ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Sistema de gestión de seguridad de la Información en el Proceso de Registros Civiles de RENIEC. San Borja. Lima 2016

TESIS PARA OPTAR EL GRADO ACADEMICO DE:

Maestra en Gestión Pública

AUTOR:

Br. Natividad Gladys Bernaldo Bastidas

ASESORA:

Dra. Ana Maritza Boy Barreto

SECCIÓN:

Ciencias Empresariales

LÍNEA DE INVESTIGACIÓN:

Dirección

PERÚ – 2018

_____

Dr. Chantal Jara Aguirre

Presidente

_____

Dra. Jesselle Roxana Rodas Garcia

Secretario

_____

Dra. Ana Maritza Boy Barreto

Vocal

Dedicatoria

El presente trabajo está dedicado a mis padres y hermanos por su apoyo incondicional y por ser los pilares fundamentales que me impulsan a seguir adelante, para ser cada día mejor persona y mejor profesional.

Agradecimientos

A Dios, quien guía mis pasos. A la Universidad César Vallejo por haberme brindado la oportunidad en mi desarrollo profesional. A la PdD. Ana Boy del curso por las horas y conocimientos dedicados a la culminación de esta investigación. A mis amigos y compañeros de trabajo que participaron del presente.

Declaración de Autenticidad

Yo Natividad Gladys Bernaldo Bastidas, estudiante del Programa de Gestión Pública de la Escuela de Postgrado de la Universidad Cesar Vallejo, identificado con DNI 40097502 con la Tesis Titulada “Sistema de Gestión de Seguridad de la Información en el Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016”, declaro bajo juramento que:

1) La Tesis es de mi autoría.
2) 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.
3) La tesis no ha sido auto plagiado, es decir no ha sido publicada, ni presentada anteriormente para obtener algún grado académico previo o título profesional.
4) Los datos presentados son reales, no han sido falseados, ni duplicados, ni copiados y por tanto los resultados que se presentan en la tesis se constituirán en aportes a la realidad 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), representar falsamente las ideas de otros), asumo las consecuencias y sanciones que de mis acciones derivan, sometiéndome con la normatividad de la Universidad César Vallejos.

Lima, 10 de mayo del 2017

_____

Br. Natividad Gladys Bernaldo Bastidas

DNI 40097502

Presentación

Señores miembros del jurado, presento ante ustedes la Tesis titulada “Sistema de Gestión de Seguridad de la Información en el Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016”, con la finalidad de determinar la relación entre el sistema de gestión de seguridad de la información y el proceso de registros civiles en el Reniec. San Borja. Lima. 2016, en cumplimiento del Reglamento de Grados y Títulos de la Universidad César Vallejo para obtener el Grado Académico de Maestro en Gestión Pública.

Esperando cumplir con los requisitos de aprobación.

La autora.

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

La presente investigación tuvo como objetivo general determinar la relación significativa que existe entre el Sistema de Gestión de Seguridad de la Información y el Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016.

La población o universo de interés en esta investigación, estuvo conformada por 220 trabajadores administrativos del Reniec. San Borja. Lima. 2016, se consideró como muestra A 175 colaboradores en las cuales se han estudiado las variables: sistema de gestión de seguridad de la información y el proceso de registros civiles. Esta investigación utilizó para su propósito el diseño no experimental de nivel correlacional de corte transaccional, que recogió la información en un período específico, que se desarrolló al aplicar la encuesta sobre el Sistema de Gestión de Seguridad de la Información y la encuesta sobre Procesos de Registros Civiles y, todos con escala de Likert, que brindaron información acerca de la relación que existente entre del sistema de gestión de seguridad de la información y la encuesta de procesos de Registros civiles, en sus distintas dimensiones.

El resultado del coeficiente de correlación Rho Spearman de 0.781 indica que existe correlación positiva alta entre las variables, además se encuentra en el nivel de correlación moderada y siendo el nivel de significancia bilateral $p=0.000<0.01$ (altamente significativo), se rechaza la hipótesis nula y se acepta la hipótesis general; se concluye que: La mejora de implantar un Sistema de Gestión de Seguridad de la Información, permitirá mitigar los riesgos de los activos de la información en el proceso de Registros Civiles del Reniec. San Borja. Lima. 2016.

***Palabras Clave**:* Sistema de Gestión de Seguridad de la Información, Proceso de Registros Civiles.

Abstract

The present investigation had as general objective to determine how the implementation of an Information Security Management System will improve the Civil Registry Process of Reniec. San Borja. Lime. 2016.

The population or universe of interest in this research was made up of 220 administrative employees of Reniec. San Borja. Lime. 2016, 175 employees were considered as sample A in which the variables: information security management system and the civil registration process were studied. This research used for its purpose the non-experimental design of correlational level of transactional cut, that collected the information in a specific period, that was developed when applying the survey on the System of Management of Information Security and the Survey on Records Processes Civil and all with a Likert scale, who provided information about the relationship between the information security management system and the civil registry process survey, in its different dimensions.

The result of the Rho Spearman correlation coefficient of 0.781 indicates that there is a high positive correlation between the variables, it is also found in the moderate correlation level and the bilateral significance level $p = 0.000 < 0.01$ (highly significant), the hypothesis is rejected Null and the general hypothesis is accepted; It is concluded that: The improvement of implementing an Information Security Management System will allow mitigating the risks of the information assets in the Reniec Civil Registry process. San Borja. Lime. 2016.

Key Words: Information Security Management System, Civil Registry Process.

I. Introducción

1.1. Antecedentes

1.1.1. Antecedentes Internacionales

Lanche (2015). Tesis Maestría*: Diseño de un Sistema Seguridad de la Información para la Compañía Acontenic Cia. Ltda. Basado en la Norma NTE INEN ISO 27002*. Objetivo: establecer los lineamientos a seguir para implementar las recomendaciones de la norma de seguridad de la información NTE INEN ISO/IEC 27002 en pequeñas empresas mediante el análisis de un caso real. Propone analizar el estado de una empresa local dedicada a brindar servicios profesionales en el área de la consultoría técnica, y, con estos resultados, establecer un esquema que se pueda seguir para implementar, mejorar y mantener un sistema de gestión de seguridad de la información óptimo, acorde con los requerimientos e inversión de la compañía *Acontenic*.

La investigación se centra en el análisis de las políticas y prácticas actuales que son manejadas por la compañía *Acontenic* Cía. Ltda., en lo referente a la seguridad de la información, para el desarrollo de sus actividades diarias; considerando los factores de riesgo y las vulnerabilidades de la compañía.

El autor concluye que: durante el desarrollo del presente proyecto se ha identificado varios controles, recomendados por la norma ISO/IEC 27002, que se pueden asociar a procedimientos de carácter administrativo y procedimientos de carácter técnico con mínimos costo económico, más bien se trata de decisiones respaldadas por la Alta Gerencia que modifiquen algunos procesos y procedimientos internos.

Guamán (2015). Tesis de Maestría: *Diseño de un Sistema de Gestión de Seguridad de la Información para Instituciones Militares*. Objetivo diseñar un Sistema de Gestión de Seguridad de la Información que incorpore estándares internacionales ajustados al campo militar y nuevas tecnologías de la información y comunicaciones con el fin de contribuir a la modernización de las instituciones militares.

La técnica utilizada para obtener la información fue la encuesta, la misma que permitió la recolección de información en forma directa a fin de diagnosticar como se encuentra la seguridad de la información en la Dirección de Tecnología de la

Información y Comunicaciones y el Centro de Tecnología de la Información y Comunicaciones, con un total de sesenta y nueve (69) ítems con opciones de respuestas en un formato de escala tipo Likert. El índice de confiabilidad debe ser menor o igual a 1 para que el valor indicativo del instrumento posea un alto grado de consistencia interna, lo que indica la exactitud y objetividad en los resultados. Se aplicó el método de Alpha de Cronbach obteniéndose una confiabilidad de 0.96. De una población o universo de cincuenta y un (51) empleados.

El investigador concluye que para poder dirigir y dar soporte a la gestión de seguridad de la información de acuerdo con los requisitos de las instituciones militares, se deben realizar dos documentos para considerar la seguridad de la información que representará el nivel político o estratégico de las instituciones militares; y el segundo documento es el Plan de Seguridad, como nivel de planeamiento táctico, el cual definirá el “Cómo”.

Rebollo (2014). Tesis Doctoral. *Marco para Seguridad de la Información en servicios Cloud Computing*. Objetivo definir un proceso que sistematice el gobierno de seguridad de los servicios Cloud Computing, se ha empleado el método de investigación cualitativo denominado como investigación-acción (orientación a la acción y al cambio, consideración de un problema, modelo de proceso “orgánico” que incluye etapas sistemáticas y, en ocasiones interactivas, colaboración entre los participantes) y el método de revisión sistemática de la literatura.

En conclusión, el autor manifiesta que teniendo en cuenta que se ha conseguido satisfacer objetivos parciales propuestos, se puede afirmar que el objetivo principal, especificado en líneas precedentes, también ha conseguido ser cumplido. Como resultado, también se puede afirmar que la hipótesis doctoral definida como: *Es posible gestionar la seguridad de los servicios Cloud Computing a nivel de gobierno corporativo*, es afirmativa, y como se ha demostrado.

Aguirre, Palacios (2014). Tesis Maestría. *Evaluación Técnica de seguridad del data center del Municipio de Quito según, las normas ISO/IEC 27001:2005 SGSIE ISO/IEC 27002:2005*. Objetivo aplicar una evaluación técnica informática al Data Center del MDMQ, utilizando matrices de impacto y probabilidad además de validar el grado de cumplimiento de la Norma ISO/IEC 27001:2005, para que en base a los hallazgos encontrados se presente en un informe a las autoridades y estas puedan

tomar medidas preventivas y correctivas, metodología basada en riesgos, utilizando métodos de investigación de fuentes primarias como son encuestas, entrevistas, y observación.

Conclusión, el personal del municipio metropolitano de Quito a pesar que cuenta con políticas de gestión tecnológicas no tiene una conciencia sobre la seguridad de la información. Por tal motivo se puede producirse fugas de información crítica y confidencial; el data center no posee una evaluación continua; conciencia sobre la seguridad de la información.

Sanabria (2013) en su Tesis de Maestría. *Propuesta para la mejora de los sistemas de seguridad y telecomunicaciones de una organización de transporte marítimo*. Objetivo analizar alternativas de mejoras en los sistemas de seguridad y telecomunicaciones de una organización de transporte marítimo, tipo de investigación aplicada, el diseño es de tipo documental. Conclusión de investigador: Al estudiar la situación actual de los sistemas de seguridad y sistemas de telecomunicaciones, se detectan las fallas y vulnerabilidades (problemas con las líneas telefónicas, lo lenta que es la conexión a Internet y sus constantes interrupciones, la falta de seguridad y resguardo de la información), las cuales son las que se desean corregir con el presente trabajo. En cuanto a los sistemas de seguridad, se realizó un estudio detallado de los riesgos a los que se encuentra expuesta la información, junto con los servicios y equipos. La información física está mal organizada y guardada, estando a disponibilidad de cualquier persona ajena a la empresa. No existen normas para el uso de Internet, permitiendo navegar en cualquier página web y descargar programas o archivos que resultan potencialmente peligrosos para la información, dejando en riesgo la información que se encuentra en las estaciones de trabajo.

1.1.2. Antecedentes Nacionales

Seclén (2016). *Tesis en Maestría. Factores que afectan la implementación del sistema de sistema de gestión de seguridad de la información en las entidades públicas de acuerdo a la NTP-ISO/IEC 27001*. Objetivo analizar las principales limitaciones y problemas que vienen enfrentando las entidades del sector público en la implementación del SGSI, así como también investigar las estrategias y metodologías que vienen aplicando las entidades públicas que ya han completado

su ejecución, los beneficios obtenidos de haberlo realizado en sus instituciones y la importancia de fomentar la capacitación y especialización en seguridad de la información que permitan un desarrollo integral de esta implementación en las entidades del Estado, el diseño de la investigación es cualitativa, básica, descriptiva, de tipo no experimental y transversal.

La población objetivo para este proyecto de investigación abarca a los Organismos Públicos Descentralizados que conforman el Sistema Nacional de Informática adscritos a la Presidencia del Consejo de Ministros (PCM) del Gobierno Central, unidad de análisis: entidades públicas en el marco de la NTP ISO /IEC 27001:2014, muestra:07 entidades públicas del Sistema Nacional de Informática.

Conclusión, establecer estrategias, respecto de la implementación del SGSI en la Administración Pública Peruana basadas en la NTPISO/ IEC 27001, que estén más orientadas a dotar de una estructura organizacional de gestión de la información que permita el alineamiento de TI con la estrategia de negocios de las organizaciones, el logro de beneficios, la reducción de costos, el control de riesgos y en general la mejora de las operaciones de TI en las organizaciones.

Guzmán (2015).Tesis Maestría. *Diseño de un Sistema de Gestión de Seguridad de la Información para la entidad financiera de segundo piso*. Objetivo diseñar un Sistema de Gestión de Seguridad de la Información para la empresa IGM S.A., tomando como referencia la norma NTC-ISO-IEC 27001:2013, método de investigación de tipo factible, el método de investigación es de campo.

Conclusión, debido a la complejidad de la infraestructura tecnología y a la capacidad del área de tecnología, la entidad se encuentra clasificada en un nivel MEDIO de estratificación, que implica un esfuerzo considerable para la implementación del Sistema de Gestión de Seguridad de la Información, lo cual, se ve reflejado en los diferentes planes de acción que se generaron a lo largo del proyecto que están orientado a dar cumplimiento a los requerimientos de la norma ISO/IEC 27001:2013.

Condori (2012). Tesis Maestría. *Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de la Seguridad en Sistemas de Información para determinar su influencia en la intención del usuario*. Objetivo determinar, mediante un modelo estructural, el grado de influencia que ejercen los Factores Críticos de

Éxito en la intención del usuario para la Implementación de Seguridad de Sistemas de Información en la Universidad Nacional del Altiplano Puno durante el año 2011, técnica utilizada la encuesta, a través de un cuestionario, que ha sido desarrollado a partir de las variables e indicadores de acuerdo a la investigación teórica y propuesta del investigador.

La población del personal administrativo en las diferentes dependencias hace un total de 681, Con un nivel de confianza del 95%, una variabilidad positiva de 0,05 y un porcentaje de error del 5%, se ha tomado una muestra de 84 personas. Conclusiones: Se desarrolló el Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de Seguridad de Sistemas de Información para determinar su influencia en la intención del usuario, con nueve factores y tres dimensiones, adecuadamente sustentadas, tomando como base la teoría del comportamiento planificado (TPB) Se diseñó una guía de implementación del modelo propuesto, que considera 17 pasos para una adecuada implementación del modelo, siendo flexible en la selección de factores y soportado con un cuestionario adaptable dependiendo del contexto organizacional que se quiera estudiar.

Calderón (2012). Tesis Maestría. *Análisis e implementación de un sistema de gestión de riesgos para la prevención de accidentes en la mina broncal S.A.A. Unidad Colquijirca - Pasco*. Objetivo analizar y medir del estado actual, (Fotografía Cero) del cumplimiento y efectividad de la gestión Seguridad y Salud Ocupacional, en cumplimiento de la normativa nacional D.S. N° 055-2010-EM; D.S. N° 009-2005-TR, D.S. N° 016-2009-EM y la R.M. N° 148-2007-TR Constitución Comité Paritario, método de investigación inductivo, deductivo, análisis, síntesis y estadístico, tipo de investigación es aplicada, se utilizó un diseño de investigación cuasi experimental. Población: en vista que mina Colquijirca está en evaluación, se está considerando para este estudio todas las áreas: mina, geología-ingeniería, relaciones comunitarias, medio ambiente, mantenimiento-logística.

Conclusión, que el ISO 31000 es una herramienta que permite la mejora en la gestión de riesgos en la seguridad en el trabajo de las organizaciones y se recomienda que las empresas trabajan e incorporen del ISO 9000, ISO 14001, OSHAS 18001 y se integren al ISO 31000. Para una mejora continua de su organización.

Dextre, Huamán, Sánchez (2012). *Tesis de Maestría. Propuesta de marco de gobierno de seguridad de la información para el mercado de valores de Lima*. La tesis ha sido elaborada considerando los lineamientos de la metodología de Samsung para proyectos innovadores y se basa principalmente en la norma ISO/IEC

DIS 27014-Gobierno de Seguridad de la Información.

Conclusión, el gobierno de seguridad de la información, a pesar de ser un componente fundamental para lograr la confianza de los inversionistas y la competitividad del Mercado de Valores del Perú, actualmente es “inefectivo”. Por ello se recomienda que la Superintendencia del Mercado de Valores fortalezca la cultura de gobierno, ejecute la propuesta compuesta de 5 proyectos de implementación gradual y promueva que los participantes del Mercado de Valores del Perú, especialmente los agentes de intermediación inicien la implementación de su sistema de gestión de seguridad de la información.

1.2. Fundamentación científica, técnica o humanística

1.2.1. Fundamentación teórica de la variable Sistema de Gestión de la Información

Definición de Sistema de Gestión de Seguridad de la Información

“Es una estructura organizativa, técnica y procedimental que busca conseguir la seguridad de la información a través de: análisis de la situación planificada, aplicación de controles, revisión para su funcionamiento, aplicación de menores y correcciones”. (Miguel, 2016, p. 243).

Es la construcción de un conjunto de procesos sistemáticos, documentados que permita la mantener la seguridad de la información, así como establecer medidas preventivas durante el funcionamiento de una organización.

Joyanes (2015), desde una visión más integral señala que:

> El sistema de gestión de seguridad de la información (ISMS, Information Security Management System) es la parte del sistema

> general de gestión en una organización que consta de: la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información en una organización. (p. 507).

Una organización tiene como principal activo la información que maneja, la cual debe encontrarse protegida a efectos de evitar vulnerabilidades respecto a su confidencialidad, disponibilidad e integración, considerando que ello impactaría en todas las áreas que tiene a su cargo. Si bien las organizaciones cuentan con métodos de alertas para la custodia de su información, es importante complementar a ello un sistema de que involucre diversos controles que pueda medir los riesgos al que puede estar expuesto la organización.

Merino y Cañizares (2011):

> Los Sistemas de Gestión de Seguridad de la Información desarrollados según la Norma ISO 27001, igual que otros muchos sistemas de gestión, se basan en el concepto de mejora continua.
>
> Sobre la base de un sistema de gestión de seguridad de la información se construye la ISO 27001, que tiene en su alcance diversos requisitos que permite a una organización establecer una estructura importante para gestionar la información que se maneja, utilizando un ciclo de mejora para crear, implementar, supervisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.

Seguridad de la Información

Joyanes (2015) señala que:

> La Seguridad de la información consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y disponibilidad de los activos de los sistemas informáticos (de información) incluyendo hardware, software, firmware y aquella información que se procesan, almacenan y comunican. (p. 488).

> La seguridad de la información es un conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información.

Según Miguel (2016) afirma que “La seguridad de la información es la protección de la integridad, disponibilidad y confidencialidad de la información, según el nivel requerido para los objetivos de negocio de la empresa”. (p. 13).

Uno de los parámetros fundamentales a medir y analizar en la seguridad de la información son los incidentes, es decir, los sucesos no deseados que se detectan en la red o en los servicios y que pueden poner en peligro la disponibilidad, la confidencialidad o la integridad de la información. Cada evento debe ser registrado y calificado para así poder determinar cómo reaccionar ante cada incidente.

La Ongei (2014) señala que “La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones que permiten resguardar y proteger la información buscando mantener las dimensiones (confidencialidad, disponibilidad e integridad) de la misma”. (p. 9).

La Seguridad de la Información abarca todo tipo de información: impresa o escrita a mano, grabada con asistencia técnica, transmitida por correo electrónico o electrónicamente, incluida en un sitio web, mostrada en videos corporativos, mencionada durante las conversaciones, etc.

(Merino y Cañizares, 2012) señala que:

> La seguridad de información debe formar parte de todos los procesos de negocio, tanto si los procesos son manuales como automatizados, ya que en todos ellos interviene la información de la organización como parte fundamental, teniendo en cuenta que dicho procesos involucran a personas, a tecnologías y a relaciones con socios de negocios, clientes o terceros. (p. 11).

Los contextos actuales del mercado dan lugar a economías, gobiernos y organizaciones cada vez más interconectadas que requieren compartir información, que evolucionan constantemente, que deben responder a las necesidades de sus grupos de interés y que deben generar un componente diferenciador ante la competencias, decir que hoy en día la preocupación de un negocio no es solo el de ser productivos y el de generar nuevos productos o servicios sino también el de protegerse ante cualquier tipo de ataque informático y que adicionalmente, a pesar de estos ataques, la continuidad del negocio en los procesos relacionados a sus servicios de misión crítica sigan operativos en los niveles acordado

(Gómez y Suarez, 2012) señala también sobre la importancia sobre la seguridad de la información:

> Muchas de las actividades que se realizan de forma cotidiana en los países desarrollados dependen en mayor o menor medida de sistemas y de redes informáticas. El espectacular crecimiento del internet y de los servicio telemáticos comercio electrónico, servicios multimedia de banda ancha, administración electrónica, herramientas de comunicación como el correo electrónico o la video conferencia…) ha contribuido a popularizar aún más, si cabe, el uso de la informática y de las redes de ordenadores, hasta el punto que en la actualidad no se circunscriben en el ámbito laboral y profesional, sino que incluso se han convertido en un elemento cotidiano en muchos hogares, con un creciente impacto en las propias actividades de comunicación y de ocio de los ciudadanos (p.257).

Principios de la Seguridad de la Información

“La confidencialidad, integridad y disponibilidad (conocida como la triada en inglés: “Confidentiality, Integrity y Availability”, son los principios básicos de la seguridad de la información” (Lemus, 2014, p.56).

Confidencialidad

Joyanes (2015), afirma que:

> La confidencialidad, es la propiedad de prevenir la divulgación no autorizada de la información. Es decir, es la accesibilidad sólo para los usuarios autorizados y se opone a la divulgación no autorizada. Hace referencia a la necesidad de ocultar o mantener un secreto sobre determinada información o recursos. (p. 489).

La confidencialidad, considerada como un principio de seguridad de la información, que tiene como parámetros evitar que usuarios que no están autorizados a cierta información pueda acceder a ella.

La confidencialidad es la "cualidad de un mensaje, comunicación o datos, para que solo se entiendan de manera comprensible o sean leídos, por la persona o sistema que esté autorizado, comprende por tanto la privacidad o protección de dicho mensaje y datos que contiene" (Costas, 2014, p. 17).

La confidencialidad, es una característica que garantiza el acceso de información, evitando a usuarios no identificados.

"La confidencialidad en todas las etapas del procesamiento de la información está protegida contra accesos no autorizados que pueden derivar en la alteración o robo de información confidencial" (Baca, 2015, p. 176).

"La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización" (Ongei, 2014, p.11).

Esta característica de la información tiene como propiedad evitar la divulgación de información a individuos no acreditados.

“La confidencialidad es la garantía de que la información no es conocida por personas, organizaciones o procesos que no disponen de la autorización necesaria” (Merino y Cañizares, 2011, p.12).

Integridad

“La Integridad, es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados” (Ongei, 2014, p.12).

Esta propiedad, consiste en mantener intacta, sin modificación alguna a la información que se maneja en cualquier nivel.

“La Integridad, cualidad de mensaje, comunicación o datos, que permite comprobar que no se ha producido manipulación alguna en el original, es decir que no ha sido alterado” (Costas, 2014, p. 17).

La información que se manipula tiene que mantener siempre su precisión y completitud de todos sus datos.

Miguel (2016), señala que:

> La Integridad, es la propiedad de salvaguardar la exactitud y completitud de los datos almacenados. Consta de dos facetas: Integridad de la información (asegurar que la información no haya sido alerta de manera no autorizada durante el almacenamiento, tratamiento o tránsito) y la Integridad de los sistemas (asegurar la calidad de un sistema para cumplir una función definida de manera equivocada, libre de cualquier manipulación). Es, decir que los datos almacenados reflejen la realidad y no hayan sido manipulados. (p. 13).

