluye que existe una correlación entres sus variables de forma significativa y positiva, así mismo recomienda que debe tener como finalidad la aplicación de seguridad de información relacionado a gestionar los riesgos y efectividad en los resultados, también menciona aplicar adecuados controles y mantener los riesgos en un nivel aceptables, así como formular planes de acción y mejorar los controles existentes.

Así mismo la dimensión confidencialidad estudiada en la presente investigación se relaciona con gestión de riesgos, con una correlación moderado (Rho 0.585 y p-valor 0,000); estos resultados son avalados por Calderón (2019) quien señala en su investigación una alta relación y concluyendo que existe una relación directa entre sus variables de estudio, estos resultados son apoyados por el marco teórico de Soriano (2014) se debe proteger la información a una posible divulgación de parte de entidades o individuos que no están autorizados. Así como Aenor (2015) manifiestan que es quien da garantía de acceso autorizados para tal fin.

Al respecto, la dimensión integridad estudiada en la presente investigación se relaciona con gestión de riesgos, con una correlación moderado (Rho 0.628 y p-valor 0,000); estos resultados son avalados por Calderón (2019) quien señala en su investigación una alta relación y concluyendo que existe una relación directa entre sus variables de estudio, estos resultados son apoyados por el marco teórico de Soriano (2014) concuerdan que la protección de datos en una posible modificación parcial o total por parte de entidades que no están autorizadas. Así como Aenor (2015) fundamenta quien da preservación de la información completa y exacta.

Por último, la dimensión disponibilidad se relaciona con gestión de riesgos, con una correlación moderado (Rho 0.488 y p-valor 0,000); estos resultados son avalados por Calderón (2019) quien señala en su investigación una alta relación y concluyendo que existe una relación directa entre sus variables de estudio, estos resultados son apoyados por el marco teórico de Soriano (2014) concuerdan que tener acceso a la información en el momento adecuado y cuando se requiera. Así como Aenor (2015) quien da garantía al usuario acceder a la información que necesita en ese preciso momento.

V. Conclusiones

Primera: Luego de la aplicación de los instrumentos y el estudio estadístico respectivo, podemos concluir que existe una relacion directa entre seguridad de la información y gestión de riesgos en los colaboradores del proceso servico electoral de Reniec, Lima, 2020, se relacionan fuertemente obteniendo un valor de significancia igual a 0 y con un Rho spearman 0,722.

Segunda: Luego de la aplicación de los instrumentos y el estudio estadístico respectivo, podemos concluir que existe una relacion directa entre confidencialidad y gestión de riesgos en los colaboradores del proceso servico electoral de Reniec, se relacionan moderadamente con un Rho 0,585.

Tercera: Luego de la aplicación de los instrumentos y el estudio estadístico respectivo, podemos concluir que existe una relacion directa entre integridad y gestión de riesgos en los colaboradores del proceso servico electoral de Reniec, se relacionan moderadamente con un Rho 0,628.

Cuarta: Luego de la aplicación de los instrumentos y el estudio estadístico respectivo, podemos concluir que existe una relacion directa entre disponibilidad y gestión de riesgos en los colaboradores del proceso servico electoral de Reniec, se relacionan moderadamente con un Rho 0,488.

VI. Recomendaciones

Primera: Los gestores de Seguridad de la Información de la Gerencia de Registro Electoral de Reniec, deben dar cumplimiento al ejecutar las actividades que demande la gestión de riesgos así como proponer y coordinar la implementación o ejecución de controles relacionados a la seguridad de la información del proceso de servicio electoral.

Segunda: Realizar capacitaciones donde se debe sensibilizar a los colaboradores sobre seguridad de la informacion para mejorar el nivel de gestion de riesgos en el proceso servicio electoral.

Tercera: Aplicar la confidencialidad teniendo en consideración los procedimientos y conductas para establecer la gestion de riesgo.

Cuarta: Aplicar la integridad teniendo en consideración los procedimientos y conductas para establecer la gestion de riesgo.

Quinta: Aplicar la disponibilidad teniendo en consideración los procedimientos y conductas para establecer la gestion de riesgo.

Sexto: Realizar medidas de contingencia ante posibles riesgos que afecten la continuidad de los servicios que tengan involucrado la información que maneje la organización.

Referencias

Aenor (2015) *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad.*

Alvarado, F. (2016) *La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales*. Foro Jurídico, (15), 26-41.

Aguilar, N. (2020) *Modelo de seguridad de la información para instituciones de educación superior* (Doctoral dissertation).

Alexander, A. (2007) *Diseño de un Sistema de Gestión de Seguridad de Información. Óptica ISO 27001:2005.*

Arévalo, J., Bayona, R., & Rico, D. (2015) *Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: Análisis del riesgo de la información*. Revista Tecnura, 19(46), 123-134. doi:10.14483/udistrital.jour.tecnura.2015.4.a10

Areito, J. (2008) *Seguridad de la información, redes informática y sistemas de información*. España (https://books.google.es/books?hl=es&lr=&id=_z2GcB-D3deYC&oi=fnd&pg=IA1&dq=seguridad+de+la+informacion&ots=wsqlwCEXNm&sig=cUyO07LHbb49fkSMYH1WmcpBmBU#v=onepage&q=seguridad%20de%20la%20informacion&f=false)

Baca, V. (2016) *Diseño de un sistema de gestión de la seguridad de la información para la unidad de gestión educativa local - Chiclayo*. Rev. Ingeniería: Ciencia, Tecnología e Innovación VOL. 3/N° 1 – ISSN 2313-1926/Julio 2016

Barrantes, C. y Hugo, J. (2012) *Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos*. (Tesis de maestria) Universidad San Martín de Porras, Lima – Perú.

Bernaldo, N. (2018) *Sistema de gestión de seguridad de la Información en el Proceso de Registros Civiles de Reniec. San Borja. Lima 2016.* (Tesis de maestria) Universidad César Vallejo

Calderón, J. (2019) Seguridad de la información y la gestión de riesgos en los trabajadores de la Digere del Ministerio de Educación, 2018. (Tesis de maestria) Universidad César Vallejo

Cabezas, E. Andrade, D. & Torres, J. (2018) Introducción a la metodología de la investigación científica. Sangolquí: Universidad de las Fuerzas Armadas ESPE.

Cano, J. y Almanza, A. (2020) Estudio de la evolución de la Seguridad de la Información en Colombia: 2000-2018. Revista Ibérica de Sistemas e Tecnologias de Informação, (E27), 470-483.

Condori, H. y Mauricio, D. (2012) Un modelo de evaluación de factores críticos de éxito en la implementación de la seguridad en sistemas de información respecto a la intención del usuario. Revista de investigación de Sistemas e Informática, 9(1), 9-22.

De Freitas, V. (2012) Sistema de Gestión de Seguridad de la Información, EAE, 2012

Espinosa, J., García, R. & Giraldo, A. (2016) Sistema de gestión de seguridad de la información para los tres procesos misionales de la corporación autónoma regional de risaralda (CARDER).

Fernández, E. y Piattini, M. (2003) Seguridad de las tecnologías de la Información: La construcción de la confianza para una sociedad conectada. Madrid : Ediciones Aenor, 2003.

Gallardo, E. (2017) Metodología de la investigación. Huancayo: Universidad Continental.

Genesis, M. y Romero, S. (2019) Tesis. Recuperado a partir de http://repositorio.ug.edu.ec/handle/redug/44386

Gerber, M. y Von-Solms, R. (2005) “Management of risk in the information age”. Computers & security, v. 24, n. 1, pp. 16-30. https://www.researchgate.net/publication/222827356_Management_of_risk_in_the_information_age https://doi.org/10.1016/j.cose.2004.11.002

Guerrero, Y. y Tabango, R. (2014) Sistema de gestión de seguridad de la información (SGSI) basada en la Norma ISO 27001 y 27002 para la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño. (Tesis de grado) Universidad de Nariño, Colombia.

Godoy, R. (2014) Seguridad de Información. Guatemala: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica.

Huayllani, O. (2020) Sistema de gestión de seguridad de la información y la gestión del riesgo en el Ministerio de Salud, 2019.

Hernández, A. (2018) Metodología de la investigación científica. 3 Ciencias. Universidad Estatal de Manabí. Recuperado de http://bit.ly/2Hv4BXQ

Isaca (2012) Cobit 5 para Seguridad de la Información. Estados Unidos.

ISO 27001 (2014) NTP-ISO/IEC-27001,2014. Norma Tecnica Peruana-ISO/IEC-2700, Indecopi, 2014

ISO/IEC 27003:2010 (2010) Information technology Security techniques - Informa tion security management system implementation guidance.

ISO/IEC 27004:2009 (2009) Information technology - Security techniques - Informa tion security management - Measurement.

ISO/IEC 27005-2011 (2011) Information technology - Security techniques - Information security risk management.

ISO/IEC 27006:2011 (2011) Information technology - Security techniques - Require ments for bodies providing audit and certification of information security management systems

ISO/IEC 27032:2012 (2012) Information technology - Security techniques - Gui delines for cybersecurity

Jara, O. (2018) Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018

Javier, F., Enriquez, E. & Benavides, M. (2015) Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001: Revista Tecnológica ESPOL – RTE, Vol. 28, N. 5, 492-507, (Diciembre 2015).

Levin, R. y Rubin, D. (2004) Estadística para administración y economía. (7ª ed.). México: Pearson.

Lorenzo, A. (2014) Gestión de riesgo, un enfoque estratégico, 2da edición

Magerit (2012) Metodología de Análisis y Gestión de Riesgos de los sistemas de Información, Libro I Método - versión 3.0. Madrid, España: Ministerio de Hacienda y Administraciones Públicas.

Merino, C. y Cañizares, R. (2014) Auditoría de Sistemas de Gestión de Seguridad de la Información

Medina, Y. y Rico, D. (2008) Modelo de gestión de servicios para la universidad de pamplona: itil. Scientia et Technica , 14 (39), 315.

