REPÚBLICA DEL ECUADOR

INSTITUTO DE ALTOS ESTUDIOS NACIONALES

UNIVERSIDAD DE POSGRADO DEL ESTADO

Trabajo de titulación para obtener la Maestría Profesional en Auditoría Gubernamental y Control

ARTÍCULO CIENTÍFICO

TÍTULO DEL TRABAJO: INFLUENCIA DE UN MODELO DEL SGSI (NORMA ISO/IEC 27001:2013) EN LA EFICACIA DE LA ADMINISTRACIÓN DE LOS RECURSOS PÚBLICOS. REGISTRO DE LA PROPIEDAD Y MERCANTIL DEL CANTÓN PEDRO MONCAYO, PERÍODOS 2019, 2020 Y 2021.

Autor: Mónica Patricia Hidalgo Narváez

Director: PhD. Romel Alfredo Tintín Hidalgo

Quito, abril del 2022

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO

Autoría

Yo, Mónica Patricia Hidalgo Narváez, máster, con CC. 1713729638, declaro que las ideas, juicios, valoraciones, interpretaciones, consultas, bibliografías, definiciones y conceptualizaciones expuestas en el presente trabajo, así como los procedimientos y herramientas utilizadas en la investigación, son de absoluta responsabilidad como autora del trabajo de titulación. Asimismo, me acojo a los reglamentos internos de la universidad correspondientes a los temas de honestidad académica.

Mónica Patricia Hidalgo Narváez

C.C.: 1713729638

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO

Autorización de Publicación

Yo, Mónica Patricia Hidalgo Narváez, cedo al IAEN, los derechos de publicación de la presente obra por un plazo máximo de cinco años, sin que deba haber un reconocimiento económico por este concepto. Declaro además que el texto del presente trabajo de titulación no podrá ser cedido a ninguna empresa editorial para su publicación u otros fines, sin contar previamente con la autorización escrita de la universidad.

Quito, abril del 2022

FIRMA DEL CURSANTE

MÓNICA PATRICIA HIDALGO NARVÁEZ
C.C. 1713729638

Agradecimientos

Mi agradecimiento a Dios todopoderoso por bendecirme y hacer realidad este sueño anhelado, A mi esposo e hijos que son la fuente de inspiración para alcanzar esta meta. A mi tutor PhD. Romel Tintín por brindarme su asesoramiento, apoyo y confianza.

Al Registro de la Propiedad y Mercantil del Cantón Pedro Moncayo, por fomentar la formación del Talento Humano. Al Instituto de Altos Estudios Nacionales por darme la oportunidad de estudiar y ser una gran profesional comprometida a la vocación del servicio público.

A mis docentes, por haber compartido sus conocimientos y experiencias para desarrollar el presente artículo y a todos quienes aportaron para que esta investigación se haga una realidad.

Mónica Hidalgo

Dedicatoria

El presente trabajo de investigación está dedicado a aquellos lectores perseverantes que, inspirados en el desarrollo del conocimiento, consideren el presente artículo científico y sea como referencia para futuras investigaciones en beneficio del control gubernamental.

Mónica Hidalgo

Influencia de un modelo del SGSI (Norma ISO/IEC 27001:2013) en la eficacia de la administración de los recursos públicos. Registro de la Propiedad y Mercantil del Cantón Pedro Moncayo, períodos 2019, 2020 y 2021.

Mónica Patricia Hidalgo Narváez
Instituto de Altos Estudios Nacionales[1]

Resumen

El presente artículo demuestra cómo influye el diseño e implementación de un modelo de Sistema de Gestión de Seguridad de la Información (SGSI) bajo el estándar internacional ISO/IEC 27001:2013 en la eficacia de la administración de los recursos públicos. Para ello se ha tomado como referencia el modelo del SGSI implementado por el Registro de la Propiedad y Mercantil del Cantón Pedro Moncayo (RPMPM); que, por su operatividad en el manejo de datos públicos, logró obtener una marca internacional en Seguridad de la Información (SI) y se convirtió en un referente de buenas prácticas a nivel nacional.

La metodología cualitativa describe el SGSI adoptado por el RPMPM, bajo los estándares de la Norma ISO/IEC 27001: 2013 y la integración con la Norma de Control Interno (NCI) expedido por la Contraloría General del Estado (CGE), que al ser aplicados son eficaces al estar completamente segura la información. Del mismo modo, a través de la matriz de riesgos y actas del Comité de SI, se analiza cuantitativamente la evolución del SGSI antes, durante y posterior para asegurar su correcta implementación. Para la comprobación de los beneficios de dichas aplicaciones, se formuló una encuesta a través de Google a 200 personas relacionadas directamente con el SGSI, para determinar el nivel de conocimientos respecto al estándar, y, proponiendo un prototipo de índice para evaluar la eficacia de los recursos públicos asignados a la SI, administrados por las Registradurías en el Ecuador, determinando que existe un 93% (2020) y 100% (2021) de eficacia al tener la capacidad para lograr los objetivos estratégicos de SI y a contribuir al buen control gubernamental.

Los datos que se analizan comprenden los períodos 2019, 2020 y 2021.

Palabras Claves: Eficacia en la administración de los recursos públicos, Norma ISO/IEC 27001:2013, Seguridad de la Información, Sistema de Gestión de Seguridad de la Información.

[1] Instituto de Altos Estudios Nacionales. Avenida Amazonas N37-271 y Villalengua, Quito, Ecuador. Teléfono: 02382990 (email: monica.hidalgo@iaen.edu.ec)

Abstract:

This article demonstrates how the design and implementation of an Information Security Management System (ISMS) model under the international standard ISO/IEC 27001:2013 influences the effectiveness of public administration. For this, the ISMS model implemented by the Property and Mercantile Registry of the Pedro Moncayo Canton (RPMPM) has been taken as a reference; which, due to its operability in the management of public data, needed to obtain an international mark in Information Security (IS) and became a benchmark of good practices at the national level.

The qualitative methodology describes the ISMS adopted by the RPMPM, under the standards of the ISO/IEC 27001: 2013 Standard and the integration with the Internal Control Standard (NCI) issued by the Comptroller General of the State (CGE), which at be applied are effective as the information is completely secure. In the same way, through the risk matrix and IS Committee minutes, the evolution of the ISMS is quantitatively analyzed before, during and after to ensure its correct implementation. To verify the benefits of these applications, a survey was formulated through Google to 200 people directly related to the ISMS, to determine the level of knowledge regarding the standard, and proposing an index prototype to evaluate the effectiveness of the public resources allocated to the IS, administered by the Registrars in Ecuador, determining that there is 93% (2020) and 100% (2021) of effectiveness by having the capacity to achieve the strategic objectives of IS and to contribute to the good government control.

The data analyzed includes the periods 2019, 2020 and 2021.

Key Words: Efficiency in the administration of public resources, ISO/IEC 27001:2013 Standard, Information Security, Information Security Management System.

Índice General

Listado de figuras

Lista de gráficos

Lista de Tabla

Lista de Acrónimos

CGE	Contraloría General del Estado
CRE	Constitución de la República del Ecuador
COVID 19	Corona Virus Enfermedad 2019
DINARDAP	Dirección Nacional de Registro de Datos Públicos
ISO/IEC	International Standarization for Organitation – IEC International Electrotechnical Commission
INEN	Servicio Ecuatoriano de Normalización
NCI	Normas de Control Interno
MINTEL	Ministerio de Telecomunicaciones y de la Sociedad de la Información
PHVA	Planificar, Hacer, Verificar y Actuar
POA	Plan Operativo Anual
PAC	Plan Anual de Contratación
RPMPM	Registro de la Propiedad y Mercantil del Cantón Pedro Moncayo
SGSI	Sistema de Gestión de Seguridad de la Información
SNAP	Secretaria Nacional de la Administración Pública
SI	Seguridad de la información
TI	Tecnología de la información

1. Introducción

En la actualidad, la información se ha convertido en el activo más valioso que generan las organizaciones, siendo la misma esencial para el logro de sus objetivos estratégicos y buen funcionamiento (Vite, Dávila, & Molina, 2019, p. 33), De igual forma, es indispensable proteger sus datos frente a los riesgos que se pudieran presentar debido a amenazas y vulnerabilidades provocados por eventos naturales, fallas técnicas y recursos humanos, afectando la disponibilidad de la información y recursos; (Americanos, 2000).

Ante tal situación, las organizaciones han estimado a la información como uno de los principales pilares para su funcionamiento, invirtiendo recursos para evitar el robo y manipulación de sus datos confidenciales mediante el uso de la tecnología para la creación, procesamiento y almacenamiento en sistemas de información (Sisti, 2019, p. 24), como es el caso de los Registros de la Propiedad que por su operatividad administran bases de datos públicos.

Los Registros de la Propiedad como tales, funcionan en el Ecuador a partir de la expedición de la (Ley de Registro, 1980), marco legal en el cual se estructuró esta dependencia con carácter privado que brindaba servicios públicos, administrados financieramente por los Registradores y vigilados por las Cortes Superiores de cada provincia. A partir de la expedición de la (Constitución de la República del Ecuador [CRE], 2008), cambia su estructura funcional a carácter público para ser administrados de manera concurrente entre la Dirección Nacional de Registro de Datos Públicos (DINARDAP) y los Municipio de cada cantón, cuyos recursos públicos provenientes del cobro de aranceles, son destinados a los gastos de operatividad.