Esta cualidad se obtiene cuando se impide eficazmente la inserción, modificación o destrucción no autorizada, sea accidental o intencional del contenido de los datos.

Joyanes (2015) manifiesta que:

> El objetivo de la integridad ese prevenir modificaciones no autorizadas de la información. En esencia, la integridad hacer referencia a la fidelidad de la información o recursos que han de ser auténticos, exactos y completos. La integridad hace referencia a la integridad de los datos (volumen de la información) y la integridad del origen (fuente de datos) o autenticación (por ejemplo, un periódico puede difundir una información cuya información no es correcta. No ha mantenido la integridad del origen ya que la fuente utilizada no es correcta). Las modificaciones no se hacen a los datos por personas o por procesos autorizados. Los datos son interna y externamente consistentes. (p.200).

Esta cualidad de la información, ayuda a evitar la manipulación intencionada de la información que se maneja en cualquier nivel de cualquier organización, sistemas informáticos u otros.

“La Integridad: que la información que se recibe es precisa y está completa (su contenido es el necesario) para los fines que se persiguen con su procesamiento, así como su validez, de acuerdo con los valores y expectativas del negocio” (Baca, 2015, p. 176).

Es la búsqueda de mantener los datos libres sin modificaciones no autorizadas. La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información. Está característica de la información hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad.

Disponibilidad

Miguel (2016), señala que:

> La disponibilidad, es la propiedad de ser accesible y utilizable por una entidad autorizada. Debemos asegurar que los sistemas funcionen puntualmente y que los servicios no sean denegados a los usuarios autorizados, es decir, que se tenga acceso en todo momento a la información. (p. 237).

La disponibilidad debe garantizar el acceso a todos los datos e información, siendo los tiempos de respuesta de forma inmediata, para ello debe verificarse diversos factores de la información de acuerdo al repositorio donde se encuentren almacenadas.

“La información del sistema debe permanecer accesible a todos los elementos autorizados. La disponibilidad garantiza que los sistemas están funcionando adecuadamente cuando se necesitan. Un ataque de denegación del servicio es un ejemplo de una amenaza contra la disponibilidad” (Joyanes, 2015, p. 490).

Se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran. Supone que la información pueda ser recuperada en el momento en que se necesite, evitando su pérdida o bloqueo.

“Disponibilidad: Es la garantía de que la información es accesible en el momento en el que los usuarios autorizados (personas, organizaciones o procesos, tienen la necesidad de acceder a ella” (Merino y Cañizares, 2011, p. 12)

Costas (2014), señala que:

> La disponibilidad, es la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran. Supone que la información

> pueda ser recuperada en el momento que se necesite, evitando su pérdida o bloqueo. (p. 17).

Por otro lado, Joyanes (2015) afirma que dentro de los principios complementarios de seguridad de la información se encuentran la autenticación y el no repudio:

> *La autenticación*, es la verificación de la identidad del usuario. La autenticación establece la identidad de un usuario consta del nombre del usuario y asegura que los usuarios son quienes realmente dicen ser. La identidad de un usuario consta del nombre de usuario y una contraseña, de modo que para entrar a un sitio ha de presentar una identidad (ID del nombre de usuario) y a continuación una contraseña. El sistema de computación autentica al usuario verificando que la contraseña corresponde a la persona que presenta el ID. Existen numerosos métodos de autenticación: contraseña, tarjeta magnética, huellas dactilares y biometría. (p. 490).

Es la propiedad que permite identificar el generador de la información algunos métodos de autenticación son: Biomédicas, por huellas dactilares, retina del ojo, etc. Tarjetas inteligentes que guardan información de los certificados., con el objetivo de asegurar que una comunicación sea auténtica, es decir, verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos también sean correctos.

“El servicio de no repudio es impedir que un usuario pueda negar haber recibido un documento electrónico. Estos servicios pretenden cubrir las funcionabilidades de una firma manuscrita de modo mucho más seguro” (Joyanes, 2015, p. 491).

Costas (2014), también señala que:

> El no repudio está estrechamente relacionado con la autenticación y permite probar la participación de las partes en una comunicación. Existen dos posibilidades: No repudio en origen (el emisor no puede negar el envío. La prueba la crea el propio emisor y la recibe el

> destinatario) y No repudio en destino (el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor). Si la autenticidad prueba quién es el autor o el propietario de un documento y cuál es su destinatario, el no repudio prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino) (p. 178).

El no repudio, es utilizado más en los temas de seguridad informática en la cual permite verificar la comunicación de mensajes comprobando si los actores que han participado son los dueños de la información.

"Al grupo de estas características y objetivos de la seguridad se les conoce como CIDAN nombre sacado de la inicial de cada característica. La relación de los mismos se presenta en la siguiente figura" (Costas, 2014, p. 179):

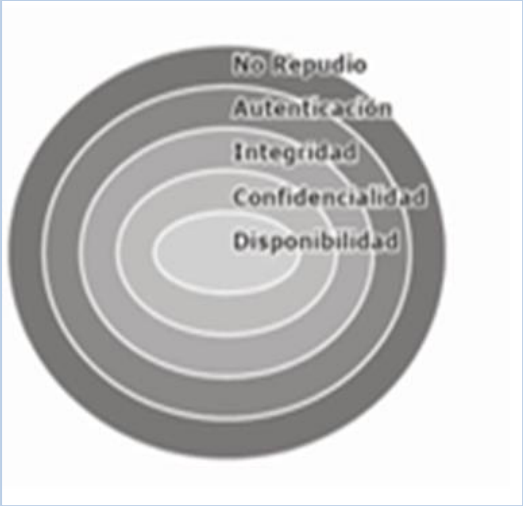


Figura 1. CIDAN. Se ilustra cómo se relacionan los diferentes servicios de seguridad, unos dependen de otros jerárquicamente, así si no existe el de nivel interior, no puede aplicarse el exterior. De esta manera, la disponibilidad se convierte en el primer requisito de seguridad, cuando existe ésta, se puede disponer de confidencialidad, que es imprescindible para conseguir integridad, imprescindible para poder obtener autenticación y por último el no repudio que solo se obtiene si se produce previamente la autenticación. (Costas, 2014)

Gestión de Seguridad

La gestión de seguridad se define como:

> La protección de la información de una amplia gama de amenazas con el objetivo de asegurar la continuidad del negocio (ISO/IEC, 2005). La gestión de la seguridad de la información se ha convertido en una disciplina corporativa crítica al igual que el marketing, la gestión financiera, la administración o la gestión de los recursos humanos (Joyanes, 2015, p.526).

Es una doctrina que las organizaciones vienen adoptando, mediante una planificación que incluya una metodología de rápida aplicación con estándares de seguridad que permitan mejorar su situación frente a la seguridad de la información.

Gómez y Suárez (2012) señale que:

> Para gestionar la seguridad de la información es preciso contemplar toda una serie de tareas y de procedimientos que permitan garantizar los niveles de seguridad exigibles en una organización, teniendo en cuenta que los riesgos no se pueden eliminar totalmente, pero si se puede gestionar. En ese sentido conviene destacar que la práctica resulta imposible alcanzar la seguridad al 100% y, por este motivo algunos expertos prefieren hablar de la fiabilidad del sistema informático, entendiendo como tal la probabilidad de que el sistema se comporte tal como se espera de él. (p. 261).

La gestión de la seguridad de la información es un proceso continuo que consiste en garantizar que los riesgos de la seguridad de la información sean identificados, valorados, gestionados y tratados por todos los miembros de la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. La gestión de la seguridad de la información requiere la participación activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar

la seguridad de la información, así como el debido control de acceso a los recursos y activos de información.

La gestión de la seguridad de la información, implica que las organizaciones clasifican sus activos de información en términos de su valor, requerimientos legales, sensibilidad y criticidad, con el propósito de identificar los riesgos que pueden afectar su seguridad y determinar las medidas de prevención, detección, retardo y reacción que se requieran implementar para controlar el acceder no autorizado a las instalaciones, recursos, sistemas e información de la organización, o cualquier amenaza proveniente del entorno, la naturaleza y las acciones del hombre que pueda llegar a comprometer el normal funcionamiento y operación del negocio.

Ongei (2014), señala que:

> Un sistema de gestión es una estructura probada para la gestión y mejora continua de las políticas, los procedimientos y procesos de la organización. Ayuda a lograr los objetivos de la organización mediante una serie de estrategias, que incluyen la optimización de procesos, el enfoque centrado en la gestión y el pensamiento disciplinado. (p. 28).

(Merino y Cañizares, 2011), afirma que:

> Un sistema de gestión, es el marco de funcionamiento de una organización en el que se integra tanto la misión, visión, valores objetivos principales y secundarios de la organización, como las políticas, procedimientos registros e indicadores, que dan forma al sistema. Disponer del marco del trabajo que proporciona un sistema de gestión permite la eficiencia y eficacia de la organización. Para el desarrollo de un sistema de gestión de una organización, es necesario realizar las siguientes actividades y tareas: determinar las necesidades y expectativas de todas las partes interesadas, establecer la política y objetivos de la organización, determinar los procesos y las responsabilidades necesarias para el logro de los objetivos, determinar y proporcionar los recursos necesarios para el logro de los objetivos, establecer los métodos para medir la eficacia y

> eficiencia de cada proceso, determinar los medios para prevenir no conformidades y eliminar sus causas.(p. 31).

El objetivo de la mejora continua del sistema de gestión de la organizaciones aumentar la eficacia y eficiencia de los procesos de la misma, lo que implica el aumento de la satisfacción de las partes interesadas. Para ello es necesario realizar una serie de actividades: el análisis y evaluación de la situación existente.

Modelo PDCA

Merino y Cañizares (2011):

> Los Sistemas de Gestión de Seguridad de la Información desarrollados según la Norma ISO 27001, igual que otros muchos sistemas de gestión, se basan en el concepto de mejora continua.

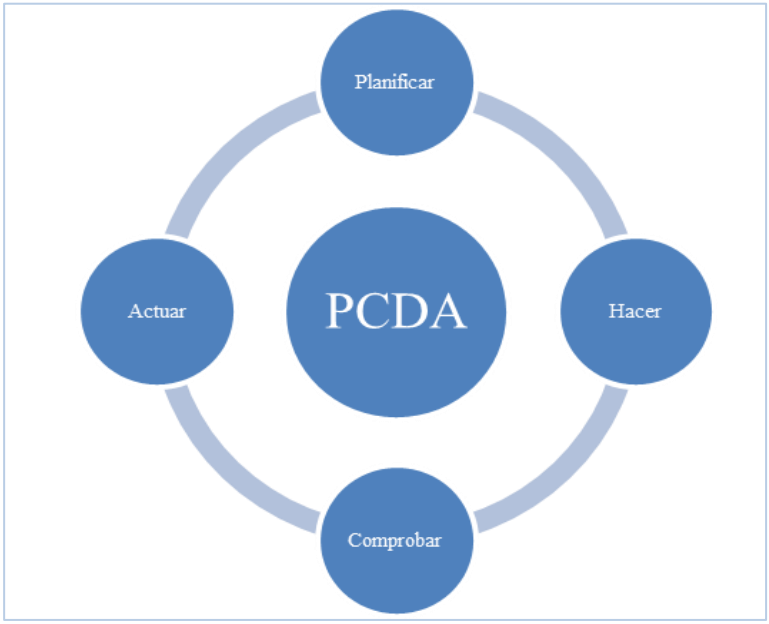


Figura 2. PCDA (Ciclo de Deming). El "circulo de Deming (de Edward Deming), también conocido como el modelo o ciclo PDCA es una estrategia de mejora continua de la calidad en cuatro pasos, basadas en un concepto ideadas por Walter A. Shewhart. Las siglas son el acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).(Merino y Cañizares, 2014)

A continuación se describen las fases de esta espiral de mejora continua, nombre con el que también se le conoce al ciclo del PCDA, como se puede comprobar son de aplicación a cualquier proyecto de mejora de procesos sea del tipo que sea:

PLAN: Identificar el proceso que se quiere mejora, recopilar datos para profundizar el conocimiento del proceso, analizar e interpretar los datos, establecer los objetivos de mejora, detallar las especificaciones de los resultados esperados y definir los procesos necesarios para conseguir estos objetivos, verificando las especificaciones.

DO: Ejecutar los procesos definidos en el paso anterior y documentar las acciones realizadas.

CHECK: Pasando un tiempo previsto de antemano, volver a recopilar datos de control y analizarlos comparándolos con los objetivos con las especificaciones iniciales si fuese necesario, aplicar nuevas mejoras, si se han detectado errores en el paso anterior, documentar el proceso.

Sistema de Gestión de Seguridad de la Información – PDCA

A continuación veremos las tareas que se realizan en las fases del *ciclo PCDA* en el caso de un *Sistema de Gestión de Seguridad de la Información*:

PLAN: Estudio de la situación de la organización (desde el punto de vista de la seguridad), para estimar las medidas que se van a implantar la función de las necesidades detectadas; realización de un análisis de riesgos que ofrezca una valorización de los activos de información y las vulnerabilidades a las que están expuestos y elaboración del plan de gestión de riesgos

DO: Ejecución del plan de acción e implementación de los controles, revisión de la documentación (políticas, procedimientos, instrucciones y registros) y concienciación y formación.

CHECK: Evaluación de la eficacia y eficiencia de los controles implantados, verificación de registros e indicadores y verificación del correcto funcionamiento del SGSI.

ACT: Mantenimiento del Sistema y realización de tareas de mejora y de corrección.

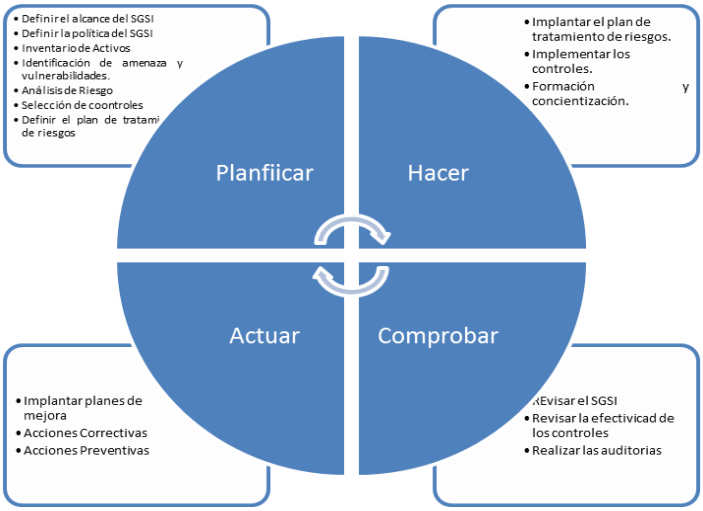


Figura 3. Fases del ciclo del PCDA (Planificar, Hacer, Verificar, Actuar) en el caso de un Sistema de Gestión de Seguridad de la Información (Merino y Cañizares, 2014).

De forma complementaria Gómez y Suarez (2012) nos presentan un modelo para la Gestión de Seguridad de la Información:

> A la hora de implantar un Sistema de Gestión de Seguridad de la Información una organización debe contemplar los siguientes aspectos: formalizar la gestión de la seguridad de la información, analizar y gestionar los riesgos, establecer procesos de gestión de la seguridad siguiendo la metodología PCDA: Plan (selección y definición de las medidas y los procedimientos), Do (implantación de las medidas y los procedimientos de mejora), Check (comprobación y verificación de las medidas implantas) y Act (actuación para corregir las deficiencias detectadas en el sistema) y certificación de la gestión de la seguridad.(p.262).

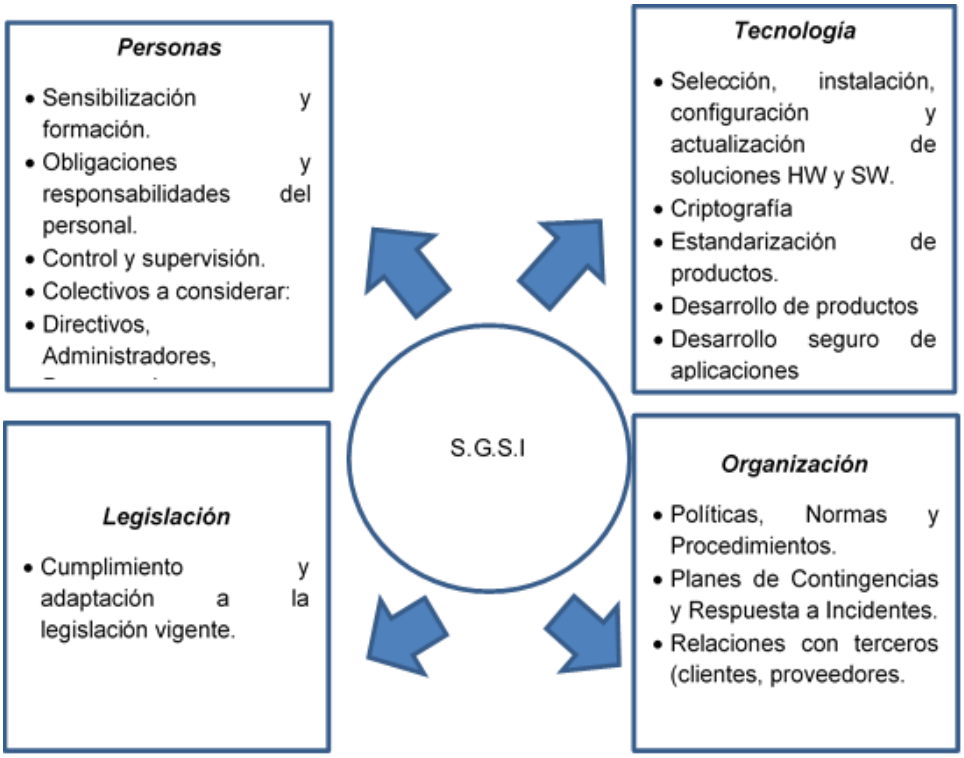


Figura 4. Modelo para la Gestión de Seguridad de la Información. En todo este proceso es necesario contemplar un modelo que tenga en cuenta los aspectos tecnológicos, organizativos, el cumplimiento del marco legal y la importancia del factor humano Gómez y Suarez (2012).

Podemos distinguir varias etapas o niveles de madurez en la Gestión de la Seguridad de la Información en una organización:

Implantación de medidas básicas de seguridad por sentido común. Es una primera etapa la organización se preocuparía de la implementación de las medidas básicas de seguridad aplicadas por "sentido común"

Adaptación a los requisitos del marco legal y de las exigencias de los clientes. En esta segunda etapa la organización toma conciencia de la necesidad de cumplir con las exigencias de la legislación vigente o de otras derivadas de sus relaciones y compromisos con terceros (clientes, proveedores u otras instituciones): protección de datos de carácter personal (delitos informáticos protección de la propiedad intelectual.

Gestión integral de la Seguridad de la Información. Es la tercera etapa la organización ya se preocupa de gestionar con un planteamiento global e integrado la Seguridad de la Información, mediante la definición de una serie de Políticas de Seguridad, la implantación de planes y procedimientos de seguridad, el análisis y gestión de riesgos, y la definición de un plan de respuesta a incidentes y de continuidad del negocio.

Certificación de la Gestión de la Seguridad de la Información. Por último, en la cuarta etapa se pretende llevar a cabo una certificación de la Gestión de la Seguridad de la Información, para obtener el reconocimiento de buenas prácticas implantadas por la organización y poder acreditarlo ante terceros (confianza y verificabilidad por parte de terceros); clientes, administraciones públicas y otras instituciones. Para ello, se recurre a un proceso de certificación basado en estándares como ISO 27001.

Evaluación y medición de la seguridad de la información

Una vez implantado un Sistema de Gestión de Seguridad de la Información requiere un monitoreo sobre su desempeño mediante diferentes mecanismos, teniendo como uno de ellos las métricas (indicadores) que permiten medir el avance de la gestión. Al respecto Merino y Cañizares (2011) afirma que:

Medir y evaluar los procesos de una organización nos permite analizar, comprender y controlar mejor su funcionamiento, lo que a su vez nos permite predecir su comportamiento, así como mejorar su eficiencia y eficacia. Tenemos que distinguir entre medidas, métricas e indicadores. Una medida proporciona una indicación cuantitativa de la extensión, cantidad, dimensión capacidad o tamaño de algunos atributos de un proceso o producto. En el caso que nos atañe, mediremos factores que nos permitan evaluar el funcionamiento de un proceso. Una métrica es una medida cuantitativa del grado en que

> un sistema, componente o proceso posee un atributo dado. Las métricas nos van a permitir relacionar y comparar mediciones. Las métricas nos permiten medir de forma objetiva y especificar en el mundo formal, la correspondencia de un atributo del mundo empírico además de servir como base para la utilización de métodos cuantitativos de evaluación y predicción. (p.40).

Por otro lado Corletti y Del Alba (2008), brindan conceptos principales sobre métricas e indicadores:

> Un Indicador de Seguridad es un valor que se obtiene comparando datos (o atributos según ISO-27004) lógicamente relacionados, referentes al comportamiento de una actividad, proceso o control, dentro de un tiempo específico. Una Métrica de Seguridad podría definirse como el conjunto de preceptos y reglas, necesarios para poder medir de forma real el nivel de seguridad de una organización. Un Cuadro de Mando es una herramienta de gestión que facilita la toma de decisiones que recoge un conjunto coherente de indicadores que proporcionan a la Dirección y a los responsables, una visión comprensible del estado de seguridad de la compañía y de su área de responsabilidad, que indica si se han marcado los objetivos propuestos.
>
> No todos los indicadores técnicos y operativos de seguridad nos sirven para medir la efectividad de los controles que tenemos, y es imposible medir falsos positivos y negativos para todo tipo de controles. De igual manera, resulta imposible medir la efectividad técnica de controles en todos los casos.
>
> Sin embargo, con estimados de costos de protección por día y costos promedio por incidente podemos generar indicadores clave del negocio que son fáciles de entender y aceptar por la alta dirección.
>
> Esto nos permite justificar plenamente el beneficio de los controles para la empresa, así como la inversión realizada.

Más aún, podemos estimar el margen de maniobra para agregar controles adicionales (algunos seguramente más complejos y costosos) y demostrar el beneficio potencial de los mismos a través del componente de costo de incidentes reales", ya que los controles adicionales deberán reducir aún más la probabilidad de ocurrencia de estos eventos, o bien su impacto. A continuación el modelo PCDA para el establecer el ciclo de indicadores de un Sistema de Gestión de Seguridad de la Información:

Tabla 1

Ciclo de Mejora de métricas en un Sistema de Gestión de Seguridad de la Información

CICLO DE MEJORA	IMPLANTACIÓN DE UN SGSI	METRICAS DE UN SGSI
PLAN	Establecer SGSI	Definir la métricas
DO	Implementar y operar el SGSI	Implantar la métricas
CHECK	Supervisar y Revisar el SGSI	Revisar los datos de las métricas
ACT	Mantener y Mejorar el SGSI	Revisar /Mejorar las métricas.

Nota: Desde el primer momento de este ciclo PDCA aplicado a las métricas, debe tenerse en cuenta la “escalabilidad” de las mismas, pues a medida que se van agrupando deben proporcionar menor información de detalle y mayor información “gerencial” y de importante valor agregado para la toma de decisiones. Corletti y Del Alba (2008).

Las métricas de seguridad no se contemplan como un “accesorio” más a añadir al SGSI según le convenga a la organización, sino que lo absorbe y pasa a formar parte de él a lo largo de su ciclo de vida. Esto garantiza que tanto el SGSI como su sistema de medición son revisados y mejorados de forma continua.

PLAN -Definir las Métricas, para que una métrica de seguridad sea efectiva, debe cumplir con los siguientes requisitos: debe ser relevante para la organización, de ser reproducible y justificable, debe ser objetiva e imparcial y debe ser capaz de medir la evolución de la seguridad en la compañía a lo largo del tiempo.