Moreno, M. y Camacho, O. (2011) Riesgos tecnológicos en la enseñanza de la ingeniería. Ciencia e Ingeniería. Mérida Venezuela, 43-52. Recuperado de http://erevistas.saber.ula.ve/index.php/cienciaeingenieria/article/view/3232/3140

NTP-ISO/IEC 17799 (2007) Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información -2007/INDECOPI-CRT. Publicada el 2007-01-22

Peltier, T. (2014) Information Security Fundamentals. 2da. Edición. Florida: CRC Press, 2014. 375 pp. ISBN 9781439810620.

Reniec (2014) Guia del archivo registral, Lima: Reniec, 2014

Reniec (2019) El Padrón Electoral en el Perú. Hitos, tecnologías e itinerarios. 1812-2019 Lima: Reniec, 2019

Romero M., Figueroa, G., Vera, D., Álava, José., Parrales, R., Álava, C., Murillo, A. & Castillo, M. (2018) Introducción a la seguridad informática y el análisis de vulnerabilidades. Primera edición: octubre 2018. Editorial Área de Innovación y Desarrollo,S.L.

Secaira, J., Ocampo, R., Mera, E. & Kovalenko, I. (2020) El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador).(Original). Roca. Revista científico-educacional de la provincia Granma, 16, 546-559.

Seclén, J. (2016) Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001.

Soriano, M. (2014) Seguridad en redes y seguridad de la información. Obtenido de http://improvet.cvut. z/project/download/C2ES/Seguridad_de_Red_e_Informacion. pdf.

Tarazona, C. (2007) Amenazas informáticas y seguridad de la información. Derecho Penal y Criminología, 28, 137.

UNE-ISO/IEC 27000:2014 (2014) Information technology - Security techniques - Information security management systems - Overview and vocabulary

UNE-ISO/IEC 27001:2014 (2014) Information technology - Security techniques - Information security management systems - Requirements.

UNE-EN ISO/IEC 27002:2017 Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)

UNE-ISO 31000:2010 Risk management. Principles and guidelines.

Westerman, G. (2006) IT Risk Management: From IT Necessity to Strategic Business Value

Anexos

UNIVERSIDAD CÉSAR VALLEJO

Anexo 1: Matriz de consistencia

Título: Seguridad de la información y Gestión de riesgos del proceso servicio electoral, Reniec, Lima, 2020

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES				
Problema general	**Objetivo general**	**Hipótesis general**	**Variable 1: Seguridad de la información**				
¿Cómo se relaciona la seguridad de la información y la Gestión de riesgos del proceso servicio electoral, Reniec, Lima, 2020?	Determinar la relación entre la seguridad de la información y la gestión de riesgos del proceso servicio electoral, Reniec, Lima, 2020.	Seguridad de la información se relaciona con la Gestión de riesgos del proceso servicio electoral, Reniec, Lima, 2020.	**Dimensiones**	**Indicadores**	**Ítems**	**Escalas valores**	**Niveles o rangos**
Problemas específicos	**Objetivos específicos:**	**Hipótesis específicas**				Nunca 1 Casi nunca 2 A veces 3 Casi siempre 4 Siempre 5	Bajo [22 -51] Medio [52 - 81] Alto [82 -111]
¿Cómo se relaciona la confidencialidad de la seguridad de la información y la Gestión de riesgos del proceso servicio electoral, Reniec, Lima, 2020?	Determinar la relación entre la confidencialidad de la seguridad de la información y la Gestión de riesgos del proceso servicio electoral, Reniec, Lima, 2020.	La confidencialidad de la seguridad de la información se relaciona con la Gestión de riesgos del proceso servicio electoral, Reniec, Lima, 2020.	Confidencialidad	Control de Acceso. Autenticación. Autorización.	1 al 6		
¿Cómo se relaciona la integridad de la seguridad de la información y la Gestión de riesgo del proceso servicio electoral, Reniec, Lima, 2020?	Determinar la relación entre la integridad de la seguridad de la información y la Gestión de riesgo del proceso servicio electoral, Reniec, Lima, 2020.	La integridad de la seguridad de la información se relaciona con la Gestión de riesgo del proceso servicio electoral, Reniec, Lima, 2020.	Integridad	Seguridad de la comunicación. Seguridad del procedimiento. Protección.	7 al 14		
¿Cómo se relaciona la disponibilidad de la seguridad de la información y la Gestión de riesgo del proceso servicio electoral, Reniec, Lima, 2020?	Determinar la relación entre la disponibilidad de la seguridad de la información y la Gestión de riesgo del proceso servicio electoral, Reniec, Lima, 2020.	La disponibilidad de la seguridad de la información se relaciona con la Gestión de riesgo del proceso servicio electoral, Reniec, Lima, 2020.	Disponibilidad	Continuidad de la regla del negocio. Acceso en el tiempo requerido. Acceso a la información.	15 al 22		

			Variable 2: Gestión de riesgo				
			Dimensiones	**Indicadores**	**Ítems**	**Escalas valores**	**Niveles o rangos**
			Cultura consciente sobre riesgos	Grado de concientización. Efectividad del monitoreo de las actividades de Gestión de riesgos.	1 al 7	Nunca 1 Casi nunca 2 A veces 3 Casi siempre 4 Siempre 5	Bajo [20 - 46] Medio [47 - 73] Alto [74 -100]
			Proceso de gobernanza del riesgo	Grado de planeamiento. Efectividad en la definición de los riesgos según las categorías de Información.	8 al 13		
			Implantación eficaz de riesgos	Efectividad de la Implantación de controles y seguimiento de las brechas de seguridad. Efectividad en los niveles de riesgos.	14 al 20		

TIPO Y DISEÑO DE INVESTIGACIÓN	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS	ESTADÍSTICA DESCRIPTIVA E INFERENCIAL
ENFOQUE: Cuantitativo **MÉTODO.** Hipotético-deductivo **TIPO:** Básica **NIVEL:** Explicativo **DISEÑO:** No experimental – Correlacional Transversal	**Población censal:** Estuvo conformada por 64 colaboradores de la Gerencia de Registro Electoral – RENIEC.	**Técnica:** Encuesta **Instrumentos:** Cuestionario de seguridad de la información. Cuestionario de gestión de riesgos.	**DESCRIPTIVA:** - Tablas de frecuencia - Figuras estadísticas **INFERENCIAL**: Para la prueba de Hipótesis se realizarán los cálculos estadísticos necesarios mediante la Correlación de Spearman: Dónde: $r_s=1-\frac{6\sum d^2}{n(n^2-1)}$ rs= Coeficiente de correlación por rangos de Spearman d = Diferencia entre los rangos (X menos Y) n = Número de datos

Anexo 2: Opercionalización de variables

Tabla 1

Operacionalización de la variable 1: Seguridad de la información

Dimensiones	Indicadores	Ítems	Escala y valores	Nivel y rango
Confidencialidad	Control de Acceso.	1 al 6	Nunca (1),	Bajo [22 -51]
			Casi nunca (2),	Medio [52 - 81]
	Autenticación.		A veces (3),	Alto [82 -111]
			Casi siempre (4),	
	Autorización.		Siempre (5)	
Integridad	Seguridad de la comunicación.	7 al 14		
	Seguridad del procedimiento.			
	Protección.			
Disponibilidad	Continuidad de la regla del negocio.	15 al 22		
	Acceso en el tiempo requerido.			
	Acceso a la información.			

Tabla 2

Operacionalización de la variable 2: Gestión de riesgos

Dimensiones	Indicadores	Ítems	Escala y valores	Nivel y rango
Cultura consciente sobre riesgos	Grado de concientización. Efectividad del monitoreo de las actividades de Gestión de riesgos.	1 al 7	Nunca (1), Casi nunca (2), A veces (3), Casi siempre (4), Siempre (5)	Bajo [20 - 46] Medio [47 - 73] Alto [74 -100]
Proceso de gobernanza del riesgo	Grado de planeamiento. Efectividad en la definición de los riesgos según las categorías de Información.	8 al 13		
Implantación eficaz de riesgos	Efectividad de la Implantación de controles y seguimiento de las brechas de seguridad. Efectividad en los niveles de riesgos	14 al 20		

Anexo 3: Instrumentos de recolección de datos

CUESTIONARIO DE SEGURIDAD DE LA INFORMACIÓN

INSTRUCCIONES: Estimado colaborador, a continuación, tienes 20 preguntas sobre la Gestión de seguridad de la información, para lo cual debes marcar con el número de la tabla la opción que consideras correcta.

Nunca	Casi nunca	Algunas veces	Siempre	Siempre Casi
1	2	3	4	5

	ÍTEMS					
N°	Dimensión 1: Confidencialidad	1	2	3	4	5
1	Asegura que los usuarios deben tener autorización a los accesos de los activos de información, equipos de cómputo, aplicativos y otros.					
2	Gestiona periódicamente la política de cambio de contraseñas en los aplicativos y equipos de cómputo.					
3	Gestiona buenas prácticas en el buen uso de la información y control de los documentos a ser eliminados, evitando así la destrucción de aquellos con valor administrativo.					
4	Asegura que los equipos de cómputo se encuentren protegidos mediante claves de bloqueo, contraseñas u otros controles cuando no están en uso.					
5	Gestiona para que los equipos, la información o el software no deban ser retirados de su lugar sin autorización previa.					
6	Realiza controles apropiados para asegurar solo el ingreso del personal autorizado al centro de labores.					
	Dimensión 2: Integridad					
7	Establece lineamientos para detectar, reportar, evaluar y responder a los incidentes de Seguridad de la Información.					
8	Garantiza que los activos de la información se encuentren disponibles para realizar sus labores.					
9	Impulsa a todos los colaboradores a aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos.					

