Universidad Inca Garcilaso de la Vega

FACULTAD DE INGENIERÍA DE SISTEMAS Y CÓMPUTO

Implementación de un sistema de gestión de seguridad de la información en una institución del sector cooperativo - Lima 2022.

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el título profesional de Ingeniero de Sistemas y Cómputo

AUTOR

Tirado Limay, César Juan Carlo

(https://orcid.org/0009-0000-1590-5994)

ASESOR

Mg. Muñoz Muñoz, Ricardo

(https://orcid.org/0000-0002-1768-0650)

Lima, noviembre 2023

Turnitin_TSP_Tirado_Limay

INFORME DE ORIGINALIDAD

20%	19%	7%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Inca Garcilaso de laVega Trabajo del estudiante	1%
2	repositorioacademico.upc.edu.pe Fuente de Internet	1%
3	www.slideshare.net Fuente de Internet	1%
4	hdl.handle.net Fuente de Internet	1%
5	www.coursehero.com Fuente de Internet	1%
6	repositorio.uigv.edu.pe Fuente de Internet	1%
7	repositorio.utp.edu.pe Fuente de Internet	1%
8	repositorio.usil.edu.pe Fuente de Internet	1%
9	repositorio.ucv.edu.pe Fuente de Internet	

DEDICATORIA

A mis padres César Luis y Tehelma Ydanea, a mis hermanos José Luis y Magaly por su inquebrantable apoyo incondicional a lo largo de los años.

Resumen

La seguridad de la información constituye uno de los pilares básicos de toda organización justamente al tener como elemento alrededor del cual gira todo proceso a la información en sí. La aplicación de controles que la resguarden y más aún que se integren a la complejidad particular de cada organización de manera transversal, en este caso particular de la institución cooperativa, hacían necesario es imprescindible que se implemente un sistema de gestión de seguridad de la información (SGSI) que interactuara con todos sus procesos de negocio. El SGSI debía tener un enfoque de riesgos con objetivos específicos de implementación que generasen cambios beneficiosos en la organización, para lo cual, considero que, se debía lograr un compromiso continuo de la alta dirección, la sensibilización constante del factor humano estableciendo una cultura de seguridad, la formalización de los procesos y la medición de todo lo actuado contribuyó al éxito de su implementación y mediante esto se logró un impacto positivo para la institución mediante el aporte de valor a sus operaciones y por consiguiente a sus partes interesadas. La mejora continua como un proceso evolutivo empleando estándares internacionales, marcos de trabajo y buenas prácticas brindaron las herramientas necesarias para medir adecuadamente el desempeño proactivo y la madurez del SGSI e integrarlo con otros sistemas de gestión con un enfoque holístico, permitiendo además estar constantemente alineado a los objetivos estratégicos de la cooperativa inclusive cuando se presentan períodos de alta incertidumbre con entornos cambiantes.

Palabras clave**:** seguridad de la información, gestión de riesgos, mejora continua, holístico, alineamiento estratégico.

Abstract

Information security represent one of the basic pillars of any organization precisely as it has the information itself as the element which every process revolves around. Theapplication of controls that protect it and even more so that would integrate into the particular complexity of each organization in a transversal manner, in this particular case of the credit union, made it necessary and essential that an information security management system be implemented (ISMS) that could interact with all its business processes. The ISMS should had a risk approach with specific objectives for the implementation generated beneficial changes for the organization, for which, I believe, a continuous commitment of the board, constant and immersive awareness program for the human factor in order to achieve a security culture, the formalization of processes and the measurement of the performance carried out contributed to the success of its implementation and through this a positive impact was achieved for the institution by adding value to its operations and consequently to its interested parties. Continuous improvement as an evolutionary process using international standards, frameworks and good practices provided the necessary tools to adequately measure the proactive performance and maturity of the ISMS and integrate it with other management systems with a holistic approach, therefore allowing to be constantly aligned to the strategic objectives of the credit union even in high uncertainty periods.

Keywords: information security, risk management, continuous improvement, holistic, strategic alignment.

Índice General

Índice de Figuras

Introducción

La información es el activo principal de toda organización. Esto hace que la aplicación de la gestión de seguridad de la información esté dirigida a toda persona natural o jurídica sin importar su tamaño u obligación de implementación y que dada su importancia se convierte en un factor de sobrevivencia y de éxito para el negocio. Para efectos de este trabajo, la implementación de un sistema de gestión de seguridad de la información (SGSI) debe alinearse con los objetivos estratégicos de la institución cooperativa y por ende ser un medio de generación de valor. Considero que se debe aplicar sobre tres ejes principales: procesos, personas y tecnología, a los cuales los acompaña o rige una estrategia de visión de la institución. La evolución natural del SGSI debe darse en asociación con los sistemas de gestión de continuidad de negocio, de protección de datos personales, de ciberseguridad e inclusive los de crisis para tener un panorama completo de las causas-consecuencias derivadas de un incidente, para lo cual es necesario realizar una identificación y evaluación de riesgos adecuada de manera iterativa y periódica que permita minimizar el efecto residual. El monitoreo, evaluación, medición de la efectividad de los controles, del desempeño de los planes de acción establecidos e inclusive de los incidentes que se hayan producido deben contribuir a enriquecer el sistema de gestión en un ciclo de mejora continua ante un contexto cambiante como se viene presentando en los últimos años, para beneficio de la institución y de sus partes interesadas.

El presente informe consta de cinco capítulos, los cuales poseen el siguiente contenido:

En el primer capítulo se describe la teoría sobre la cual se desarrolla el informe, incluyendo también el marco legal asociado, las metodologías usadas y los marcos de trabajo relevantes para la implementación del SGSI.

A continuación, en el segundo capítulo se realiza la descripción del contexto de la institución, los principales puntos de dolor y los móviles que generan las posibles soluciones al problema para lo cual se plantean los objetivos (generales y específicos) que se desean alcanzar.

En el tercer capítulo, se describe la justificación e importancia del desarrollo de la experiencia profesional en la solución del problema, haciendo hincapié en los puntos más

álgidos y de mayor relevancia que deben ser resueltos, estableciendo la delimitación correspondiente.

En el cuarto capítulo se describe el diseño de la solución, el mismo que se afianza en los conocimientos impartidos en la carrera profesional de Ingeniería de Sistemas y Cómputo, permitiendo establecer una visión centrada del resultado que se espera alcanzar.