Como herramienta de gestión, un Cuadro de Mando debe poner el foco en aquellos indicadores de la compañía que no se ajustan a los

límites establecidos por ésta, y avisar sobre aquellos otros indicadores que puedan llegar a sobrepasar los límites establecidos. Debe también ser útil para asignar responsabilidades y facilitar la comunicación entre los diferentes niveles de responsables, permitiendo mejorar los resultados.

Las claves para implantar un buen Cuadro de Mando son: obtener el apoyo de la Dirección y alcanzar el mayor consenso posible entre los participantes del diseño, ligar los indicadores a los objetivos, es decir conocer qué es lo que se está midiendo, plasmar la información que sea imprescindible, de una manera sencilla, resumida y eficaz para la toma de decisiones, destacar lo relevante para la compañía, poniendo de relieve aquellos indicadores que no evolucionan según lo planificado, simplificar su representación utilizando un juego de colores que sirva para marcar los cambios de estado y uniformidad en su construcción para facilitar el trabajo de comparar resultados entre áreas diferentes.

DO: Implantar las Métricas, es posible que en esta fase surja la necesidad de adaptar ciertos controles y procedimientos para que la obtención de los datos sea posible. Toda métrica debe tener asignado un responsable que se encargue de recoger, procesar y comunicar los resultados obtenidos al Cuadro de Mando. Esto implica que hay que formar y concienciar al personal involucrado en los procesos a evaluar, ya que el hecho de implantar métricas de seguridad implica un trabajo adicional para los afectados y la inversión de recursos adicionales. Es evidente que no sirve de nada tener un sistema de medición fabuloso, si luego resulta que las prácticas asociadas al proceso de recogida de los datos son ajenas al proceso establecido. La comunicación periódica a las personas del resultado de su trabajo, sirve para mejorar los resultados. En muchos casos, la visualización de los resultados a través de un Cuadro de Mando, puede generar un cambio en la manera de afrontar el trabajo de los empleados de la compañía.

CHECK- Revisar los Datos de las Métricas, el grado de desarrollo del cuadro de mando, y por ende, de las métricas y de los indicadores, irá reflejando el nivel de madurez de la compañía. De hecho, la calidad de las decisiones que tome la Dirección está estrechamente ligada a la información utilizada.

La revisión de los datos obtenidos, se realiza una vez que se han implantado los indicadores. Lo que se pretende comprobar es que los indicadores sean útiles y rentables. Al revisar los datos obtenidos, es muy recomendable considerar la opinión de los usuarios de los indicadores.

*ACT: Revisar/Mejorar las Métricas, s*e planearán revisiones de los objetivos y de la calidad de las métricas para asegurarse que siguen siendo útiles y que siguen cumpliendo con los objetivos definidos. Durante estas revisiones es necesario comprobar que: las métricas son leídas y revisadas por las personas destinatarias, ya que, en caso contrario, terminarán por dejar de utilizarse, el coste de recolectar y mantener las métricas no supera al valor que aportan, los objetivos que marcan las métricas no son demasiado bajos para que todo salga bien, refleja la evolución de los objetivos de seguridad marcados y evalúan la eficiencia del Sistema de Gestión de Seguridad de la Información (SGSI).

Conforme va madurando el SGSI, las métricas se irán actualizando en función de la evolución del SGSI, eliminándose, modificándose indicadores existentes, o, creándose indicadores nuevos. Por norma general, indicadores que en un principio son de progreso, a medida que pasa el tiempo se convierten en indicadores de nivel de madurez del SGSI.

Finalmente, manifestar que a la hora de definir las métricas e indicadores hay que tener en cuenta que *todo lo que se mide no siempre es importante*, y lo que es importante no siempre se puede medir (Albert Einstein). No es posible que un SGSI vaya madurando

> correctamente si no existe un sistema que mida los niveles de eficiencia de todos sus componentes (*todo aquello que no se puede medir, no se puede mejorar*). Las métricas irán madurando y cambiando en función del nivel de madurez que vaya adquiriendo la compañía.

Dimensión Familia Norma ISO 27000

"La implantación de un sistema de gestión de seguridad (SGSI) se realiza, mediante las normas estándares de la familia ISO/IEC 27000; y en particular de la ISO /IEC 27001:2013 y la ISO 27002:2013" (Joyanes, 2015, p.526).

Baca (2015), señala que:

> La Organización Internacional de Estandarización (ISO, por sus siglas en inglés) se dio a la tarea de elaborar y emitir las normas ISO/IEC 27000, que complementan el uso e implementación de un ISMS. Los requerimientos de la Norma 27000 se pueden aplicar a cualquier tipo de organización, sin importar su tamaño, sector al que pertenecen u objetivo de la organización, y declaran cómo establecer, administrar, documentar y mejorar de manera continua un ISMS, tomando como base un enfoque de administración del riesgo, pues solo controlando el riesgo que corren los datos es posible garantizar su confidencialidad. La profundidad de la administración del riesgo la decide la propia empresa, pero antes de la implementación, personal ajeno a la empresa deberá identificar, analizar y evaluar los riesgos para reducirlos a un nivel que sea aceptado por la organización. Los estándares de la norma se basan en el conocido modelo de mejora continua de la calidad de planear, hacer, verificar y actuar (PDCA, por sus siglas en inglés). (p.175)

La última versión de la Norma ISO / IEC 27000: 2016, la cual brinda una visión general de los sistemas de gestión de la seguridad de la información y los términos y definiciones comúnmente utilizados en la familia de estándares del SGSI. Esta Norma Internacional es aplicable a todos los tipos y tamaños de

organización (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro).

Una de las normas internacionales más importantes en el caso de seguridad de la información, es la ISO 27001. Sistema de Gestión de Seguridad de la Información (SGSI), esta norma forma parte de la serie de las Normas 27000, y permite el establecimiento de una metodología de gestión de la seguridad clara y estructurada. Asimismo manifestar que, el primer patrón en seguridad de la información fue elaborado en el año 1990 en Inglaterra, en mérito a las necesidades de la industria, el gobierno y las empresas para promover un sentido común sobre el tema y establecer lineamientos generales.

La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica un conjunto de buenas prácticas para la gestión de la seguridad de su información. La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente. Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión. En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO, con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión. En Marzo de 2006, posteriormente a la publicación de ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

La última versión de la Norma ISO 27001 es del 25 de septiembre del 2013. ISO / IEC 27001: 2013, en ella especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la

información adaptados a las necesidades de la organización. Los requisitos establecidos en ISO / IEC 27001: 2013 son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente del tipo, tamaño o naturaleza.

La Norma ISO 27001 proporciona, a partir de un enfoque por procesos, un modelo para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI. Esta norma es la definición de los procesos de gestión de la seguridad, por lo tanto, es una especificación para un Sistema de Gestión de Seguridad de la Información y, en la actualidad, es la única norma certificable, dentro de la familia ISO 27000.

La Norma ISO / IEC 27002: 2013.Tecnología de la Información – Técnicas de Seguridad – Códigos de Buenas Prácticas para los controles de seguridad de la información, proporciona directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluyendo la selección, implementación y administración de controles teniendo en cuenta el entorno de seguridad de la información de la organización. Está diseñado para ser utilizado por organizaciones que tienen la intención de: seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de la Seguridad de la Información basado en ISO / IEC 27001; Implementar controles de seguridad de la información comúnmente aceptados y desarrollar sus propias directrices de gestión de la seguridad de la información.

Dimensión Formación y Capacitación en ISO 27001:2013

Merino y Cañizares (2011) señala que:

> Un factor clave en la implantación, control y gestión de seguridad de la información es la comunicación a las partes que lo integran, personas u organizaciones, de los objetivos y responsabilidades que se derivan de las actividades que se realizan.
>
> El factor humano, y no el tecnológico suele ser el eslabón más débil en la cadena de la seguridad. Por más políticas, procedimientos y

> controles tecnológicos que se implanten, sin la adecuada implicación del personal, se estará perdiendo la mayor parte de la eficacia de las medidas implantadas.
>
> Como fase transversal durante la fase de la implantación debe realizar esta formación específica en materia de seguridad de la información. La formación debe ser impartida en base al perfil de los diferentes grupos de la organización. Para ello se sigue la siguiente sistemática: identificación de las necesidades de formación, elaboración del plan de formación, realización de las actividades y evaluación de los resultados.

Dimensión Implantación de un Sistema de Gestión de Seguridad de la Información

"La implantación de un Sistema de Gestión de Seguridad de la Información es un proceso metódico, por lo cual es necesario establecer ciertas consideraciones y definir la estrategia a seguir antes de su implantación" (Miguel, 2016, p. 243)

Merino y Cañizares (2011):

> La implantación de un Sistema de Gestión de Seguridad de la Información en una organización se ve influenciada por todas las necesidades y objetivos, por los requisitos de seguridad y por los procesos implicados, así como como por el tamaño y estructura de la organización.(p.89).
>
> Las fases y actividades en que se organiza un proyecto de plantación de un SGSI, según el estándar ISO 27001 son:
>
> *Fase I*: planificación del Proyecto, análisis de situación respecto a la norma (Gap análisis), definición de la organización de seguridad de la información.
>
> *Fase II:* análisis de riesgo, gestión de riesgo, elaboración de los planes y programas de acción.

Fase III: Elaboración de la documentación del sistema de gestión (PDCA), definición de las acciones para la comunicación, formación y concienciación, evaluación del control operativo, elaboración de los indicadores de gestión y puesta en funcionamiento del sistema de gestión.

Fase IV: Rodaje y mejora del sistema de gestión, indicadores y auditoría interna.

Fase V: acciones correctivas y la mejora del sistema de gestión. (p.90).

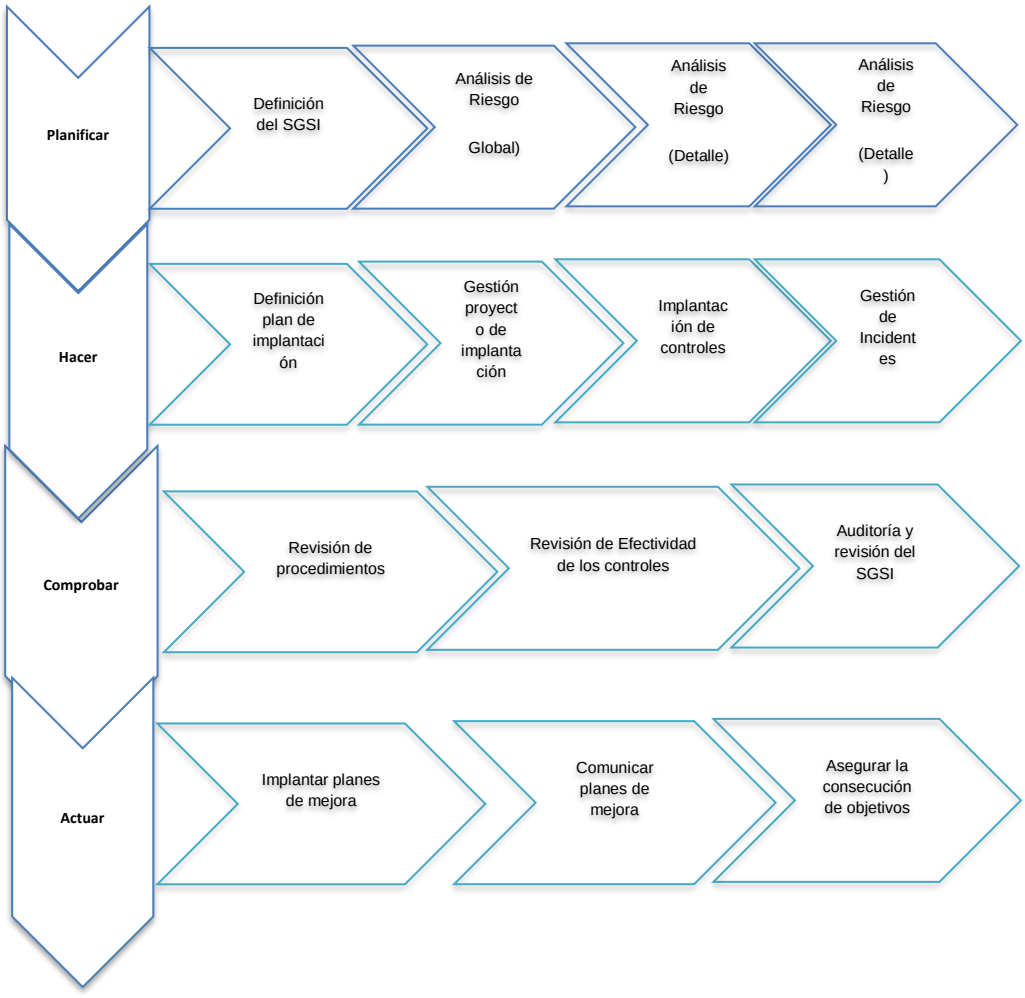


Figura 5. Actividades para la implantación de un Sistema de Gestión de Seguridad de la Información. El proyecto de implantación de un SGSI puede considerarse como el primer ciclo de mejora continua del SGSI en cuestión, cómo éste se gestiona mediante un modelo de PCDA, existe una correspondencia clara entre las actividades de implantación y las actividades del ciclo de vida del SGSI.(Miguel, 2011)

Tabla 2

Actividades de Implantación de un SGSI

ACTIVIDAD	Proyecto Implantación	Implantación SGSI (1° Ciclo PDCA)	Mejora Continua PDCA
Planificación del Proyecto	FASE I		
Análisis de Situación respecto de la Norma (Gap análisis)	FASE I		
Definición de la organización de la seguridad de la información	FASE I	PLAN	PLAN Revisión de la definición de la organización de la seguridad de la información
Análisis de Situación respecto de la Norma (Gap análisis)	FASE I	PLAN	PLAN Nuevo análisis del riesgos
Elaboración de los planes y programas de acción	FASE II	PLAN	Revisión anteriores y nuevos planes y programas de seguridad
Elaboración de documentación del sistema de gestión	FASE III	DO	DO
Definición de las acciones para la comunicación formación y concienciación	FASE III	DO	Revisión
Evaluación del control operativo	FASE III	DO	Revisión
Elaboración de indicadores de gestión	FASE III	DO	Revisión elaboración de nuevos indicadores
Puesta en funcionamiento del sistema de gestión	FASE III	DO	
Rodaje y mejora del sistema de gestión.	FASE IV	DO	
Indicadores	FASE IV	DO	
Auditoría Interna	FASE IV	CHECK	
Acciones Correctivas y mejora del sistema de gestión	FASE V	ACT - PLAN	

Nota: Relación de las actividades con las fases de implantación de un Sistema de Gestión de Seguridad de la Información y el primer ciclo PDCA. (Miguel, 2011).

Planificación del Proyecto

Miguel (2011), expresa que:

> En esta actividad se definirá el alcance del proyecto, la metodología que se va a utilizar, cuáles son las necesidades, cómo va a definir el modelo. Asimismo como parte de las tareas de esta actividad se encuentra en realizar una análisis de cuáles son los objetivos principales que desean alcanzar adoptando la ISO 27001. Asimismo es indispensable definir claramente el ámbito del SGSI, el alcance puede abarcar a toda o sólo una parte de la organización, en función de la estrategia a seguir que adopte una organización, se puede implementar un SGSI cuyo alcance comprenda un único proceso, una unidad de negocio, un tipo de servicio, o un marco único que englobe la seguridad (p.94).

En esta etapa es importante establecer el propósito de la implantación de un SGSI así como la matriz de expectativa y necesidades de los grupos de interés vinculantes a la organización, todo ello en resumen constituye el contexto de la organización.

Análisis de la Situación respecto a la Norma

Para esta tarea consiste en realizar un análisis diferencial (GAP Analysis), permitirá evaluar a alto nivel el grado de cumplimiento de cada una de las cláusulas de la ISO 27001y los controles que establece la norma en su anexo (ISO 27002).

Política de Seguridad

Instituto Nacional de Estadística e Informática [Inei] (2012) señala que:

> Una Política de Seguridad de la información es una estrategia frente a los riesgos que pueden atentar contra la confidencialidad, la integridad y la disponibilidad de los recursos informáticos, dichas estrategias se elaboran en base a la identificación de los riesgos tanto internos como externos de toda la infraestructura informática de una institución. (p. 2)

Una política de seguridad, como declaración de principios de la organización, debe plasmar las directrices generales y principios de actuación que seguirá la organización en materia de seguridad, así como la estrategia a seguir para la definición de objetivos. La política de seguridad debe ser un documento robusto y a la vez lo suficientemente preciso para que pueda aplicar de forma horizontal en toda la organización, de tal forma que desde el primero hasta el último pueda cumplirla. A partir de ella, se desarrollará todo el cuerpo normativo y se establecerán los procedimientos acordes a la misma.

Enfoque para la evaluación de Riesgos

Merino, Cañizares (2011) indica que:

> El objetivo de la evaluación de riesgos es definir la metodología para identificar los activos, las amenazas, las vulnerabilidades, los impactos y las probabilidades, y así identificar tanto el nivel de riesgos existente como el nivel aceptable por la Dirección. La metodología a implementar debe ser capaz de analizar procesos complejos y reducir los mismos a un conjunto de componentes de fácil comprensión, para que a partir de ellos sea posible describir y entender dichos procesos complejos. Al final de la metodología debe asegurarse que los cálculos del riesgo produzcan resultados comparables y reproducibles, para ello la metodología deberá reunir las siguientes características: objetiva, fiable, medible, repetible, permitir la revisión continua, enfocada en términos entendibles por la organización, estar soportada por una herramienta de gestión. Por lo tanto, la elección de la metodología debe estar basada en las mejores prácticas, para que de este modo se adecue a nuestras necesidades y nos permita realizar las tareas de análisis y gestión de riesgo de forma eficaz y eficiente. (p. 100)

La evaluación de riesgos está enfocado en realizar un cálculo de las amenazas a los activos de la información con vistas a seleccionar controles adecuados a la Norma ISO 27001 y 27002 para mitigar los riesgos que se puedan presentar utilizando estrategias de acuerdo al score del negocio.

Análisis de riesgos

El riesgo es la probabilidad que una amenaza impacte en un recurso de información**.** El nivel de riesgo depende por consiguiente, del análisis previo de vulnerabilidades del sistema, de las amenazas y del posible impacto que puedan tener en el funcionamiento de la organización. (Joyanes, 2015, p.498).

“El riesgo, es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto sobre la organización”. (Gómez y Suarez, 2012, p. 270)

Joyanes (2015), define al análisis de riesgo de la siguiente manera:

> Es el proceso por el cual se identifican las amenazas y vulnerabilidades contra seguridad del sistema de información, se determina su magnitud y se describen las áreas que necesitan salvaguardas o contramedidas. El Análisis de Riesgo sirve para identificar el riesgo existente y evaluar el actual sistema de seguridad que ayudará a decidir las medidas de seguridad que deben adoptarse. No es una tarea que se realiza de una sola vez y para siempre. Si no que debe efectuarse periódicamente, y si es posible utilizar una herramienta de análisis de riesgo autorizada, con una metodología sólida, como algunas de las recomendadas. (Joyanes, 2015, p.498).

Merino y Cañizares, 2011, define al análisis de riesgo como:

> El proceso de identificar los riesgos de la seguridad que podrían impedir a una organización lograr sus objetivos, determinando su magnitud e identificando que requieren medidas de salvaguarda o controles en función del riesgo detectado. El análisis de riesgos intenta que los criterios en los que se apoya la seguridad sean más objetivos, permitiendo a la organización gestionar sus riesgos y tomar decisiones en base a los riesgos propios. (p. 102)

Esta actividad se divide en las distintas tareas: identificar los activos, identificar las amenazas, identificar las vulnerabilidades, identificar el impacto, obtener el riesgo intrínseco, identificar las salvaguardas y obtener el riesgo residual. (Merino y Cañizares, 2011, p. 103)

Gestión de riesgos

El objetivo de la gestión de riesgos es identificar, controlar y minimizar el impacto de las amenazas. Supone una planificación, organización, dirección y control de los recursos para garantizar que riesgo permanece dentro de unos límites y costes aceptables. El proceso de gestión de riesgos ha de definir un plan para implantar de ciertas salvaguardas o contramedidas en el sistema de información que permitan disminuir la probabilidad de que se materialice una amenaza, reducir la vulnerabilidad de un sistema o impacto en la organización y permitir la recuperación y la continuidad del negocio. La gestión de riesgos se puede considerar que consta de tres procesos: análisis de riesgo, mitigación de los riesgos y evaluación de los controles. (Joyanes, 2015, p. 498):

El análisis de riesgos implica tres etapas: evaluación del valor de cada activo a proteger, estimación de la probabilidad de que cada activo estará comprometido, comparación de los costes probables del activo comprometido con los costes de protección de ese activo. La organización entonces considera como mitigar el riesgo.

Mitigación de Riesgos*,* la organización ha de tomar acciones frente a los riesgos que deben cumplir dos funciones: implementación de controles para prevenir ocurran amenazas identificadas, desarrollar un medio de recuperación si la amenaza se hace realidad. Las estrategias de mitigación de riesgos según Rainer (2013) son: aceptación de riesgos, limitación de riesgos y transformación de riesgos.

Aceptación del Riesgo, acepta el riesgo potencial, continua el funcionamiento sin controles y asume cualquier daño que ocurre.
Limitación del riesgo, limita el riesgo implementado controles que minimizan el impacto de la amenaza.
Transferencia de Riesgo, transfiere el riesgo utilizando otros medios para compensar la pérdida tales como la suscripción de seguros específicos.

Evaluación de los Controles, en esta última etapa la organización examina los costes de implementación de medidas de control adecuadas frente al valor de esas medidas de control, sobre la base, como es normal, de que si los costes de implementación del control son mayores que el activo a proteger, está claro que el control no es eficiente ni efectivo.

El auge en el rol que ha tomado la información, sin embargo, no exime a las organizaciones de una serie de peligros, que se han visto incrementados por las nuevas amenazas surgidas del uso de tecnologías de la información y las comunicaciones. De esta manera, toda organización se encuentra constantemente expuesta a una serie de riesgos mientras que resulta imposible establecer un entorno totalmente seguro.

La gestión de riesgos se presenta entonces como una actividad clave para el resguardo de los activos de información de una organización y en consecuencia protege la capacidad de cumplir sus principales objetivos. Es un proceso constante que permite a la administración balancear los costos operacionales y económicos causados por la interrupción de las actividades y la pérdida de activos, con los costos de las medidas de protección a aplicar sobre los sistemas de información y los datos que dan soporte al funcionamiento de la organización, reduciendo los riegos que presentan los activos de información a niveles aceptables para la misma

Dimensión Proceso de Registros Civiles

Conjunto de actividades relacionadas entre sí para la salida de los producto comprendidos : Acta Registral Procesada, Acta Depurada, Expedientes de Reposición, Expedientes de Delegación de Funciones, Expedientes de Investigación, con niveles de calidad y seguridad.

Riesgos que afectan la seguridad de la información del proceso de registros civiles

El Reniec, con el objetivo de establecer la interoperabilidad interinstitucional viene proporcionando un sistema a las Oficinas de Registros de Estado Civil (Orec) denominado “Sistema de Integración de Registros Civiles y Microformas (Sircm)”, mediante el cual se realiza el registro en línea de las actas registrales de nacimiento, matrimonio y defunción, quedando la data almacenada en la base de datos del Reniec. En ese sentido con la finalidad de evitar riesgos en la transmisión de la información por la red informática es necesario establecer controles que permitan asegurar y prevenir riesgos que contravengan la disponibilidad, confidencialidad e integridad de la información.

Brechas de seguridad de la información en el proceso de registros civiles

El proceso de registros civiles, es uno de los procesos clave del Reniec, que tiene a su cargo la base de registros civiles de todos los peruanos, el cual contiene información importante que debe ser protegida de forma integral, evitando riesgos que puedan producir daños irreparables. Teniendo como lineamientos impulsores los tres pilares de seguridad de la información: confidencialidad, disponibilidad e integridad de la información.