10	Implementa la restricción de USB o dispositivos Extraíbles de Almacenamiento como medida de prevención contra malware, fuga y pérdida de información.					
11	Proporciona solución a las incidencias en forma rápida ante fallos del sistema o alguna avería en los equipos de cómputo.					
12	Establece controles por perdidas de activos de información en sus procedimientos.					
13	Aplica procedimientos de resguardo de la documentación clasificada en lugares seguro y protegido.					
14	Previene de pérdida, daño o robo de activos de información en las operaciones de sus funciones.					
	Dimensión 3: Disponibilidad					
15	Cuenta con disponibilidad existente de políticas de seguridad de la información.					
16	Gestiona con la continuidad de medidas de emergencia del servicio ante cortes eléctricos imprevistos.					
17	Cuenta con un plan de contingencia para recuperación de los activos de información en caso de desastres.					
18	Establece controles por perdidas de activos de información dentro de la institución.					
19	Garantiza la rapidez en los aplicativos con el objetivo de agilizar las actividades encomendadas.					
20	Permite el acceso a la página web e intranet institucional en el momento oportuno.					
21	Permite el acceso a la información y a las funciones del sistema de aplicación en concordancia con la política de control de acceso para sus funciones.					
22	Garantiza que el acceso a la información se encuentre disponible para realizar sus labores.					

Cuestionario de productividad

IN**STRUCCIONES:** Estimado colega, a continuación, tienes 20 preguntas sobre la Gestión de riesgos del proceso del servicio electoral, para lo cual debes marcar con el número de la tabla la opción que consideras correcta.

Nunca	Casi nunca	Algunas veces	Siempre	Siempre Casi
1	2	3	4	5

	ÍTEMS					
N°	**Dimensión 1: Cultura consciente sobre riesgos**	**1**	**2**	**3**	**4**	**5**
1	Brinda capacitación referente a seguridad de la información.					
2	Implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos.					
3	Proporciona capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información.					
4	Recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información.					
5	Establece Capacitación de sensibilización y concientización sobre los riesgos a los que está expuesta los activos de información.					
6	Promueve el compromiso con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información.					
7	Aplica y asegura las buenas prácticas relacionadas a las políticas de seguridad de la información.					
	Dimensión 2: Proceso de gobernanza del riesgo					
8	Implementa roles y responsabilidades definidos de seguridad de la información.					
9	Promueve la buena práctica del plan de gestión de riesgos de la seguridad de la información.					
10	Identifica los riesgos que pueden afectar el desarrollo de las actividades diarias.					
11	Participa en la identificación de los riesgos a los que está expuesta la información de la Gerencia de Registro Electoral.					
12	Determina y cuantifica la posibilidad de que ocurran los riesgos identificados.					

13	Implementa las acciones necesarias para afrontar los riesgos evaluados.					
	Dimensión 3: Implantación eficaz de riesgos					
14	Implanta políticas para minimizar posibles riesgos vinculados a la seguridad de la Información.					
15	Monitorea la plataforma virtual del servicio electoral en las cuales se actualizan las buenas prácticas vinculados a los activos de la información					
16	Seguimiento efectivo de los controles aplicados a los probables riesgos en la Gerencia de Registro Electoral.					
17	Seguimiento a las brechas entorno a la seguridad de la información.					
18	Propone invertir en nuevas tecnologías de información (servidores, PC, antivirus, etc.) para una mayor seguridad de la información.					
19	Verifica e informa la obsolescencia de equipos de cómputo para proponer la renovación de estas.					
20	Participa en el plan de contingencia para recuperación de los activos de información en caso de desastres.					

Anexo 4: Ficha técnica

Ficha técnica 1

Denominación: Cuestionario de seguridad de la información

Finalidad : Determinar el nivel seguridad de la información

Autor : Calderón (2019)

Adaptado : Leon (2020)

Sujetos de aplicación: Colaboradores

Administración: Individual

Ficha técnica de instrumento 2

Nombre : Cuestionario gestión de riesgos

Finalidad : Determinar el nivel de la gestión de riesgos

Autora : Calderón (2019).

Adaptación : Leon (2020)

Sujetos de aplicación: Colaboradores

Administración: Individual

Validez de contenido a través de juicio de expertos

	Validación			
Expertos	Pertinencia	Relevancia	Claridad	Calificación
Dra. Francis Ibarguen Cueva	si	si	si	Aplicable
Mg. Juana Litz Tupa Quispe	si	si	si	Aplicable
Mg. Tito Orlando Chunga Díaz	si	si	si	Aplicable

Fuente: Certificado de validez

Anexo 5: Certificados de validez de expertos

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACIÓN.

Nº	/ ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Confidencialidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Asegura que los usuarios deben tener autorización a los accesos de los activos de información, equipos de cómputo, aplicativos y otros.	✓		✓		✓		
2	Gestiona periódicamente la política de cambio de contraseñas en los aplicativos y equipos de cómputo.	✓		✓		✓		
3	Gestiona buenas prácticas en el buen uso de la información y control de los documentos a ser eliminados, evitando así la destrucción de aquellos con valor administrativo.	✓		✓		✓		
4	Asegura que los equipos de cómputo se encuentren protegidos mediante claves de bloqueo, contraseñas u otros controles cuando no están en uso.	✓		✓		✓		
5	Gestiona para que los equipos, la información o el software no deban ser retirados de su lugar sin autorización previa.	✓		✓		✓		
6	Realiza controles apropiados para asegurar solo el ingreso del personal autorizado al centro de labores.	✓		✓		✓		
	Integridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	Establece lineamientos para detectar, reportar, evaluar y responder a los incidentes de Seguridad de la Información.	✓		✓		✓		

8	Garantiza que los activos de la información se encuentren disponibles para realizar sus labores.	✓		✓		✓		
9	Impulsa a todos los colaboradores a aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos.	✓		✓		✓		
10	Implementa la restricción de USB o dispositivos Extraíbles de Almacenamiento como medida de prevención contra malware, fuga y pérdida de información.	✓		✓		✓		
11	Proporciona solución a las incidencias en forma rápida ante fallos del sistema o alguna avería en los equipos de cómputo.	✓		✓		✓		
12	Establece controles por perdidas de activos de información en sus procedimientos.	✓		✓		✓		
13	Aplica procedimientos de resguardo de la documentación clasificada en lugares seguro y protegido.	✓		✓		✓		
14	Previene de pérdida, daño o robo de activos de información en las operaciones de sus funciones.	✓		✓		✓		
	Disponibilidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
15	Cuenta con disponibilidad existente de políticas de seguridad de la información.	✓		✓		✓		
16	Gestiona con la continuidad de medidas de emergencia del servicio ante cortes eléctricos imprevistos.	✓		✓		✓		
17	Cuenta con un plan de contingencia para recuperación de los activos de información en caso de desastres.	✓		✓		✓		

18	Establece controles por perdidas de activos de información dentro de la institución.	✓		✓		✓		
19	Garantiza la rapidez en los aplicativos con el objetivo de agilizar las actividades encomendadas.	✓		✓		✓		
20	Permite el acceso a la página web e intranet institucional en el momento oportuno.	✓		✓		✓		
21	Permite el acceso a la información y a las funciones del sistema de aplicación en concordancia con la política de control de acceso para sus funciones.	✓		✓		✓		
22	Garantiza que el acceso a la información se encuentre disponible para realizar sus labores.	✓		✓		✓		

Observaciones (precisar si hay suficiencia):_ Hay suficiencia

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

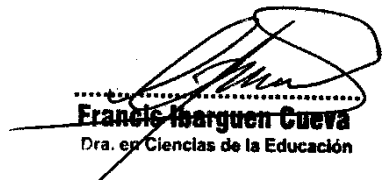
28 de mayo del 2020

Apellidos y nombre s del juez evaluador: *Francis Esmeralda Ibarguen Cueva*
DNI: 09637865

Especialidad del evaluador: Dra. Ciencias de la educación – metodología de la investigación científica.

[1] **Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA GESTIÓN DE RIESGO.

Nº	/ ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Cultura consciente sobre riesgos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Brinda capacitación referente a seguridad de la información.	✓		✓		✓		
2	Implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos.	✓		✓		✓		
3	Proporciona capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información.	✓		✓		✓		
4	Recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información.	✓		✓		✓		
5	Establece Capacitación de sensibilización y concientización sobre los riesgos a los que está expuesta los activos de información.	✓		✓		✓		
6	Promueve el compromiso con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información.	✓		✓		✓		
7	Aplica y asegura las buenas prácticas relacionadas a las políticas de seguridad de la información.	✓		✓		✓		
	Proceso de gobernanza del riesgo	**Si**	**No**	**Si**	**No**	**Si**	**No**	
8	Implementa roles y responsabilidades definidos de seguridad de la información.	✓		✓		✓		

9	Promueve la buena práctica del plan de gestión de riesgos de la seguridad de la información.	✓		✓		✓		
10	Identifica los riesgos que pueden afectar el desarrollo de las actividades diarias.	✓		✓		✓		
11	Participa en la identificación de los riesgos a los que está expuesta la información de la Gerencia de Registro Electoral.	✓		✓		✓		
12	Determina y cuantifica la posibilidad de que ocurran los riesgos identificados.	✓		✓		✓		
13	Implementa las acciones necesarias para afrontar los riesgos evaluados.	✓		✓		✓		
	Implantación eficaz de riesgos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
14	Implanta políticas para minimizar posibles riesgos vinculados a la seguridad de la Información.	✓		✓		✓		
15	Monitorea la plataforma virtual del servicio electoral en las cuales se actualizan las buenas prácticas vinculados a los activos de la información	✓		✓		✓		
16	Seguimiento efectivo de los controles aplicados a los probables riesgos en la Gerencia de Registro Electoral.	✓		✓		✓		
17	Seguimiento a las brechas entorno a la seguridad de la información.	✓		✓		✓		
18	Propone invertir en nuevas tecnologías de información (servidores, PC, antivirus, etc.) para una mayor seguridad de la información.	✓		✓		✓		

19	Verifica e informa la obsolescencia de equipos de cómputo para proponer la renovación de estas.	✓		✓		✓		
20	Participa en el plan de contingencia para recuperación de los activos de información en caso de desastres.	✓		✓		✓		

Observaciones (precisar si hay suficiencia):_ Hay suficiencia

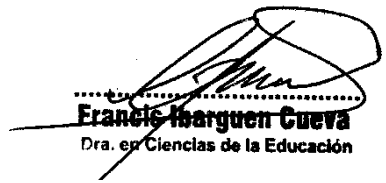
Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

28 de mayo del 2020

Apellidos y nombre s del juez evaluador: *Francis Esmeralda Ibarguen Cueva*
DNI: 09637865

Especialidad del evaluador: Dra. Ciencias de la educación – metodología de la investigación científica.