El capítulo quinto describe de manera detallada y gráfica la forma en que cada uno de los objetivos planteados en el segundo capítulo han sido abordados y más aún como han contribuido a la solución de los problemas identificados siguiendo el diseño descrito en el cuarto capítulo.

Finalmente se presentan la conclusiones y recomendaciones derivadas del desarrollo de los capítulos previos y que se alinean a los objetivos planteados.

CAPÍTULO I: MARCO TEÓRICO DE LA INVESTIGACIÓN

En esta sección se revisan los conceptos más importantes que se relacionan con el objetivo del trabajo que se enfoca no solo en la implementación de un sistema de gestión de la seguridad de la información, sino que también promueva su continua evolución para adaptarse a los cambios del entorno.

1.1 Bases teóricas

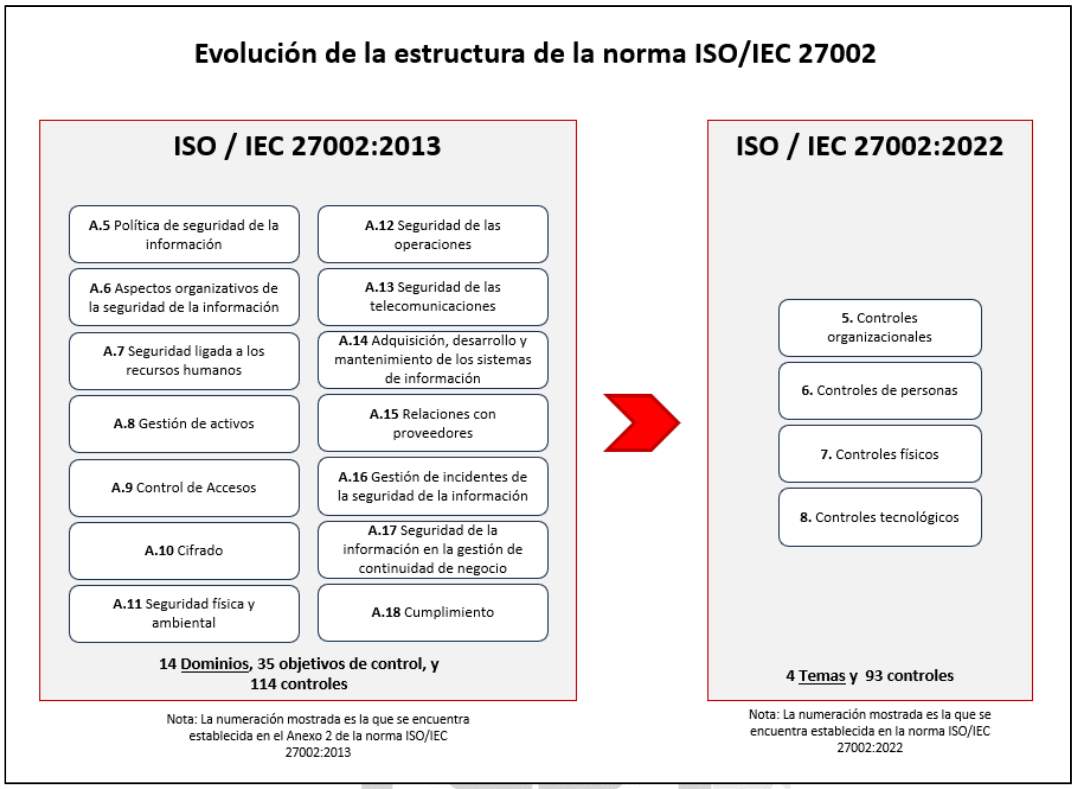
Gestión de la Seguridad de la Información. Abarca todos los conceptos, funcionalidades procedimientos, lineamientos y estrategias desarrolladas con el objetivo de asegurar la confidencialidad, integridad y disponibilidad (CID) de la información. Estos tres conceptos son conocidos como los principios de la seguridad de la información. Cabe destacar que la seguridad informática no es un sinónimo de la seguridad de la información: la primera está referida a la información que se recibe como ingreso (input), se procesa y tiene una salida (output) como parte de un proceso automatizado a través de sistemas informáticos, mientras que lo segundo abarca todo tipo de información que posee la empresa, no solo aquella procesada en una infraestructura tecnología, sino documentación física, equipamiento, audios, conferencias, personas que participan de procesos, estrategias, propiedad intelectual, etc., por lo cual la gestión es transversal a todas las áreas de la organización.

Uno de los marcos más importantes y de mayor uso a nivel mundial es el estándar internacional ISO/IEC 27001 referido al Sistema de Gestión de Seguridad de la Información, el cual agrupa las mejores prácticas para la adecuada protección de los principios CID. Este es un marco evolutivo que hasta la versión del 2013 del ISO/IEC 27002 se dividía en 14 dominios, 35 objetivos de control y 114 controles.

En la última versión ISO 27002:2022, conforme se muestra también en la figura 1, la estructura ha cambiado para reflejar un mejor alineamiento entre Personas, Procesos y Tecnología (considerando además a la parte física) los cuales representan sobre qué ámbitos se deben aplicar los controles propuestos por la norma, que para la mayoría de los casos es un remapeo de los controles previamente existente en la versión anterior con algunas supresiones, unificaciones y agregados para incluir también los temas relacionados con la ciberseguridad y servicios en la nube. Estos aspectos mencionados de controles físicos, de personas, de procesos y de tecnología son considerados “temas”, los cuales a su vez en total poseen 93 controles.

Se incluyen ambas versiones pues al ser de alguna manera reciente laactualización, la mayoría de las instituciones aún tienen sus políticas, procedimientos y controles basados en la 2013, agregando solo los nuevos a sus planes de gestión.

Figura 1. *Evolución de la norma ISO/IEC 27002 del 2013 - 2022*



Nota: Elaboración propia basado en las estructuras de la norma referida en ISO.org.

En la figura 1 se observa el cambio de estructura de la norma ISO/IEC 27002 las cuales pasan de tener 14 dominios de acción a solo 4, lo cual le permite hacer mayor incidencia en los entes sobre la cual se implementan los controles.