Confianza de ciudadano del servicio que presta Reniec

Los entregables que genera el proceso de registros civiles son los siguiente productos, los cuales deben contar con controles de seguridad que permitan mantener confiable, disponible e integra la base de datos de registros civiles que contiene data e imágenes con valor legal, lo cual permitirá al ciudadano realizar cualquier trámite, generando con ello alta confianza en la ciudadanía.

Mejorar la disponibilidad y tiempo de respuesta de los servicios finales a los ciudadanos.

El Reniec, a través de su carta de servicios ha establecido indicadores de calidad dentro de los cuales se encuentran los plazos de atención de los productos y servicios que se ofrece al ciudadano, los cuales son evaluados mensualmente y los resultados se publican en la página oficial del Reniec a los cuales tiene acceso todos los usuarios. La evaluación de los resultados ha impulsado implementar buenas prácticas en dicha institución, reforzando la seguridad informática y complementarla con estrategias que permitan mejorar la disponibilidad de la información a través del en todas las oficinas

1.3. Justificación

1.3.1. Justificación Teórica

Este trabajo en el marco de un Sistema de Seguridad de la Información, servirá como referencia para la aplicabilidad de los requisitos de la Norma ISO 27001, y coadyuvará a impulsar a las instituciones públicas del Perú a continuar con la implantación de buenas prácticas para la protección de sus activos, convirtiéndose en una necesidad frente a las brechas de seguridad existentes.

Condori Alejo H. (2012). *Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de Seguridad de la Información para determinar su influencia en la atención del usuario*. Universidad Garcilaso de la Vega (pág. 70). La seguridad de información se ha convertido en uno de los aspectos de mayor importancia para cualquier organización. De tal forma que las organizaciones necesitan asegurar sus activos de información para mantener un alto nivel de seguridad. Lo que repercute en la eficiencia organizacional.

1.3.2. Justificación Práctica

La implantación de un Sistema de Seguridad de la Información, bajo la Norma ISO 27001, contribuirá al proceso de registros civiles del Reniec en prevenir riesgos, amenazas o vulnerabilidad de uno sus principales activos: la información de la base

de datos de registros civiles (registros de hechos vitales de nacimiento, matrimonio y defunción de los peruanos) además de cada uno de los colaboradores que forman parte de los mismos siendo estos la columna vertebral de la institución. Este modelo bajo la aplicabilidad de sus tres componentes de confidencialidad, disponibilidad e integridad de la información, ayudará a gestionar la seguridad de la información convirtiéndose en una estrategia de protección, asegurando la continuidad de las operaciones y en consecuencia la continuidad de la organización.

1.3.3. Justificación Legal

Para la investigación nos apoyaremos en las siguientes bases legales: Resolución Ministerial N° 004-2016-PCM, de fecha 08 de enero del 2016, apruébese el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2° Edición, en todas las entidades integrantes del Sistema Nacional de Informática; (Ongei, 2016), Resolución Comisión de Normalización y de Fiscalización de barreras comerciales no arancelarias N° 129-2014/CNB-INDECOPI, de fecha 20 de noviembre del 2014, que aprueba la NTP – ISO /IEC 27001:2014 Tecnologías de la Información. Sistema de Gestión de Seguridad de la Información. Requisitos. 2da Edición. Reemplaza a la NTP – ISO /IEC 27001:2008; (Ongei, 2016), Resolución Ministerial N° 129-2012-PCM, de fecha 23 de mayo del 2012, apruébese el uso obligatorio de la Norma Técnica Peruana “NTP-ISO/ IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos” en todas las entidades integrantes del Sistema Nacional de Informática; (Ongei, 2016) Resolución Ministerial N° 197- 2011-PCM, de fecha 14 de julio del 2011, establece: Artículo 1°.- De la fecha de implementación de la Norma de Seguridad, Establézcase como fecha límite el 31 de diciembre del 2012, para que las entidades e la Administración Pública a que se refiere el artículo 2 de la presente norma, implemente el Plan de Seguridad de la Información. Código de Buenas Prácticas para la Gestión de Seguridad de la Información. 2da Edición, aprobada mediante Resolución Ministerial N° 246-2007 fecha límite para que diversas entidades de la

administración pública implemente el Plan de Seguridad de la información dispuesto en la Norma Técnica Peruana señalada.

Este trabajo, también se ha sustentado en el marco de la Ley N° 29733 –Ley de Protección de datos personales; Ley N° 30096 –Ley de Delitos Informáticos; Ley N° 28493 –Ley de SPAM; Ley N° 27806 –Ley de Transparencia y Acceso a la Información Pública; Ley N° 27269 –Ley de Firmas y Certificados Digitales, modificada por la Ley N° 27310.

1.4. Problema

Problema General

¿Qué relación existe entre el sistema de gestión de seguridad de la información y el proceso de registros civiles del Reniec?

Problema Específicos 1

¿Qué relación existe entre el sistema de gestión de seguridad de la información y los riesgos que afectan la seguridad de la información del proceso de registros civiles del Reniec.

Problema Específicos 2

¿Qué relación existe entre el sistema de gestión de seguridad de la información y la confianza del ciudadano del servicio que presta Reniec?

1.5. Hipótesis

1.5.1. Hipótesis General

Existe relación entre el sistema de gestión de seguridad de la información y el proceso de registros civiles del Reniec. San Borja. Lima 2016.

1.5.2. Hipótesis Específica

Hipótesis Especifica 1

Existe una relación entre el sistema de gestión de seguridad de la información y los riesgos que afectan la seguridad de la información del proceso de registros civiles.

Hipótesis Especifica 2

Existe una relación entre el sistema de gestión de seguridad de la información y la confianza del ciudadano del servicio que presta Reniec.

1.6. Objetivos

1.6.1. Objetivo General

Determinar la relación que existe entre el sistema de gestión de seguridad de la información y el proceso de registros civiles del Reniec.

1.6.2. Objetivos Específicos

Objetivo Especifico 1

Determinar la relación que existe entre el sistema de gestión de seguridad de la información y los riesgos que afectan la seguridad de la información del proceso de registros civiles del Reniec.

Objetivo Especifico 2

Determinar la relación que existe entre el sistema de gestión de seguridad de la información y la confianza del ciudadano del servicio que presta el Reniec.

II. Marco Metodológico

2.1. Variables de investigación

Definición de la Variable 1: Sistema de Gestión de Seguridad de la Información

Merino y Cañizares (2011), señala que el Sistema de Gestión de Seguridad de la Información:

> Es la parte del Sistema General de la Gestión en una organización que consta de: la política, estructura organizativa, los procedimientos, los procesos y los recursos necesarios la gestión de la seguridad de la información en una organización. Considerando los factores tales como:
>
> - Sistema de Gestión de Seguridad de la Información
> - Gestión de Seguridad de la Información
> - Familia de Norma ISO 27000
> - Implantación de un Sistema de Seguridad de la Información

Definición de la variable 2: Proceso de Registros Civiles

Conjunto de actividades relacionadas entre sí para la salida de los producto comprendidos : Acta Registral Procesada, Acta Depurada, Expedientes de Reposición, Expedientes de Delegación de Funciones, Expedientes de Investigación, con niveles de calidad y seguridad.

El Reniec es un organismo autónomo, que tiene definida como parte de su misión y lineamientos de políticas institucionales establecer estrategias para implementar buenas prácticas que permitan mitigar *los riesgos que afectan la seguridad de la información del proceso de registros civiles*, así como mejorar cada día la *confianza del ciudadano del servicio que presta Reniec.*

2.2. Operacionalización de Variables

Tabla 3

Operacionalización de la variable Sistema de Gestión de Seguridad de la Información

Dimensión	Indicadores	Ítems	Escala de medición	Niveles y Rango
Sistema de Gestión de Seguridad de la Información	Confidencialidad de la Información Integridad de la Información Disponibilidad de la Información	Del 1 al 6	Totalmente de acuerdo (1) De acuerdo (2) No sabe/no opina (3) En desacuerdo (4) Totalmente en desacuerdo (5)	Bajo [34 - 79] Medio [80 - 125] Alto [126 - 170]
Gestión de Seguridad de la Información	Sistema de Gestión Modelo PDCA Sistemas de Gestión de Seguridad de la Información- Modelo PDCA Evaluación y medición de la seguridad de la información	Del 7 al 14		
Familia de Norma ISO 27000	Formación y Capacitación en ISO 27001:2013	Del 15 al 16		
Implantación de un Sistema de Seguridad de la Información	Planificación del Proyecto Análisis de situación respecto a la norma Política de Seguridad Enfoque para la evaluación de Riesgos Análisis de riesgos Gestión de riesgos Plan de Tratamiento de Riesgo Sistema de Métricas Elaboración de cuerpo documental Formación y Concienciación Responsabilidad de la Gerencia Monitorización y revisión Auditorías Internas del SGS Mantenimiento y mejora	Del 17 al 34		

Tabla 4

Operacionalización de la variable Proceso de Registros Civiles

Dimensiones	Indicadores	Número de ítems	Escala de medición	Niveles y Rangos
Riesgos que afectan la seguridad de la información del proceso de registros civiles.	Brechas de seguridad de la información en el proceso de registros civiles.	Del 1 al 7	Totalmente de acuerdo (1) De acuerdo (2) No sabe/no opina (3) En desacuerdo (4) Totalmente en desacuerdo (5)	Aceptable [9 - 21] Regular [22 - 33] No Aceptable [34 - 45]
Confianza de ciudadano del servicio que presta RENIEC.	Mejorar la disponibilidad y tiempo de respuesta de los servicios finales a los ciudadanos.	Del 8-9		

2.3. Metodología

"La metodología implica el empleo de los recursos pertinentes; por ejemplo, en las investigaciones sociales las pruebas estadísticas proporcionan una visión más precisa del objeto de estudio, ya que apoyan o no las hipótesis para su validación o rechazo". (Hernández, Fernández y Bautista, 2014, p.14)

Es también seguir una serie de procesos metodológicos previamente establecidos para lograr un resultado.

2.4. Tipo de Estudio

Aunque el método científico es uno, existen diversas maneras de identificar su práctica o aplicación en la investigación.

Según la finalidad: Es aplicada porque tiene como finalidad plantear la resolución a problemas prácticos, además que el aporte de conocimiento teórico es secundario. (Landeau Rebeca, 2007, p.56).

Según su carácter: Es descriptiva porque tiene por objetivo analizar como es y se manifiesta un fenómeno y sus componentes, utiliza métodos descriptivos como la observación, estudios correlacionales, etc.

Hernández, R, Fernández (2010 p, 103), sostiene que "la investigación descriptiva busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice.

Según su naturaleza: Es cuantitativa porque utiliza la metodología empírico analítico y se sirve de pruebas estadísticas para el análisis de datos.

2.5. Diseño de la Investigación

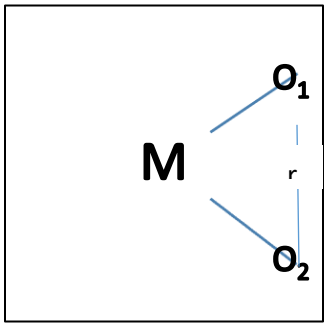
Una vez ya precisado el planteamiento del problema se puede definir el alcance tentativo del mismo ya que se formularon las hipótesis, el diseño constituirá si se confirma o falsea la hipótesis.

Para la presente investigación será del tipo no experimental (diseños transversales y longitudinales).

Para la presente investigación se utiliza el diseño No experimental debido a que se realiza sin manipular deliberadamente las variables independientes, también es conocida como investigación expost-facto (los hechos y las variables ya ocurrieron).

Además de ser de tipo de diseño correlacional porque se examina la relación o asociación que existen entre dos o más variables en la misma unidad de investigación.

Esquema:



Dónde:

M: Muestra
O_1: Variable 1 Sistema de Gestión de Seguridad de la Información
O_2: Variable 2 Proceso de Registros Civiles
r: Relación de las variables de estudio

2.6. Población, muestra y muestreo

Población:

"La población, es un conjunto formado por la totalidad de individuos, objetos o medidas de interés, sobre los que se realiza un estudio" (Gutiérrez y De la Vara, 2013, p.62).

Todos los miembros de la población pertenecen al Proceso de Registros Civiles representado a través de la Gerencia de Proceso de Registros Civiles además todos poseen características de acuerdo a las variables en estudio.

El estudio se realizó en un determinado periodo de tiempo (III trimestre 2016) a la población de interés.

El lugar donde se ubica la población de interés está en la Sede San Borja del Reniec Av. Javier Prado Este 2392 - San Borja.

El tamaño de la población son los trabajadores de la Gerencia de Procesos de Registros Civiles [GPRC] incluye también a sus unidades orgánicas (sub gerencias).

La población de objeto de estudio está constituido por 175 trabajadores de ambos sexos de la GPRC de la Sede San Borja.

Tabla 5

Tamaño de la Población

Proceso/ Gerencia	Sub Procesos	N° Trabajadores	%
Gerencia de Procesos de Registros Civiles	Integración de Registros Civiles	31	17.70%
	Delegación de Registros Civiles	47	26.90%
	Procesamiento de Registros Civiles	81	46.30%
	Depuración de Registros Civiles	16	9.10%
	Total	175	100%

Muestra

La muestra es un subconjunto fielmente representativo de la población. La muestra es la parte de la población que se selecciona, de la cual realmente se obtiene la información para el desarrollo del estudio y sobre la cual se efectuarán la medición y la observación de las variables objeto de estudio. Bernal (2006, p.165).

Muestreo Probabilístico

Los métodos de muestreo probabilísticos son aquellos que se basan en el principio de equiprobabilidad. Es decir, aquellos en los que todos los individuos tienen la misma probabilidad de ser elegidos para formar parte de una muestra y, consiguientemente, todas las posibles muestras de tamaño n tienen la misma probabilidad de ser seleccionadas.

Determinación del tamaño de la muestra

Para está investigación se utilizará una muestra probabilística estratificada, cuyas unidades de análisis o elementos muestrales se elegirán aleatoriamente.

Para encontrar la muestra se aplicó la siguiente formula:

$$n = \frac{\delta^2 \delta.\text{p.q.N}}{E^2(N-1)+p.q.\delta^2}$$

Dónde:

n: tamaño de la muestra

N: tamaño de la población (universo)

δ^2 = Nivel de confianza

E^2 = Margen de error

p: Posibilidad de ciertas características que están presentes en la población o universo.

q: Posibilidad de ciertas características que no están presentes en la población o universo.

Para la población de 175 colaboradores del Proceso de Registros Civiles representado por la Gerencia de Procesos de Registros Civiles, se determinará el tamaño de muestra a fin de recolectar información a través de entrevista y/o encuestas.

Se utiliza el tipo de muestreo probabilístico y la técnica método aleatorio simple

Con un nivel de confianza del 95% y un error margen de error o nivel de precisión de 0.05 se procederá al cálculo del tamaño de muestra. Además 50% es la proporción de la población que tiene la misma característica de interés.

Tabla 6

Nivel de Confianza

Nivel de Confianza	99.73%	99.00%	96%	95.45%	95.00%	80%	68.27%
Valores de Z	3.00	2.58	2.05	2.00	1.65	1.28	1.00

Nota: Elaboración propia

Con la información proporcionada tenemos:

N	175
δ^2	1.96
E^2	0.05
p	0.5
q	0.5

Reemplazando en:

Tenemos:

$$n = \frac{(1.96^2)(0.5)(0.5)(220)}{(0.05^2)(220-1)+(0.5)(0.5)(1.96^2)}$$

n = 120

Y para la muestra por sub proceso se ha tenido que hallar la muestra específica (estratos), mediante el cálculo de la constante K a través de la fórmula siguiente:

Donde:

$$k = \frac{n}{N}$$

n: muestra

N: población

$$k = \frac{120}{175} = 0.685$$

K= 69%

Quedando constituida la muestra por el 69% del total de la población.

Tabla 7

Muestra representativa

Proceso/ Gerencia	Sub Procesos	Población		Muestra	
		Cantidad	%	Cantidad	%
Gerencia de Procesos de Registros Civiles	Integración de Registros Civiles	31	18%	21	18%
	Delegación de Registros Civiles	47	27%	32	27%
	Procesamiento de Registros Civiles	81	46%	56	46%
	Depuración de Registros Civiles	16	9%	11	9%
	Total	175	100%	120	100%

Criterios de selección

Criterios de inclusión

Colaboradores del Reniec. San Borja. Lima. 2016, que son voluntarios y asistieron de la encuesta realizada.

Criterios de Exclusión.

No ser colaboradores del Reniec. San Borja. Lima. 2016, que no son voluntarios a la encuesta, y que no asistieron el día de la encuesta.

2.7. Técnicas e instrumentos de recolección de datos

Técnicas

Contreras (2014, cito a Hurtado, 2000): “Las técnicas de recolección de datos, son los procedimientos y actividades que le permiten al investigador obtener la información necesaria para dar cumplimiento a su objetivo de investigación”. (p.1)

Para llevar a cabo la investigación se utilizará la técnica de la encuesta que es una técnica de investigación que consiste en una interrogación verbal o escrita que se realiza a las personas con el fin de obtener determinada información necesaria para la investigación.

El sondeo o encuesta es un método científico de recolección de datos de carácter cuantitativo que permite recopilar información sobre opiniones, creencias y/o actitudes de los sujetos estudiados e indagar acerca de temas múltiples, tales como pautas de conducta o consumo, prejuicios sociales, trayectorias académicas, laborales, sociales, entre otros aspectos (Marradi, Archenti y Piovani, 2010). Brinda información acerca de cómo se manifiestan muchas propiedades (dimensiones, características o variables) en innumerables individuos y se aplica en ámbitos diversos tales como el comercial, el académico y el político (Blanco, 2011).

Instrumento

El instrumento que se utilizará en la presente investigación es el cuestionario, el cual es elaborado mediante una serie de ítems con el propósito de obtener información de los consultados.

Tabla 8

Técnica e Instrumento para la investigación

TÉCNICAS	INSTRUMENTOS
Encuesta. La encuesta permitirá inquirir la opinión de los colaboradores de cómo la implantación de un Sistema de Gestión de Seguridad de la Información mejorará el proceso de registros civiles del Reniec.	Cuestionario. El cuestionario se encuentra integrado por |un conjunto de preguntas que abarca las dimensiones de cada variable de la investigación

Ficha Técnica: De la Variable 1 Sistema de Gestión de Seguridad de la Información

Nombre del Instrumento: Cuestionario de Sistema de Gestión de Seguridad de la Información en el proceso de registros civiles.

Autor: Condori, Alejo, 2012

Adaptado: Bernaldo Bastidas Natividad Gladys, 2016

Tipo de instrumento: Cuestionario.

Objetivo: Valoración del diagnóstico para la implantación de un Sistema de Gestión de Seguridad de la Información en el proceso de registros civiles del Reniec.

Población: Colaboradores del Proceso de Registros Civiles del Reniec.

Numero de ítem: 34

Aplicación: Directa

Tiempo de administración: 20 minutos aproximadamente

Normas de aplicación: El colaborador marcará en cada ítem de acuerdo lo que considere evaluado respecto lo observado.
Escala: De Likert
Niveles o Rangos: Bajo [34 - 79] Medio [80 - 125] Alto [126 – 170]
Ficha Técnica: De la Variable 2 Proceso de Registros Civiles
Nombre del Instrumento: Cuestionario de Proceso de Registros Civiles.

Autor: Condori, Alejo, 2012

Adaptado: Bernaldo Bastidas Natividad Gladys, 2016

Tipo de instrumento: Cuestionario.

Objetivo: Valoración del diagnóstico para la implantación de un Sistema de Gestión de Seguridad de la Información en el proceso de registros civiles del Reniec.

Población: Colaboradores del Proceso de Registros Civiles del Reniec.

Numero de ítem: 9

Aplicación: Directa

Tiempo de administración: 20 minutos aproximadamente

Normas de aplicación: El colaborador marcará en cada ítem de acuerdo lo que considere evaluado respecto lo observado.

Escala: De Likert

Niveles o Rangos: Aceptable [9 - 21] Regular [22 - 33] No Aceptable [34 - 45]

2.8. Método de Análisis de datos

Para analizar cada una de las variables se ha utilizado del programa SPSS V. 22, porcentajes en tablas y figuras para presentar la distribución de los datos, la estadística descriptiva, para la ubicación dentro de la escala de medición, para la contrastación de las hipótesis se aplica la estadística descriptiva.

Método estadístico

Hernández et al (2014).Define: “En estadística, el coeficiente de correlación de Spearman, ρ es una medida de la correlación (la asociación o interdependencia) entre dos variables aleatorias continuas. Para calcular “ρ”, los datos son ordenados y reemplazados por su respectivo orden”. (p.271).

Validez y Confiabilidad.

Hernández et al (2014):”La validez es el grado en que una prueba o ítem de la prueba mide lo que pretende medir; es la característica más importante de una prueba. (p.127).

La validez de los instrumentos se corrobora mediante el juicio de expertos y su validación por parte de ellos de acuerdo al resultado de la evaluación. Los resultados obtenidos en las encuestas están ligados a otra medición de las mismas características.

Para obtener la confiabilidad de los instrumentos se someterá al estadígrafo de Alfa de Cronbach y para su validación se hará a través de un docente con el grado de maestría en investigación y un docente especialista en el área de investigación. La validadora del instrumento es la Dra. Ana Boy Barreto, quien le otorgó la validez respectiva.

Quero, (2010). Define a la confiabilidad como:
"La confiabilidad de una medición o de un instrumento, con el denominador común de que todos son básicamente expresados como diversos coeficientes de correlación". (p.227).

La confiabilidad de los instrumentos se hizo por la aplicación del coeficiente "Alfa de Cron Bach" que nos dio el grado en que el instrumento es confiable.

Para la interpretación se ha considerado la siguiente escala (De Vellis, 2006, p.8):
Por debajo de .60 es inaceptable
De .60 a .65 es indeseable.
Entre .65 y .70 es mínimamente aceptable.
De .70 a .80 es respetable.
De .80 a .90 es buena
De .90 a 1.00 Muy buena

Confiabilidad Cuestionario de la variable Sistema de Gestión de Seguridad de la Información

Tabla 9

Confiabilidad cuestionario sobre Sistema de Gestión de Seguridad de la Información

Resumen del procesamiento de los casos

		N	%
Casos	Válidos	120	100,0
	Excluidos[a]	0	,0
	Total	120	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,922	34

Cuanto el valor del alfa de cronbach es más cercano al 1, más alto es el grado de confiabilidad, para nuestro caso el α =0.922 para la variable Sistema de Gestión de Seguridad de la información que consta de 34 ítems por lo cual concluimos que es confiable los resultados obtenidos.

Tabla 10

Confiabilidad cuestionario sobre Seguridad de la Información

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,813	6

Cuanto el valor del alfa de cronbach es más cercano al 1, más alto es el grado de confiabilidad, para nuestro caso el α =0.813 para la dimensión Seguridad de la información que consta de 6 ítems por lo cual concluimos que es confiable los resultados obtenidos.

Tabla 11

Confiabilidad cuestionario sobre Gestión de Seguridad de la Información

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,811	8

Cuanto el valor del alfa de cronbach es más cercano al 1, más alto es el grado de confiabilidad, para nuestro caso el α =0.811 para la dimensión Gestión de Seguridad de la información que consta de 8 ítems por lo cual concluimos que son confiable los resultados obtenidos.

Tabla 12

Confiabilidad cuestionario sobre la dimensión Familia de Norma ISO 27000

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,801	2

Cuanto el valor del alfa de cronbach es más cercano al 1, más alto es el grado de confiabilidad, para nuestro caso el α =0.801 para la dimensión Familia de la Norma ISO 27000 que consta de 2 ítems por lo cual concluimos que son confiable los resultados obtenidos.