[1] **Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo



Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: LA SEGURIDAD DE LA INFORMACIÓN.

Nº	/ ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Confidencialidad	Si	No	Si	No	Si	No	
1	Asegura que los usuarios deben tener autorización a los accesos de los activos de información, equipos de cómputo, aplicativos y otros.	✓		✓		✓		
2	Gestiona periódicamente la política de cambio de contraseñas en los aplicativos y equipos de cómputo.	✓		✓		✓		
3	Gestiona buenas prácticas en el buen uso de la información y control de los documentos a ser eliminados, evitando así la destrucción de aquellos con valor administrativo.	✓		✓		✓		
4	Asegura que los equipos de cómputo se encuentren protegidos mediante claves de bloqueo, contraseñas u otros controles cuando no están en uso.	✓		✓			✓	
5	Gestiona para que los equipos, la información o el software no deban ser retirados de su lugar sin autorización previa.	✓		✓		✓		
6	Realiza controles apropiados para asegurar solo el ingreso del personal autorizado al centro de labores.	✓		✓			✓	

	Integridad	Si	No	Si	No	Si	No	
7	Establece lineamientos para detectar, reportar, evaluar y responder a los incidentes de Seguridad de la Información.	✓		✓		✓		
8	Garantiza que los activos de la información se encuentren disponibles para realizar sus labores.	✓		✓		✓		
9	Impulsa a todos los colaboradores a aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos.	✓		✓		✓		
10	Implementa la restricción de USB o dispositivos Extraíbles de Almacenamiento como medida de prevención contra malware, fuga y pérdida de información.	✓		✓		✓		
11	Proporciona solución a las incidencias en forma rápida ante fallos del sistema o alguna avería en los equipos de cómputo.	✓		✓		✓		
12	Establece controles por perdidas de activos de información en sus procedimientos.	✓		✓		✓		
13	Aplica procedimientos de resguardo de la documentación clasificada en lugares seguro y protegido.	✓		✓		✓		
14	Previene de pérdida, daño o robo de activos de información en las operaciones de sus funciones.	✓		✓		✓		

	Disponibilidad	Si	No	Si	No	Si	No	
15	Cuenta con disponibilidad existente de políticas de seguridad de la información.	✓		✓			✓	
16	Gestiona con la continuidad de medidas de emergencia del servicio ante cortes eléctricos imprevistos.	✓		✓		✓		
17	Cuenta con un plan de contingencia para recuperación de los activos de información en caso de desastres.	✓		✓		✓		
18	Establece controles por perdidas de activos de información dentro de la institución.	✓		✓		✓		
19	Garantiza la rapidez en los aplicativos con el objetivo de agilizar las actividades encomendadas.	✓		✓		✓		
20	Permite el acceso a la página web e intranet institucional en el momento oportuno.	✓		✓		✓		
21	Permite el acceso a la información y a las funciones del sistema de aplicación en concordancia con la política de control de acceso para sus funciones.	✓		✓		✓		
22	Garantiza que el acceso a la información se encuentre disponible para realizar sus labores.	✓		✓		✓		

Observaciones (precisar si hay suficiencia): ***Tiene suficiencia***

Opinión de aplicabilidad: **Aplicable [✓]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Lima, 29 de mayo del 2020.

Apellidos y nombres del juez evaluador: ***JUANA LITZ TUPA QUISPE*****……..DNI: 23839591**

Especialidad del evaluador: ***Maestro en Gestión Pública***

Firma del Experto Informante

[1] **Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: LA GESTIÓN DE RIESGO.

Nº	/ ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Cultura consciente sobre riesgos	Si	No	Si	No	Si	No	
1	Brinda capacitación referente a seguridad de la información.	✓		✓		✓		
2	Implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos.	✓		✓		✓		
3	Proporciona capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información.	✓		✓		✓		
4	Recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información.	✓		✓		✓		
5	Establece Capacitación de sensibilización y concientización sobre los riesgos a los que está expuesta los activos de información.	✓		✓		✓		
6	Promueve el compromiso con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información.	✓		✓		✓		
7	Aplica y asegura las buenas prácticas relacionadas a las políticas de seguridad de la información.	✓		✓		✓		
	Proceso de gobernanza del riesgo	Si	No	Si	No	Si	No	

8	Implementa roles y responsabilidades definidos de seguridad de la información.	✓		✓		✓		
9	Promueve la buena práctica del plan de gestión de riesgos de la seguridad de la información.	✓		✓		✓		
10	Identifica los riesgos que pueden afectar el desarrollo de las actividades diarias.	✓		✓		✓		
11	Participa en la identificación de los riesgos a los que está expuesta la información de la Gerencia de Registro Electoral.	✓		✓		✓		
12	Determina y cuantifica la posibilidad de que ocurran los riesgos identificados.	✓		✓		✓		
13	Implementa las acciones necesarias para afrontar los riesgos evaluados.	✓		✓		✓		
	Implantación eficaz de riesgos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
14	Implanta políticas para minimizar posibles riesgos vinculados a la seguridad de la Información.	✓		✓		✓		
15	Monitorea la plataforma virtual del servicio electoral en las cuales se actualizan las buenas prácticas vinculados a los activos de la información	✓		✓		✓		
16	Seguimiento efectivo de los controles aplicados a los probables riesgos en la Gerencia de Registro Electoral.	✓		✓		✓		
17	Seguimiento a las brechas entorno a la seguridad de la información.	✓		✓		✓		

18	Propone invertir en nuevas tecnologías de información (servidores, PC, antivirus, etc.) para una mayor seguridad de la información.	✓		✓		✓		
19	Verifica e informa la obsolescencia de equipos de cómputo para proponer la renovación de estas.	✓		✓		✓		
20	Participa en el plan de contingencia para recuperación de los activos de información en caso de desastres.	✓		✓		✓		

Observaciones (precisar si hay suficiencia): ***Tiene suficiencia***

Opinión de aplicabilidad: **Aplicable [✓]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Lima, 29 de mayo de 2020.

Apellidos y nombres del juez evaluador: Mg. ***JUANA LITZ TUPA QUISPE*****……. DNI: 23839591**

Especialidad del evaluador: ***Maestro en Gestión Pública.***

Firma del Experto Informante

[1] **Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: LA SEGURIDAD DE LA INFORMACIÓN.

Nº	/ ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Confidencialidad	Si	No	Si	No	Si	No	
1	Asegura que los usuarios deben tener autorización a los accesos de los activos de información, equipos de cómputo, aplicativos y otros.	✓		✓		✓		
2	Gestiona periódicamente la política de cambio de contraseñas en los aplicativos y equipos de cómputo.	✓		✓		✓		
3	Gestiona buenas prácticas en el buen uso de la información y control de los documentos a ser eliminados, evitando así la destrucción de aquellos con valor administrativo.	✓		✓		✓		
4	Asegura que los equipos de cómputo se encuentren protegidos mediante claves de bloqueo, contraseñas u otros controles cuando no están en uso.	✓		✓		✓		
5	Gestiona para que los equipos, la información o el software no deban ser retirados de su lugar sin autorización previa.	✓		✓		✓		
6	Realiza controles apropiados para asegurar solo el ingreso del personal autorizado al centro de labores.	✓		✓		✓		

	Integridad	Si	No	Si	No	Si	No	
7	Establece lineamientos para detectar, reportar, evaluar y responder a los incidentes de Seguridad de la Información.	✓		✓		✓		
8	Garantiza que los activos de la información se encuentren disponibles para realizar sus labores.	✓		✓		✓		
9	Impulsa a todos los colaboradores a aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos.	✓		✓		✓		
10	Implementa la restricción de USB o dispositivos Extraíbles de Almacenamiento como medida de prevención contra malware, fuga y pérdida de información.	✓		✓		✓		
11	Proporciona solución a las incidencias en forma rápida ante fallos del sistema o alguna avería en los equipos de cómputo.	✓		✓		✓		
12	Establece controles por perdidas de activos de información en sus procedimientos.	✓		✓		✓		
13	Aplica procedimientos de resguardo de la documentación clasificada en lugares seguro y protegido.	✓		✓		✓		
14	Previene de pérdida, daño o robo de activos de información en las operaciones de sus funciones.	✓		✓		✓		
	Disponibilidad	Si	No	Si	No	Si	No	

15	Cuenta con disponibilidad existente de políticas de seguridad de la información.	✓		✓		✓		
16	Gestiona con la continuidad de medidas de emergencia del servicio ante cortes eléctricos imprevistos.	✓		✓		✓		
17	Cuenta con un plan de contingencia para recuperación de los activos de información en caso de desastres.	✓		✓		✓		
18	Establece controles por perdidas de activos de información dentro de la institución.	✓		✓		✓		
19	Garantiza la rapidez en los aplicativos con el objetivo de agilizar las actividades encomendadas.	✓		✓		✓		
20	Permite el acceso a la página web e intranet institucional en el momento oportuno.	✓		✓		✓		
21	Permite el acceso a la información y a las funciones del sistema de aplicación en concordancia con la política de control de acceso para sus funciones.	✓		✓		✓		
22	Garantiza que el acceso a la información se encuentre disponible para realizar sus labores.	✓		✓		✓		

Observaciones (precisar si hay suficiencia): ***Tiene suficiencia***

Opinión de aplicabilidad: **Aplicable [✓]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez evaluador: ***Mg. Tito Orlando Chunga Díaz.*** **DNI:** ***16746065***

Especialidad del evaluador: ***Maestro en Gestión Pública***

Lima, 01 de Junio de 2020.