El RPMPM es una institución pública adscrita al (GAD Municipal del Cantón Pedro Moncayo, 2011), creada mediante Ordenanza S/N del 10 de junio del 2011, que tiene como función principal prestar servicios de inscripción y certificación de actos registrales a los propietarios de los bienes inmuebles y muebles del cantón. Para otorgar estos servicios es indispensable contar los libros registrales que datan información de uso histórico desde el 14 de febrero de 1912, constituyéndose en los activos más valiosos que posee la organización.

Ante tales activos de valor no estimado, el problema surge en el primer trimestre del período 2018, donde el responsable de la Unidad Operativa mediante un reporte formal, indicó que en ocasiones reiteradas los libros históricos al ser manipulados por el personal para marginar las inscripciones de los nuevos propietarios de los bienes inmuebles en las actas anotadas manualmente con un número de repertorio secuencial a través de un asiento registral y firmado por los Registradores titulares de aquellos años como lo establece el artículo 24 de la (Ley de

Registro, 1980), fueron sustraídas de su libro original; encontrando también en algunos asientos cortes; y, por último, dos libros que databan del año 1950 fueron extraviados, aclarando que dicha información no pudo ser recuperada.

En resumen, los datos al ser físicos y al no estar digitalizados, fueron una pérdida significativa para la entidad, afectado a la disponibilidad de la información en la emisión de certificados que solicitan los propietarios de los bienes, lo que generó retrocesos en los procesos de inscripciones, sanciones al personal y juicios civiles.

En vista de esta problemática, la Alta Dirección conjuntamente con el equipo de apoyo, incorporó en el Plan Operativo Anual (POA), Plan Anual de Contratación (PAC) y presupuestos, el planteamiento del diseño de un modelo de (SGSI) con la ayuda de la norma internacional ISO/IEC 27001:2013, que permita a través de un conjunto de procesos gestionar la accesibilidad de la información y asegurar la integridad, disponibilidad y confidencialidad de los activos de información, reduciendo a la vez los riesgos de detectados por los hechos ocurridos (Valdiviezo & Rodríguez, 2015), e "incorporando una lista de controles para la gestión de la seguridad de la información;" (Grajales & León, 2016, p. 44); con el fin de aplicar acciones preventivas que faciliten el trabajo de la implementación del SGSI dentro de la organización (Aguilar, 2017).

El SGSI que el RPMPM implementó ha sido monitoreado por el Comité de Seguridad de la Información a través de las actas y verificados mediante los informes de auditoría externa certificado por un organismo acreditado, pues actualmente el RPMPM cuenta con una marca en SI, apegada a estándares internacionales y como un referente de buenas prácticas en su entorno de acción; sin embargo, no se ha podido evidenciar como este diseño e implementación de modelo del SGSI bajo la (Norma ISO/IEC 27001:2013), influye o no en la eficacia de la administración de los recursos públicos.

2. Revisión de Literatura

2.1 Sistemas de Gestión de Seguridad de la información

> Según British Standards Institution: "la información es la sangre de todas las organizaciones, y es en este mismo sentido que la protección de este vital elemento asegurará no solamente la vida y operación adecuada de las organizaciones, sino que al reconocer entre las entidades la salud de su activo, dará certeza de los servicios que proporciona, siendo responsable en todo momento en su contexto y ante la sociedad" (Riestra, 2017, p. 5).

Uno de los mayores retos de las organizaciones radica en la transformación digital de la información que a través del uso de sistemas informáticos permite procesar, recopilar, clasificar, interpretar y resumir grandes cantidades de datos para informar a la Alta Dirección (Medina J. ,

2006, p.7), convirtiéndose en un recurso estratégico para que la organización formule bases sólidas en la continuidad de su negocio, estar en sintonía con sus proveedores y clientes, obtener mejores resultados y asegurar el éxito a corto y largo plazo (Proaño, Orellana, & Martillo, 2018).

Ante la nueva era digital, los datos se han convertido en el valor más preciado para todas las organizaciones que se han visto obligados a invertir en sistemas, personas, recursos y demás activos para reducir la probabilidad y el impacto de los incidentes de seguridad contra desastres, errores (intencionales o no) y manipulación no autorizada, que pudiera presentarse (Silva, Segadas, & Kowask, 2014).

Chillan y Pionce señalan que la SI en una organización se obtiene implementando un sistema de gestión acorde a la realidad funcional, al establecer el diseño más apropiado para tratar los aspectos de seguridad, a través de la integración de los recursos técnicos y humanos, amparados por medidas administrativas, que garanticen el establecimiento de controles efectivos, para alcanzar el nivel de seguridad necesario en cumplimiento con los objetivos estratégicos de la organización, de forma que se mantenga el riesgo reducido del nivel asumible (Chilán & Pionce, 2017, p. 294).

En el Ecuador encontramos algunas disposiciones legales que regulan de alguna forma la SI, contempladas en la (Ley Orgánica de Datos Personales , 2021), la (Ley Orgánica del Sistema Nacional de Registro de Datos Públicos [LOSNRDP], 2010), en su artículo 26, que precisa el término de seguridad y de los cuales hacen referencia a los artículos 300 y 410.10 de las (Normas de Control Interno para las Entidades, Organismos del Sector Público y de las personas jurídicas de derecho privado que dispongan de recursos públicos [NCI], 2009); expedido por la CGE; así como la (Secretaria Nacional de Administración Pública [SNAP], Acuerdo No. SGPR-2019-0107, 2019) que emite la Regla Técnica Nacional para la Organización y Mantenimiento de los Archivo Públicos; y, por último, la disposición del (Ministerio de Telecomunicaciones y de la Sociedad de la Información [MINTEL], Acuerdo Ministerial No. 025-2019, 2019) que expide el Esquema Gubernamental de SI-EGSI, versión 2.0, basado en la norma ISO/IEC 27001:2013.

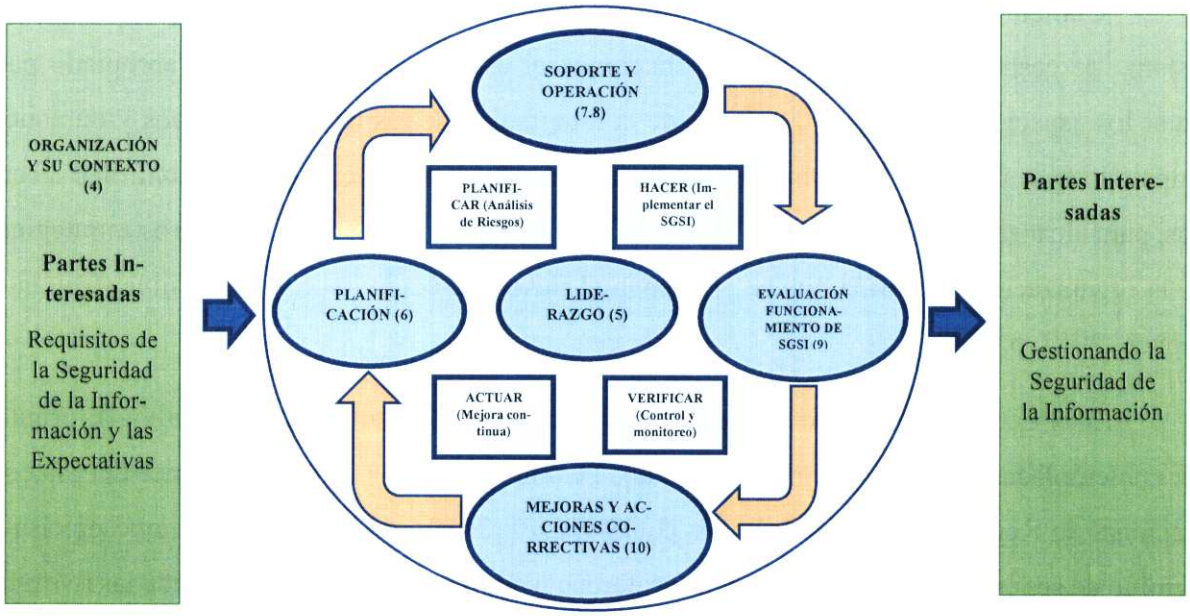
La Norma ISO/IEC 27001:2013 traducida en el Ecuador por el (Servicio Ecuatoriano de Normalización [INEN], 2018) indica que "El SGSI preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas que los riesgos se gestionan adecuadamente"; así como también, especifica los requisitos para establecer, implementar, mantener y mejorar continuamente

un SGSI dentro del contexto organizacional, considerando los procesos, tamaño y estructura, pues su adopción depende de la decisión estratégica de la organización (p. iv).

El SGSI forma parte y se integra con los procesos de la estructura organizacional a través del ciclo Deming PHVA con un enfoque basado en riesgos, con el propósito de aplicar los controles de SI contenidas en el anexo A del estándar divida por 14 dominios y 114 controles que ayudan a proteger los activos de información, como lo representa la figura No. 1.

Figura No. 1

SGSI y su relación con ciclo PHVA



Fuente: Adaptado de la Norma ISO/IEC 27001:2013 (INEN, 2018)
Elaborado por: la autora (2022)

(Pedraza, 2017) determina que "los SGSI adoptados en instituciones públicas bajo los requisitos de la Norma ISO/IEC 27001:2013 es vista como un proceso dinámico que debe contemplar el análisis del contexto organizacional; además de evaluar los riesgos de la seguridad de la información en dicha empresa" (p. 66).