Tabla 13

Confiabilidad cuestionario sobre Implantación de un Sistema de Gestión de Seguridad de la Información.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,922	18

Como el valor del alfa de cronbach es más cercano a 1, más alto es el grado de confiabilidad, para nuestro caso el α =0.825 para la dimensión Implantación de un Sistema de Gestión de Seguridad de la Información que consta de 18 ítems por lo cual concluimos que son confiables los resultados obtenidos.

Confiabilidad Cuestionario de la variable Proceso de Registros Civiles

Tabla 14

Confiabilidad cuestionario sobre Procesos de Registros Civiles

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,821	9

Como el valor del alfa de cronbach es más cercano a 1, más alto es el grado de confiabilidad, para nuestro caso el α =0.821 para la variable Proceso de Registros Civiles. Reniec. San Borja. Lima. 2016 que consta de 9 ítems por lo cual concluimos que son confiables los resultados obtenidos.

Tabla 15

Confiabilidad cuestionario sobre riesgos que afectan la seguridad de la información del proceso de registros civiles

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,814	7

Como el valor del alfa de cronbach es más cercano a 1, más alto es el grado de confiabilidad, para nuestro caso el α =0.814 para la dimensión Riesgos que afectan la seguridad de la información del proceso de registros civiles de la Información que consta de 7 ítems por lo cual concluimos que son confiables los resultados obtenidos.

Tabla 16

Confiabilidad encuesta sobre confianza del servicio que presta el Reniec.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,820	2

Como el valor del alfa de cronbach es más cercano a 1, más alto es el grado de confiabilidad, para nuestro caso el α =0.820 para la dimensión Riesgos que afectan la seguridad de la información del Proceso de Registros Civiles. Reniec. San Borja. de la Información que consta de 2 ítems por lo cual concluimos que son confiables los resultados obtenidos.

2.9. Aspectos éticos

Se siguieron los siguientes princípios:

Reserva de identidad de los trabajadores

Citas de los textos y documentos consultados

No manipulación de resultado.

.

III. Resultados

3.1. Descripción de los Resultados

Tabla 17

Sistema de Gestión de Seguridad de la Información. San Borja. Lima. 2016

Nivel	Rango	Frecuencia	%	% válido	% Acumulado
Bajo	[34 - 79]	87	72.50%	72.50%	72.50%
Medio	[80 - 125]	32	26.67%	26.67%	99.17%
Alto	[126 - 170]	1	0.83%	0.83%	100.00%
	Total	120	100.00%	100.00%	

Nota: *Cuestionario de Sistema de Gestión de Seguridad de la Información (Anexo 2)*

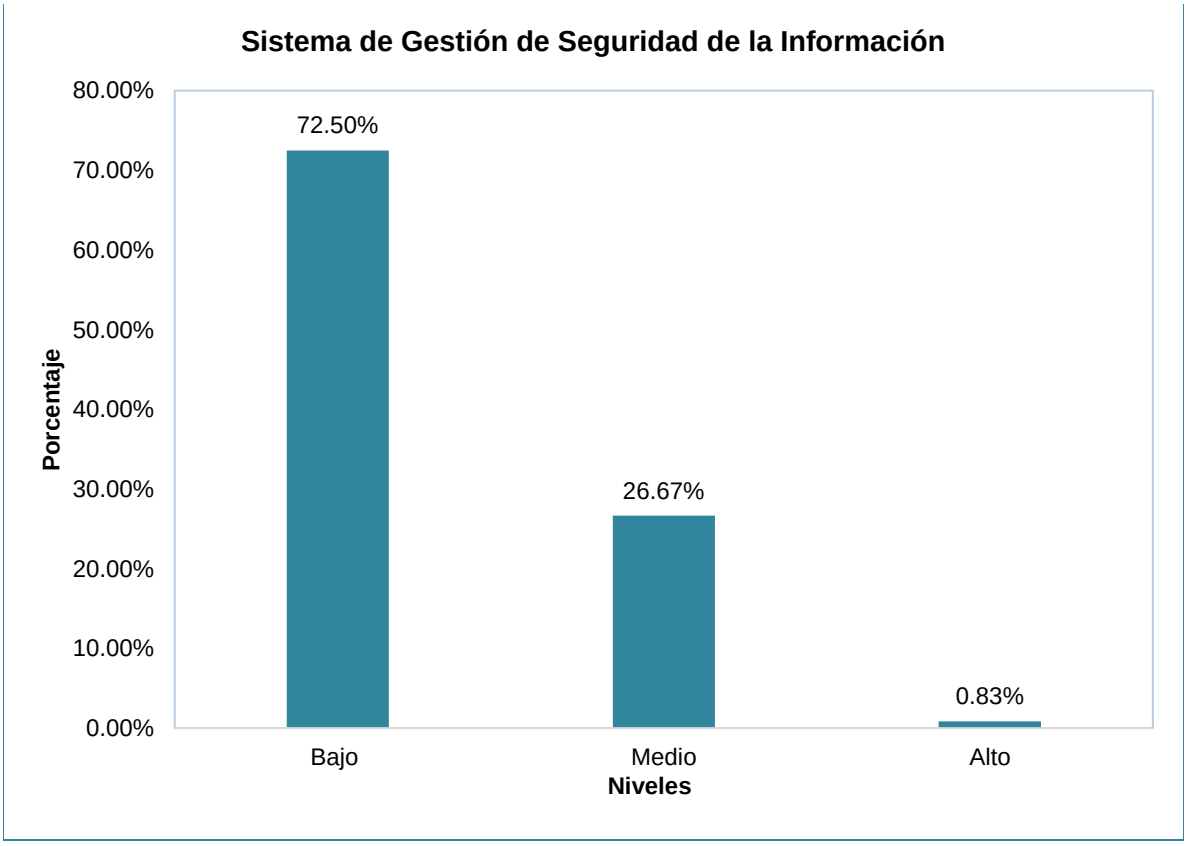


Figura 6. Se ilustra los niveles alcanzados en mérito a las encuestas realizadas en el marco de la variable Sistema de Gestión de Seguridad de la Información.

Interpretación:

Como se observa en la tabla 17 y figura 6; el sistema de gestión de seguridad de la información representa un nivel bajo 72.50% de acuerdo a nuestra valoración los colaboradores se encuentran en acuerdo positivo respecto a la implementación de un SGSI, medio un 26.67% y alto en un 0.83%.

Tabla 18

Proceso de Registros Civiles. Reniec. San Borja. Lima. 2016

Nivel	Rango	Frecuencia	%	% válido	% Acumulado
Aceptable	[9 - 21]	84	70.00%	70.00%	70.00%
Regular	[22 - 33]	35	29.17%	29.17%	99.17%
No Aceptable	[34 - 45]	1	0.83%	0.83%	100.00%
	Total	120	100.00%	100.00%	

Nota: Cuestionario de Sistema de Gestión de Seguridad de la Información (Anexo 2)

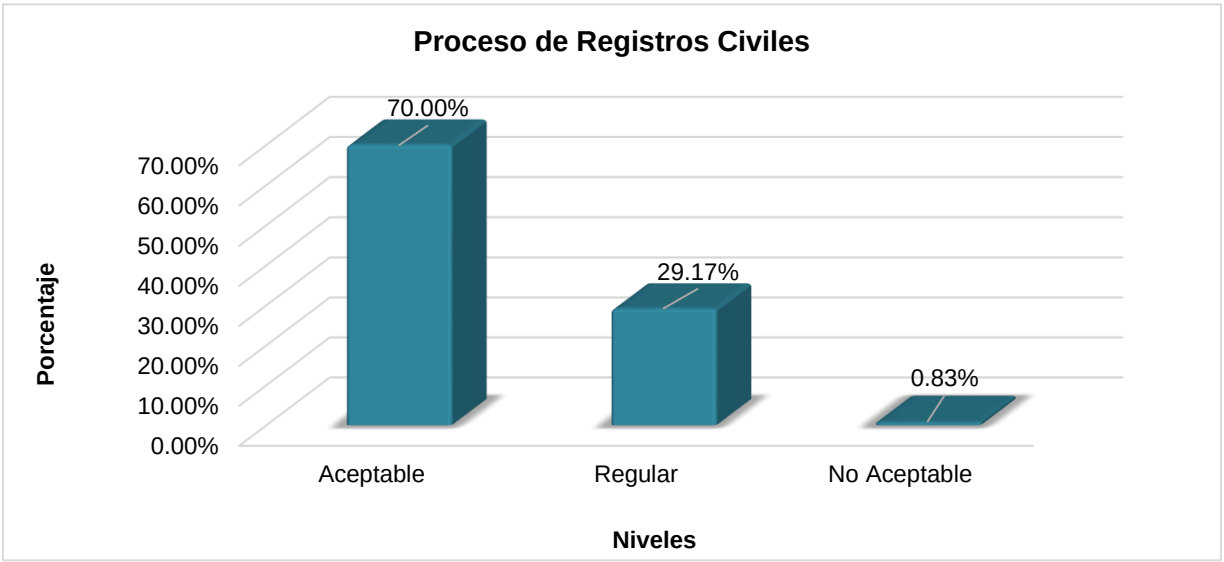


Figura 7: Se ilustra los niveles obtenidos resultado de las encuestas correspondiente a la variable Proceso de Registros Civiles. Reniec. San Borja. Lima. 2016.

Interpretación:

En la tabla 18 y figura 7 se puede visualizar que un 70% de los encuestados acepta la implementación de un SGSI en el Proceso de Registro Civiles, luego un 29.17% considera regular la implementación y por otro lado un 0.83% no acepta dicha implementación.

Tabla 19

Sistema de Gestión de Seguridad de la Información y el proceso de registros civiles. Reniec. San Borja. Lima. 2016.

		Sistema de Gestión de Seguridad de la Información			**Total**
		Alto	**Bajo**	**Medio**	
Proceso de Registros Civiles	Aceptable	0	71	13	84
		0.0%	84.5%	15.5%	100.0%
	No Aceptable	0	1	0	1
		0.0%	100.0%	0.0%	100.0%
	Regular	1	15	19	35
		2.9%	42.9%	54.3%	100.0%
Total		**1**	**87**	**32**	**120**
		.8%	**72.5%**	**26.7%**	**100.0%**

Nota: Cuestionario Sistema de Gestión de Seguridad de la Información y el Proceso de Registros Civiles (Anexo 2)

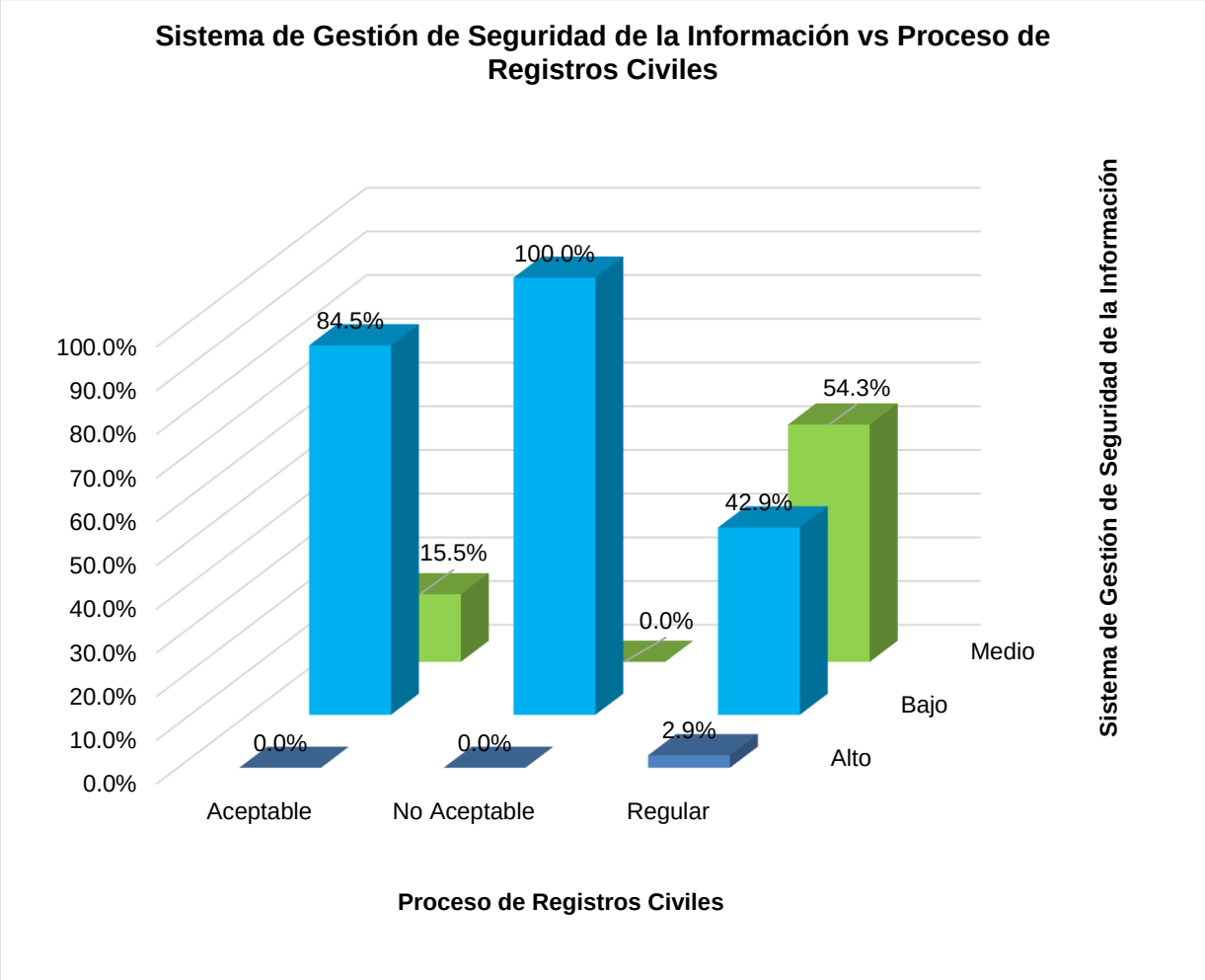


Figura 8: Niveles en columnas 3D de las variables: Sistema de Gestión de Seguridad de la Información y el Proceso de Registros Civiles. Reniec. San Borja. Lima. 2016.

Interpretación:

Como se observa en la tabla 19 y figura N°8, el proceso de registros civiles en un nivel regular 2.9% de los colaboradores percibe un sistema de gestión de seguridad de la información alto, por otro lado en una escala regular el proceso de registros civiles el 54.3% de los colaboradores percibe un SGSI medio, por otro lado en el Proceso de Registros Civiles No Aceptable, un 100% de los trabajadores se encuentra en un nivel bajo.

Tabla 20

Sistema de Gestión de Seguridad de la Información y la dimensión de riesgos que afectan la seguridad de la información del Proceso de Registros Civiles. Reniec. San Borja. Lima. 2016.

		Sistema de Gestión de Seguridad de la Información			Total
		Alto	Bajo	Medio	
Riesgos que afectan la seguridad de la información del proceso de registros civiles	Aceptable	0	73	11	84
		0.0%	86.9%	13.1%	100.0%
	No Aceptable	0	1	0	1
		0.0%	100.0%	0.0%	100.0%
	Regular	1	13	21	35
		2.9%	37.1%	60.0%	100.0%
Total		**1**	**87**	**32**	**120**
		.8%	**72.5%**	**26.7%**	**100.0%**

Nota: Cuestionario Sistema de Gestión de Seguridad de la Información y el Proceso de Registros Civiles (Anexo 2).

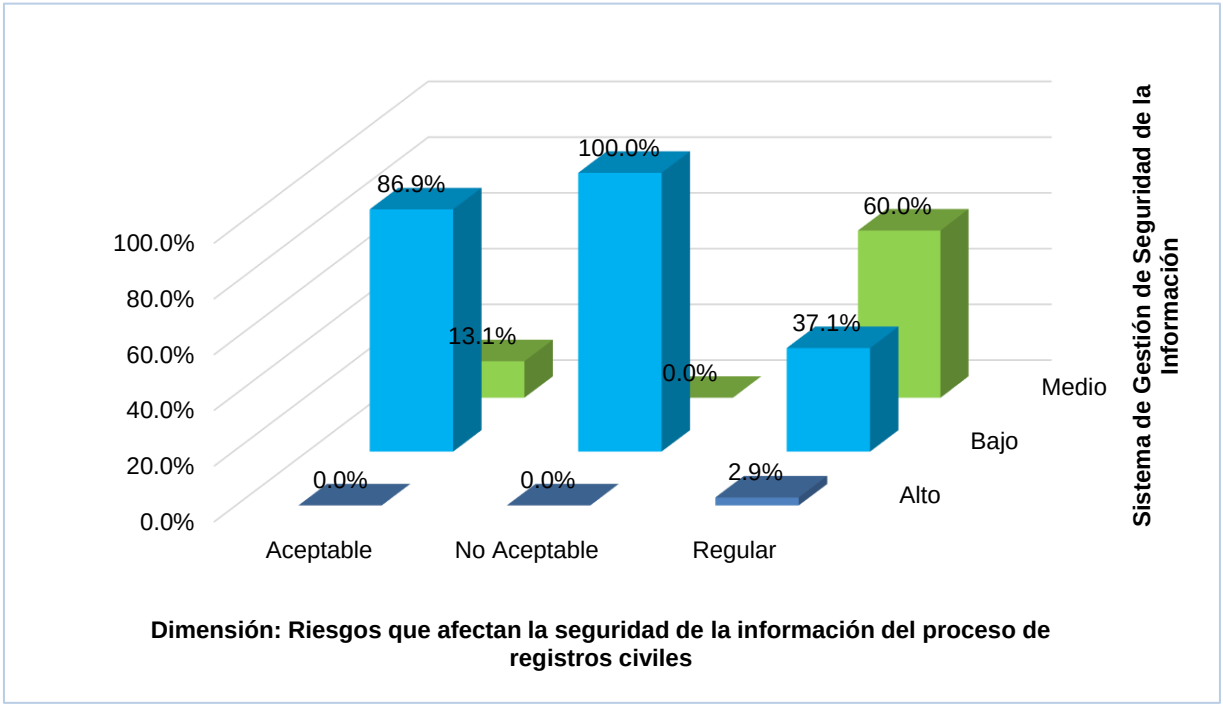


Figura 9. Se ilustra gráfico en columna 3D del Sistema de Sistema de Gestión de Seguridad de la Información y la dimensión Riesgos que afectan la seguridad de la información del Proceso de Registros Civiles. Reniec. San Borja. Lima. 2016.

Interpretación:

Como se observa en la tabla N°20 y figura N°9; la dimensión Riesgos que afectan la seguridad de la información del Proceso de Registros Civiles. Reniec. San Borja. Lima. 2016 en un nivel aceptable el 86.9% de los trabajadores percibe un SGSI baja, por otro lado; la dimensión de Riesgos que afectan la seguridad de la información del Proceso de Registros Civiles en escala regular el 37.1% de los colaboradores percibe un sistema de gestión de seguridad de la información baja.

Tabla 21

Sistema de Gestión de Seguridad de la Información y la dimensión confianza del ciudadano del servicio que presta Reniec. San Borja. Lima. 2016.

		Sistema de Gestión de Seguridad de la Información			**Total**
		Alto	**Bajo**	**Medio**	
Confianza de ciudadano del servicio que presta Reniec	Aceptable	1	77	13	91
		1.1%	84.6%	14.3%	100.0%
	No Aceptable	0	5	11	16
		0.0%	31.3%	68.8%	100.0%
	Regular	0	5	8	13
		0.0%	38.5%	61.5%	100.0%
Total		**1**	**87**	**32**	**120**
		.8%	**72.5%**	**26.7%**	**100.0%**

Nota: Cuestionario Sistema de Gestión de Seguridad de la Información y el Proceso de Registros Civiles (Anexo 2).

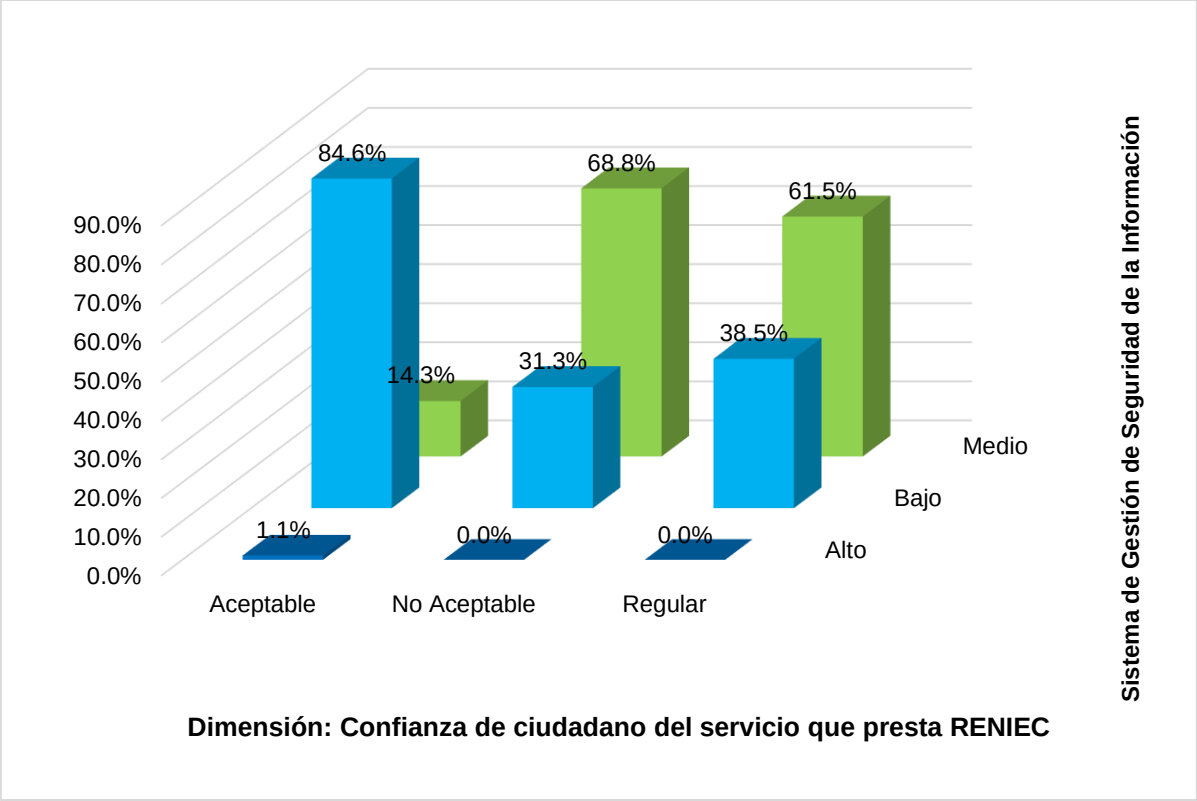


Figura 10. Se ilustra gráfico en columna 3D del Sistema de Sistema de Gestión de Seguridad de la Información y la dimensión Confianza del ciudadano del servicio que presta Reniec.

Interpretación:

Como se observa en la tabla N°21 y figura N°10; la dimensión de confianza del ciudadano del servicio que presta Reniec en un nivel no aceptable 0% de los colaboradores percibe una sistema de gestión de seguridad de la información Alto, por otro lado; la dimensión confianza del ciudadano del servicio que presta Reniec en un nivel regular 61.5% de los colaboradores percibe un sistema de gestión de seguridad de la información medio. En el nivel Aceptable de confianza del ciudadano del servicio que presta Reniec el 84.6% de los colaboradores percibe nivel bajo en cuanto SGSI.

3.2. Prueba de Hipótesis General y Específica

Hipótesis General:

HA: Existe una relación altamente significativa entre el sistema de gestión de seguridad de la información, y el proceso de registros civiles del Reniec.

HO: No existe una relación altamente significativa entre el sistema de gestión de seguridad de la información y el proceso de registros civiles del Reniec.