[1] **Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

[3] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: LA GESTIÓN DE RIESGO.

Nº	/ ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Cultura consciente sobre riesgos	Si	No	Si	No	Si	No	
1	Brinda capacitación referente a seguridad de la información.	✓		✓		✓		
2	Implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos.	✓		✓		✓		
3	Proporciona capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información.	✓		✓		✓		
4	Recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información.	✓		✓		✓		
5	Establece Capacitación de sensibilización y concientización sobre los riesgos a los que está expuesta los activos de información.	✓		✓		✓		
6	Promueve el compromiso con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información.	✓		✓		✓		
7	Aplica y asegura las buenas prácticas relacionadas a las políticas de seguridad de la información.	✓		✓		✓		
	Proceso de gobernanza del riesgo							

		✓		✓		✓		
8	Implementa roles y responsabilidades definidos de seguridad de la información.	✓		✓		✓		
9	Promueve la buena práctica del plan de gestión de riesgos de la seguridad de la información.	✓		✓		✓		
10	Identifica los riesgos que pueden afectar el desarrollo de las actividades diarias.	✓		✓		✓		
11	Participa en la identificación de los riesgos a los que está expuesta la información de la Gerencia de Registro Electoral.	✓		✓		✓		
12	Determina y cuantifica la posibilidad de que ocurran los riesgos identificados.	✓		✓		✓		
13	Implementa las acciones necesarias para afrontar los riesgos evaluados.	✓		✓		✓		
	Implantación eficaz de riesgos	✓		✓		✓		
14	Implanta políticas para minimizar posibles riesgos vinculados a la seguridad de la Información.	✓		✓		✓		

15	Monitorea la plataforma virtual del servicio electoral en las cuales se actualizan las buenas prácticas vinculados a los activos de la información	✓		✓		✓		
16	Seguimiento efectivo de los controles aplicados a los probables riesgos en la Gerencia de Registro Electoral.	✓		✓		✓		
17	Seguimiento a las brechas entorno a la seguridad de la información.	✓		✓		✓		
18	Propone invertir en nuevas tecnologías de información (servidores, PC, antivirus, etc.) para una mayor seguridad de la información.	✓		✓		✓		
19	Verifica e informa la obsolescencia de equipos de cómputo para proponer la renovación de estas.	✓		✓		✓		
20	Participa en el plan de contingencia para recuperación de los activos de información en caso de desastres.	✓		✓		✓		

Observaciones (precisar si hay suficiencia): ***Tiene suficiencia***

Opinión de aplicabilidad: **Aplicable [✓]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombre s del juez evaluador: ***Mg. Tito Orlando Chunga Díaz.*** **DNI:** ***16746065***

Especialidad del evaluador: ***Maestro en Gestión Pública***

Lima, 01 de Junio de 2020.

[1] **Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

[3] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

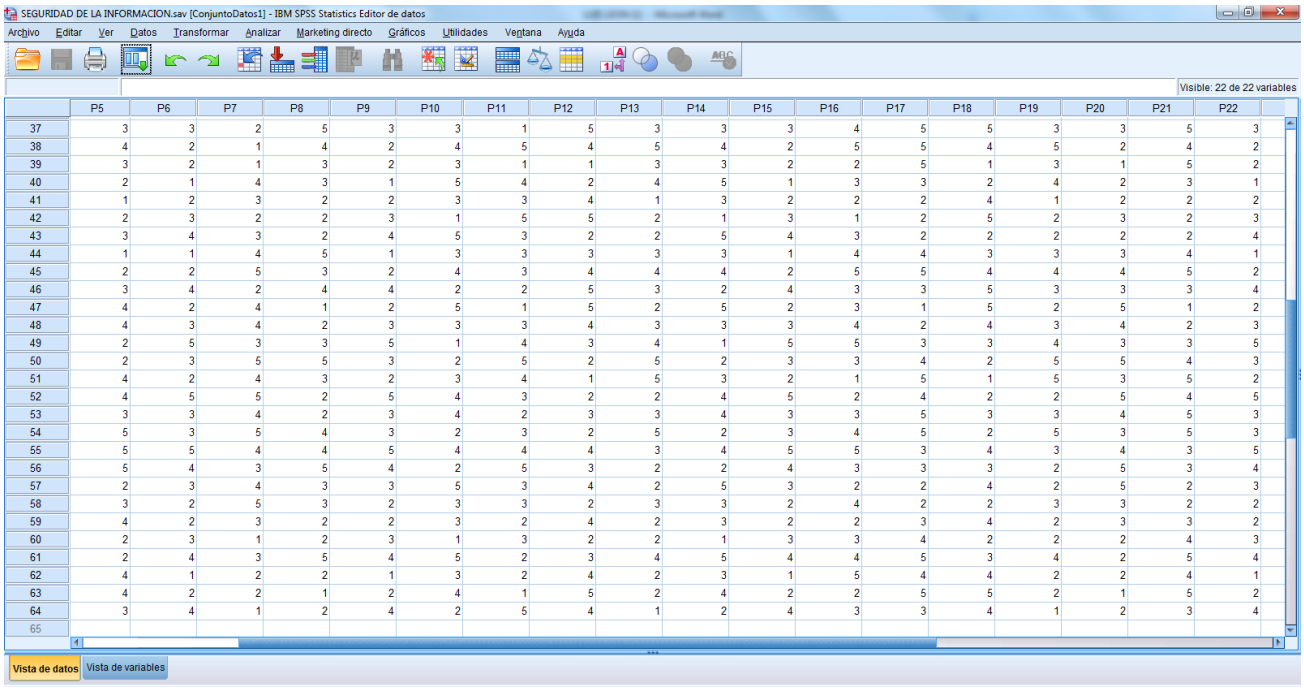
Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Anexo 6: Confiabilidad

Base de datos: Confiabilidad de Seguridad de la información



	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22
37	3	3	2	5	3	3	1	5	3	3	3	4	5	5	3	3	5	3
38	4	2	1	4	2	4	5	4	5	4	2	5	5	4	5	2	4	2
39	3	2	1	3	2	3	1	1	3	3	2	2	5	1	3	1	5	2
40	2	1	4	3	1	5	4	2	4	5	1	3	3	2	4	2	3	1
41	1	2	3	2	2	3	3	4	1	3	2	2	2	4	1	2	2	2
42	2	3	2	2	3	1	5	5	2	1	3	1	2	5	2	3	2	3
43	3	4	3	2	4	5	3	2	2	5	4	3	2	2	2	2	2	4
44	1	1	4	5	1	3	3	3	3	3	1	4	4	3	3	3	4	1
45	2	2	5	3	2	4	3	4	4	4	2	5	5	4	4	4	5	2
46	3	4	2	4	4	2	2	5	3	2	4	3	3	5	3	3	3	4
47	4	2	4	1	2	5	1	5	2	5	2	3	1	5	2	5	1	2
48	4	3	4	2	3	3	3	4	3	3	3	4	2	4	3	4	2	3
49	2	5	3	3	5	1	4	3	4	1	5	5	3	3	4	3	3	5
50	2	3	5	5	3	2	5	2	5	2	3	3	4	2	5	5	4	3
51	4	2	4	3	2	3	4	1	5	3	2	1	5	1	5	3	5	2
52	4	5	5	2	5	4	3	2	2	4	5	2	4	2	2	5	4	5
53	3	3	4	2	3	4	2	3	3	4	3	3	5	3	3	4	5	3
54	5	3	5	4	3	2	3	2	5	2	3	4	5	2	5	3	5	3
55	5	5	4	4	5	4	4	4	3	4	5	5	3	4	3	4	3	5
56	5	4	3	5	4	2	5	3	2	2	4	3	3	3	2	5	3	4
57	2	3	4	3	3	5	3	4	2	5	3	2	2	4	2	5	2	3
58	3	2	5	3	2	3	3	2	3	3	2	4	2	2	3	3	2	2
59	4	2	3	2	2	3	2	4	2	3	2	2	3	4	2	3	3	2
60	2	3	1	2	3	1	3	2	2	1	3	3	4	2	2	2	4	3
61	2	4	3	5	4	5	2	3	4	5	4	4	5	3	4	2	5	4
62	4	1	2	2	1	3	2	4	2	3	1	5	4	4	2	2	4	1
63	4	2	2	1	2	4	1	5	2	4	2	2	5	5	2	1	5	2
64	3	4	1	2	4	2	5	4	1	2	4	3	3	4	1	2	3	4
65																		