Es necesario que la organización conozca los riesgos de SI que se enfrentan aplicando una gestión de riesgos que permita "abarcar la evaluación y el análisis del riesgo, al igual que la ejecución de estrategias y de acciones específicas para controlar, reducir y transferir el riesgo" (Corda, Coria, Cuervo, & Viñas, 2016, p.2), con el propósito de minimizar el riesgo; ya que, de acuerdo a la revista (Haz, 2017), los mayores riesgos que enfrentan las organizaciones en la actualidad son los delitos cibernéticos, hacking, virus y códigos maliciosos que pueden afectar a

la "información valiosa que se puede encontrar de diferentes formas: impresa, almacenada electrónicamente, transmitida por diferentes medios de comunicación o de transporte, divulgada por medios audiovisuales, en el conocimiento de las personas, etc." (Tarzona, 2007, p.143).

Un SGSI tiene como propósito esencial la protección de los sistemas de información de uso, acceso, divulgación y disrupción no autorizada de la misma. La adecuada gestión de SI persigue establecer y mantener políticas y controles que tengan como objetivos estratégicos conservar la integridad, disponibilidad y confidencialidad de la información; por tanto, estos tres elementos son el pilar fundamentar de todo SGSI en cualquier organización que busca eficacia en el modelo ideal de su información (Chaverra, 2021).

Para (Fonseca, 2019) un SGSI es un elemento clave dentro del Plan estratégico, debido a que más allá, de proteger sus activos, le permite obtener un valor diferenciador dentro de la operación de sus servicios, incrementa la percepción positiva de la imagen de la organización, mejora los procesos y disminuye costos (p. 103).

De acuerdo con (Guzmán, 2015) el diseño de un SGSI basado en un modelo de mejores prácticas y lineamientos de seguridad, como es la Norma ISO/IEC 27001:2013, es una herramienta de gran ayuda que permite identificar los diferentes aspectos que se deben tener en cuenta las organizaciones cuando deciden establecer un modelo de SI; ya que, si logran cumplir lo establecido en el estándar, podrán llegar a forjar en el tiempo un adecuado y sostenible SGSI. La implementación comienza con el compromiso demostrable de la Alta directiva cuando la SI es concebida dentro de los objetivos estratégicos de la organización (p. 166).

2.2 Eficacia en la administración de los recursos públicos

El Instituto de Informática Legal. Quito, 1986, define a la "gestión pública, como el conjunto de acciones mediante las cuales las entidades tienden al logro de sus fines, objetivos y metas, los que están enmarcados por las políticas gubernamentales establecidas por el Poder Ejecutivo"; es decir, la gestión pública dirige a una organización alcanzar el cumplimiento de los objetivos estratégicos (Hidalgo, 2015, p.8).

Según lo indica Reyna:

> La eficacia consiste "en alcanzar los objetivos propuestos, las metas programadas. Para ello, es necesario que la institución cuente con una planificación detallada, con sistemas de información e instrumentos que permitan conocer en forma oportuna y confiable determinada situación en el momento preciso y la existencia de desvíos respecto a las metas proyectadas, para medir el grado de eficacia." (Reyna, 2017, p. 158).

En concordancia con (Vinueza, 2021, p.4) "La gestión pública permite la optimización del uso de los recursos públicos, con el fin de obtener eficacia en la gestión de los mismos. La incorporación de un modelo de gestión al procedimiento administrativo permite una reducción del mal uso de los recursos públicos"; en otras palabras, "la eficacia se relaciona al aprovechamiento oportuno de los recursos para el cumplimiento de los objetivos institucionales" (Reyna, 2017, p. 158).

Así mismo, (Escudero, 2020) señala que "los recursos públicos son aquellos medios materiales o inmateriales que posee la administración para satisfacer las necesidades de los ciudadanos y de la administración misma para la correspondiente prestación de servicios. Estos deben estar debidamente distribuidos y controlados a fin de que esta pueda cumplir su misión de administrar y gestionar el Estado" (p.21).

El control es un sistema de derecho público, que consiste en verificar si los recursos humanos, materiales, tecnológicos y financieros han sido utilizados correctamente en la ejecución de un plan de manera que se pueda comparar continuamente los resultados obtenidos con lo planteados y tomar medidas útiles para asegurar la ejecución de sus objetivos (Amoroso, 2018).

Según (Medina M. , 2015) "la administración de recursos públicos permite a la entidad ordenar la implantación del control interno, ya que es un proceso integral efectuado por el titular, funcionarios y servidores de una entidad, diseñada para enfrentar los riesgos y para asegurar que se alcancen los objetivos" (p. 15), cuyo propósito es promover las acciones, a través de la aplicación de controles efectivos que impulsen hacia la eficacia de la organización (Meigs, 2004).

Para (Mantilla, 2018) el control interno comprende todos los métodos y acciones que se adoptan en una organización para salvaguardar sus activos, los cuales pueden ser políticas, procedimientos, elementos de software y hardware, mecanismos de protección de la infraestructura física y de seguridad, así como la adecuada selección y entrenamiento del personal que utiliza los recursos de información (Figueroa, Rodríguez, Bone, & Saltos, 2017, p. 154), con el objetivo de resguardar los recursos y bienes del Estado contra cualquier pérdida, deterioro, actos ilegales y uso indebido de todo hecho irregular o situación perjudicial que pudiera afectarlos (Mendoza, García, Delgado, & Barreiro, 2018).

Las entidades públicas deben mejorar continuamente sus procesos, y que las acciones a tomar se vean reflejado en la correcta utilización de los recursos públicos y en la entrega de servicios eficaces y de calidad para la sociedad ecuatoriana (González, Narváez, & Erazo, 2019).

3. Metodología

El presente estudio describe y analiza la interrogante: ¿cómo influye el diseño e implementación de un modelo de (SGSI) bajo el estándar internacional ISO/IEC 27001:2013, en la eficacia de la administración de los recursos públicos? Para ello, se utilizó la metodología de investigación con enfoque mixto cualitativo y cuantitativo, que "representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación que implican la recolección y análisis de los datos cuantitativos y cualitativos, así como su integración y discusión conjunta para realizar inferencias producto de toda información recabada (metainferencias)" (Hernández R. , 2014, pág. 534); por consiguiente, utilizan evidencia de datos numéricos, textuales, simbólicos y otros para lograr un mayor entendimiento del fenómeno bajo estudio (Hernández R. , 2014).

Para la recolección de datos cualitativos referente a la descripción del diseño e implementación del modelo del SGSI adoptado por el RPMPM en relación a la eficacia de la administración de los recursos públicos, se aplicó el método de revisión documental, que sirvió para extraer información científica, en tesis de grados, libros, artículos científicos y revistas; así también, información relativa de la normativa internacional ISO/IEC 27001:2013 y demás normativas ecuatoriana vigentes, tales como: Ley Orgánica de Datos Personales, Ley Orgánica de Datos Públicos, Normas de Control Interno, Regla Técnica Nacional para la Organización y Mantenimiento de los archivos Públicos y el esquema Gubernamental de SI – EGSI, versión 2.0.

Para el análisis de datos cuantitativos, se utilizó el método de revisión documental de registros oficiales contenidas en la matriz de riesgos y actas del Comité de SI de la organización objeto de estudio, que sirvió para establecer la evolución del SGSI antes, durante y posteriormente a la implementación en la aplicación de los controles determinados en el estándar; así como, también permitió obtener un detalle de los beneficios obtenidos luego de las acciones tomadas por la organización. El análisis de datos fue realizado mediante tablas dinámicas y gráficos en Excel, a través de la integración de los períodos 2019, 2020 y 2021.

Con el objeto de determinar los niveles de conocimientos del estándar ISO/IEC 27001:2013, se diseñó una encuesta digital por formularios Google, la cual fue enviada a 200 personas que se relacionaron durante la implementación del SGSI, entre los que se encontraba personal de apoyo tecnológico, proveedores de sistemas y equipos informáticos, auditores lideres de SI y técnicos operativos del varias Registradurías y de entidades que operan datos públicos a nivel nacional.

Finalmente, con la información recabada de los beneficios obtenidos se planteó un prototipo de índice por medio del método de diseño métricas para evaluar la eficacia de los recursos públicos destinados a los objetivos estratégicos de SI para las Registradurías a nivel nacional.

4. Discusión de Resultados

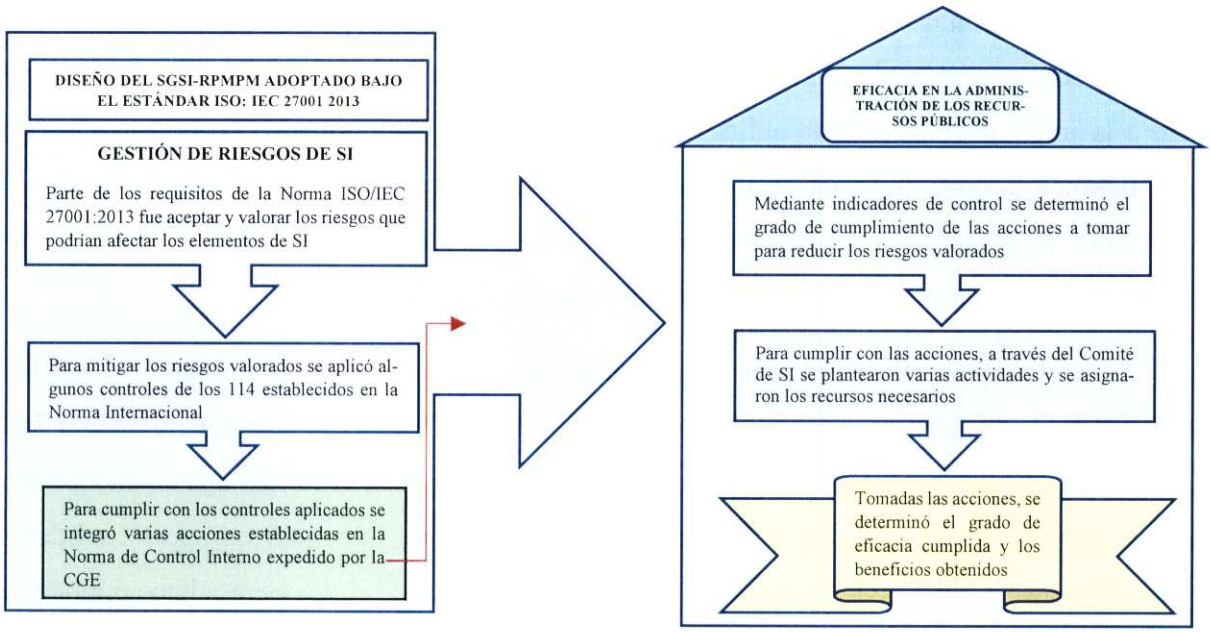
4.1 Descripción del modelo del SGSI diseñado