Para interpretar el coeficiente de correlación utilizamos la siguiente escala:

Valor	Significado
-1	Correlación negativa grande y perfecta
-0,9 a -0,99	Correlación negativa muy alta
-0,7 a -0,89	Correlación negativa alta
-0,4 a -0,69	Correlación negativa moderada
-0,2 a -0,39	Correlación negativa baja
-0,01 a -0,19	Correlación negativa muy baja
0	Correlación nula
0,01 a 0,19	Correlación positiva muy baja
0,2 a 0,39	Correlación positiva baja
0,4 a 0,69	Correlación positiva moderada
0,7 a 0,89	Correlación positiva alta
0,9 a 0,99	Correlación positiva muy alta
1	Correlación positiva grande y perfecta

Tabla 22

Correlación Sistema de Gestión de Seguridad de la Información y el Proceso de Registros Civiles

Correlaciones

			Sistema de Gestión de Seguridad de la Información.	Proceso de Registros Civiles
Rho de Spearman	Sistema de Gestión de Seguridad de la Información.	Coeficiente de correlación	1,000	,781**
		Sig. (bilateral)	.	,000
		N	120	120
	Proceso de Registros Civiles	Coeficiente de correlación	,781**	1,000
		Sig. (bilateral)	,000	.
		N	120	120

**. La correlación es significativa al nivel 0,01 (2 colas/bilateral).

El resultado del coeficiente de correlación Rho Spearman de 0.781 indica que existe relación positiva entre las variables además se encuentra en el nivel de correlación positiva alta y siendo el nivel de significancia bilateral p=0.000<0.01 (altamente significativo), se rechaza la hipótesis nula y se acepta la hipótesis general; se concluye que: La mejora de implantar un Sistema de Gestión de Seguridad de la Información, permitirá mitigar los riesgos de los activos de la información en el Procesos de Registros Civiles del Reniec. San Borja. Lima. 2016.

Hipótesis Específica 1:

HA: Existe una relación altamente significativa entre el Sistema de Gestión de Seguridad de la Información y los riesgos que afectan la seguridad de la información del Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016.

HO: No existe una relación altamente significativa entre el Sistema de Gestión de Seguridad de la información y los riesgos que afectan la seguridad de la información del proceso de registros civiles del Reniec. San Borja. Lima. 2016.

Tabla 23

Correlación Sistema de Gestión de Seguridad de la Información y Riesgos que afectan la seguridad de la Información del Proceso de Registros Civiles

Correlaciones

			Sistema de Gestión de Seguridad de la Información.	Riesgos que afectan la seguridad de la Información del Proceso de Registros Civiles.
Rho de Spearman	Sistema de Gestión de Seguridad de la Información.	Coeficiente de correlación	1,000	,781**
		Sig. (bilateral)	.	,000
		N	120	120
	Riesgos que afectan la seguridad de la Información del Proceso de Registros Civiles.	Coeficiente de correlación	,781**	1,000
		Sig. (bilateral)	,000	.
		N	120	120

**. La correlación es significativa al nivel 0,01 (2 colas/bilateral).

El resultado del coeficiente de correlación Rho Spearman de 0.781 indica que existe relación positiva entre las variables además se encuentra en el nivel de correlación positiva alta y siendo el nivel de significancia bilateral p=0.000<0.01 (altamente significativo), se rechaza la hipótesis nula y se acepta la hipótesis especifica 1; se concluye que: Existe una relación el Sistema de Gestión de Seguridad de la Información y riesgos que afectan la seguridad de la información del proceso de registros civiles del Reniec. San Borja. Lima. 2016.

Hipótesis Específica 2:

HA: Existe una relación positiva moderada entre el Sistema de Gestión de Seguridad de la Información y la confianza del ciudadano del servicio que presta el Reniec.

HO: No existe una relación positiva moderada entre el Sistema de Gestión de Seguridad de la Información y la confianza del ciudadano del servicio que presta Reniec.

Tabla 24

Correlación Sistema de Gestión de Seguridad de la Información y la Confianza de ciudadano del servicio que presta el Reniec

Correlaciones

			Sistema de Gestión de Seguridad de la Información.	Confianza de ciudadano del servicio que presta el Reniec.
Rho de Spearman	Sistema de Gestión de Seguridad de la Información.	Coeficiente de correlación	1,000	,495**
		Sig. (bilateral)	.	,000
		N	120	120
	Confianza de ciudadano del servicio que presta el Reniec.	Coeficiente de correlación	,495**	1,000
		Sig. (bilateral)	,000	.
		N	120	120

**. La correlación es significativa al nivel 0,01 (2 colas/bilateral).

El resultado del coeficiente de correlación Rho Spearman de 0.495 indica que existe relación positiva entre las variables además se encuentra en el nivel de correlación moderada y siendo el nivel de significancia bilateral p=0.000<0.01 (altamente significativo), se rechaza la hipótesis nula y se acepta la hipótesis especifica 2; se concluye que: Existe una relación entre el Sistema de Gestión de Seguridad de la Información y la confianza del ciudadano del servicio que presta el Reniec. San Borja. Lima. 2016.

IV. Discusión

En la Tabla 22, se presentan los resultados para contrastar la hipótesis general: Existe una relación altamente significativa entre el Sistema de Gestión de Seguridad de la Información y el proceso de registros civiles. Se obtuvo un coeficiente de correlación positiva alta, Rho Spearman de 0.781 con una p=0.000<0.01 (altamente significativo)

En la Tabla 23, se presentan los resultados para contrastar la hipótesis específica 1: Existe una relación altamente significativa entre el Sistema de Gestión de Seguridad de la Información y los riesgos que afectan la seguridad de la información del proceso de registros civiles del Reniec. Se obtuvo un coeficiente de correlación positiva alta, Rho Spearman de 0.781 con una p=0.000<0.01 (altamente significativo), este resultado confirma que un Sistema de Gestión de Seguridad de la Información es una herramienta de gestión que nos va a permitir conocer, gestionar y minimizar los riesgos que atenten con la seguridad de la información de nuestra organización. Al identificar los activos de la información tenemos que tener en cuenta que estos pueden proceder de distintas fuentes de información dentro de la organización y que pueden encontrarse en diferentes soportes, como papel o medios digitales.

En ese sentido podemos garantizar la seguridad de toda esta información mediante la implantación de un Sistema de Gestión de Seguridad de la Información, esta metodología nos va a permitir, en primer lugar analizar y ordenar la estructura de los sistemas de información, en segundo lugar nos facilitará la definición de procedimientos de trabajo para mantener la seguridad y por último nos ofrecerá la posibilidad de disponer de controles que permitan medir la eficacia de las medidas tomadas, protegiéndonos de las amenazas y riesgos que sitúen en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal necesarios para alcanzar los objetivos de la organización.

En la Tabla 24, se presentan los resultados para contrastar la hipótesis específica 2: Existe una relación positiva moderada entre el Sistema de Gestión de Seguridad de la Información y la confianza del ciudadano del servicio que presta Reniec. Se obtuvo un coeficiente de correlación positiva moderada, Rho Spearman de 0.495 con una p=0.000<0.01 (altamente significativo).

V. Conclusiones

Primera: En cuanto al objetivo general, la presente investigación demuestra que el Sistema de Gestión de Seguridad de la Información se relaciona de forma altamente significativa con el Proceso de Registros Civiles. Reniec. San Borja. Lima. 2016; siendo que el coeficiente de correlación Rho de Spearman de 0.781, representó una correspondencia positiva alta entre las variables.

Segunda: En cuanto al objetivo 1, la presente investigación demuestra que el Sistema de Gestión de Seguridad de la Información se relaciona de manera altamente significativamente con la dimensión Riesgos que afectan la seguridad de la información del proceso de registros civiles. Reniec. San Borja. Lima. 2016; siendo que el coeficiente de correlación Rho de Spearman de 0.781 representó afinidad positiva alta entre las variables.

Tercera: En cuanto al objetivo 2, la presente investigación demuestra que el Sistema de Gestión de Seguridad de la Información con la dimensión de confianza de ciudadano del servicio que presta Reniec se relacionan de una forma positiva alta moderada; siendo que el coeficiente de correlación Rho de Spearman de 0.495, representó una moderada asociación entre las variables.

Cuarta: El Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016; si bien cuenta con procedimientos sobre seguridad informática, no cuenta con un Sistema de Gestión de Seguridad de la Información que resguarde los activos de la información de acuerdo a los requisitos que exige la Norma ISO 27001:2013.

Quinta: Se realizó una encuesta para determinar cómo se encuentra la seguridad de la información en función a los objetivos definidos, aplicando un cuestionario estructurado con preguntas que cubren todos los aspectos

de riesgos y vulnerabilidades, incluso amenazas que puedan afectar a los tres pilares de seguridad de la información: confidencialidad, integridad y disponibilidad de la información en el marco de la ISO 27001:2013, se realizó a 120 colaboradores del Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016, contiene 43 ítems, se utilizó el Alfa de Cronbach para determinar la validez del instrumento, lo que permitió trabajar con información de alta confiabilidad debido a que el resultado fue 0, 872.

Sexta: Se realizó un levantamiento de información de acuerdo a los requisitos que exige la Norma ISO 27001:2013, 10 cláusulas, se identificó los activos de la información asociados a sus riesgos, asimismo se evaluó los controles en el marco del ISO 27002:2005, identificándose la aplicación de 75 controles necesarios para el procesos de registros civiles del Reniec. San Borja, Lima. 2016.

Séptima: Se determinó la factibilidad operativa, técnica y económica para elaborar un diseño de implantación de un Sistema de Seguridad de la Información para el Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016. Asimismo se estableció que el proyecto sea puesto en marcha, considerando la disponibilidad de recursos para su ejecución. Asimismo lograr la sensibilización y compromiso por parte de los colaboradores sobre la seguridad de la información.

Octava: Para la implantación de un Sistema de Gestión de Seguridad de la Información se diseñó un modelo bajo la estrategia de la mejora continua de la calidad llamado el ciclo de Deming, también conocido como el PDCA acrónimo de Plan, Do Check, Act (planificar, hacer, verificar, actuar).

VI. Recomendaciones

Primera: Se recomienda aplicar el presente trabajo de investigación, para realizar la implementación del Sistema de Gestión de Seguridad de la Información para el Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016, para garantizar la seguridad de toda la información protegiéndola de las amenazas y riesgos que sitúen en peligro la integridad, disponibilidad y confiabilidad de la información, en cumpliendo con los objetivos estratégicos de la institución.

Segunda: Se recomienda la aplicación de la Norma ISO 27001:2013 para la implantación del Sistema de Gestión de Seguridad de la Información del Proceso de Registros Civiles, ya que mediante el cumplimiento de los requisitos que exige se logrará contar con un sistema más robusto que brinde al ciudadano confianza al momento que realice algún trámite.

Tercera: Se recomienda que el Procesos de Registros Civiles una vez implantada el Sistema de Gestión de Seguridad de la Información, bajo la Norma ISO 27001:2013, se certifique lo cual permitirá mantener la sostenibilidad de su implementación.

Cuarta: Se recomienda que los procedimientos sobre seguridad informática que cuenta el Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016; sea integrado dentro del Sistema de Gestión de Seguridad de la Información que se va a implantar.

Quinta: Se recomienda utilizar el método de Alfa de Cronbach para determinar la validez del instrumento para futuras investigaciones referentes a Sistemas de Gestión, lo cual permitirá medir la confiabilidad de la información para los proyectos que se propongan.

Sexta: Se recomienda la revisión semestral de los controles descritos en la Declaración de Aplicabilidad (SOA), mediante la verificación de la

efectividad de los mismos, dichos controles tiene como base los definidos en la Norma ISO 27002:2005

Séptima: Se recomienda implementar un Plan de Sensibilización sobre temas que involucren seguridad de la información y seguridad informática mediante un enfoque integrado, generando concientización sobre la protección de la información en el marco del Sistema de Gestión de Seguridad de la Información.

Octava: Se recomienda utilizar y aplicar la información que se generó para el diseño de la implantación de un Sistema de Gestión de Seguridad de la Información bajo el modelo del PDCA.

VII. Referencias

Acosta, J. (2015). *Perspectivas sobre gobierno, riesgo y cumplimiento: Encuesta Global de Seguridad de la Información*, 5. Lima, Perú: EY Perú Library. Recuperado de: http:// www.ey.com/Publication/vwLUAssets/ Encuesta_global_de_seguridad_de_ informaci%C3%B3n_2014/$FILE/EY-enc.

Baca, G. (2015). *Proyectos de Sistemas de Información*. Recuperado de:http://site.ebrary.com/lib/ bibliotecafmhsp/reader.action?docID=11230894.

Bernal, C. (2006). *Metodología de la Investigación.* D.F, México.: Pearson educación.

Condori Alejo, H. (2012). *Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de Seguridad de la Información para determinar su influencia en la atención del usuario*. (tesis de grado). Universidad Garcilaso de la Vega. Lima, Perú.

Contreras, J. (2104). *Técnicas de recolección de información para un trabajo de investigación*. Recuperado de: http://metodelainv.blogspot.es/

Costas, J. (2014). *Mantenimiento de Seguridad en Sistemas Informáticos*. Recuperado de: http://site.ebrary.com/lib/bibliotecafmhsp/reader.action?docID=11046692.

Fitzgerald, T. (2007). *Information Secutrity Governance*. En H. Tipton, & M. Krause, Information Security Management Handbook. USA: Auerbach Publication.

Gómez, A. y Suarez, C. (2012). *Sistemas de Información* (4a ed.). México: Alfaomega. Global Conferencia on Business and Finance Proceedings. (2014), 9, 1759-1768. Recuperado de: http://www.theibfr.com/ARCHIVE/ISSN-1941-9589-V9-N1-2014.pdf.

Hernández, Fernández y Baptista. (2014). *Metodología de la investigación*. (6a ed.) México: Mc Gram - Hill.

Instituto Nacional de Estadística e Informática [NEI], (2012). *Lineamiento de Política Nacional de Seguridad de la Información en el Estado Peruano*. Recuperado de: http:// hospitalbarranca.gob.pe /estadistica /files / normas/ seguridadinformatica.pd.

ISO/IEC. (2005). ISO 27001:2005. *Tecnología de la Información –Técnicas de seguridad –Sistema de Gestión de seguridad de la información –Requerimientos*. Recuperado de: https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf.

ISO/IEC. (2010). ISO 27003:2010. *Tecnología de la Información – Técnicas de Seguridad –Información de gestión de seguridad de la guía de implementación del sistema*. Recuperado de: http://www.iso.org/iso/catalogue_detail?csnumber=42105.

ISO/IEC. (2012). ISO 27000. *ES El portal de ISO 27001en español* (2012) Recuperado de: http://www.iso27000.es/sgsi.

ISO/IEC. (2013). ISO 27001. *Gestión de Seguridad de la Información*. Recuperado de: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

ISO/IEC. (2013). ISO 27001:2013. *Tecnología de la Información –Técnicas de seguridad – Sistema de gestión de seguridad de la información –Requisitos.* Recuperado de: https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-2:v1: en http://www.iso.org/iso/catalogue_detai.

Joyanes, L. (2015). *Sistemas de Información en la Empresa*. (1a ed.). México: Alfaomega.

Merino y Cañizares. (2011). *Implantación de un Sistema de Gestión de Seguridad de la Información según la ISO 27001*. (1a ed.). Bogotá, Colombia: Ediciones de la U.

Miguel, J.C. (2016). *Protección de datos y seguridad de la información*. (4a ed.). Madrid, España: FC Editorial.

Molina, J. (2000). *Seguridad de la Información* . Recuperado de: http://site.ebrary.com/lib/bibliotecafmhsp/reader.action?docID=10018530.

Oficina Nacional de Gobierno Electrónico e Informática [Ongei], (2016). *Perú Gobierno Electrónico*. Recuperado de: http:// www.ongei.gob.pe /normas/0/ NORMA_0_RESOLUCI%C3%93N%20MINISTERIAL%20N%C2%B0%20129-2012-PCM.pdf.

Oficina Nacional de Gobierno Electrónico e Informática [Ongei], (2016). *Perú Gobierno Electrónico*. Recuperado de: http:// www.ongei.gob.pe/docs/ Aprobacion%20NTP%20ISO%20IEC%2027001 %202014.pdf.

Oficina Nacional de Gobierno Electrónico e Informática [Ongei], (2016). Lima, Perú Gobierno Electrónico. Recuperado de: http://www.ongei.gob.pe/quienes/ongei_ QUIENES.asp.

Revista del laboratorio tecnológico de Uruguay-INN. (2010). *El gobierno de la seguridad de información como instrumento de gestión,* 33-41. Recuperado de: *http://ojs.latu.org.uy/index.php/INNOTEC-Gestion/article/view/9/8.*

Anexos

Anexo 1. Matriz de Consistência

TÍTULO: Sistema de Gestión de Seguridad de la Información en el Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016
AUTOR: Br. NATIVIDAD GLADYS BERNALDO BASTIDAS.

<table>
<tr><th>PROBLEMA</th><th>OBJETIVOS</th><th>HIPÓTESIS</th><th colspan="4">VARIABLES E INDICADORES</th></tr>
<tr><td rowspan="2">PROBLEMA PRINCIPAL

¿Qué relación existe entre el Sistema de Gestión de Seguridad de la Información y el Proceso de Registros Civiles del Reniec?

PROBLEMAS ESPECÍFICOS

¿Qué relación existe entre el Sistema de Gestión de Seguridad de la Información y los riesgos que afectan la seguridad de la información del proceso de registros civiles del Reniec?

¿Qué relación existe entre el Sistema de Gestión de Seguridad de la Información y la confianza del ciudadano del servicio que presta Reniec?</td><td rowspan="2">OBJETIVO GENERAL

Determinar la relación que existe entre el Sistema de Gestión de Seguridad de la Información y el Proceso de Registros Civiles del Reniec.

OBJETIVOS ESPECÍFICOS

Determinar la relación que existe entre el Sistema de Gestión de Seguridad de la Información y riesgos que afectan la seguridad de la información del proceso de registros civiles del Reniec.

Determinar la relación que existe entre el Sistema de Gestión de Seguridad de la información y la confianza del ciudadano del servicio que presta Reniec.</td><td rowspan="2">HIPÓTESIS GENERAL

Existe una relación significacentre el Sistema de Gestión de Seguridad de la Información, y el Procesos de Registros Civiles del Reniec. San Borja. Lima. 2016.

HIPÓTESIS ESPECÍFICAS

Existe una relación entre el Sistema de Gestión de Seguridad de la Información y riesgos que afectan la seguridad de la información del proceso de registros civiles del Reniec. San Borja. Lima. 2016.

Existe una relación entre el Sistema de Gestión de Seguridad de la Información y la confianza del ciudadano del servicio que presta Reniec.</td><td colspan="4">Variable 1: Sistema de Gestión de Seguridad de la Información</td></tr>
<tr><td>Dimensiones</td><td>Indicadores</td><td>Ítems</td><td>Niveles o rangos</td></tr>
<tr><td></td><td></td><td></td><td>Seguridad de la Información</td><td>Confidencialidad de la Información
Integridad de la Información
Disponibilidad de la Información</td><td>1-6</td><td rowspan="4">Bajo [34 - 79]
Medio [80 - 125]
Alto [126 - 170]</td></tr>
<tr><td></td><td></td><td></td><td>Gestión de Seguridad de la Información.</td><td>Sistemas de Gestión Modelo PDCA
Sistemas de Gestión de Seguridad de la Información- Modelo PDCA
Evaluación y medición de la seguridad de la información</td><td>7-14</td></tr>
<tr><td></td><td></td><td></td><td>Familia de Norma ISO 27000</td><td>Formación y Capacitación en ISO 27001:2013</td><td>15-16</td></tr>
<tr><td></td><td></td><td></td><td>Implantación de un Sistema de Gestión de Seguridad de la Información.</td><td>Planificación del proyecto
Análisis de situación respecto a la norma
Política de Seguridad
Enfoque para la evaluación de Riesgos
Análisis de riesgos
Gestión de riesgos
Plan de Tratamiento de Riesgos
Sistema de Métricas
Elaboración de cuerpo documental
Formación y Concienciación
Responsabilidad de la Gerencia
Monitorización y revisión</td><td>17-34</td></tr>
</table>

<table>
<tr><td rowspan="4"></td><td rowspan="4"></td><td rowspan="4"></td><td></td><td>Auditorías Internas del SGSI
Mantenimiento y mejora</td><td></td><td></td></tr>
<tr><td colspan="4">Variable 2: Proceso de Registros Civiles</td></tr>
<tr><td>Dimensiones</td><td>Indicadores</td><td>Ítems</td><td>Niveles o rangos</td></tr>
<tr><td>Riesgos que afectan la seguridad de la información del proceso de registros civiles</td><td>Brechas de seguridad de la información en el proceso de registros civiles.</td><td>1-7</td><td rowspan="2">Aceptable [9 - 21]
Regular [22 - 33]
No Aceptable [34 - 45]</td></tr>
<tr><td>Confianza de ciudadano del servicio que presta RENIEC</td><td>Mejorar la disponibilidad y tiempo de respuesta de los servicios finales a los ciudadanos.</td><td>8-9</td></tr>
<tr><td>TIPO Y DISEÑO DE INVESTIGACIÓN</td><td>POBLACION Y MUESTRA</td><td>TECNICA E INSTRUMENTOS</td><td colspan="4">ESTADISTICA DESCRIPTIVA E INFERENCIAL</td></tr>
<tr><td>TIPO:
APLICADA
Esta investigación es aplicada, según Landeau Rebeca (2007, p.56) porque tiene como finalidad plantear la resolución a problemas prácticos, además que el aporte de conocimiento teórico es secundario.

DESCRIPTIVA
Es descriptiva porque tiene por objetivo analizar como es y se manifiesta un fenómeno y sus componentes, utiliza métodos descriptivos como la observación, estudios correlacionales, etc. Hernández, R, Fernández (2010 p, 103), sostiene que “la investigación descriptiva busca especificar</td><td>Reniec. SAN BORJA. LIMA.2016.

La población es de 175 colaboradores del Reniec.

Para está investigación se utilizará una muestra probabilística estratificada, cuyas unidades de análisis o elementos muestrales se elegirán aleatoriamente, del cálculo realizado se obtuvo que la muestra de 120 colaboradores.</td><td>VARIABLE:
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

INSTRUMENTO:
CUESTIONARIO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

AUTOR: CONDORI, ALEJO, 2012

ADAPTADO: NATIVIDAD BERNALDO BASTIDAS

MONITOREO: AGOSTO 2016.

ÁMBITO DE APLICACIÓN:
Reniec.
FORMA DE ADMINISTRACIÓN:
DIRECTA.

VARIABLE:
PROCESO DE REGISTROS CIVILES</td><td colspan="4">DESCRIPTIVA:
Tablas de contingencia, Figuras

Coeficiente de Correlación de Spearman: En estadística, el coeficiente de correlación de Spearman, ρ es una medida de la correlación (la asociación o interdependencia) entre dos variables aleatorias continuas. Para calcular “ρ”, los datos son ordenados y reemplazados por su respectivo orden.

$$\rho = 1 - \frac{6 \sum \mathrm{d}^2}{\mathrm{n}\,(\mathrm{n}^2 - 1)}$$

ρ = rs
Dónde:
ρ = Coeficiente de correlación por rangos de Spearman
∑= Diferencia entre los rangos
d = Diferencia entre los correspondientes estadísticos.
n = Número de parejas

Nivel de Significación:

Si p < 0.05 ⇒ Existe relación entre las variables</td></tr>
</table>

propiedades, características y rasgos importantes de cualquier fenómeno que se analice. **CUANTITATIVA** Es cuantitativa porque utiliza la metodología empírico analítico y se sirve de pruebas estadísticas para el análisis de datos. **NIVEL:** **CORRELACIONAL** **DISEÑO:** NO EXPERIMENTAL Según Hernández (2010), el diseño se refiere al plan o estrategia concebida para obtener la información deseada. La investigación se realizó bajo el diseño no experimental, descriptivo correlacional, Mertens (2005) citado en Hernández (2010) señala que la investigación no experimental es apropiada para variables que no pueden o deben ser manipuladas o resulta complicado hacerlo, por lo tanto una vez recopilada la data se determinó la relación que existió entre ambas.		**INSTRUMENTO**: CUESTIONARIO PROCESO DE REGISTROS CIVILES. **AUTOR**: CONDORI, ALEJO, 2012 **ADAPTADO:** NATIVIDAD BERNALDO BASTIDAS **MONITOREADO: AGOSTO** 2016. **ÁMBITO DE APLICACIÓN:** Reniec. F**ORMA DE ADMINISTRACIÓN:** DIRECTA	Si p> 0.05 ⇒ No existe relación entre las variables

Anexo 2. Instrumento de Sistema de Gestión de Seguridad de la Información

INSTRUCCIONES: Estimado colaborador, la presente encuesta tiene el propósito de recopilar información sobre el Sistema de Gestión de Seguridad de la Información*, en la institución.* Le agradeceremos leer atentamente y marcar con un **(X)** la opción correspondiente a la información solicitada, la presente es **totalmente anónima** y su procesamiento es reservado, por lo que le pedimos sinceridad en su respuesta, En beneficio de la mejora de las políticas de gestión institucional.