Gestión de la Continuidad de Negocio. Comprende el conjunto de normas, lineamientos y buenas prácticas que deben seguirse para asegurar la supervivencia de una organización ante alguna disrupción o materialización de un riesgo que impida su normal funcionamiento. La ISO compila estos lineamientos bajo el estándar ISO/IEC 22301: 2019 – Sistema de Gestión de la Continuidad del Negocio (ISO, 2019).

Gestión de la Ciberseguridad. Se puede tomar como base el concepto que concierne a la gestión de la seguridad de la información con el agregado de proteger a los activos de información que se encuentran en el ciberespacio. Esta gestión aplica controles a personas, infraestructura, proveedores, comunicaciones y partes interesadas, es decir a

toda la cadena que hace posible la entrega de información en el Internet (ISO, 2023). Las mejores prácticas se encuentran en el estándar ISO/IEC 27032:2023 que es la norma internacional para la Ciberseguridad y también en el Marco de Trabajo de Ciberseguridad de la NIST (CSF por las siglas del inglés *Cybersecurity Framework*), este último se encuentra descrito en la sección 1.4.

La ISO 27032 tiene alineamiento con la NIST para los objetivos de control, basándose en sus cinco funciones como son Identificar (saber que procesos necesitar protección), Proteger (implementar los controles de salvaguarda), Detectar (identificación de incidentes y ocurrencias de ciberseguridad), Responder (contener el impacto del incidente) y Recuperar (procesos para restaurar la capacidad de la organización para volver al estado normal).

Protección de Datos Personales. En la última década se han incrementado las iniciativas para formalizar y sobre todo dar seguridad a la información de identificación de las personas en todo el mundo. El avance de la tecnología y la proliferación de servicios en línea y en tiempo real han facilitado el intercambio de servicios de todo tipo, pero también han incrementado el riesgo sobre la confidencialidad de la información personal. La primera ley creada para la protección de datos tuvo lugar en Suecia en 1973 (Wikin , 2023). En 1998 en el Reino Unido tiene lugar una iniciativa para la regulación del tratamiento de los datos personales), basando su desarrollo en el establecimiento de los principios de protección, entre ellos el de calidad de los datos (integridad), especificación del propósito (justificación), limitación en la recolección (solo obtener lo necesario), seguridad (medidas que debe adoptar el receptor para garantizar la salvaguarda), transparencia (en cómo se usará la información y que sean accesibles para los titulares de los datos), el de responsabilidad (para el cumplimiento de las normas) y la limitación de uso (tiempo en el cual se pueden tratar los datos luego de lo cual deben eliminarse o anonimizarse (CEPAL, 2020).

Entre las normativas más sólidas en esta materia está la Regulación General de Protección de Datos de la Unión Europea, GDRP por sus siglas en inglés *General Data Protection Regulation* establecida en el 2016 (GDPR, 2016), en la que se establece la normativa a aplicar para el tratamiento de los datos personales de los ciudadanos de la UE en todo el mundo, es decir, su aplicación rebaza sus fronteras pues toda entidad en cualquier país que trate datos de europeos debe realizarlo en el marco de la GDPR.

En Perú, se oficializó la Ley 29733 - Ley de Protección de Datos Personales en el 2011 (reglamentada el 2013), la misma que tiene una base de alineamiento con los estándares de la familia ISO 27000 y su evolución se acerca a los de la GDPR.

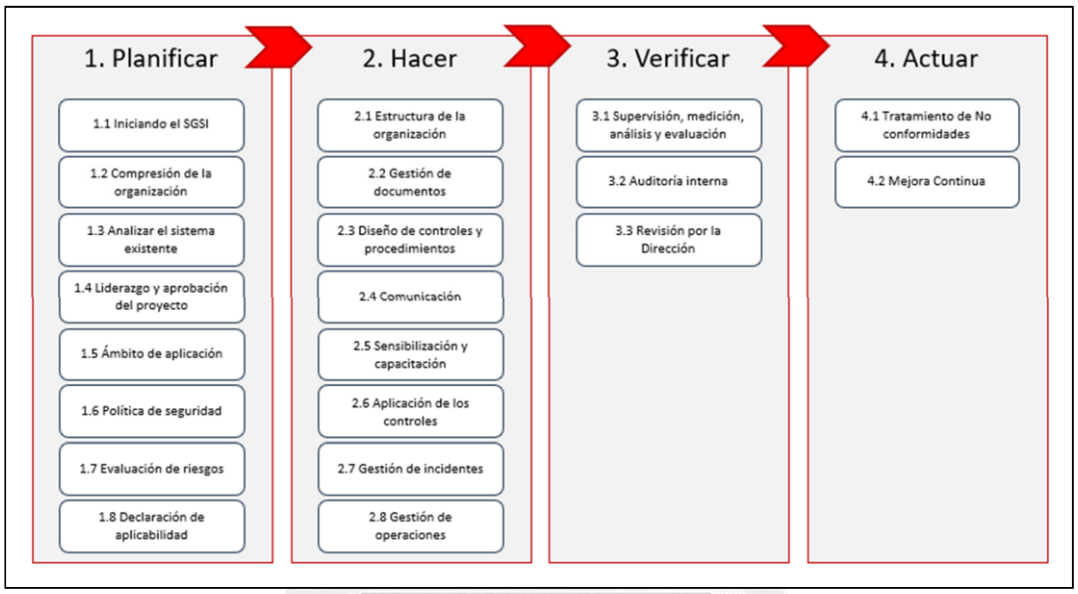
Gestión de Riesgos. Como se describe en el apartado 1.4, los riesgos son toda incertidumbre que impacta de manera positiva o negativa sobre un objetivo planteado. El tratamiento de riesgos puede realizarse implementando metodologías internacionales o marcos de trabajo/referencia, siendo un ejemplo de este último la norma ISO 31000 sobre Gestión de Riesgos, y si buscamos una aplicación más específica para los temas de seguridad de la información, ciberseguridad, protección de datos e inclusive continuidad de negocio, se puede tomar como base la norma ISO 27005 - Gestión de Riesgos de Seguridad de la Información, la cual se basa en la ISO 31000.