El RPMPM diseñó un SGSI acorde a su realidad funcional, que le permitió analizar y valorar los riesgos iniciales y residuales que podrían afectar a la confiabilidad, integridad y seguridad de la información, mediante la gestión de riesgos; con el propósito de prevenir posibles amenazas e incidentes que pudieran presentarse por varios factores (Vergara, 2017, p.21), dentro de las fases de implementación. Para la mitigación de los riesgos valorados se aplicaron varias acciones de control establecidos en el anexo de la norma ISO/IEC 27001: 2013 (p.9), e integrados con varios artículos de la NCI expedido por la CGE como lo muestra el anexo No. 1.

Para el cumplimiento de las acciones, a través del Comité de SI se plantearon varias actividades y se asignaron los recursos necesarios, los cuales mediante indicadores de control se determinó el grado de eficacia de las acciones tomadas, con el propósito de proteger los activos más valiosos de la información pública y obtener beneficios, como lo muestra la figura No. 2:

Figura No. 2

Modelo de SGSI adoptado por el RPMPM



Fuente: Adaptado del Modelo de SGSI del RPMPM
Elaborado por: la autora (2022)

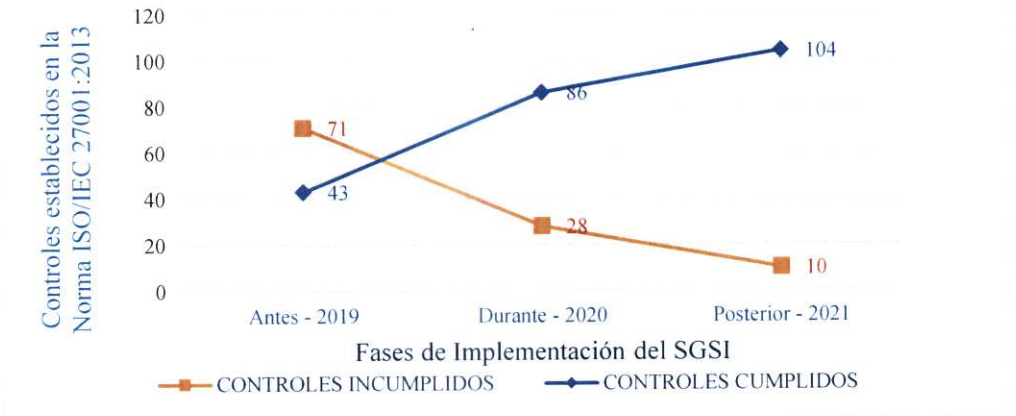
4.2 Análisis comparativo de la evolución del SGSI implementado

En el gráfico No. 1 se puede observar la evolución del SGSI adoptado por el RPMPM en las fases: antes, durante y posteriormente a su implementación, cuya variación significativa muestra cómo fue mejorando la SI paulatinamente en cada año; debido a los controles aplicados para hacer frente a las vulnerabilidades y reducir el riesgo de incidentes de SI (Silva, Segadas, & Kowask, 2014); es decir, de los 114 controles que establece el estándar, en la primera fase (antes) apenas se cumplieron 43 controles por la dotación física de la infraestructura tecnológica, los otros 71 controles no aplicados se debieron al desconocimiento del estándar.

A continuación, en la segunda fase (durante), se cumplieron 86 controles por la aplicación de las políticas de SI establecidos en los 14 dominios de la norma, necesarios para la certificación del estándar y además oportuno ante los efectos del COVID 19 por la aplicación de teletrabajo, servicios en línea y digitalización de documentos (Zuñiga, Jalón, Andrade, & Giler, 2021). Por último, en la tercera fase (posterior), satisfactoriamente se cumplieron 104 controles por la continuidad de la operatividad debido el incremento de contagios del virus que dio lugar a las transferencias de información entre entidades públicas. Los demás controles no aplicados en las dos fases últimas se debieron al desarrollo tecnológico no implantado.

Gráfico No. 1

Evolución de la implementación del SGSI



Fuente y adaptación de la autora: Actas del Comité de SI y Matriz de Riesgos.

En definitiva, las dos variables muestran la relación entre los controles cumplidos y no al aplicar el estándar, descritas en la matriz de riesgos de los períodos 2019, 2020 y 2021, como lo indica (Salcedo, 2018, p. 21) "Si los controles se aplican de una forma ordenada y organizada, entonces existirá una interrelación positiva entre ellos, la cual vendría a constituir un sistema de control sumamente más efectivo".

4.2.1 Análisis de los Beneficios obtenidos del SGSI implementado

Por otro lado, la tabla No. 1 indica el detalle de los beneficios obtenidos del SGSI implementado, luego del cumplimiento de las acciones tomadas de los períodos 2019, 2020 y 2021, a través de los datos integrados de la matriz de riesgos y actas del Comité de SI, en el cual se puede observar que sobre el 80% de la metas establecidas en los indicadores de control, el 81% de las acciones tomadas fueron eficaces, logrando el resultado esperado, el aprovechamiento oportuno de los recursos públicos, la reducción de riesgos, al identificarse las vulnerabilidades técnicas potenciales y los riesgos asociados (Valdiviezo & Rodríguez, 2015) y los potenciales de mejora que continuarán para los próximos años; tales como: la interconexión de las bases de datos entre el RPMPM con las Notarías y el catastro municipal, tomando en cuenta aún más el surgimiento de nuevas innovaciones tecnológicas que implican mayor seguridad de los datos, en vista del aumento sustancial de los incidentes de SI ocurridos en los dos últimos años (Estrada, Unas, & Flórez, 2021).

4.3 Perspectiva de las partes interesadas de un estándar ISO/IEC 27001:2013

Para determinar el nivel de conocimiento de las partes interesadas del estándar ISO/IEC 27001:2013, se diseñó una encuesta por formularios Google y se aplicó a 200 personas que estuvieron relacionados durante la implementación del SGSI, lo cual permitió detectar lo siguiente:

Como lo muestra el gráfico No. 2, la mayor parte de los encuestados fueron técnicos de varias Registradurías y de entidades que operan datos públicos de sexo masculino, con una edad promedio de 41 a 50 años y una formación en tercer nivel en las profesiones de derecho, sistemas informáticos; y, contabilidad y auditoría, de los cuales el 73% de los encuestados continuaron en la contestación de las preguntas siguientes, revelando altos niveles de conocimiento en el estándar en SI, El otro 27 % de los encuestados que no continuaron con las preguntas formuladas, afirmaron desconocer este tipo de estándar; en vista, de que no coexiste una cultura de SI en nuestro país, como lo revela el informe mundial de la Organización Internacional ISO, que ha entregado 36.362 certificados en todo el mundo, y apenas 9 certificados en el Ecuador (ISO, 2020).