N°	Preguntas
1	¿La institución ha implementado lineamientos, normas y/o estándares para proteger la información personal y privada de los ciudadanos que utilicen sus servicios?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
2	¿La institución ha implementado lineamientos, normas y/o estándares para proteger la información privada de las entidades que utilicen sus servicios?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☑ En desacuerdo ☑ Totalmente en desacuerdo
3	¿La institución ha implementado lineamientos contra modificación o pérdida accidental de información?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☑ En desacuerdo ☐ Totalmente en desacuerdo
4	¿La institución ha implementado lineamientos, normas y/o estándares para recuperar información en caso de modificación o pérdida intencional o accidental?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
5	¿La institución verifica que los lineamientos, normas y/o estándares orientados a la continuidad en la prestación de los servicios se cumplan?
	☐ Totalmente de acuerdo ☐ De acuerdo ☑ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
6	¿La institución ha implementado mecanismos para que los servicios de Gobierno en línea tengan altos índices de disponibilidad?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
7	¿Los sistemas de gestión que ha implementado la institución han permitido alcanzar los objetivos iinstitucionales y la satisfacción de los grupos de interes?
	☑ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
8	¿Considera que los sistemas de gestión que se han implantado en el proceso de registros civiles, utilizan la estrategía de la mejora continua (ciclo de deming)?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo

9	¿Considera que la implantación de un sistema de gestión de seguridad de la información se basen en el modelo del PDCA (ciclo deming)?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
10	¿Considera usted que al implementar un Sistema de Gestión de Seguridad de la Información va ayudar a gestionar la información y los recursos informáticos de manera óptima y segura?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
11	¿Considera que aplicando el criterio de la Norma ISO 27001:2013, se va a garantizar los niveles de integridad, confidencialidad y disponibilidad de la información?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
12	¿Cree usted que por medio de políticas de seguridad es posible garantizar la seguridad de la información conforme a los requisitos de nuestros grupos de intereses?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
13	¿Cree usted que es necesario que la organización efectúe el análisis y diseño de un SGSI, para preservar los activos informáticos?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
14	¿Considera que al implementarse indicadores de seguridad de la información van a contribuir en la medición del desempeño del proceso de registros civiles?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
15	¿La institución lo ha capacitado o formado frecuentemente con relación a la familia de la Norma ISO 27000?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
16	¿Estaría de acuerdo que su institución lo capacite con relación a la Norma ISO 27001:2013, con la finalidad de que conosca los requisitos que comprende; y así usted pueda aplicarlo en el desarrollo de sus actividades?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
17	¿Considera que debe participar en el proceso de implantación de un sistema de gestión de seguridad de la información?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
18	En general mi institución está preparada para implementar la seguridad en sistemas de información?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo

19	¿Conoce la Politica y objetivos de seguridad de la información?				
	☐ Totalmente de acuerdo	☐ De acuerdo	☐ No sabe/No Opina	☐ En desacuerdo	☐ Totalmente en desacuerdo
20	¿La insitución aplica diferentes mecanismos de difusión sobre la política y objetivos de seguridad de la información?				
	☑ Totalmente de acuerdo	☐ De acuerdo	☐ No sabe/No Opina	☐ En desacuerdo	☐ Totalmente en desacuerdo
21	¿Conoce que riesgos pueden ocurrir durante el desarrollo de su trabajo en el marco de seguridad de la información?				
	☐ Totalmente de acuerdo	☐ De acuerdo	☐ No sabe/No Opina	☐ En desacuerdo	☐ Totalmente en desacuerdo
22	¿Cree usted que debe realizarse un análisis de riesgos, a fin de evitar que afecten la seguridad de la información en el desarrollo de sus actividades?				
	☐ Totalmente de acuerdo	☐ De acuerdo	☐ No sabe/No Opina	☐ En desacuerdo	☐ Totalmente en desacuerdo
23	¿Considera, que a fin de evitar amenazas y vulnerabilidades, deben existir lineamientos para tratar los riesgos que afecten a los activos de la institución ?				
	☐ Totalmente de acuerdo	☐ De acuerdo	☐ No sabe/No Opina	☐ En desacuerdo	☐ Totalmente en desacuerdo
24	¿Cree usted que la institución dispone de recursos para implantar un plan de tratamiento de riesgos de seguridad de la información, en caso se implante el sistema de gestión de seguridad de la información en el proceso de registros civiles?				
	☐ Totalmente de acuerdo	☐ De acuerdo	☐ No sabe/No Opina	☐ En desacuerdo	☐ Totalmente en desacuerdo
25	¿Cree que el uso de indicadores ayuden a medir el desempeño de un Sistema de Gestión de Seguridad de la Información?				
	☐ Totalmente de acuerdo	☐ De acuerdo	☐ No sabe/No Opina	☐ En desacuerdo	☐ Totalmente en desacuerdo
26	¿Considera que la implementación de la Declaración de Aplicabilidad en el marco de seguridad de la información contribuye verificar los controles de seguridad de la información en el proceso de registros civiles				
	☐ Totalmente de acuerdo	☐ De acuerdo	☐ No sabe/No Opina	☐ En desacuerdo	☐ Totalmente en desacuerdo
27	¿Ha recibido por parte de su institución capacitaciones con relación a la intepretación de la Norma ISO 27001:2013				
	☐ Totalmente de acuerdo	☐ De acuerdo	☐ No sabe/No Opina	☐ En desacuerdo	☐ Totalmente en desacuerdo

28	¿Ha recibido capacitación útil por parte del área de sistemas de como proteger su información?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
29	¿En su institución se implementan talleres de formación y entrenamiento en temas de seguridad y protección de la información?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
30	¿Siente que existe el compromiso de la Alta Dirección para implantar un sistena de gestión de seguridad de la información en el proceso de registros civiles?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
31	¿Cree usted que es importante contar con controles que garanticen la seguridad de la información en el proceso de registros civiles?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
32	¿Considera usted, que para medir el desempeño de un Sistema de Gestión de Seguridad de la Información se deben llevar auditorias internas y externas que permitan verificar el cumplimiento de los requisitos de la Norma ISO 27001:2013?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
33	¿Tengo suficientes conocimientos para adaptarme a la implantación de un Sistema de Gestión de Seguridad de la Información?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
34	¿Tengo suficientes habilidades y competencias para adaptarme a la implantación del Sistema de Gestión de Seguridad de la Información?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo

Instrumento Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016

INSTRUCCIONES: Estimado colaborador, la presente encuesta tiene el propósito de recopilar información sobre el Proceso de Registros Civiles*, en la institución.* Le agradeceremos leer atentamente y marcar con un **(X)** la opción correspondiente a la información solicitada, la presente es **totalmente anónima** y su procesamiento es reservado, por lo que le pedimos sinceridad en su respuesta, En beneficio de la mejora de las políticas de gestión institucional.

N°	Preguntas
1	¿Considera que la Seguridad de la información en su trabajo que desarrolla es importante y debe tomarse las medidas adecuadas de protección?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
2	¿Siente que podría ocurrir que un virus informático ocasione pérdida o deterioro de su información que retrase o perjudique su trabajo por lo que se debe proteger la información ?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☑ Totalmente en desacuerdo
3	¿Siente que un fallo eléctrico ocasione la pérdida o deterioro de su información que retrase o perjudique su trabajo por lo que se debe proteger la información?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
4	¿Siente que podría ocurrir que un robo ocasione pérdida o deterioro de su información que retrasaría o perjudicaría su trabajo por lo que se debe proteger la información?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
5	¿Es importante cambiar las contraseñas de acceso al sistema frecuentemente?
	☐ Totalmente de acuerdo ☐ De acuerdo ☑ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
6	¿Es importante no compartir su computador, contraseñas del sistema con otras personas?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
7	¿Realiza frecuentemente copias de su información?
	☑ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
8	¿La implantación de un Sistema de Gestión de Seguridad de la Información en el Proceso de Registros Civiles, contribuirá en aumentar el grado de confianza del ciudadano sobre los servicios que se presta?
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo
9	¿Considera usted, que debe aplicarse la implantación del SGSI para toda la institución?.
	☐ Totalmente de acuerdo ☐ De acuerdo ☐ No sabe/No Opina ☐ En desacuerdo ☐ Totalmente en desacuerdo

Anexo 3. Validación de cuestionario de juicio de expertos

VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Apellidos y Nombres del Experto: Dra. Boy Barreto, Ana Maritza

1.2 Cargo e Institución donde labora: Docente Universitaria

1.3 Nombre del instrumento motivo de Evaluación:.....

1.4 Autor del Instrumento: Natividad Gladys Bernabé Bautista

INDICADORES	CRITERIOS	Deficiente 0 –20 %	Regular 21– 40 %	Bueno 41–60 %	Muy bueno 61–80 %	Excelente 81–100 %
1. CLARIDAD	Esta formulada con lenguaje apropiado			X		
2. OBJETIVIDAD	Esta expresado en conductas observables			X		
3. ACTUALIDAD	Adecuado el alcance de ciencia y tecnología			X		
4. ORGANIZACIÓN	Existe una organización lógica			X		
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad			X		

6. INTENCIONALIDAD	Adecuado para valorar aspectos del sistema de evaluación y desarrollo de capacidades cognoscitivas			✓		
7. CONSISTENCIA	Basados en aspectos Teóricos – científicos de la Tecnología Educativa			✓		
8. COHERENCIA	Entre los indices, indicadores y las dimensiones			✓		
9. METODOLOGIA	La estrategia responde al propósito del diagnostico.			✓		

II. OPINIÓN DE APLICABILIDAD: El instrumento es aplicable para poder aplicar la Prueba Piloto.

III. PROMEDIO DE VALORACIÓN: 60%

Lima, 02 de Noviembre del 2016

VALIDACIÓN DEL INSTRUMENTO

ITEMS	PREGUNTA	APRECIACIÓN		OBSERVACIONES
		SI	NO	
1	¿El instrumento responde al planteamiento del problema?	X		
2	¿El instrumento responde a los objetivos del problema?	X		
3	¿Las dimensiones que se han tomado en cuenta son adecuadas para la realización del instrumento?	X		
4	¿El instrumento responde a la operacionalización de las variables?	X		
5	¿La estructura que presenta el instrumento es de forma clara y precisa?	X		
6	¿Los ítems están redactados en forma clara y precisa?	X		
7	¿El número de ítems es el adecuado?	X		
8	¿Los ítems del instrumento son válidos?	X		
9	¿Se debe incrementar el número de ítems?		X	
10	¿Se debe eliminar algunos ítems?		X	

Aportes y/o sugerencias:

.....

.....

.....

.....

Nombre y Firma

Fecha: 02 / Nov / 16

VALIDACIÓN DE EXPERTOS

I. DATOS GENERALES

Nombre: Ana Maritza Borja Acosta

Especialidad: Estudiante de la Investigación

Fecha: .....

II. OBSERVACIONES EN CUENTA A:

1. FORMA:

.....

.....

.....

.....

2. CONTENIDO:

Se adecua al contenido coincidente en la investigación

3. ESTRUCTURA:

Se adapta a la estructura del esquema de la UEV

III. APORTES Y/O SUGERENCIAS:

El instrumento es aplicable

.....

.....

Luego, de revisado el documento procede a su aprobación.

SI [X] [ ]

Nombre y Firma

0676650+

Anexo 4. Base de Datos

Variable 1: Sistema de Gestión de Seguridad de la Información																																		
N°	Seguridad de la Información						Gestión de Seguridad de la Información								Familia de Norma ISO 27000		Implantación de un Sistema de Gestión de Seguridad de la Información																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
1	1	1	1	2	1	3	1	1	1	2	1	3	2	1	1	1	3	1	2	1	3	3	1	2	1	2	1	2	1	1	1	1	2	1
2	4	4	3	1	4	2	4	4	3	1	4	2	5	3	1	1	2	1	3	1	1	2	3	3	1	5	3	2	1	4	4	3	1	4
3	1	1	4	3	2	1	1	1	4	3	2	1	1	1	1	1	4	4	2	1	4	1	2	1	1	5	4	2	1	1	1	4	3	2
4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	1	1	1	2	1	1	1	1	2	1	2	1	1	1	1	1	1
5	1	1	2	1	2	2	1	1	2	1	2	2	1	2	1	1	1	1	2	2	1	1	1	1	1	1	2	1	1	1	1	2	1	2
6	2	2	3	2	2	3	2	2	3	2	2	3	4	2	1	1	2	3	5	3	5	4	5	4	2	3	1	2	5	2	2	3	2	2
7	1	1	1	2	1	1	1	1	1	2	1	1	1	1	1	1	1	2	1	2	1	1	2	2	1	1	1	1	2	1	1	1	2	1
8	2	2	2	1	2	3	2	2	2	1	2	3	2	1	2	2	5	3	1	3	3	1	4	5	5	1	4	3	4	2	2	2	1	2
9	2	2	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	1	2	1	1	2	1	2	2	2	1	1	1	2	2	1	1	1
10	2	2	3	4	1	4	2	2	3	4	1	4	2	4	4	5	3	2	3	2	1	3	1	2	3	2	2	2	3	2	2	3	4	1
11	1	1	1	2	2	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	2	1	2	1	1	1	1	2	1	1	1	1	2	2
12	1	1	1	1	1	1	1	1	1	1	1	1	3	2	2	3	2	2	2	4	2	2	2	2	2	5	2	1	1	1	1	1	1	1
13	1	1	2	2	4	4	1	1	2	2	4	4	1	2	5	4	1	1	2	5	1	2	4	3	1	5	5	2	3	1	1	2	2	4
14	4	1	1	1	3	1	4	1	1	1	3	1	4	2	3	1	1	2	1	5	3	4	1	2	2	3	3	2	1	4	1	1	1	3
15	5	3	1	2	2	2	5	3	1	2	2	2	3	2	1	1	1	2	2	1	1	1	1	1	1	1	1	2	2	5	3	1	2	2
16	1	2	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	2	1	1	2	2	2	1	2	1	1	2	1	2	1	1	1
17	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	2	1	1	2	1	1	1	2	2	1	1	1	1	1
18	4	2	2	3	2	4	4	2	2	3	2	4	1	1	1	1	1	1	3	3	3	3	1	1	2	2	3	1	4	4	2	2	3	2
19	3	5	5	5	1	4	3	5	5	5	1	4	2	4	5	5	4	4	1	5	2	1	2	2	2	1	1	5	3	3	5	5	5	1
20	1	1	3	3	1	5	1	1	3	3	1	5	1	3	2	2	2	5	1	3	1	2	2	1	4	1	2	3	4	1	1	3	3	1
21	2	2	2	1	1	3	2	2	2	1	1	3	1	3	4	5	3	4	1	3	1	1	1	1	1	3	1	1	2	2	2	2	1	1
22	3	4	4	2	2	4	3	4	4	2	2	4	4	1	5	5	4	1	1	4	1	3	1	3	1	2	2	4	1	3	4	4	2	2
23	1	2	1	1	2	4	1	2	1	1	2	4	5	3	1	5	4	4	1	2	2	3	2	2	2	2	5	2	1	1	2	1	1	2
24	2	1	1	1	1	1	2	1	1	2	1	1	2	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	2	1	1	2	1
25	2	2	1	2	1	1	2	2	1	2	1	1	1	1	2	1	1	2	1	1	1	1	1	1	1	1	2	2	2	2	2	1	2	1
26	2	2	1	1	2	1	2	2	1	1	2	1	1	2	2	2	1	2	1	1	1	2	1	1	2	1	1	1	1	2	2	1	1	2
27	4	1	2	1	4	3	4	1	2	1	4	3	1	1	1	1	1	1	1	1	3	1	3	4	2	3	1	3	3	4	1	2	1	4
28	4	4	1	3	3	2	4	4	1	3	3	2	3	1	1	2	1	3	4	3	4	4	1	3	1	3	2	2	1	4	4	1	3	3
29	1	1	1	2	1	3	1	1	1	2	1	3	2	1	1	2	3	1	2	1	3	3	1	2	1	2	1	2	1	1	1	1	2	1
30	4	4	3	1	4	2	4	4	3	1	4	2	1	3	1	1	2	1	3	1	1	2	3	3	1	5	3	2	1	4	4	3	1	4
31	1	1	4	3	2	1	1	1	4	3	2	1	1	1	1	1	4	4	2	1	4	1	2	1	1	5	4	2	1	1	1	4	3	2
32	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	1	1	1	2	1	1	1	1	2	1	2	1	1	1	1	1	1
33	1	1	2	1	2	2	1	1	2	1	2	2	1	2	1	1	1	1	2	2	1	1	1	1	1	1	2	1	1	1	1	2	1	2
34	2	2	3	2	2	3	2	2	3	2	2	3	4	2	1	1	2	3	5	3	5	4	5	4	2	3	1	2	5	2	2	3	2	2
35	1	1	1	2	1	1	1	1	1	2	1	1	1	1	1	1	1	2	1	2	1	1	2	2	1	1	1	1	2	1	1	1	2	1
36	2	2	2	1	2	3	2	2	2	1	2	3	2	1	2	2	5	3	1	3	3	1	4	5	5	1	4	3	4	2	2	2	1	2
37	2	2	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	1	2	1	1	2	1	2	2	2	1	1	1	2	2	1	1	1
38	2	2	3	4	1	4	2	2	3	4	1	4	2	4	5	5	3	2	3	2	1	3	1	2	3	2	2	2	3	2	2	3	4	1
39	1	1	1	2	2	1	1	1	1	2	2	1	1	1	2	2	1	1	1	1	2	1	2	1	1	1	1	2	1	1	1	1	2	2
40	1	1	1	1	1	1	1	1	1	1	1	3	2	2	3	2	2	2	4	2	2	2	2	2	5	2	1	1	1	1	1	1	1	1
41	1	1	2	2	4	4	1	1	2	2	4	4	1	2	2	4	1	1	2	5	1	2	4	3	1	5	5	2	3	1	1	2	2	4
42	4	1	1	1	3	1	4	1	1	1	3	1	4	2	3	4	1	2	1	5	3	4	1	2	2	3	3	2	1	4	1	1	1	3
43	5	3	1	2	2	2	5	3	1	2	2	2	3	2	3	1	1	2	2	1	1	1	1	1	1	1	1	2	2	5	3	1	2	2
44	1	2	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	2	1	1	2	2	2	1	2	1	1	2	1	2	1	1	1
45	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	2	1	1	2	1	1	1	2	2	1	1	1	1	1
46	4	2	2	3	2	4	4	2	2	3	2	4	1	1	1	1	1	1	3	3	3	3	1	1	2	2	3	1	4	4	2	2	3	2
47	3	5	5	5	1	4	3	5	5	5	1	4	2	4	4	5	4	4	1	5	2	1	2	2	2	1	1	5	3	3	5	5	5	1
48	1	1	3	3	1	5	1	1	3	3	1	5	1	3	2	2	2	5	1	3	1	2	2	1	4	1	2	3	4	1	1	3	3	1
49	2	2	2	1	1	3	2	2	2	1	1	3	1	3	5	5	3	4	1	3	1	1	1	1	1	3	1	1	2	2	2	2	1	1
50	3	4	4	2	2	4	3	4	4	2	2	4	4	1	5	5	4	1	1	4	1	3	1	3	1	2	2	4	1	3	4	4	2	2