Mejora Continua. Son procesos que inciden en la búsqueda de hacer las cosas cada vez con una mayor calidad y una vez logrado se vuelve a analizar para mejorarlo. Existen numerosas metodologías para su implementación entre las cuales tenemos por ejemplo a *Lean, Six Sigma, Kaizen,* entre otras. Estas fueron aplicadas con gran éxito en compañías representativas de Japón, Estados Unidos de América y luego por todo el mundo. Este proceso involucra, más allá que solo herramientas y consultorías, un cambio en la cultura organizacional y los objetivos estratégicos del negocio, pues en algún momento se deben tomar decisiones sobre que procesos se deben mejorar, cuales eliminar y especialmente sobre cuales se debe realizar alguna disrupción en el camino a la innovación (Ashkenas, 2012).

Ciclo de Mejora Continua: Deming. Es un proceso iterativo en el cual se promueve la continua medición y revisión para lograr su optimización y mejora. Comprende cuatro etapas: Planear (*Plan*), Hacer, (*Do*), Verificar (*Check*) y Actuar (*Act*), de ahí que se conoce como PDCA (por sus siglas en inglés) o como el Ciclo Deming. Existen varias metodologías que han adoptado este ciclo, entre ellas está la metodología IMS2 (*Integrated Management Systems*) de PECB (*Professional Evaluation and Certification Board*) (PECB, 2020).

Para la implementación de un SGSI la organización es libre de elegir el marco o metodología que más se acomode al logro de sus objetivos sea una nueva o en todo caso una que ya se encuentre en ejecución, considerando en ambos casos que la adopción pueda darse en sincronía o alineamiento con la cultura organizacional.

Figura 2. *Metodología de Mejora Continua IMS2 de PECB aplicado al SGSI*



Nota: Tomado de *Certificación Implementador Líder ISO 27001*, por PECB, 2016.

En la figura 2 se muestra la forma en que la metodología IMS2 de PECB se aplica a la implementación del SGSI en una organización.

En el caso del Sistema de Gestión de la Continuidad del Negocio (ISO/IEC 22301) y la Gestión de Ciberseguridad (ISO/IEC 27032), si se desea aplicar la misma metodología, la estructura planteada será similar.

1.2 Marco legal

Resoluciones SBS. En el 2009, la SBS emitió las Circulares G-139-2009 y la G-140- 2009 referidas a la Gestión de la Continuidad del Negocio y la Gestión de la Seguridadde la Información respectivamente, las cuales se hicieron de obligatorio cumplimiento para todas sus entidades supervisadas, entre las que se incluye el sector financiero. Más adelante, en el 2020 se emite la Resolución S.B.S. N.º 877-2020 - SBS, Reglamento para la Gestión de Continuidad de Negocio, la misma que derogaba a la Circular G-139-2009. El mismo caso se presentó en el 2021 cuando la Resolución S.B.S. N.º 504-2021 - SBS, acerca del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad derogaba a la Circular G-140-2009. Es conveniente resaltar que inclusive hasta las publicaciones y entrada en vigor de estas normas, aún no se incluyen las cooperativas como parte obligada en su cumplimiento al no pertenecer expresamente al sector financiero.

Ley N.ª 29733 – Ley de Protección de Datos Personales (y sus modificatorias). Comprende el conjunto de normas en lo concerniente a los derechos de las personas naturales sobre el tratamiento de sus datos personales y sensibles, estableciendo criterios de salvaguarda basados en seguridad de la información (confidencialidad, integridad y disponibilidad). Asimismo, se establece como órgano rector a la Autoridad Nacional de Protección de Datos Personales, adscrita al Ministerio de Justicia y Derechos Humanos, quienes tienen capacidad de fiscalización y también sancionadora sobre toda persona natural o jurídica que contravengo lo estipulado en la ley y su reglamento (Congreso de la República del Perú, 2011).

Ley N.ª 30822 – Ley que modifica la Ley 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, y otras normas concordantes, respecto de la Regulación y Supervisión de Cooperativas de Ahorro y Crédito. Aprobada el 19 de julio de 2018, establece el marco para que en adelante las cooperativas de ahorro y crédito puedan ser supervisadas por la SBS. La ley entró en vigor el 1 de enero de 2019, sin embargo, no las incluye como parte del sistema financiero (Congreso de la República del Perú, 2018).

1.3 Antecedentes del estudio

Para la elaboración de la presente investigación se ha consultado fuentes a nivel internacional entre las que tenemos a Farinango y Negrete (2022) Desarrollo del programa del sistema de gestión de seguridad de la información de una Cooperativa de Ahorro y Crédito (Tesis de grado de Magister en Gerencia de Seguridad de la Información) Universidad de las Américas, Quito – Ecuador, que desarrollaron su trabajo basado en la implementación de un SGSI también en el ámbito cooperativo, partiendo de la identificación de riesgos y análisis de brechas, lo cual conllevó a plantear un objetivo / meta y el plan de acción con la priorización necesaria para alcanzarlo. Concluyen que el SGSI debe establecer los requisitos mínimos formalizados y respaldados por la Alta Dirección de la institución, así como la incorporación a sus respectivos planes estratégicosinstitucionales, realizando las mediciones correspondientes que permitan evaluar el desempeño del programa y reportándolos a ese órgano.

Según Toro (2021) Modelo de Políticas Estrategias y Controles que Permitan Minimizar los Riesgos para la Seguridad de la Información en la Nube Híbrida Existente en las Organizaciones (Tesis de grado de Magíster en Gestión de Tecnologías de la Información) Tecnológico de Antioquia, Institución Universitaria – Colombia, ocupa su

investigación en la seguridad de los espacios de almacenamiento híbridos, desarrollando un modelo para mitigar los riesgos de las entidades que deciden migrar a la nube parte de su información y los servicios asociados a esta. Para ello hace uso de marcos de trabajo, como por ejemplo el propuesto por la NIST (*National Institute of Standards and Technology*) de los Estados Unidos de América, hasta inclusive el juicio experto para elaborar un conjunto de estrategias, políticas y controles con el objetivo de minimizar los riesgos de materialización de incidentes de seguridad. Concluye mencionando que más que la adopción de un solo modelo, se requiere tomar las mejores prácticas en un ciclo de mejora continua para asegurar la información de la organización que opta por una nube híbrida.

Según Morales (2019) Balanced ScoreCard para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito (Tesis de grado de Magister en Gerencia de Sistemas de Información) Universidad Técnica de Ambato – Ecuador, comprende que el análisis de los activos críticos del negocio y su grado de riesgo son cruciales para construir un plan de seguridad que impacte positivamente en las áreas de riesgo y de tecnología. Mediante la medición en el *balance scorecard* se asegura el monitoreo y seguimiento de las actividades a desarrollar, permitiendo también llevar un adecuado control de la gestión integral de la seguridad de la información, lo cual es replicable a otra actividad económica o proyecto de la institución.