Tabla No. 1

Beneficios obtenidos del SGSI implementado

Riesgos que podrían afectar a la SI	Controles aplicados de la Norma ISO/IEC 27001:2013	Acciones integradas con la Norma de Control Interno de la CGE	Meta de las acciones $\overline{X}$ de los 3 períodos	∑ Datos obtenidos en las fases de implementación 2019, 2020 y 2021 Indicador de control - % de eficacia de la acción tomada = (actividades cumplidas/actividades planteadas) + (recursos utilizados/recursos asignados) /2								Evidencia	Beneficios obtenidos
				Actividades Planteadas	Actividades Cumplidas	Recursos Asignados	Recursos Utilizados	% Actividades cumplidas	% Recursos Utilizados	Eficacia de la acción	Desvíos		
No contar con políticas de SI	A.5 Políticas de SI	Aprobar, actualizar y socializar las políticas de SI	80%	10	8	45.130,59	35.843,01	60%	60%	60%	- 20%	Certificación del SGSI bajo la Norma ISO/IEC 27001:2013	Ahorro de recursos en la contratación del diseño del SGSI Aplicación paulatina de las políticas de SI
Falta de asignación de roles en SI y en el contexto Organizacional	A.6 Organización de la SI	Asignar roles y responsabilidades de SI Actualización de la Planificación estratégica con SI	80%	17	15	59.980,00	56.025,01	83%	76%	80%	0%	Manual de puestos, POA, Estatuto Organizacional con SI	Asignación de roles, responsabilidades y obligaciones para el buen desempeño de SI.
Falta de procedimientos de SI en los recursos humanos	A.7 Seguridad en los recursos humanos	Asegurar la información que tienen acceso el recurso humano	80%	23	20	23.770,00	18.645,08	83%	82%	82%	+2%	Acuerdos de confidencialidad, Concientización de la SI	Generó una cultura de SI en el personal y partes interesadas
Inadecuado manejo de Activos	A.8 Gestión de Activos	Llevar un correcto manejo de los activos de información documental y bienes	80%	38	36	76.435,27	69.415.01	94%	90%	92%	+12 %	Sistemas de control documental digitalizado y control de bienes	Fomento al gobierno digital Manejo adecuado de los activos de SI
No disponer de controles de Acceso	A.9 Control de Acceso	Adecuar controles de acceso a los sistemas de información	80%	40	35	13.844,00	10.734,92	85%	85%	85%	+5%	Contraseñas, privilegios de acceso a redes	Respuesta óptima frente a cualquier incidente de SI
No contar con controles Criptográficos	A.10 Controles Criptográficos	Mantener un control de los códigos encriptados de información sensible	80%	6	5	4.633,00	4.503,80	83%	82%	83%	+3%	Respaldo documental de códigos criptográficos	Resguardo de la información sensible y confidencial
Insuficiente Seguridad física y del Entorno	A. 11 Seguridad física y del Entorno	Mantener áreas seguras para resguardo de la información	80%	63	60	116.900,54	110.620,08	95%	95%	95%	+15 %	Áreas seguras en el Data Center, Backus y UPS.	Áreas seguras para la protección de los activos de la información
Inseguridad de las operaciones	A.12 Seguridad de las operaciones	Asegurar las operaciones ante posibles eventos e incidentes de SI	80%	53	47	40.936,78	32.944,31	83%	79%	81%	+1%	Respaldo periódico de los sistemas operativo, nube y licencias antivirus	Protección de los datos públicos, privacidad y control de la TI a través de los respaldos periódicos
Inseguridad en las Comunicaciones	A. 13 Seguridad en las Comunicaciones	Asegurar los accesos de comunicación, considerando los ataques cibernéticos	80%	25	22	27.796,00	21.199,89	80%	79%	80%	0%	Verificación de acceso a la red de internet y mensajería	Fomento al gobierno electrónico mediante servicios en línea por la página web
No velar por los requisitos de SI en la adquisición, desarrollo y mantenimiento de los sistemas de información	A 14 Requisitos de seguridad en la adquisición, desarrollo y mantenimiento de los sistemas de información	Considerar los aspectos relevantes y elementos de SI en las etapas contractuales	80%	29	25	8.116,00	6.791,33	81%	80%	80%	0%	Términos de referencia de los procesos de Contratación e informes técnicos	Infraestructura tecnológica y de comunicación funcional a la SI
Inseguridad de la información en relación con proveedores	A.15 Seguridad de la información en relación con proveedores	Asegurar la no divulgación o mal uso de la información entregada a terceros	80%	12	10	4.290,00	3.584,00	77%	76%	76%	-4%	Acuerdos de confidencialidad Evaluación periódica	Proveedores comprometidos con la SI
Inadecuada gestión de seguimiento a los incidentes de SI y mejoras	A. 16 Gestión de incidentes de SI y mejoras	Gestionar oportunamente los incidentes o eventos de SI que pudiera presentarse	80%	24	21	5.184,00	4.502,00	80%	80%	80%	0%	Informes de seguimientos de incidentes y eventos de SI	Disminución de gastos por incidentes de SI
Falta de Continuidad de la seguridad de la información	A.17 Continuidad de seguridad de la información	Aplicar un Plan de Contingencia ante cualquier entorno que pudiera presentarse	80%	15	13	44.564,92	41.443,20	84%	84%	84%	-4%	Plan de contingencia Anual Aplicación de teletrabajo	Interconexión con los sistemas operativos y aplicación del teletrabajo
Incumplimiento de requisitos y revisiones de seguridad de la información	A.18 Cumplimiento de requisitos y revisiones de seguridad de la información	Cumplir con los requisitos normativos y revisiones a la SI	80%	21	18	73.253,57	62.154,18	81%	80%	81%	+1%	Informe de vulnerabilidades técnicas Informe de Auditorias del SGSI	Revisiones periódicas al SGSI y SI
TOTAL			80%	376	335	544.834,67	478.405,84	82%	81%	81%	+1%		

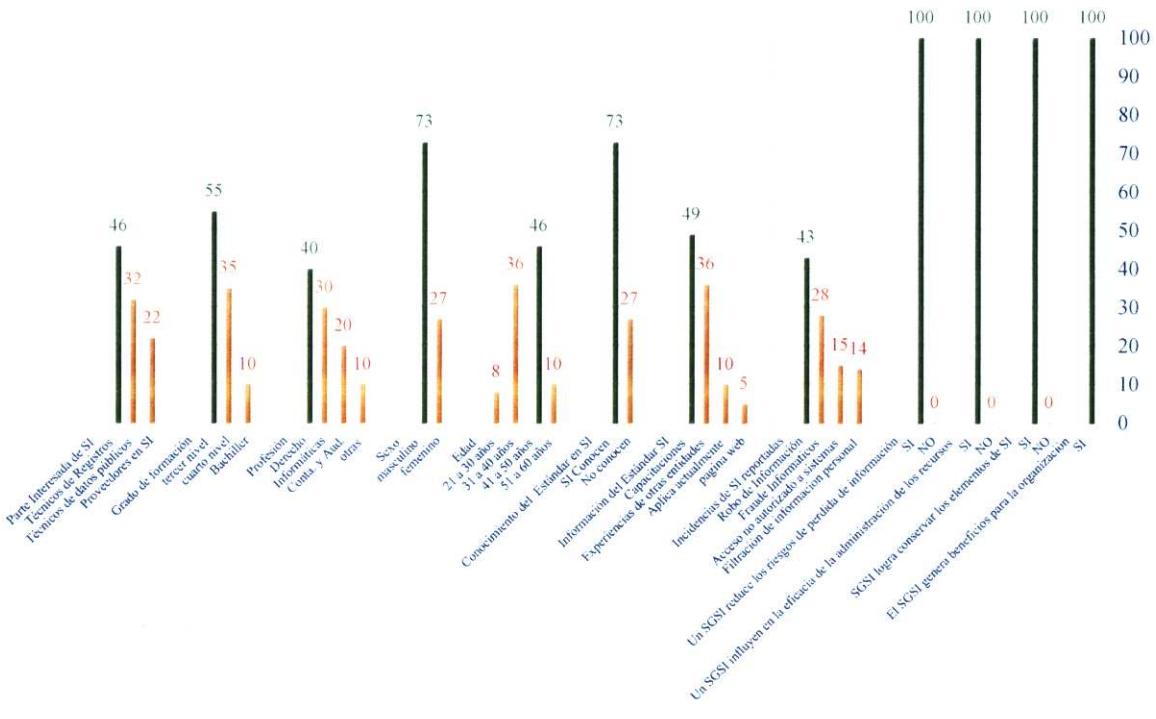
Fuente y adaptación de la autora: Actas de Comité de SI y Matriz de Riesgos de los períodos 2019, 2020 y 2021.

Del 73% de los encuestados que confirmaron conocer el estándar, el 49% obtuvieron estos conocimientos a través de cursos y talleres, seguido del 36% que se enteraron por experiencias de buenas prácticas de SI en otras entidades y escasamente el 10% aplica actualmente.

Ante los altos niveles de conocimientos del estándar, el 100% de los encuestados afirmaron que el implementar un SGSI bajo el estándar internacional ISO/IEC 27001:2013, reduce los riesgos de perdida de la información, influye en la eficacia de la administración de los recursos públicos, logra conservar los elementos de SI y genera beneficios futuros para la organización que adopte estos sistemas de gestión; en vista de que el 43% de los encuestados alguna vez tuvieron incidentes por robos de información y los recientes presentados en él (Registro de la Propiedad de Portoviejo, 2021).

Gráfico No. 2

Conocimiento de la norma internacional ISO/IEC 27001:2013



Fuente: Encuestas Google realizadas por la autora en el (Formulario de Perspectivas de las partes interesadas de un estándar en Seguridad de la Información, 2021)

Una vez evidenciado la descripción del modelo de SGSI diseñado bajo la integración de dos normativas; analizado la evolución del SGSI implementado y sus beneficios obtenidos, así como también, la interpretación de las perspectivas de las partes interesadas del estándar; y, tomando en cuenta que mi hipótesis al respecto es: "El diseño e implementación de un modelo de SGSI influye positivamente en la eficacia de la administración de los recursos públicos", **en opinión de las personas encuestadas la hipótesis planteada es verdadera;** debido, a que el modelo de SGSI adoptado por el RPMPM e implementado por fases bajo los estándares de SI y las NCI al aplicar sí fue eficaz al obtener completamente el 81% garantizada la seguridad de la información en la organización (Arévalo, 2021).

4.4 Propuesta de un prototipo de índice

Como producto de los hallazgos, propongo un prototipo de índice para poder cuantificar la eficacia de los recursos públicos asignados a los objetivos estratégicos de SI, administrados por las Registradurías en el Ecuador representada en la tabla No. 2, tomando en cuenta las líneas de investigación de trabajos relacionados a modelos de indicadores de los autores tales como (Leonel, 2015) en su artículo científico denominado: "Indicadores en el Modelo de Seguridad de la Información"; (Paus, 2016) en su obra titulada: "Como generar métricas de seguridad efectivas en la empresa"; y, la (CGE, 2001) en su "Manual de Auditoria de Gestión" (p. 110).