Variable 1: Sistema de Gestión de Seguridad de la Información																																		
N°	Seguridad de la Información						Gestión de Seguridad de la Información								Familia de Norma ISO 27000		Implantación de un Sistema de Gestión de Seguridad de la Información																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
51	1	2	1	1	2	4	1	2	1	1	2	4	5	3	1	5	4	4	1	2	2	3	2	2	2	2	5	2	1	1	2	1	1	2
52	1	1	1	2	1	1	1	1	1	2	1	1	2	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	2	1	1	2	1
53	1	2	1	2	1	1	1	2	1	2	1	1	1	1	2	1	1	2	1	1	1	1	1	1	1	1	2	2	2	2	2	1	2	1
54	1	2	1	1	2	1	1	2	1	1	2	1	1	2	2	5	1	2	1	1	1	2	1	1	2	1	1	1	1	2	2	1	1	2
55	4	1	2	1	4	3	4	1	2	1	4	3	1	1	1	1	1	1	1	1	3	1	3	4	2	3	1	3	3	4	1	2	1	4
56	4	4	1	3	3	2	4	4	1	3	3	2	3	1	1	2	1	3	4	3	4	4	1	3	1	3	2	2	1	4	4	1	3	3
57	1	1	1	2	1	3	1	1	1	2	1	3	2	1	1	1	3	1	2	1	3	3	1	2	1	2	1	2	1	1	1	1	2	1
58	4	4	3	1	4	2	4	4	3	1	4	2	1	3	1	1	2	1	3	1	1	2	3	3	1	5	3	2	1	4	4	3	1	4
59	1	1	4	3	2	1	1	1	4	3	2	1	1	1	1	1	4	4	2	1	4	1	2	1	1	5	4	2	1	1	1	4	3	2
60	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	1	1	1	2	1	1	1	1	2	1	2	1	1	1	1	1	1
61	1	1	2	1	2	2	1	1	2	1	2	2	1	2	1	1	1	1	2	2	1	1	1	1	1	1	2	1	1	1	1	2	1	2
62	2	2	3	2	2	3	2	2	3	2	2	3	4	2	1	5	2	3	5	3	5	4	5	4	2	3	1	2	5	2	2	3	2	2
63	1	1	1	2	1	1	1	1	1	2	1	1	1	1	1	1	1	2	1	2	1	1	2	2	1	1	1	1	2	1	1	1	2	1
64	1	2	2	1	2	3	1	2	2	1	2	3	2	1	2	2	5	3	1	3	3	1	4	5	5	1	4	3	4	2	2	2	1	2
65	2	2	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	1	2	1	1	2	1	2	2	2	1	1	1	2	2	1	1	1
66	2	2	3	4	1	4	2	2	3	4	1	4	2	4	5	5	3	2	3	2	1	3	1	2	3	2	2	2	3	2	2	3	4	1
67	1	1	1	2	2	1	1	1	1	2	2	1	1	1	2	2	1	1	1	1	2	1	2	1	1	1	1	2	1	1	1	1	2	2
68	1	1	1	1	1	1	1	1	1	1	1	1	3	2	2	3	2	2	2	4	2	2	2	2	2	5	2	1	1	1	1	1	1	1
69	1	1	2	2	4	3	1	1	2	2	4	3	2	2	1	4	1	1	2	3	1	2	4	3	1	3	3	2	3	1	1	2	2	4
70	1	1	1	1	3	1	1	1	1	1	3	1	4	2	3	1	1	2	1	5	3	4	1	2	2	3	3	2	1	4	1	1	1	3
71	5	3	1	2	2	2	5	3	1	2	2	2	3	2	3	1	1	2	2	1	1	1	1	1	1	1	1	2	2	3	3	1	2	2
72	1	2	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	2	1	1	2	2	2	1	2	1	1	2	1	2	1	1	1
73	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	2	1	1	2	1	1	1	2	2	1	1	1	1	1	1
74	4	2	2	3	2	4	4	2	2	3	2	4	1	1	1	1	1	1	3	3	3	3	1	1	2	2	3	1	4	4	2	2	3	2
75	3	5	5	5	4	4	3	5	5	5	1	4	2	4	1	5	4	4	1	5	2	1	2	2	2	1	1	5	3	3	5	5	5	1
76	1	1	3	3	1	5	1	1	3	3	1	5	1	3	2	2	2	5	1	3	1	2	2	1	4	1	2	3	4	1	1	3	3	1
77	1	2	2	1	1	3	1	2	2	1	1	3	1	3	4	5	3	4	1	3	1	1	1	1	1	3	1	1	2	2	2	2	1	1
78	3	4	4	5	2	4	3	4	4	5	2	4	4	5	5	5	4	1	1	4	1	3	1	3	1	2	2	4	1	3	4	4	2	2
79	1	2	1	1	2	4	1	2	1	1	2	4	5	3	1	5	4	4	1	2	2	3	2	2	2	2	5	2	1	1	2	1	1	2
80	1	1	1	2	1	1	1	1	1	2	1	1	2	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	2	1	1	2	1
81	1	2	1	2	1	1	1	2	1	2	1	1	1	1	2	1	1	2	1	1	1	1	1	1	1	1	2	2	2	2	2	1	2	1
82	1	2	1	1	2	1	1	2	1	1	2	1	1	2	1	1	1	2	1	1	1	2	1	1	2	1	1	1	1	2	2	1	1	2
83	4	1	2	1	4	3	4	1	2	1	4	3	1	1	1	1	1	1	1	1	3	1	3	4	2	3	1	3	3	4	1	2	1	4
84	4	4	1	3	3	2	4	4	1	3	3	2	3	1	1	2	1	3	4	3	4	4	1	3	1	3	2	2	1	4	4	1	3	3
85	1	1	1	2	1	3	1	1	1	2	1	3	2	1	1	2	3	1	2	1	3	3	1	2	1	2	1	2	1	1	1	1	2	1
86	4	4	3	1	4	2	4	4	3	1	4	2	1	3	1	1	2	1	3	1	1	2	3	3	1	5	3	2	1	4	4	3	1	4
87	1	1	4	3	2	1	1	1	4	3	2	1	1	1	1	1	4	4	2	1	4	1	2	1	1	5	4	2	1	1	1	4	3	2
88	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	1	1	1	2	1	1	1	1	2	1	2	1	1	1	1	1	1
89	1	1	2	1	2	2	1	1	2	1	2	2	1	2	1	1	1	1	2	2	1	1	1	1	1	2	1	1	1	1	2	1	2	2
90	2	2	3	2	2	3	2	2	3	2	2	3	4	2	5	4	2	3	5	3	5	4	5	4	2	3	1	2	5	2	2	3	2	2
91	1	1	1	2	1	1	1	1	1	2	1	1	1	1	1	1	1	2	1	2	1	1	2	2	1	1	1	1	2	1	1	1	2	1
92	2	2	2	1	2	3	2	2	2	1	2	3	2	1	2	2	5	3	1	3	3	1	4	5	5	1	4	3	4	2	2	2	1	2
93	2	2	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	1	2	1	1	2	1	2	2	2	1	1	1	2	2	1	1	1
94	2	2	3	4	1	4	2	2	3	4	1	4	2	4	2	4	3	2	3	2	1	3	1	2	3	2	2	2	3	2	2	3	4	1
95	1	1	1	2	2	1	1	1	1	2	2	1	1	1	3	4	1	1	1	1	2	1	2	1	1	1	1	2	1	1	1	1	2	2
96	1	1	1	1	1	1	1	1	1	1	1	1	3	2	5	3	2	2	2	4	2	2	2	2	2	5	2	1	1	1	1	1	1	1
97	1	1	2	2	4	1	1	1	2	2	4	1	1	2	1	4	1	1	2	5	1	2	4	3	1	5	5	2	3	1	1	2	2	4
98	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1	1	1	2	1	5	3	4	1	2	2	3	3	2	1	4	1	1	1	3
99	5	3	4	4	5	5	5	3	4	4	5	5	3	2	1	1	1	2	2	1	1	1	1	1	1	1	1	2	2	5	3	1	2	2
100	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	2	2	2	1	2	1	1	2	1	2	1	1	1

Variable 1: Sistema de Gestión de Seguridad de la Información																																		
N°	Seguridad de la Información						Gestión de Seguridad de la Información								Familia de Norma ISO 27000		Implantación de un Sistema de Gestión de Seguridad de la Información																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
111	4	1	2	1	4	3	4	1	2	1	4	3	1	1	1	1	1	1	1	1	3	1	3	4	2	3	1	3	3	4	1	2	1	4
112	4	4	1	3	3	2	4	4	1	3	3	2	4	5	1	2	1	3	4	3	4	4	1	3	1	3	2	2	1	4	4	1	3	3
113	4	1	3	3	1	5	4	1	3	3	1	5	1	3	2	2	2	5	1	3	1	2	2	1	4	1	2	3	4	1	1	3	3	1
114	1	2	2	1	1	3	2	2	2	1	1	3	1	3	4	5	3	4	1	3	1	1	1	1	1	3	1	1	2	2	2	2	1	1
115	4	4	4	2	5	4	4	4	4	2	2	4	4	5	5	5	4	1	1	4	1	3	1	3	1	2	2	4	1	3	4	4	2	2
116	1	2	1	1	2	4	1	2	1	1	2	4	1	3	1	1	4	4	1	2	2	3	2	2	2	2	5	2	1	1	2	1	1	2
117	1	1	1	1	2	1	2	1	1	2	1	1	1	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	2	1	1	2	1
118	1	2	1	2	1	1	1	2	3	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	2	2	2	2	2	1	2	1
119	2	2	1	1	2	1	2	2	1	1	2	1	1	1	1	1	1	2	1	1	1	2	1	1	2	1	1	1	1	2	2	1	1	2
120	1	1	2	1	1	3	5	1	2	1	4	3	1	1	1	1	1	1	1	1	3	1	3	4	2	3	1	3	3	4	1	2	1	4

Variable 2: Proceso de Registros Civiles									
N°	Riesgos que afectan la seguridad de la información del proceso de registros civiles							Confianza de ciudadano del servicio que presta RENIEC	
	35	36	37	38	39	40	41	42	43
1	3	2	1	1	2	3	1	1	2
2	2	1	3	1	1	2	1	3	4
3	1	1	1	1	1	4	4	1	2
4	1	1	1	2	2	2	1	1	1
5	2	1	2	1	1	1	1	2	3
6	3	4	2	1	5	2	3	4	5
7	1	1	1	1	1	1	2	1	1
8	3	2	1	2	2	5	3	1	1
9	1	1	1	1	1	1	1	1	2
10	4	2	4	2	3	3	2	4	3
11	1	1	1	2	2	1	1	1	1
12	1	3	2	2	3	2	2	2	2
13	4	1	2	1	4	1	1	2	2
14	1	4	2	3	1	1	2	2	1
15	2	3	2	3	1	1	2	2	2
16	1	1	1	1	1	1	1	1	2
17	1	1	2	1	1	1	2	2	1
18	4	1	1	1	1	1	1	1	4
19	4	2	4	1	5	4	4	4	4
20	5	1	3	2	2	2	5	2	1
21	3	1	3	4	5	3	4	3	1
22	4	4	1	5	5	4	1	1	1
23	4	5	3	1	5	4	4	3	1
24	1	2	1	1	1	1	1	1	1
25	1	1	1	2	1	1	2	1	1
26	1	1	2	2	2	1	2	2	1
27	3	1	1	1	1	1	1	1	1
28	2	3	1	1	2	1	3	3	4
29	3	2	1	1	2	3	1	1	2
30	2	1	3	1	1	2	1	3	5
31	1	1	1	1	1	4	4	1	1
32	1	1	1	2	2	2	1	1	1
33	2	1	2	1	1	1	1	2	2
34	3	4	2	1	5	2	3	2	5
35	1	1	1	1	1	1	2	1	1

Variable 2: Proceso de Registros Civiles									
N°	Riesgos que afectan la seguridad de la información del proceso de registros civiles							Confianza de ciudadano del servicio que presta RENIEC	
	35	36	37	38	39	40	41	42	43
36	3	2	1	2	2	5	3	1	1
37	1	1	1	1	1	1	1	1	2
38	4	2	4	2	3	3	2	4	5
39	1	1	1	2	2	1	1	1	1
40	1	3	2	2	3	2	2	2	2
41	4	1	2	1	4	1	1	2	2
42	1	4	2	3	1	1	2	2	1
43	2	3	2	3	1	1	2	2	2
44	1	1	1	1	1	1	1	1	1
45	1	1	2	1	1	1	2	2	1
46	4	1	1	1	1	1	1	1	3
47	4	2	4	1	5	4	4	4	5
48	5	1	3	2	2	2	5	3	5
49	3	1	3	4	5	3	4	3	5
50	4	4	1	5	5	4	1	1	1
51	4	5	3	1	5	4	4	4	5
52	1	2	1	1	1	1	1	1	1
53	1	1	1	2	1	1	2	1	1
54	1	1	2	2	2	1	2	2	1
55	3	1	1	1	1	1	1	1	1
56	2	3	1	1	2	1	3	5	4
57	3	2	1	1	2	3	1	1	2
58	2	1	3	1	1	2	1	3	3
59	1	1	1	1	1	4	4	1	2
60	1	1	1	2	2	2	1	1	1
61	2	1	2	1	1	1	1	2	2
62	3	4	2	1	5	2	3	5	4
63	1	1	1	1	1	1	2	1	1
64	3	2	1	2	2	5	3	1	1
65	1	1	1	1	1	1	1	1	1
66	4	2	4	2	3	3	2	4	5
67	1	1	1	2	2	1	1	1	1
68	1	3	2	2	3	2	2	3	4
69	4	1	2	1	4	1	1	2	1
70	1	4	2	3	1	1	2	1	1

Variable 2: Proceso de Registros Civiles									
N°	Riesgos que afectan la seguridad de la información del proceso de registros civiles							Confianza de ciudadano del servicio que presta RENIEC	
	35	36	37	38	39	40	41	42	43
71	2	3	2	3	1	1	2	2	2
72	1	1	1	1	1	1	1	1	2
73	1	1	2	1	1	1	2	2	1
74	4	1	1	1	1	1	1	1	3
75	4	2	4	1	5	4	4	4	1
76	5	1	3	2	2	2	5	3	4
77	3	1	3	4	3	3	4	4	5
78	4	4	1	5	3	4	1	1	1
79	4	5	3	1	5	4	4	3	1
80	1	2	1	1	1	1	1	1	1
81	1	1	1	2	1	1	2	1	1
82	1	1	2	2	2	1	2	1	1
83	3	1	1	1	1	1	1	1	1
84	2	3	1	1	2	1	3	5	4
85	3	2	1	1	2	3	1	1	2
86	2	1	3	1	1	2	1	4	3
87	1	1	1	1	1	4	4	1	2
88	1	1	1	2	2	2	1	1	1
89	2	1	2	1	1	1	1	2	2
90	3	4	2	1	5	4	3	5	4
91	1	1	1	1	1	1	2	1	1
92	3	2	1	2	2	5	3	1	1
93	1	1	1	1	1	1	1	1	2
94	4	2	4	2	3	3	2	4	5
95	1	1	1	2	2	1	1	1	1
96	1	3	2	2	3	2	2	4	5
97	4	1	2	1	4	1	1	2	1
98	1	4	2	3	1	1	2	1	1
99	2	3	2	3	1	1	2	1	2
100	1	1	1	1	1	1	1	1	2
101	1	1	2	1	1	1	2	1	1
102	4	1	1	1	1	1	1	1	3
103	4	2	4	1	5	4	4	1	1
104	5	4	3	2	2	2	5	1	1
105	3	1	3	4	5	3	4	1	1

Variable 2: Proceso de Registros Civiles									
N°	Riesgos que afectan la seguridad de la información del proceso de registros civiles							Confianza de ciudadano del servicio que presta RENIEC	
	35	36	37	38	39	40	41	42	43
106	4	4	1	5	5	4	1	1	1
107	4	5	3	3	5	4	4	1	1
108	1	2	1	1	1	1	1	1	1
109	1	1	1	2	1	1	2	1	1
110	1	1	2	2	2	1	2	2	1
111	3	1	1	1	1	1	1	1	1
112	2	3	1	1	2	1	3	1	4
113	5	4	3	2	2	2	5	2	1
114	3	1	3	4	5	4	4	2	1
115	4	4	1	5	5	4	3	1	1
116	2	5	3	1	5	4	4	2	4
117	1	2	1	1	1	1	1	1	1
118	1	1	1	2	1	1	2	1	1
119	1	1	2	2	2	1	2	1	1
120	2	1	1	1	1	1	1	1	1

Anexo 5. Artículo científico

ARTÍCULO CIENTÍFICO

1. TÍTULO

Sistema de Gestión de Seguridad de la Información en el Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016.

2. AUTOR

Natividad Gladys Bernaldo Bastidas
natybernaldo@hotmail.com
Estudiante del Programa de Maestría en Gestión Pública de la Escuela de Postgrado de la Universidad Cesar Vallejo.

3. RESUMEN

La presente investigación tuvo como objetivo general el determinar qué relación existe entre Sistema de Gestión de Seguridad de la Información y el Proceso de Registros Civiles del Reniec; constituido por 175 colaboradores operativos del Reniec. Lima. San Borja. 2016, se ha considerado una muestra representativa estratificada de 120 colaboradores, en los cuales se ha empleado las variables: Sistema de Gestión de Seguridad de la Información y el Proceso de Registros Civiles.

El método empleado en la investigación fue el hipotético deductivo, esta investigación utilizó para su propósito el diseño no experimental de nivel correlacional, que recogió la información en un período específico, que se desarrolló al aplicar el instrumento: Encuesta de Sistema de Gestión de Seguridad de la Información en la escala de Likert (totalmente de acuerdo, de acuerdo, no sabe/no opina, en desacuerdo, totalmente en desacuerdo) y la Encuesta de Proceso de Registros Civiles en la escala de Likert (totalmente de acuerdo, de acuerdo, no sabe/no opina, en desacuerdo, totalmente en desacuerdo), que brindaron información acerca de la sistema de gestión de seguridad

de la información y el proceso de registros civiles en sus distintas dimensiones, cuyos resultados se presentan gráfica y textualmente.
La investigación concluye que existe evidencia significativa para afirmar que: El sistema de gestión de seguridad de la información se relaciona significativamente con el proceso de registros civiles del Reniec. San Borja. Lima. 2016.

4. PALABRAS CLAVE

Sistema de Gestión de Seguridad de la Información y el Proceso de Registros Civiles.

5. ABSTRACT

The main objective of the present investigation was to determine the relationship between the Information Security Management System and the Reniec Civil Registrations Process; Made up of 175 operational employees of Reniec. Lime. San Borja. 2016, a stratified representative sample of 120 employees has been considered, in which the following variables have been used: Information Security Management System and the Civil Registry Process.
The method used in the research was the hypothetical deductive, this research used for its purpose the non-experimental design of correlational level, which collected the information in a specific period, that was developed when applying the instrument: Security Management System Survey Information on the Likert Scale (strongly agree, agree, do not know / disagree, strongly disagree) and the Likert Scale Civil Registrations Process Survey (strongly agree, agree, do not agree) Knows, does not agree, disagrees, totally disagrees), which provided information about the information security management system and the civil registry process in its different dimensions, the results of which are presented graphically and verbatim.
The research concludes that there is significant evidence to state that: The information security management system is significantly related to the Reniec civil registration process. San Borja. Lima. 2016.

6. KEYWORDS

Information Security Management System and the civil registration process

7. INTRODUCCIÓN

El presente trabajo de investigación titulado: Sistema de Gestión de Seguridad de la Información en el Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016. Fue desarrollado con un diseño no experimental de nivel casual, tuvo como punto de partida relación entre el sistema de gestión de seguridad de la información y el proceso de registros civiles. La presente investigación consta de VI capítulos los cuales son detallados a continuación. Estos son: Capítulo I Constituido por los antecedentes de la investigación, bases teóricas y la fundamentación científica, el marco conceptual, el planteamiento del problema, que comprende el problema de investigación, formulación del problema, que son interrogantes a los cuales responde la investigación; Hipótesis; objetivos de la investigación; En el Capítulo 2: Se presenta el marco metodológico, que comprende las variable, la operacionalización de las variables, la metodología, el tipo de estudio, el diseño de investigación, la población muestra y muestreo, las técnicas e instrumentos de recolección de datos, método de análisis de datos y los aspectos éticos. En el Capítulo 3: Se presentan los resultados de la investigación, los mismos que dan cuenta de los hallazgos logrados con sus respectivos análisis. En el Capítulo 4: Se procede a la discusión de los resultados de la investigación. En el Capítulo 5: Se exponen a las conclusiones a las cuales arribó investigación. En el Capítulo 6: Se detallan las recomendaciones que se brindan. En el Capítulo 7: Se presentan las referencias bibliográficas utilizadas en la investigación.

8. METODOLOGÍA

El método empleado en la investigación fue el hipotético deductivo, esta investigación utilizó para su propósito el diseño no experimental de nivel correlacional, que recogió

la información en un período específico, que se desarrolló al aplicar el instrumento: Encuesta de Sistema de Gestión de Seguridad de la Información en la escala de Likert (totalmente de acuerdo, de acuerdo, no sabe/no opina, en desacuerdo, totalmente en desacuerdo) y la Encuesta de Proceso de Registros Civiles en la escala de Likert (totalmente de acuerdo, de acuerdo, no sabe/no opina, en desacuerdo, totalmente en desacuerdo), que brindaron información acerca del Sistema de Gestión de Seguridad de la Información y el proceso de registros civiles en sus diferentes dimensiones, cuyos resultados se presentan gráfica y textualmente.

9. RESULTADOS

Describen narrativamente los hallazgos del estudio como el análisis estadístico e interpretación de datos y la prueba de hipótesis.

Hipótesis general

Existe una relación altamente significativa entre el sistema de gestión de seguridad de la información y el proceso de registros civiles del Reniec. San Borja. Lima. 2016.

Hipótesis Nula

No existe relación altamente significativa entre el sistema de gestión de seguridad de la información y el proceso de registros civiles del Reniec. San Borja. Lima. 2016.

Tabla 12

Correlación Sistema de Gestión de Seguridad de la Información y el Proceso de Registros Civiles

Correlaciones

			Sistema de Gestión de Seguridad de la Información.	Proceso de Registros Civiles
Rho de Spearman	Sistema de Gestión de Seguridad de la Información.	Coeficiente de correlación	1,000	,781**
		Sig. (bilateral)	.	,000
		N	120	120
	Proceso de Registros Civiles	Coeficiente de correlación	,781**	1,000
		Sig. (bilateral)	,000	.
		N	120	120

**. La correlación es significativa al nivel 0,01 (2 colas/bilateral).

Tabla N° 17

El Sistema de Gestión de Seguridad de la Información. San Borja. Lima. 2016

Nivel	Rango	Frecuencia	%	% válido	% Acumulado
Bajo	[34 - 79]	87	72.50%	72.50%	72.50%
Medio	[80 - 125]	32	26.67%	26.67%	99.17%
Alto	[126 - 170]	1	0.83%	0.83%	100.00%
	Total	120	100.00%	100.00%	

Nota: Cuestionario de Sistema de Gestión de Seguridad de la Información (Anexo 2)

Tabla N° 18

Proceso de Registros Civiles. Reniec. San Borja. Lima. 2016

Nivel	Rango	Frecuencia	%	% válido	% Acumulado
Aceptable	[9 - 21]	84	70.00%	70.00%	70.00%
Regular	[22 - 33]	35	29.17%	29.17%	99.17%
No Aceptable	[34 - 45]	1	0.83%	0.83%	100.00%
	Total	120	100.00%	100.00%	

Nota: Cuestionario de Sistema de Gestión de Seguridad de la Información (Anexo 2)

Tabla N° 19

Sistema de Gestión de Seguridad de la Información y el proceso de registros civiles. Reniec. San Borja. Lima. 2016.

		Sistema de Gestión de Seguridad de la Información			Total
		Alto	Bajo	Medio	
Proceso de Registros Civiles	Aceptable	0	71	13	84
		0.0%	84.5%	15.5%	100.0%
	No Aceptable	0	1	0	1
		0.0%	100.0%	0.0%	100.0%
	Regular	1	15	19	35
		2.9%	42.9%	54.3%	100.0%
Total		**1**	**87**	**32**	**120**
		.8%	**72.5%**	**26.7%**	**100.0%**

Nota: Cuestionario Sistema de Gestión de Seguridad de la Información y el Proceso de Registros Civiles (Anexo 2)

10. DISCUSIÓN

De los hallazgos encontrados la presente investigación corrobora lo planteado por Merino y Cañizares (2011), puesto que coincide en afirmar que el sistema de gestión de seguridad de la información es la parte del sistema general de la gestión en una organización que consta de: la política, estructura organizativa, los procedimientos, los procesos y los recursos necesarios la gestión de la seguridad de la información en una organización, enfatizando en los factores tales como: sistema de gestión de seguridad de la información, gestión de seguridad de la información, familia de norma ISO 27000, implantación de un sistema de seguridad de la información, con el objetivo de mitigar los riesgos que afectan la seguridad de la información del proceso de registros civiles, así como mejorar cada día la confianza del ciudadano del servicio que presta Reniec, fortalecimiento los pilares de seguridad de la información (confidencialidad, disponibilidad e integridad), a través de la implantación de un sistema de gestión de seguridad de la información bajo la Norma ISO 27001.

11. CONCLUSIONES

En cuanto a la hipótesis general, se demuestra que existe una relación altamente significativa entre el sistema de gestión de seguridad de la información y el proceso de registros civiles. San Borja. Lima. 2016.

12. REFERENCIAS

Condori Alejo, H. (2012). *Un Modelo de Evaluación de Factores Críticos de Éxito {en la Implementación de Seguridad de la Información para determinar su influencia en la atención del usuario*. (tesis de grado). Universidad Garcilaso de la Vega. Lima, Perú.

Joyanes, L. (2015). *Sistemas de Información en la Empresa*. (1a ed.). México: Alfaomega.

Merino y Cañizares. (2011). *Implantación de un Sistema de Gestión de Seguridad de la Información según la ISO 27001*. (1a ed.). Bogotá, Colombia: Ediciones de la U.

Miguel, J.C. (2016). *Protección de datos y seguridad de la información*. (4a ed.). Madrid, España: FC Editorial.

DECLARACIÓN JURADA

DECLARACIÓN JURADA DE AUTORÍA Y AUTORIZACIÓN PARA LA PUBLICACIÓN DEL ARTÍCULO CIENTÍFICO

Yo, Natividad Gladys Bernaldo Bastidas, estudiante (X), egresado ( ), docente ( ), del Programa de Maestría en Gestión Pública de la Escuela de Postgrado de la Universidad César Vallejo, identificado(a) con DNI N° 40097502, con el artículo titulado:

"Sistema de Gestión de Seguridad de la Información en el Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016."

Declaro bajo juramento que:

1) El artículo pertenece a mi autoría.
2) El artículo no ha sido plagiada ni total ni parcialmente.
3) El artículo no ha sido autoplagiada; es decir, no ha sido publicada ni presentada anteriormente para alguna revista.
4) De identificarse la falta de fraude (datos falsos), plagio (información sin citar a autores), autoplagio (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.
5) Si, el artículo fuese aprobado para su publicación en la Revista u otro documento de difusión, cedo mis derechos patrimoniales y autorizo a la Escuela de Postgrado, de la Universidad César Vallejo, la publicación y divulgación del documento en las condiciones, procedimientos y medios que disponga la Universidad.

Lugar y fecha: Los Olivos, 10 de mayo del 2017

Nombres y apellidos: Natividad Gladys Bernaldo Bastidas