Escala: SEGURIDAD DE LA INFORMACION

Resumen de procesamiento de casos

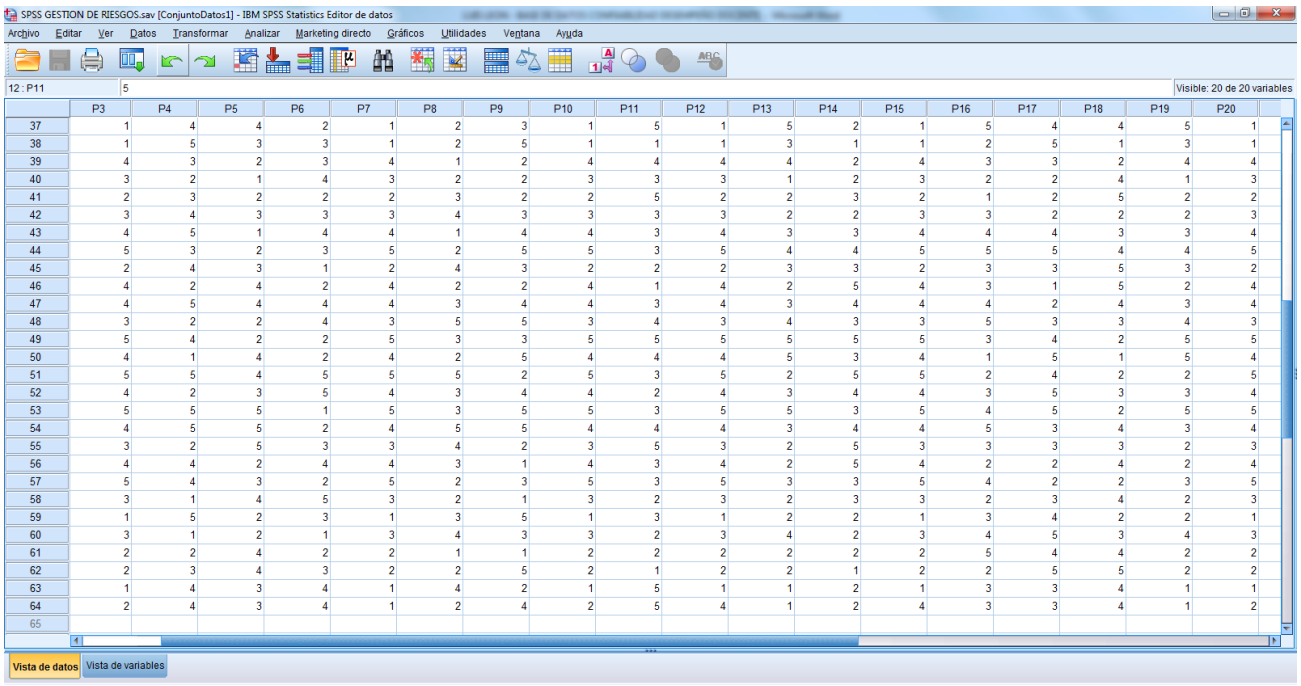
		N	%
Casos	Válido	64	100,0
	Excluido[a]	0	,0
	Total	64	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,823	22

Base de datos: Confiabilidad de Gestión de riesgos



	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20
37	1	4	4	2	1	2	3	1	5	1	5	2	1	5	4	4	5	1
38	1	5	3	3	1	2	5	1	1	1	3	1	1	2	5	1	3	1
39	4	3	2	3	4	1	2	4	4	4	4	2	4	3	3	2	4	4
40	3	2	1	4	3	2	2	3	3	3	1	2	3	2	2	4	1	3
41	2	3	2	2	2	3	2	2	5	2	2	3	2	1	2	5	2	2
42	3	4	3	3	3	4	3	3	3	3	2	2	3	3	2	2	2	3
43	4	5	1	4	4	1	4	4	3	4	3	3	4	4	4	3	3	4
44	5	3	2	3	5	2	5	5	3	5	4	4	5	5	5	4	4	5
45	2	4	3	1	2	4	3	2	2	2	3	3	2	3	3	5	3	2
46	4	2	4	2	4	2	2	4	1	4	2	5	4	3	1	5	2	4
47	4	5	4	4	4	3	4	4	3	4	3	4	4	4	2	4	3	4
48	3	2	2	4	3	5	5	3	4	3	4	3	3	5	3	3	4	3
49	5	4	2	2	5	3	3	5	5	5	5	5	5	3	4	2	5	5
50	4	1	4	2	4	2	5	4	4	4	5	3	4	1	5	1	5	4
51	5	5	4	5	5	5	2	5	3	5	2	5	5	2	4	2	2	5
52	4	2	3	5	4	3	4	4	2	4	3	4	4	3	5	3	3	4
53	5	5	5	1	5	3	5	5	3	5	5	3	5	4	5	2	5	5
54	4	5	5	2	4	5	5	4	4	4	3	4	4	5	3	4	3	4
55	3	2	5	3	3	4	2	3	5	3	2	5	3	3	3	3	2	3
56	4	4	2	4	4	3	1	4	3	4	2	5	4	2	2	4	2	4
57	5	4	3	2	5	2	3	5	3	5	3	3	5	4	2	2	3	5
58	3	1	4	5	3	2	1	3	2	3	2	3	3	2	3	4	2	3
59	1	5	2	3	1	3	5	1	3	1	2	2	1	3	4	2	2	1
60	3	1	2	1	3	4	3	3	2	3	4	2	3	4	5	3	4	3
61	2	2	4	2	2	1	1	2	2	2	2	2	2	5	4	4	2	2
62	2	3	4	3	2	2	5	2	1	2	2	1	2	2	5	5	2	2
63	1	4	3	4	1	4	2	1	5	1	1	2	1	3	3	4	1	1
64	2	4	3	4	1	2	4	2	5	4	1	2	4	3	3	4	1	2
65																		

Escala: GESTION DE RIESGOS

Resumen de procesamiento de casos

		N	%
Casos	Válido	64	100,0
	Excluido[a]	0	,0
	Total	64	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,821	20

Anexo 7: Bases de datos

BASE DE DATOS VARIABLE 1: SEGURIDAD DE LA INFORMACIÓN																						
	D1: CONFIDENCIABILIDAD						D2: INTEGRIDAD								D3: DISPONIBILIDAD							
N°	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	5	5	1	2	4	5	3	3	5	1	2	1	2	1	5	2	3	1	2	1	3	5
2	3	3	4	1	3	3	2	3	3	4	3	4	3	4	3	2	3	4	3	3	3	3
3	2	2	1	5	2	2	1	2	2	1	2	4	5	1	2	5	2	4	5	3	2	2
4	2	2	1	1	2	2	3	2	2	1	2	1	5	1	2	1	2	1	5	2	2	2
5	3	3	4	1	5	3	2	2	3	4	5	4	1	4	3	1	3	4	1	1	3	3
6	2	2	1	2	2	2	3	2	2	1	2	1	2	1	2	2	2	1	2	3	2	2
7	2	2	5	2	1	2	1	2	2	5	2	5	2	5	2	2	2	5	2	2	2	2
8	5	5	1	4	5	5	3	5	5	1	5	2	4	1	5	4	3	2	4	2	3	5
9	2	2	1	2	2	2	2	2	2	1	2	1	2	1	2	2	4	1	2	2	4	2
10	1	1	2	1	1	1	2	1	1	2	3	2	2	2	1	2	1	2	2	1	1	1
11	2	2	2	1	2	2	1	2	2	2	2	2	1	2	2	1	2	2	1	2	2	2
12	2	2	1	4	2	2	3	2	2	1	2	1	4	1	2	4	2	5	4	2	2	2
13	5	5	1	1	5	5	1	5	5	1	5	1	4	1	5	1	5	1	4	3	1	5
14	1	1	3	2	1	1	2	4	1	3	4	3	2	3	1	2	1	3	2	3	1	1
15	2	2	1	1	3	2	2	2	2	1	2	1	1	1	2	5	2	1	1	2	2	2
16	1	1	1	1	2	1	1	3	1	1	2	1	1	1	1	1	5	1	1	2	5	1
17	4	4	3	3	3	4	4	3	4	3	3	3	2	3	4	3	4	3	2	1	4	4
18	4	4	4	4	4	4	1	4	4	4	4	3	3	4	4	4	5	3	3	2	5	4
19	2	2	2	2	5	2	5	5	2	2	3	4	4	2	2	2	3	4	4	5	3	2
20	5	5	5	4	4	5	2	3	5	5	2	4	5	5	5	3	4	1	5	3	4	5
21	2	2	2	3	3	2	4	1	2	2	1	4	4	2	2	4	5	4	4	4	5	2
22	3	3	3	4	4	3	5	2	3	3	3	2	3	3	3	5	5	2	3	3	1	3

23	4	4	4	2	2	4	4	3	4	4	3	2	2	4	4	3	3	2	2	4	3	4
24	5	5	2	1	4	5	5	4	5	2	3	4	1	2	5	2	2	4	1	3	2	5
25	2	2	3	5	2	2	5	5	2	3	4	4	2	3	2	1	3	4	2	2	1	2
26	1	1	5	1	2	1	4	3	1	5	4	3	3	5	1	2	5	3	3	3	5	1
27	2	2	3	2	4	2	5	2	2	3	5	1	3	3	2	3	2	1	3	4	2	2
28	4	4	2	3	4	4	2	2	4	2	3	3	4	2	4	3	3	3	4	4	3	4
29	5	5	4	4	3	5	3	3	5	4	4	3	3	4	5	4	4	3	3	3	4	5
30	2	2	2	2	3	2	3	5	2	2	3	4	2	2	2	5	5	4	2	2	5	2
31	3	3	3	2	4	3	2	4	3	3	2	3	1	3	3	3	4	3	1	4	4	3
32	4	4	4	3	2	4	1	2	4	4	1	3	2	4	4	2	4	3	2	4	5	4
33	1	1	5	5	2	1	3	2	1	5	2	4	3	5	1	1	1	4	3	3	1	1
34	2	2	3	5	3	2	4	3	2	3	3	2	3	3	2	1	2	2	3	3	2	2
35	3	3	2	1	4	3	2	4	3	2	2	3	5	2	3	2	3	3	5	5	3	3
36	2	2	1	2	5	2	1	5	2	1	2	4	3	1	2	3	4	4	3	4	4	2
37	3	3	3	3	3	3	2	5	3	3	1	5	3	3	3	4	5	5	3	3	5	3
38	2	2	4	4	4	2	1	4	2	4	5	4	5	4	2	5	5	4	5	2	4	2
39	2	2	3	5	3	2	1	3	2	3	1	1	3	3	2	2	5	1	3	1	5	2
40	1	1	5	3	2	1	4	3	1	5	4	2	4	5	1	3	3	2	4	2	3	1
41	2	2	3	2	1	2	3	2	2	3	3	4	1	3	2	2	2	4	1	2	2	2
42	3	3	1	3	2	3	2	2	3	1	5	5	2	1	3	1	2	5	2	3	2	3
43	4	4	5	4	3	4	3	2	4	5	3	2	2	5	4	3	2	2	2	2	2	4
44	1	1	3	5	1	1	4	5	1	3	3	3	3	3	1	4	4	3	3	3	4	1
45	2	2	4	3	2	2	5	3	2	4	3	4	4	4	2	5	5	4	4	4	5	2
46	4	4	2	4	3	4	2	4	4	2	2	5	3	2	4	3	3	5	3	3	3	4
47	2	2	5	2	4	2	4	1	2	5	1	5	2	5	2	3	1	5	2	5	1	2
48	3	3	3	5	4	3	4	2	3	3	3	4	3	3	3	4	2	4	3	4	2	3
49	5	5	1	2	2	5	3	3	5	1	4	3	4	1	5	5	3	3	4	3	3	5
50	3	3	2	4	2	3	5	5	3	2	5	2	5	2	3	3	4	2	5	5	4	3