Para su medición, se ha propuesto la aplicación del método diseño métricas, con el fin de indicar cuantitativamente el grado de seguridad relativa al punto de referencia, que permita guiar el desarrollo de los beneficios obtenidos de SI luego de cumplir con los indicadores de control establecidos en el estándar internacional. La implementación dependerá de la naturaleza de la organización y del entendimiento de los índices por las personas que van hacer uso de ellos.

Tabla No. 2

Prototipo modelo de índice

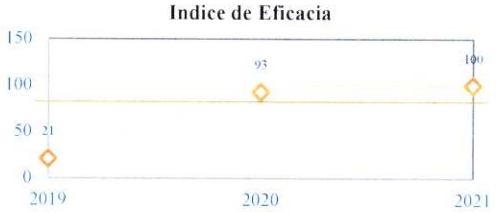
ÍNDICE PARA EVALUAR LA EFICACIA DE LOS RECURSOS PÚBLICOS DESTINADOS A LOS OBJETIVOS ESTRATÉGICOS DE SI			
IDENTIFICADOR:	**VERSIÓN: 00**	**CÓDIGO: SGSI-00**	**Fecha de Elaboración:**
FUENTE DE DATOS:	Matriz de Riesgos, Actas del Comité de SI, Matriz de Control del SGSI		
FRECUENCIA:	Anual (previo al informe de rendición de cuentas)		
CRITERIOS DE EVALUACIÓN DE EFICACIA: Determinar el % eficaz o no de los recursos públicos destinados a los objetivos estratégicos relacionados a la SI			

METODO DE CÁLCULO, ANÁLISIS Y REPORTE

Controles establecidos en la Norma ISO 27001:2013	Indicador Evaluado en la matriz de Riesgos Beneficios obtenidos	Resultado								
		Esperado			Obtenido			Cumplido		
		2019	2020	2021	2019	2020	2021	2019	2020	2021
A.5 Políticas de seguridad de la información	Ahorro de recursos en la contratación del diseño del SGSI Aplicación paulatina de las políticas de SI	70%	80%	90%	0%	80%	100%		X	X
A.6 Organización de la Seguridad de la Información	Asignación de roles, responsabilidades y obligaciones para el buen desempeño de SI.	70%	80%	90%	59%	83%	97%		X	X
A.7 Seguridad en los recursos humanos	Generó una cultura de SI en el personal y partes interesadas	70%	80%	90%	60%	88%	99%		X	X
A.8 Gestión de Activos	Fomento al gobierno digital Manejo adecuado de los activos de SI	70%	80%	90%	88%	92%	96%	X	X	X
A.9 Control de Acceso	Respuesta óptima frente a cualquier incidente de SI	70%	80%	90%	75%	80%	100%	X	X	X
A.10 Controles Criptográficos	Resguardo de la información sensible y confidencial	70%	80%	90%	50%	99%	100%		X	X
A. 11 Seguridad física y del Entorno	Áreas seguras para la protección de los activos de la información	70%	80%	90%	90%	95%	99%	X	X	X
A.12 Seguridad de las operaciones	Protección de los datos públicos, privacidad y control de la TI a través de los respaldos periódicos	70%	80%	90%	53%	90%	99%		X	X
A. 13 Seguridad en las Comunicaciones	Fomento al gobierno electrónico mediante servicios en línea por la página web	70%	80%	90%	50%	91%	99%		X	X
A 14 Requisitos de seguridad en la adquisición, desarrollo y mantenimiento de los sistemas de información	Infraestructura tecnológica y de comunicación funcional a la SI	70%	80%	90%	67%	81%	92%		X	X
A.15 Seguridad de la información en relación con proveedores	Proveedores comprometidos con la SI	70%	80%	90%	50%	79%	100%			X
A. 16 Gestión de incidentes de Seguridad de la Información y mejoras	Disminución de gastos por incidentes de SI	70%	80%	90%	49%	90%	100%		X	X
A.17 Continuidad de seguridad de la información	Interconexión con los sistemas operativos y aplicación del teletrabajo	70%	80%	90%	66%	86%	99%		X	X
A.18 Cumplimiento de requisitos y revisiones de seguridad de la información	Revisiones periódicas al SGSI y SI	70%	80%	90%	60%	83%	99%		X	X
TOTAL								**21%**	**93%**	**100%**

Índice de Eficacia de los recursos públicos asignados a SI Referencia (IE) 80%	**Resultados de la evaluación**	**No eficaz: X 21% (2019) SI Eficaz: X 93% (2020) y 100% (2021)**

RESULTADOS: El 21% de no eficaz, corresponde a los datos obtenidos antes de la implementación del SGSI, es decir que por desconocimiento del estándar, no se asignaron los recursos suficientes para los objetivos estratégicos de SI; al contrario, como lo muestra en la fase de implementación donde el 93% y 100% si fueron eficaces en la administración de recursos públicos al tener la capacidad para lograr los objetivos estratégicos de SI planteados y como referente de buenas prácticas, siendo el referente eficaz del 80%.



Fuente y adaptación del autor: Diseño de hoja de vida de indicador, propuesto por los autores (Leonel, 2015); (Paus, 2016);y, fórmulas extraído del Manual de Auditoría de Gestión (CGE, 2001)

5. Conclusiones y Recomendaciones

5.1 Conclusiones

En conclusión, el presente estudio permitió obtener una visión más clara sobre los resultados del diseño e implementación de un (SGSI) bajo el estándar internacional ISO/IEC 27001:2013 y el aporte en el control gubernamental al administrar correctamente los recursos públicos, cuya metodología mixta cuantitativa y cualitativa, permitió indagar lo siguiente:

El análisis cualitativo permitió adquirir un conocimiento más profundo sobre el estándar ISO/IEC 27001:2013, en virtud de que el activo más preciado para la operatividad de las organizaciones es la información; la cual demanda mayor protección ante la nueva era digital y por ende al surgimiento de implementar un sistema de gestión bajo los estándares de SI que al ser aplicados, son eficaces al estar completamente segura la información de la organización; esto es, preservar la confidencialidad, integridad y disponibilidad de la información a través de la administración correcta de los recursos públicos asignados específicamente alcanzar los objetivos estratégicos de SI; mediante la gestión de riesgos y al tener un buen control gubernamental, generando beneficios futuros para la organización que adopte este estándar.

La descripción del diseño del modelo de SGSI implementado por el RPMPM, permitió evidenciar que a través de la gestión de riesgos si es posible integrar un SGSI con la Norma Internacional ISO/IEC 27001:2013 y con la Norma Nacional de Control Interno expedido por la CGE, como lo mencionó (Moledo, 2016) que la "integración de un sistema basados en normas nacionales e internacionales", constituye una oportunidad de mejora y eficacia en la gestión organizacional, con el propósito de asegurar el correcto cumplimiento de los objetivos institucionales.

Del análisis cuantitativo realizado, en las bases de datos de las actas del comité de SI y matriz de riesgos, se aseguró que el modelo implementado por el RPMPM es correcto y que generó beneficios, a través de la evolución del SGSI, en las fases: antes (planeación), durante (implementación) y posterior (seguimiento), a través del cumplimiento paulatino de los controles establecidos en la Norma Internacional ISO/IEC 27001:2013, lo cual muestran que mientras más controles del estándar se aplican existe mayor eficacia en las acciones tomadas, generando mayor seguridad de la información y minimizando los riesgos valorados; así como, al no aplicar los controles del estándar existe más probabilidad de incidencias y perdidas de la información.

Por otro lado, al aplicar acciones de control acorde a lo estipulado en las NCI expedido por la CGE determinó mayor eficacia en las acciones tomadas, por cuanto se plantearon actividades específicas y se asignaron los recursos necesarios para su cumplimiento eficaz, logrando obtener los siguientes beneficios: (1) reducción de riesgos debido a la aplicación de controles; (2) reducción de las amenazas de SI al estar por debajo del nivel asumible, en el sentido que si se produjera una incidencia los impactos se minimicen; (3) aseguramiento de la continuidad funcional por efectos del COVID 19; (4) ahorro de costos derivados de la administración correcta de los recursos destinados específicamente para el cumplimiento de los objetivos de SI; (5) eliminación de las inversiones innecesarias; (6) aseguramiento del cumplimiento de la legislación internacional y nacional vigente; (7) obtención de la certificación del estándar internacional; y, (8) mejoramiento de la imagen, fomento a la cultura en SI y confianza de los usuarios.

Mediante encuesta formuladas se evidenció que el 73% de los encuestados, afirmaron poseer altos niveles de conocimientos del estándar ISO/IEC 27001:2013 por medio de cursos, talleres y experiencias de buenas prácticas en otras entidades, de los cuales el 100% percibió que si influye implementar un modelo de SGSI bajo la norma internacional ISO/IEC 27001:2013 en la eficacia de la administración de los recursos públicos, al lograr conservar la confidencialidad, integridad y disponibilidad de la información, a través del manejo correcto de los recursos asignados específicamente a cumplir los objetivos estratégicos de SI, mediante la gestión de riesgos, para obtener beneficios futuros. El otro 27 % de los encuestados desconocen el estándar; por cuanto, no hay una cultura de SI en nuestro país, de acuerdo a la entrevista realizada a la directora de la DINARDAP en (Primicias, 2021).