En el ámbito nacional se ha encontrado a Moscaiza (2018) Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013 (Tesis de pregrado en Ingeniería de Redes y Comunicaciones) Universidad Peruana de Ciencias Aplicadas, que describe y explica el correcto alineamiento que se debe tener entre los objetivos institucionales y la seguridad de la información con la que se realizan los procesos de negocio, además de cumplir con el marco regulatorio vigente. Se concluye que la identificación de los activos de información, así como el adecuado tratamiento de sus riesgos, acompañado de un marco de trabajo adecuado permiten elaborar y dar seguimiento a los planes estratégicos de seguridad de la información para la madurez de esta gestión y primordialmente en el acompañamiento de los objetivos estratégicos del negocio (Moscaiza, 2018).

Según Silva (2021) Implementación de un Sistema de Gestión de Seguridad de la Información para mejorar la Seguridad de la Información en una empresa MYPE - 2021 (Tesis de pregrado en Ingeniería de Sistemas e Informática) Universidad Tecnológica del Perú, resalta la importancia del sector de las MYPES que emplean al 26.6% de la

población económicamente activa (PEA) y al mismo tiempo que no todas la dan la importancia debida a su información institucional, por lo cual propone establecer los lineamientos basados en riesgos y en un proceso de mejora continua para implementar un SGSI. Concluye que la implementación de dicho sistema promueve la productividad de los empleados mediante la reducción de posibles incidentes de seguridad, salvaguardando sus activos de información e involucrando a toda la estructura organizacional con el respaldo de la Alta Dirección para el cumplimiento de las políticas establecidas. Asimismo, menciona que la implementación debe realizarse de acuerdo con las necesidades reales y recursos disponibles de cada MYPE de acuerdo con el objetivo que esperan alcanzar.

Según Niño (2019) Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI filial Lambayeque (Tesis) Universidad Nacional Pedro Ruiz Gallo, destaca también la necesidad de controlar los riesgos latentes para proteger la información de la institución, para lo cual propone el modelo de seguridad de la información basado en el ciclo PDCAde mejora continua, concluyendo que este último permite a la organización la identificación de potenciales vulnerabilidades que puedan presentarse por el lado de los recursos, las personas y la información tratada en los procesos.

1.4 Marco conceptual

Cooperativa de Ahorro y Crédito (COOPAC). Institución sin fines de lucro que basa sus operaciones en el apoyo mutuo y bienestar de sus asociados, promoviendo valores de cooperación y de superación colectiva (Superintendencia de Banca, Seguros y AFP, 2022).

FENACREP - Federación Nacional de Cooperativas de Ahorro y Crédito del Perú. Institución creada en abril de1959 para agrupar a las cooperativas de ahorro y crédito con el objetivo de fomentar su estandarización y formalización siempre en el marco de los valores cooperativos. En 1992 el Estado peruano le confirió facultades de supervisión, lo cual no incluía capacidad de sanción. Estas facultadas se mantuvieron hasta el 2018. (FENACREP, 2023)

SBS - Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones**.** Institución estatal que regula a todo el sistema financiero, el de seguros y a las administradoras de fondos de pensiones en el Perú. Establece las normativas y

lineamiento para el buen gobierno, solvencia y estabilidad de las entidades a las que supervisa y con ello brindar la seguridad al público usuario sobre los productos activos y pasivos que estas ofrecen, promoviendo la inclusión financiera y fortaleciendo la lucha contra el lavado de activos y financiamiento del terrorismo.

Sector Financiero. Compuesto por las instituciones que captan y administran los fondos de los ahorristas para ofrecerlos a inversionistas, personas naturales o jurídicas que requieran financiamiento. Se encuentra conformados por los bancos, financieras, cajas rurales y cajas municipales. Este sector se encuentra regulado por la SBS (PRESTAMYPE, 2023).

Sistema de Gestión. Conjunto de elementos interrelacionados de una organización parael establecimiento de políticas y procedimientos para alcanzar los objetivos propuestos (ISO, 2015)

Seguridad de la Información. Protección de la confidencialidad, integridad y disponibilidad de la información (ISO, 2022).

Ciberseguridad. Salvaguardar a las personas, organizaciones, sociedad y naciones de los riesgos del ciberespacio (ISO, 2023).

Continuidad de Negocio. Capacidad de la organización para continuar brindando sus productos y servicios de acuerdo con los parámetros planificados en caso de materialización de una interrupción y dentro de un plazo aceptable (ISO, 2019).

Datos personales. Los datos personales es toda información perteneciente a una persona natural que lo hace identificable a través de diversos medios (Congreso de la Repúblicadel Perú, 2011).

Datos sensibles. Son una parte de los datos personales que comprenden un ámbito aún más privado como son los biométricos, origen racial, información de salud, ingresos económicos, creencias religiosas o políticas, orientación sexual, entre otros (Congreso de la República del Perú, 2011).

Riesgo. Un riesgo es definido como la incertidumbre sobre los objetivos trazados, sea este positivo o negativo (ISO, 2018).

Gestión de Riesgos. Proceso iterativo que permite a las organizaciones desarrollar estrategias y/o tomar decisiones informadas que les permita alcanzar sus objetivos (ISO, 2018).

Marco de Ciberseguridad de la NIST (*National Institute of Standards and Technology*). Propuesto por el instituto de estándares y tecnología de los Estados Unidos de América consta de un grupo de lineamientos, controles y buenas prácticas enfocadas a reducir el

riesgo de ciberseguridad, el mismo que es de uso voluntario de cualquier organización (NIST, 2023).

COBIT (*Control Objectives for Information Technologies)*. Marco de trabajo para las mejores prácticas en gestión y gobierno de tecnologías de la información (ISACA, 2023).

Mejora continua. Es un proceso iterativo en el cual se promueve la continua medición y revisión para lograr su optimización y mejora (ISOTOOLS.US, 2015).

CAPÍTULO II: PLANTEAMIENTO DEL PROBLEMA

En esta sección se revisan la situación o contexto que afronta la organización en consideración de un problema que afecta o que podría mermar su funcionamiento en el futuro, con lo cual se busca establecer objetivos que permitan disminuir los impactos negativos y convertirlos en una oportunidad de mejora.