51	2	2	3	1	4	2	4	3	2	3	4	1	5	3	2	1	5	1	5	3	5	2
52	5	5	4	5	4	5	5	2	5	4	3	2	2	4	5	2	4	2	2	5	4	5
53	3	3	4	2	3	3	4	2	3	4	2	3	3	4	3	3	5	3	3	4	5	3
54	3	3	2	5	5	3	5	4	3	2	3	2	5	2	3	4	5	2	5	3	5	3
55	5	5	4	5	5	5	4	4	5	4	4	4	3	4	5	5	3	4	3	4	3	5
56	4	4	2	2	5	4	3	5	4	2	5	3	2	2	4	3	3	3	2	5	3	4
57	3	3	5	4	2	3	4	3	3	5	3	4	2	5	3	2	2	4	2	5	2	3
58	2	2	3	4	3	2	5	3	2	3	3	2	3	3	2	4	2	2	3	3	2	2
59	2	2	3	1	4	2	3	2	2	3	2	4	2	3	2	2	3	4	2	3	3	2
60	3	3	1	5	2	3	1	2	3	1	3	2	2	1	3	3	4	2	2	2	4	3
61	4	4	5	1	2	4	3	5	4	5	2	3	4	5	4	4	5	3	4	2	5	4
62	1	1	3	2	4	1	2	2	1	3	2	4	2	3	1	5	4	4	2	2	4	1
63	2	2	4	3	4	2	2	1	2	4	1	5	2	4	2	2	5	5	2	1	5	2
64	4	4	2	4	3	4	1	2	4	2	5	4	1	2	4	3	3	4	1	2	3	4

BASE DE DATOS VARIABLE 2: GESTIÓN DE RIESGOS																				
	D1: CULTURA CONSCIENTE SOBRE RIESGOS								D2: PROCESO DE GOBERNANZA DEL RIESGO					D3: IMPLANTACIÓN EFICAZ DE RIESGOS						
N°	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	3	5	3	2	4	1	3	5	1	3	2	3	2	1	3	2	3	1	2	3
2	2	3	2	1	3	4	2	3	4	2	3	2	3	3	2	2	3	4	3	2
3	5	2	1	5	2	1	1	2	1	1	2	1	5	3	1	5	2	4	5	1
4	1	2	3	1	2	1	3	2	1	3	2	3	5	2	3	1	2	1	5	3
5	1	3	2	1	5	4	2	3	4	2	5	2	1	1	2	1	3	4	1	2
6	2	2	3	2	2	1	3	2	1	3	2	3	2	3	3	2	2	1	2	3
7	2	2	1	2	1	5	1	2	5	1	2	1	2	2	1	2	2	5	2	1
8	4	5	3	4	5	5	3	5	3	3	5	3	4	2	3	4	3	2	4	3
9	4	2	2	2	2	1	2	2	1	2	2	2	2	2	2	2	4	1	2	2
10	2	1	2	1	1	2	2	1	5	2	3	2	2	1	2	2	1	2	2	2
11	1	2	1	1	2	2	1	2	2	1	2	1	1	2	1	1	2	2	1	1
12	4	2	3	4	2	1	3	2	5	3	2	3	4	2	3	4	2	5	4	3
13	1	5	1	1	5	1	1	5	1	1	5	1	4	3	1	1	5	1	4	1
14	2	1	2	2	1	3	2	1	3	2	4	2	2	3	2	2	1	3	2	2
15	4	2	2	1	3	1	2	2	1	2	2	2	1	2	2	5	2	1	1	2
16	5	1	1	1	2	4	1	1	1	1	2	1	1	2	1	1	5	1	1	1
17	5	4	4	3	3	4	4	4	3	4	3	4	2	1	4	3	4	3	2	4
18	3	4	1	4	4	3	1	4	4	1	4	1	3	2	1	4	5	3	3	1
19	2	2	5	2	5	4	5	2	5	5	3	5	4	5	5	2	3	4	4	5
20	3	5	2	4	4	5	2	5	5	2	2	2	5	3	2	3	4	1	5	2
21	1	2	4	3	3	3	4	2	5	4	1	4	4	4	4	4	5	4	4	4
22	2	3	5	4	4	2	5	3	4	5	3	5	3	3	5	5	5	2	3	5

23	4	4	4	2	2	3	4	4	3	4	3	4	2	4	4	3	3	2	2	4
24	5	5	5	1	4	5	5	5	2	5	3	5	1	3	5	2	2	4	1	5
25	3	2	5	5	2	3	5	2	3	5	4	5	2	2	5	1	3	4	2	5
26	4	1	4	1	2	1	4	1	4	4	4	4	3	3	4	2	5	3	3	4
27	5	2	5	2	4	2	5	2	3	5	5	5	3	4	5	3	2	1	3	5
28	5	4	2	3	4	3	2	4	1	2	3	2	4	4	2	3	3	3	4	2
29	4	5	3	4	3	4	3	5	2	3	4	3	3	3	3	4	4	3	3	3
30	3	2	3	2	3	4	3	2	3	3	3	3	2	2	3	5	5	4	2	3
31	5	3	2	2	4	5	2	3	4	2	2	2	1	4	2	3	4	3	1	2
32	2	4	1	3	2	2	1	4	5	1	1	1	2	4	1	2	5	3	2	1
33	4	1	3	5	2	3	3	1	4	3	2	3	3	3	3	1	1	4	3	3
34	5	2	4	5	3	4	4	2	2	4	3	4	3	3	4	1	2	2	3	4
35	1	3	2	1	4	5	2	3	3	2	2	2	5	5	2	2	3	3	5	2
36	2	2	1	2	5	3	1	2	4	1	2	1	3	4	1	3	4	4	3	1
37	3	3	2	3	3	4	2	3	4	2	1	2	3	3	2	4	5	5	3	2
38	5	2	1	4	4	2	1	2	3	1	5	1	5	2	1	5	4	4	5	1
39	2	2	1	5	3	3	1	2	5	1	1	1	3	1	1	2	5	1	3	1
40	5	1	4	3	2	3	4	1	2	4	4	4	4	2	4	3	3	2	4	4
41	1	2	3	2	1	4	3	2	2	3	3	3	1	2	3	2	2	4	1	3
42	2	3	2	3	2	2	2	3	2	2	5	2	2	3	2	1	2	5	2	2
43	3	4	3	4	3	3	3	4	3	3	3	3	2	2	3	3	2	2	2	3
44	4	1	4	5	1	4	4	1	4	4	3	4	3	3	4	4	4	3	3	4
45	3	2	5	3	2	3	5	2	5	5	3	5	4	4	5	5	5	4	4	5
46	4	4	2	4	3	1	2	4	3	2	2	2	3	3	2	3	3	5	3	2
47	5	2	4	2	4	2	4	2	2	4	1	4	2	5	4	3	1	5	2	4
48	2	3	4	5	4	4	4	3	4	4	3	4	3	4	4	4	2	4	3	4
49	2	5	3	2	2	4	3	5	5	3	4	3	4	3	3	5	3	3	4	3
50	3	3	5	4	2	2	5	3	3	5	5	5	5	5	5	3	4	2	5	5

51	4	2	4	1	4	2	4	2	5	4	4	4	5	3	4	1	5	1	5	4
52	5	5	5	5	4	5	5	5	2	5	3	5	2	5	5	2	4	2	2	5
53	1	3	4	2	3	5	4	3	4	4	2	4	3	4	4	3	5	3	3	4
54	2	3	5	5	5	1	5	3	5	5	3	5	5	3	5	4	5	2	5	5
55	3	5	4	5	5	2	4	5	5	4	4	4	3	4	4	5	3	4	3	4
56	5	4	3	2	5	3	3	4	2	3	5	3	2	5	3	3	3	3	2	3
57	4	3	4	4	2	4	4	3	1	4	3	4	2	5	4	2	2	4	2	4
58	2	2	5	4	3	2	5	2	3	5	3	5	3	3	5	4	2	2	3	5
59	1	2	3	1	4	5	3	2	1	3	2	3	2	3	3	2	3	4	2	3
60	2	3	1	5	2	3	1	3	5	1	3	1	2	2	1	3	4	2	2	1
61	3	4	3	1	2	1	3	4	3	3	2	3	4	2	3	4	5	3	4	3
62	4	1	2	2	4	2	2	1	1	2	2	2	2	2	2	5	4	4	2	2
63	3	2	2	3	4	3	2	2	5	2	1	2	2	1	2	2	5	5	2	2
64	4	4	1	4	3	4	1	4	2	1	5	1	1	2	1	3	3	4	1	1

Anexo 8: Constancia de haber aplicado el instrumento

UNIVERSIDAD CÉSAR VALLEJO

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año de la Universalización de la Salud"

Lima, 26 de mayo de 2020
Carta P. 048-2020-EPG-UCV-LN-F05L01/J-INT

Abg. MIGUEL ANGEL ROA QUINTANA
GERENTE
GERENCIA DE REGISTRO ELECTORAL
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL - RENIEC

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a LEON ALVARADO, LUIS ENRIQUE; identificado con DNI N° 09742840 y con código de matrícula N° 7002313009; estudiante del programa de MAESTRÍA EN GESTIÓN PÚBLICA quien, en el marco de su tesis conducente a la obtención de su grado de MAESTRO, se encuentra desarrollando el trabajo de investigación titulado:

"Seguridad de la información y Gestión de riesgo del proceso servicio electoral, Reniec .2020"

Con fines de investigación académica, solicito a su digna persona otorgar el permiso a nuestro estudiante, a fin de que pueda obtener información, en la institución que usted representa, que le permita desarrollar su trabajo de investigación. Nuestro estudiante investigador LEON ALVARADO, LUIS ENRIQUE asume el compromiso de alcanzar a su despacho los resultados de este estudio, luego de haber finalizado el mismo con la asesoría de nuestros docentes.