Finalmente, bajo el contexto analizado se pone en consideración un prototipo de índice para cuantificar en forma anual la eficacia de los recursos públicos destinado a los objetivos estratégicos de SI, administrados por las Registradurías públicas en el Ecuador, herramienta administrativa que permitirá guiar el desarrollo de las acciones de control planteadas por el Comité de SI. En el caso del RPMPM, los resultados indican que el 93% (2020) y 100% (2021) fueron eficaces en la administración de los recursos públicos al tener la capacidad para lograr los objetivos estratégicos de SI, lo cual contribuyó al buen control gubernamental y como referente de buenas prácticas a nivel nacional reconocida mediante el (Oficio Nro. DINARDAP-2020-0671-OF, 2020) como ganadora en la categoría: "Capacidad de Resiliencia en época de pandemia".

5.2 Recomendaciones

(Páliz, 2017) en su investigación, recomendó a la CGE actualizar los artículos 410 de las NCI relacionados a la Tecnología de la Información (p. 80), lo cual concuerda con la presente investigación, siendo primordial que la CGE actualice la normativa nacional de los artículos referentes a la SI a la realidad de los lineamientos establecidos en la Norma ISO/IEC 27001:2013 para llegar a los estándares de SI deseados.

En el Ecuador el INEN es la institución encargada de adaptar la Norma Internacional ISO/IEC 27001:2013; sin embargo, la última versión ha sido traducida idénticamente a la norma original, por lo que es necesario que el esquema normativo de SGSI se adapte a la realidad ecuatoriana, con la finalidad de incrementar su implementación y cultura de SI en las demás organizaciones.

Es necesario que la DINARDAP socialice la Ley de Protección de Datos Personales con los demás entes públicos; en vista de los aumentos alarmantes de ataques cibernéticos como lo muestra el informe de la (Organización International de Policía Criminal [INTERPOL], 2020), causados por los ciberdelincuentes que se aprovechan del "miedo y la incertidumbre provocados por la inestabilidad de la situación socioeconómica generada por la COVID-19" y el avance tecnológico.

Sugiero que este modelo de SGSI adoptado por el RPMPM, como referente de buenas prácticas, pueda ser aplicado por otras organizaciones que manejan datos públicos para generar nuevos datos que fortalezcan la SI en el Ecuador y a las nuevas investigaciones.

6. Referencias

Aguilar, M. (6 de 2017). *Plan de Seguridad informática basado en estándar ISO 27001, para proteger la Información y activos del GAD Cantonal de Pastaza.* Ambato: (Tesis de Grado) Universidad Regional Autónoma de los Andes.

Americanos, O. d. (28 de 4 de 2000). *Desastres, Planificación y Desarrollo:Manejo de Amenazas Naturales para Reducir los Daños.* (O. d. Americanos, Ed.) Obtenido de Publicación sobre aspectos de riesgos naturales en la Planificación de Desarrollo: Recuperado de http://www.oas.org/usde/publications/Unit/oea57s/begin.htm (2 of 3) [4/28/2000 11:05:29 AM]

Amoroso, R. (2018). *El control gubernamental frente a la titularidad del ejercicio público.* Quito: (Tesis de grado) Universidad Andina Simón Bolívar .

Arévalo, R. (8 de 2021). La Transparencia en la administración de los recursos públicos. *Ciencia Latina Revista Científica Multidisciplinar*, 4.

CGE. (2001). Manual de Auditoría de Gestión para la Contraloría General del Estado y entidades sometidos y organismos del sector público sometidos a control. 110. Quito: Contraloría General del Estado.

Chaverra, J. (2021). *Implementación de sistema de gestión de la seguridad de la información para el aseguramiento del proceso de ingreso de notas en un portal wev universitario.* Medellin: (Tesis de grado) Universidad de San Buenaventura.

Chilán, E., & Pionce, W. (2017, p. 294). Apuntes teóricos introductorios sobre la seguridad de la información. *Revista Científica Dominio de las Ciencias, Vol. 3, núm 4*(ISSN: 2477-8818), 284-295.

Constitución de la República del Ecuador [CRE]. (2008). *Constitución de la República del Ecuador.* Montecristi - Ecuador: Publicado en el Registro Oficial 449 de 20-oct-2008.

Corda, M., Coria, M., Cuervo, E., & Viñas, M. (2016, p.2). Nociones de gestión del riesgo en relación a las bibliotecas: apuntes conceptuales para su caracterización. *VII Jornadas Temas Actuales en Bibliotecología* , 2.

Escudero, I. (12 de 05 de 2020). *Administración eficiente de los recursos públicos asociados a la contratación pública en el marco de gestión de resultados para el desarrollo.* Quito: (Tesis de maestría) Universidad Andina Simón Bolívar.

Estrada, R., Unas, J., & Flórez, O. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle,sede Tuluá. *Revista Logos Ciencia & Tecnología, vol.13*(no.3), 108.

Figueroa, J., Rodríguez, R., Bone, C., & Saltos, J. (2017, p. 154). La seguridad informática y la seguridad de la información. *Polo del Conocimiento, 2*(12), 145-155.

Fonseca, O. (2019). *Modelo de un Sistema de Gestión de Seguridad de la Información en las organizaciones GEOCONSULT CS.* Bogotá: (Tesis de maestría). EAN Universidad.

Formulario de Perspectivas de las partes interesadas de un estándar en Seguridad de la Información. (11 de 06 de 2021). Quito, Pichincha, Ecuador: Encuestas formularios Google.

GAD Municipal del Cantón Pedro Moncayo. (2011). *Ordenanza para la administración y funcionamiento del Registro de la Propiedad y Mercantil del Cantón Pedro Moncayo.* Quito - Ecuador: GAD Municipal del Cantón Pedro Moncayo.

González, L., Narváez, C., & Erazo, J. C. (2019). La auditoria gubernamental y su inccidencia en la gestión institucional y manejo de recursos públicos. *Revista Interdisciplina de Humanidades, Educación, Ciencia y Tecnología, Vol. V*(N°1.), 480. doi:DOI 10.35381/cm.v5i1.277

Grajales, L., & León, M. (2016, p. 44). *Diagnóstico del grado de madurez de los controles de seguridad establecidos en la Norma NTC ISO/IEC 27001:2013 para asegurar la confidencialidad, integridad, disponibilidad y control de la información en instituciones de educación preescolar de la ciudad.* Pereira: (Tesis de grado). Universidad Católica de Pereira.

Guzmán, C. (2015). *Diseño de un sistema de gestión de seguridad de la información para entidad financiera de segundo piso.* Bogotá: (Tesis de grado). Instituto Universitaria Politécnico Gran Colombia.

Haz, F. (12 de 09 de 2017). *Revista Haz Fundación.* Obtenido de EL "Top Ten" de riesgos a los que se enfrentan las empresas: Recuperado de https://hazrevista.org/rsc/2017/09/el-top-ten-de-riesgos-a-los-que-se-enfrentan-las-empresas/

Hernández, R. (2014). *Metología de la Investigación.* Distrito Federal , México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.ISBN: 978-1-4562-2396-0.

Hidalgo, J. (2015, p.8). *Modelo de Gestión para mejorar la calidad de atención al usuario del GADM cantón Babahoyo.* Babahoyo: (Tesis de grado) Universidad Regional Autónoma de los Andes.

ISO, O. I. (14 de 09 de 2020). *The ISO Survey of Management System Standard Certifications.* Obtenido de ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements: Recuperado de https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

Leonel, A. S. (15 de 02 de 2015). Indicadores en el modelo de Seguridad de la Información. Obtenido de Universidad Piloto de Colombia: Recuperado de http://polux.unipiloto.edu.co:8080/00002244.pdf

Ley de Registro. (1980). *Ley de Registro.* Quito - Ecuador: Publicado en el Registro Oficial 136 de 28 de Febrero de 1980.

Ley Orgánica de Datos Personales . (2021). Quito: Publicado en el Registro Oficial No. 459.

Ley Orgánica del Sistema Nacional de Registro de Datos Públicos [LOSNRDP]. (2010). *Ley Orgánica del Sistema Nacional de Registro de Datos Públicos.* Quito: Asamblea Nacional del Ecuador - Registro Oficial Suplemento 162 de 31-mar.-2010.

Mantilla, S. (2018). *Auditoría del control interno* (Vols. e-ISBN 978-958-771-653-5). Bogotá: Ecoe Ediciones.

Medina, J. (2006, p.7). *Estandares para la seguridad de información con tecnologías de información.* Otoño: Universidad de Chile.

Medina, M. (2015). *Control Interno en la Administración de Recursos Públicos de la Municipalidad Distrital de Pucará.* Huancayo: (Tesis de grado). Universidad Nacional del Centro del Perú.

Meigs, L. (2004). *Principios de Auditoría, Segunda Edición.* México : Editorial Diana.

Mendoza, García, Delgado, & Barreiro, I. M. (28 de 10 de 2018). El control interno y su influencia en la gestión. *Revista cientifica Dominio de las Ciencias, Vol. 4*(núm. 4), pp. 206-240. Obtenido de Recuperado de file:///C:/Users/Registrador/Downloads/Dialnet-ElControlInternoYSuInfluenciaEnLaGestionAdministra-6656251%20(6).pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información [MINTEL], Acuerdo Ministerial No. 025-2019. (14 de 11 de 2019). Acuerdo Ministerial No. 025-2019. *"Esquema Gubernamental de Seguridad de la Información EGSI", versión 2.0.* Quito - Ecuador, Pichincha, Ecuador: Registro Oficial Especial No. 228, publicado el 10 de enero del 2020.