2.1 Descripción de la realidad problemática

A nivel mundial, en las últimas tres décadas, el desarrollo y auge de la tecnología ha sido exponencial, lo cual ha llevado a que la información que poseen o tratan las organizaciones, en cualquiera de las formas en que se encuentre, esté expuesta cada vez más a mayores amenazas. La globalización ha permitido que hasta la institución o empresa más pequeña pueda publicar sus productos en el Internet para tener un segmento de mercado mucho más amplio. Este es el caso no solo de las entidades del sistema financiero mundial, sino también del cooperativo cuya cultura tiene presencia en todoslos continentes. Según datos del WOCCU (*World Council of Credit Unions*) del 2013 se identificaban en ese momento más de 57,000 cooperativas de ahorro y crédito (COOPACs) ubicadas en 103 países, las cuales atendían a 208 millones de personas con más de US$ 1.7 billones en activos (WOCCU, 2014).

Durante ese rango de décadas, también tuvieron una importante evolución las normativas, tanto a nivel de leyes como de marcos de trabajo (como se mencionó en el primer capítulo del presente trabajo), que establecieron los lineamientos para la protección de los datos personales y en general para todos los activos de información de las instituciones. Si bien es cierto, inicialmente estos fueron adoptados en su mayoría por grandes corporaciones, considerando la idea que requería de inversiones considerables, esto ha ido masificándose para más que considerarse un asunto de cumplimiento se vuelvauna necesidad de supervivencia.

En Latinoamérica se ubican el 4.5% de las COOPACs, las cuales concentran un volumen de activos de 3.96% del global mencionado. Las cooperativas afiliadas al WOCCU, siguen principios de estandarización promovidos por las Naciones Unidas, la Comunidad Europea, el G20, el Comité de Supervisión de la Banca de Basilea (*Bank for International Settlements*), entre otros.

En el Perú, la cantidad de COOPACs en el 2013 era de 167 (0.3% del global) sirviendo a casi 1.3 millones de socios. El organismo base para la membresía en el WOCCU es la FENACREP, la cual promueve los valores y apoyo mutuo no solo a nivel nacional y regional sino también mundial.

Como se había señalado en el capítulo previo, con las COOPACS se iniciaron las acciones de supervisión por parte de la SBS desde enero de 2019, pero sin ser incluidas como parte de sector financiero hasta la actualidad. Esto tiene vital importancia pues muchas normas generales que emite la SBS son dirigidas al sector financiero, con lo cual tácitamente las cooperativas quedan exentas de su cumplimiento, salvo en aquellas que son específicamente dirigidas al sector cooperativo.

Según lo previamente establecido, la cooperativa no tenía obligación en el cumplimiento de las normativas emitidas el 2009, pero eso no evita que sus activos se encontraran bajo amenazas externas o internas, sea intencional o involuntario (por inducción al error).

Es así que, a finales del 2013, la institución toma como decisión incorporar el puesto de Oficial de Seguridad de la Información para implementar las circulares G-139- 2009 y la G-140-2009 referidas a la Gestión de la Continuidad del Negocio y la Gestiónde la Seguridad de la Información respectivamente, para iniciar con ello el alineamiento normativo con miras a una futura supervisión y también como adopción de las buenas prácticas de la industria en la salvaguarda de sus activos de información como parte de no solo sobrevivencia de la organización, sino también como un factor diferencial para mejorar sus estrategias de negocio y relacionamiento con partes interesadas . En resumen, se opta por cubrir necesidades y obligaciones: por estar un paso adelante en el sector, por regulación y por adaptación ante amenazas latentes (supervivencia).

En el análisis inicial realizado en el primer trimestre del 2014 se buscó caracterizar la gestión de la seguridad de la información en la institución utilizando el diagrama de Ishikawa, conforme se muestra más adelante en la figura 3. Para tener un mejor entendimiento, se tomaron solo 5 de las 6 categorías: mano de obra, maquinaria, materiales, método y medición, renombrándolas como personas, tecnología, información, procesos y estrategia respectivamente. Se dejó de lado la categoría Medio ambiente, por no considerarse relevante en el momento en que se llevó a cabo el análisis. En el siguiente párrafo se expondrán los principales hallazgos de cada una de las categorías mencionadas, no siendo estos los únicos sino los que tenían un mayor grado de compromiso y riesgo por atender.

Conforme lo señalado, describiremos los hallazgos más destacados ubicándolos en las categorías previamente mencionadas:

Mano de obra (Personas). La cultura organizacional es un factor determinante para una adecuada gestión y el factor humano, quien finalmente es el que mueve a la institución basada en su misión, visión, valores, principios y normativa interna. En este aspecto, se observó que la concientización sobre seguridad de la información era muy baja y que eso había llevado a un casi nulo control de los privilegios otorgados a los usuarios, los mismos que a su vez no les generaba el incentivo de reportar posibles incidentes toda vez que no se tenía una noción del impacto que podría tener una brecha o materialización de alguna amenaza. A este punto el usuario se mostraba reacio a cualquier cambio que signifique tener menos permisos o libertadas sobre los accesos que tenían asignados, uno de ellosque quizá sea el más representativo era el privilegio de navegación en Internet sin mayor restricción.

Maquinaria (Tecnología). La infraestructura tecnológica había evolucionado con controles perimetrales adecuados pero básicos en sus configuraciones: existía un gran espacio y oportunidad para optimizar y mejorar la seguridad externa, perimetral e interna. Existía una falta de identificación de la dependencia tecnológica con respecto a los procesos críticos de la institución, lo cual pasaba por una posible afectación del servicio al socio al carecer de pruebas que pudieran asegurar la continuidad de las operaciones en caso de falla de algún elemento de la infraestructura. Adicionalmente, los servicios contratados con terceros necesitaban ser optimizados en cuanto a la formalización de sus procesos de soporte, así como la idoneidad de los acuerdos de nivel de servicio y el monitoreo sobre el mismos para asegurar su cumplimiento.