Agradeciendo la gentileza de su atención al presente, hago propicia la oportunidad para expresarle los sentimientos de mi mayor consideración.

Atentamente,

ESCUELA DE POSGRADO UCV JEFATURA CAMPUS LIMA NORTE

Dr. Carlos Venturo Orbegoso
Jefe
ESCUELA DE POSGRADO
UCV FILIAL LIMA
CAMPUS LIMA NORTE

MIGUEL ÁNGEL ROA QUINTANA
Gerente de Registro Electoral
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ROA QUINTANA Miguel Angel FAU 20295613620 soft
Motivo: Soy el autor del documento
Fecha: 27/05/2020 17:12:11-0500

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
"AÑO DE LA UNIVERSALIZACION DE LA SALUD"

Jesus Maria, 27 de Mayo del 2020

CARTA N° 000025-2020/GRE/RENIEC

Doctor
CARLOS VENTURO ORBEGOSO
Jefe de la Escuela de PosGrado Filial Norte
Universidad César Vallejo. Campus Lima Norte

Asunto: **Autorización para aplicación de encuestas**

Referencia : **Carta P. 048-2020-EPG-UCV-LN-F05L01/J-INT**

De nuestra consideración:

Sirva la presente para hacerle llegar nuestro más afectuoso saludo y aprovechamos la oportunidad para comunicarlo que nos es muy grato brindar la autorización al Sr. LUIS ENRIQUE ALVARADO LEON a efectos que pueda obtener información en nuestra Gerencia y que le permita desarrollar el trabajo de investigación para obtener el grado académico de Maestro en Gestión Pública en la institución que usted representa.

Sin otro en particular y agradeciéndole su gentil atención, queda de Ud.

Atentamente,

Anexo 09: Dictamen de la sustentación de Tesis

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Dictamen Final

Vista la Tesis:

"SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE RIESGOS DEL PROCESO SERVICIO ELECTORAL, RENIEC, LIMA, 2020"

Y encontrándose levantadas las observaciones prescritas en el Dictamen, del graduando(a):

LEON ALVARADO LUIS ENRIQUE

Considerando:

Que se encuentra conforme a lo dispuesto por el artículo 36 del REGLAMENTO DE INVESTIGACIÓN DE POSGRADO 2013 con RD N. ° 3902-2013/EPG-UCV, se DECLARA:

Que la presente Tesis se encuentra autorizada con las condiciones mínimas para ser sustentada, previa Resolución que le ordene la Unidad de Posgrado; asimismo, durante la sustentación el Jurado Calificador evaluará la defensa de la tesis y como documento respectivamente, indicando las observaciones a ser subsanadas en un tiempo máximo de seis meses a partir de la sustentación de la tesis.

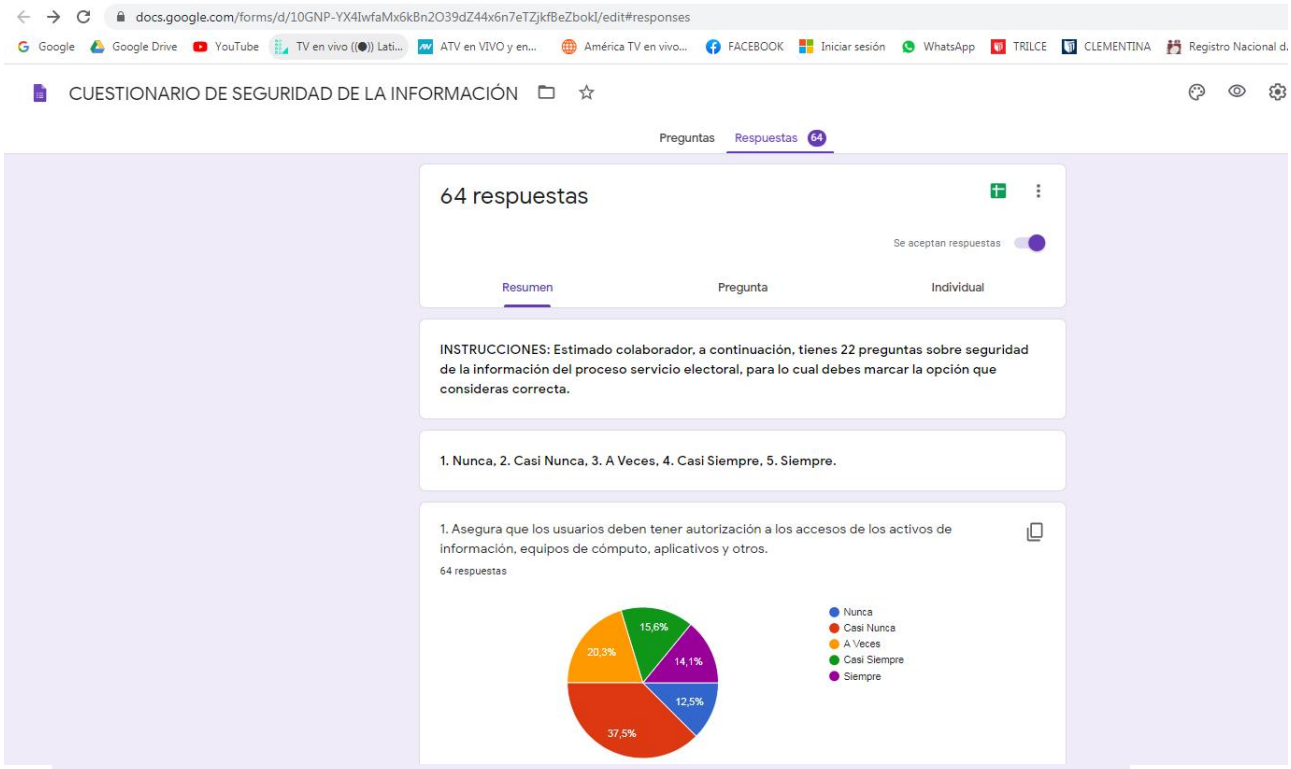
Comuníquese y archívese.

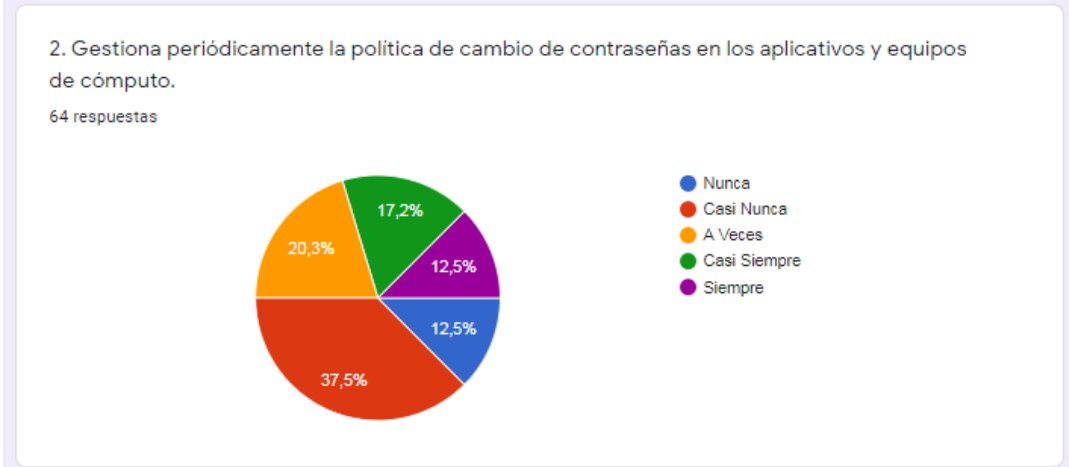
Lima, 01 de agosto del 2020

Francis Ibarguen Cueva
Dra. en Ciencias de la Educación
Dra. Francis Esmeralda Ibarguen Cueva
Asesora de la tesis

Dr. Alejandro Sabino Menacho Rivera
Revisor de la tesis

Anexo 10: Evidencias





CUESTIONARIO DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE RIESGOS

*Obligatorio

INSTRUCCIONES: Estimado colaborador, a continuación, tienes 22 preguntas sobre seguridad de la información del proceso servicio electoral, para lo cual debes marcar la opción que consideras correcta.

1. Nunca, 2. Casi Nunca, 3. A Veces, 4. Casi Siempre, 5. Siempre.

CUESTIONARIO DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE RIESGOS

*Obligatorio

INSTRUCCIONES: Estimado Colaborador, a continuación, tienes 20 preguntas sobre Gestión de riesgos del proceso servicio electoral, para lo cual debes marcar la opción que consideras correcta.

1. Nunca, 2. Casi Nunca, 3. A Veces, 4. Casi Siempre, 5. Siempre.