Moledo, F. (31 de 5 de 2016). *Integración de Sistemas de Gestión basados en Normas.* Obtenido de Asociación, Colegio Nacional de Ingenieros del ICAI: Recuperado de https://www.icai.es/articulo-revista/integracion-de-sistemas-de-gestion-basados-en-normas/

Normas de Control Interno para las Entidades, Organismos del Sector Público y de las personas jurídicas de derecho privado que dispongan de recursos públicos [NCI]. (2009). *Normas de Control Interno para las Entidades, Organismos del Sector Público y de las personas jurídicas de derecho privado que dispongan de recursos públicos.* Quito - Ecuador: Registro Oficial Suplemento 87 de 14-dic.-2009 - Contraloría General del Estado.

Oficio Nro. DINARDAP-2020-0671-OF. (11 de 12 de 2020). Reconocimiento como Ganadores de la categoría "Capacidad de Resiliencia en época del pandemia". Quito, Pichincha, Ecuador.

Organización International de Policía Criminal [INTERPOL]. (8 de 4 de 2020). *Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19.* Obtenido de Recuperado de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

Páliz, V. (2017). *Propuesta de complemento al artículo 410 de la Norma de Control Gubernamental Moderno emitida en el año 2009 por la Contraloría General del Estado del Ecuador sobre las tecnologías de la información y comunicaciones, aplicando estándares y buenas práctica.* Quito: (Tesis de maestría). Instituto de Altos Estudios Nacionales.

Paus, L. (06 de 09 de 2016). *Cómo generar métricas de seguridad efectivas en la empresa.* Obtenido de Welyvesecurity: Recuperado de https://www.welivesecurity.com/la-es/2016/09/16/metricas-de-seguridad-efectivas/

Pedraza, G. (2017). *Plan de implementación de un sistema de Gestión de Seguridad de la información en una entidad del Secto Público basado en la NTC ISO 27001:2013.* Bogota: (Monografía de especialidad). Fundación Universidad de América.

Primicias. (31 de 07 de 2021). *PRIMICIAS.* Obtenido de Recuperado de https://www.primicias.ec/noticias/tecnologia/lorena-naranjo-ecuador-cultura-proteccion/

Proaño, M., Orellana, S., & Martillo, I. (2018). Los sistemas de información y su importancia en la transformación digital de la empresa atual. *Revista Espacios, Vol. 39*(Nº 45), 4.

Registro de la Propiedad de Portoviejo. (18 de 3 de 2021). *https://registropropiedadportoviejo.gob.ec.* Obtenido de Recuperado de: https://www.facebook.com/REGISTRORPP

Reyna, Y. (2017, p. 158). El control a la gestión en la administración pública: una mirada a las legislaciones de Ecuador y Perú. *San Gregorio, iSSN 1390-7247; eISSN: 2528-7907*(19), 158.

Riestra, E. (1 de 12 de 2017, p. 5). *Seguridad de la información y delitos informáticos.* Obtenido de ordenjuridico.gob.mx/Congreso/pdf/133.pdf: Recuperado de https://lagesoft.files.wordpress.com/2017/12/seguridad-de-la-informacic3b3n-y-delitos-informc3a1ticos.pdf

Salcedo, Z. (5 de 2018, p. 21). *Exigencia de Implementar los procesos de control interno en las Organizaciones.* Bogotá: (Tesis de grado) Universidad Militar Nueva Granada.

Secretaria Nacional de Administración Pública [SNAP], Acuerdo No. SGPR-2019-0107. (10 de 04 de 2019). Acuerdo No. SGPR-2019-0107. *Regla Técnica Nacional para la Organización y Mantenimiento de los Archivo Públicos*. Quito, Pichincha, Ecuador: Registro Oficial, Suplemento No. 487, publicado el 14 de mayo del 2019.

Servicio Ecuatoriano de Normalización [INEN]. (22 de 02 de 2018). Servicio Ecuatoriano de Normalización [INEN]. *NTE INEN - ISO/IEC 27001 Segunda Edición*. Quito - Ecuador, Pichincha, Ecuador: [INEN], Servicio Ecuatoriano de Normalización.

Silva, F., Segadas, L., & Kowask, E. (2014). Gestión de la seguridad de la información. *REDCEDIA*, 23-32.

Sisti, M. A. (2019, p. 24). *Seguridad Informática: la protección de la información en una Empresas VITIVINÍCOLA de Mendoza.* Mendoza: (Tesis de grado) Universidad Nacional de Cuyo.

Tarzona, C. (2007, p.143). Amenazas Informáticas y Seguridad de la información. *Dialnet, 28*(84 (2007)), 143.

Valdiviezo, J., & Rodríguez, R. (5 de 2015). *Informe de Evaluación de Seguridad de la Información Basada en la Norma ISO 27001 en el departamente de TI de una empresa de lácteos.* Guayaquil: (Tesis de Grado) Universidad Politécnica Salesiana.

Vergara, G. (2017, p.21). *Seguridad de información y calidad de servicio en la Universidad Nacional Federico Vilarreal, 2016.* Lima: (Tesis de grado) Escuela de Posgrado Universidad Cesar Vallego.

Vinueza, J. (10 de 2021, p.4). La Optimización y el control interno en el uso de los recuros públicosen la mejora de la gestión administrativa. *Repositorio de la Universidad Estatal de Milagro, 5*(16), 4. doi:https://doi.org/10.23857/fipcaec.v5i14.158

Vite, H., Dávila, J., & Molina, B. (12 de 12 de 2019, p. 33). Gestión de la información en las instituciones de educación superior (IES) con base a la norma ISO 27001. *Journal of Science and Research: Revista Ciencia e investigación, E-ISSN: 2528-8083, Vol. 4, No. 1, ENERO - MARZO 2019*, 29-34. Obtenido de JOURNAL OF SCIENCE AND RESEARCH: REVISTA CIENCIA E INVESTIGACI´ON, E-ISSN: 2528-8083, VOL. 4, NO. 1, ENERO - MARZO 2019, PP. 29 -34.

Zuñiga, A., Jalón, E., Andrade, M., & Giler, J. (2021). Análisis de seguridad informática en entornos virtuales de la Universidad regional autónoma de los Andes extensión Quevedo en tiempos de covid-19. *Revista Universidad y Sociedad*, 455.

Anexos

Relación de la Norma ISO/IEC 27001:2013 con las NCI

Requisitos de la Norma ISO/IEC 27001:2013	Controles a los requisitos del Numeral 6 de la Norma ISO/IEC 27001:2013 (Anexo A)	Artículos de la Norma de Control Interno 2009
4.1 Contexto de la Organización 4.2 Comprensión de las necesidades 4.3. Determinar el alcance del SGSI 4.4. SGSI	A6. Organización de seguridad de la información	200-02 Administración estratégica 410-03 Plan informático estratégico de tecnología
5 Liderazgo 5.1. Liderazgo y compromiso 5.2 Política 5.3 Roles organizacionales y responsabilidades 6.2 Objetivos de SI y la planificación 6 Planificación 6.1 Acciones para aborda riesgos (Anexo A) 6.1.2 Apreciación de riesgos de SI 6.1.3 Tratamiento de riesgos de seguridad de la información 7. Soporte 7.1. Recursos	A5. Políticas para la seguridad de la información	200-05 Delegación de autoridad 410-16 Comité informático 410-02 Segregación de funciones 410-04 Políticas y procedimientos 300-01 Identificación de Riesgos 300-03 Valoración de Riesgos 300-02 Plan de Mitigación de Riesgos 300-04 Respuesta de Riesgo 402-04 Control de la evaluación en la ejecución del presupuesto
7.2. Competencias	A.7 Seguridad en recursos humanos	407-02 Manual de puestos 407-03 Incorporación de personal
7.3 Conciencia 7.4 Comunicación	A.16 Gestión de incidentes de seguridad de la información	410-15 Capacitación informática
7.5 Información documentada 7.5.2 Creación y actualización 7.5.3 Control de la información documentada	A8 Gestión de activos	500-01 Controles sobre SI 410-05 Modelo de información Organizacional 405-04 Documentación de respaldo
8. Operación 8.1 Planificación y Control Operacional	A 9 Control de acceso A.12 Seguridad de las Operaciones A.10 Criptografía A.13. Seguridad en las comunicaciones A14. Adquisición, desarrollo y mantenimiento del sistema A.11 Seguridad física y del entorno A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio A.15 Relaciones con proveedores	410-10-1 Ubicación adecuada y control de acceso físico a la Unidad de TIC 410.10-2 Definición de procedimientos de obtención periódica de respaldos 410.10-3 Actualización de tecnologías 410-12 Administración de soporte 410-17 Firmas electrónicas 410.10-4 Almacenamiento de respaldos 410-14 Sitio web, internet e intranet 410.10-5 Implementación de seguridades por incidentes identificados. 410-09 Mantenimiento y control de TIC 410.10-6 Instalaciones físicas adecuadas 410.10-7 Consideración de sitios de procesamiento alternativos 410-11 Plan de contingencias 410-07 Desarrollo y adquisición de software aplicativo 410-08 Adquisiciones de infraestructura tecnológica
9.1 Monitoreo, medición, análisis y evaluación	A.12.4 Registro y monitoreo	410-13 Monitoreo y evaluación de los procesos y servicios
9.2 Auditoría Interna 10 Mejora 10.1 No conformidad y acciones correctivas 10.2 Mejora continua	A.12.7 Consideraciones de auditoría de sistemas de información A.18 Cumplimiento	600-02 Evaluaciones periódicas

Fuente y adaptación de la autora: Manual del SGSI, Matriz de Riesgos y Declaración de Aplicabilidad