Materiales (Información). Como se había mencionado, para esta gestión no solo se está considerando a la seguridad informática sino a la seguridad de toda la información de la institución representada en cualquiera de sus estados y formas. En la institución se necesitaba realizar una identificación de sus activos de información considerando los aspectos de hardware, software y aplicaciones, infraestructura de redes, equipos auxiliares, personas, lugares físicos o instalaciones, servicios institucionales, estructura organizacional y partes interesadas, procesos de negocio y datos / información *per se* (los mismos que se encuentran definidos como categorías de acuerdo con la ISO 27005:2018

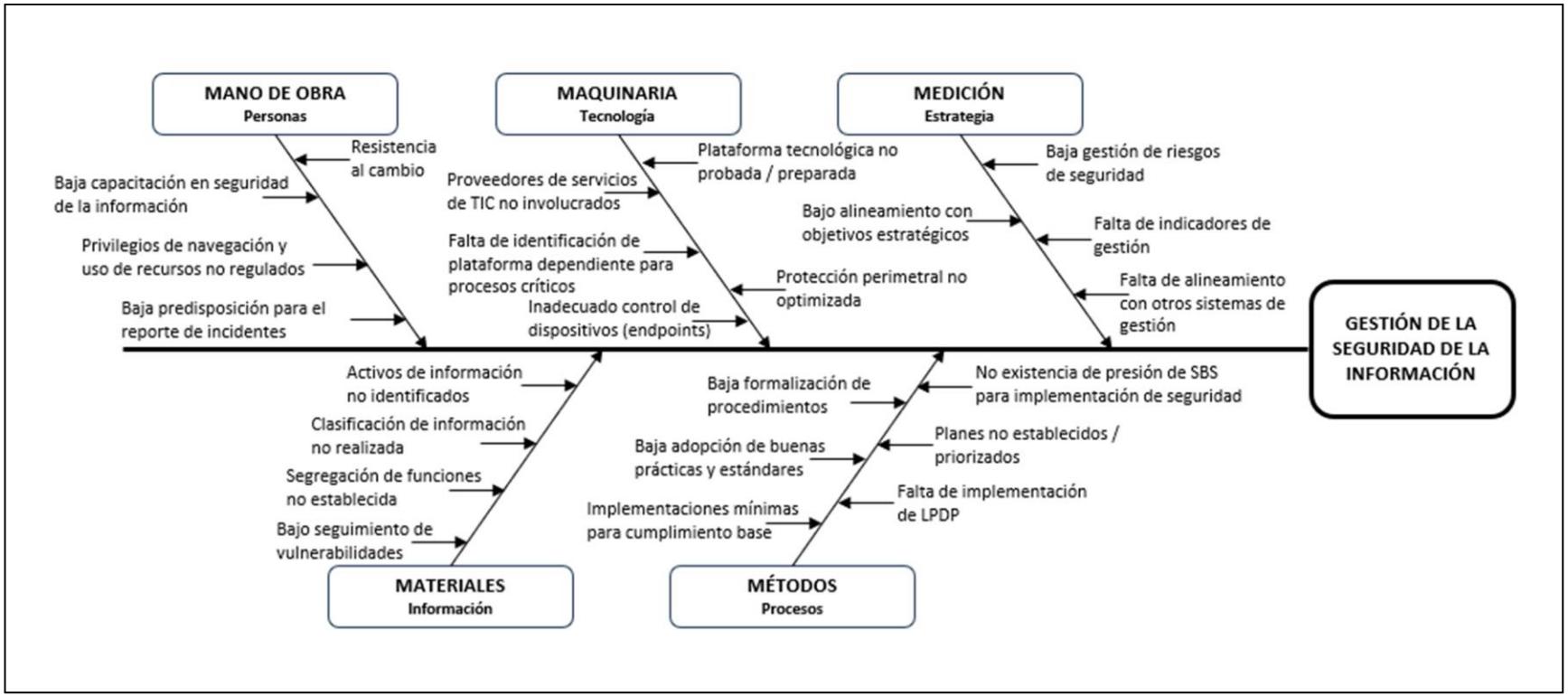
- Gestión de riegos de seguridad de la información). Se debía establecer una adecuada clasificación para determinar que activos son de uso público, cuales son internos y también cuales entrar en la esfera de poseer un carácter confidencial, lo cual determina asu vez el grado de protección a asignar a cada uno de ellos y quienes deben tener acceso

a su tratamiento. Por último, se requería realizar una adecuada gestión de las vulnerabilidades a las que estaba expuesto cada activo, lo cual debía ser realizado mediante la identificación de amenazas latentes, es decir con una adecuada gestión de riesgos.

Métodos (Procesos). La institución venía laborando y cumpliendo con sus obligaciones y un servicio adecuado hacia sus socios y partes interesadas, pero en cuanto a la formalización de sus procesos internos, como parte de su madurez, se encontraban en un grado bajo. Esto impactaba en su grado de planificación, optimización y mejora al necesitar una normativa base y completa (ampliación y especificación de políticas, procesos, procedimiento y guías) que documenten y marquen los lineamientos de la operatividad diaria. Lo mencionado, impedía la rápida adopción de normas y buenas prácticas aceptadas internacionalmente, aparte que los alejaba de la formalización que requería la SBS ante una eventual supervisión. Asimismo, a esa fecha aún no se contaba con una ruta establecida que permitiera cumplir con la Ley de Protección de Datos Personales que si era de obligatorio cumplimiento para toda persona natural o jurídicaque realice el tratamiento de datos de identificación personal.

Medición (Estrategia). En el análisis se corroboró que se contaba con implementaciones de gestión de riesgos enfocados en el lado operativo y financiero, sin embargo, no se evidenciaba que se hayan ejecutado evaluaciones relacionadas a seguridad de la información. Esto conllevaba a que se carezca de una medición, mejora, o alineamiento a los objetivos de la organización que proporcionasen una necesidad real inmediata. Si bien es cierto no se tenía una obligación explícita para cumplir con la norma, en el último trimestre del 2013 se vio por conveniente que se iniciara el camino de implementación del sistema de gestión, conforme lo señalado por la SBS.

Figura 3. *Diagrama de Ishikawa*



Nota: Elaboración propia basada en el modelo causal de Ishikawa.

En la figura 3 se presenta el diagrama causal de Ishikawa con la caracterización de la seguridad de la información en el inicio del análisis previo a la implementación del sistema de gestión.

De acuerdo con el diagrama previamente presentado, se mediarán las frecuencias tomando como base las categorías descritas, lo cual permitirá ver el grado de incidencia de cada una de ellas sobre la problemática identificada.

Tabla 1. *Frecuencia de las causas*

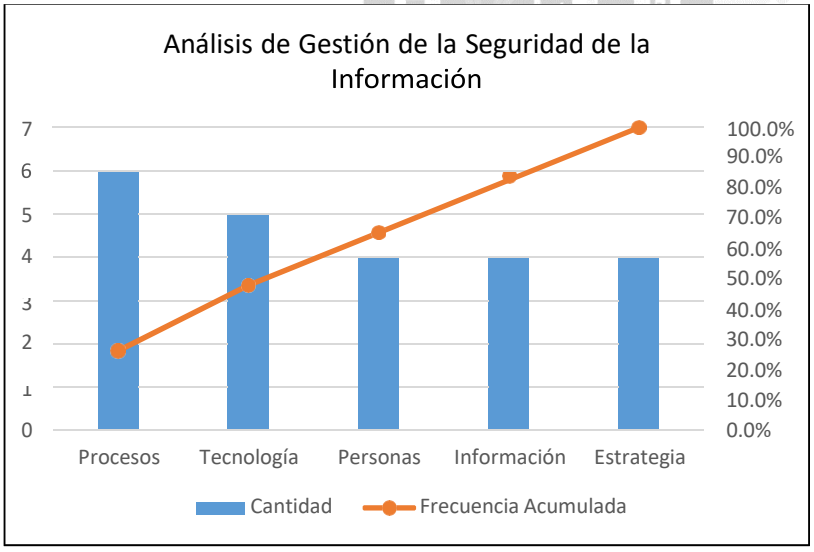
Causas	Cantidad	Frecuencia	Frecuencia Acumulada
Procesos	6	26.1%	26.1%
Tecnología	5	21.7%	47.8%
Personas	4	17.4%	65.2%
Información	4	17.4%	82.6%
Estrategia	4	17.4%	100%

Fuente: Elaboración propia.

En la tabla 1, se resumen las causas o principales problemáticas descritas en los párrafos precedentes, agrupados según las categorías descritas.

De la información resultante del análisis inicial realizado a la institución se desprende el diagrama que se muestra a continuación.

Figura 4. *Diagrama de Pareto*



Fuente: Elaboración propia.

En la figura 4, el diagrama de Pareto muestra que las causales halladas tienen una distribución proporcional, destacando ligeramente las categorías de Procesos y Tecnología. Esto finalmente nos indicaba que el estado de la seguridad de la información en aquel momento (2013) se veía impactado de manera transversal en la institución por

lo cual se necesitaba un enfoque holístico para su implementación, optimización y mejora.

2.2 Formulación del problema general y específicos

En base a lo planteado en lo puntos precedentes, se ha identificado el siguiente problema general:

¿De qué manera la implementación de un sistema de gestión de la seguridad de la información basada en riesgos favorecerá el gobierno de la institución cooperativa?

De aquí se desprenden los siguientes problemas específicos (PE):

PE1. ¿Está la Alta Dirección comprometida con la implementación y la asignación de los recursos necesarios?

PE2. ¿Está la cultura organizacional preparada para la implementación considerando los cambios que se generarán en todos los aspectos de personas, procesos y tecnología?

PE3. ¿En qué medida el estado de formalización / madurez de la organización incidirá en el proceso de implementación?

PE4. ¿El sistema a implementar apoyará los objetivos estratégicos de la institución?

2.3 Objetivo general y específicos

En base a lo planteado en lo puntos precedentes, se ha identificado el siguiente objetivo general:

Implementar un sistema de gestión de seguridad de la información utilizando los estándares y buenas prácticas internacionales que apoye los objetivos estratégicos de la institución.

De aquí se desprenden los siguientes objetivos específicos (OE):

OE1. Describir como el compromiso de la Alta Dirección en asignar los recursos y respaldar las acciones de implementación de la cultura de seguridad contribuirán al éxito de la implementación del sistema de gestión.

OE2. Describir como la sensibilización de todas las unidades organizacionales permitirá realizar los cambios requeridos considerando un enfoque basado en riesgos.

0E3. Describir como la institucionalización de todos los procesos asociados al sistema de gestión permitirán un entorno evolutivo.

0E4. Describir como la medición y evaluación constante del desempeño de los planes planteados alineados con los objetivos estratégicos permitirán no solo una implementación evolutiva sino también generar valor para la institución.

CAPÍTULO III: JUSTIFICACIÓN Y DELIMITACIÓN DE LA INVESTIGACIÓN

3.1 Justificación e importancia del estudio

La misión de la institución definida en el 2014 era la de brindar a sus socios una experiencia financiera adaptada a sus necesidades para apoyar su desarrollo y bienestar en el marco de un modelo de cooperación innovador y de compromiso institucional con la sociedad.

La información que administrada por la cooperativa era y es su activo más importante, convirtiéndose así en la base para brindar sus servicios financieros en bien de sus asociados, por lo cual quedaba comprendida dentro de la normativa de seguridad y confidencialidad en todos sus aspectos: impresa, hablada, publicada, enviada por correo electrónico, transferida en formatos digitales, proyectada en conferencias o reuniones y remitida utilizando cualquier otro método de tratamiento.

La información gestionada por la cooperativa fue y es su activo más importante y por lo tanto se convierte en la base para la prestación de servicios financieros en beneficio de sus socios, por lo que está incluida en todos los aspectos de las normas de seguridad y confidencialidad: impresa, oral, publicada, remitida por correo electrónico, transferida en formato digital, difundida de una conferencia o tratada haciendo uso de cualquier otro método de procesamiento.

La naturaleza del tratamiento de la información está determinada por el grado de confidencialidad entre el remitente y el destinatario, el medio de información utilizado yel tipo de información a divulgar, que se manifiesta en tres características básicas: Confidencialidad, para garantizar que sólo el personal autorizado pueda acceder a la información; integridad, para proteger con precisión la información y sus métodos de procesamiento; y disponibilidad, para garantizar que sólo las personas o los usuarios autorizados puedan acceder a información y recursos relevantes en el momento en quesea requerido.

La proliferación de amenazas está siempre en aumento y proviene de diferentes fuentes (externas e internas), las cuales ponen en riesgo la información gestionada o tratada por la institución cooperativa, sean éstas por causas deliberadas o accidentales.

Esto suele suceder con frecuencia constituyendo incidentes o amenazas que no se pueden ignorar: los casos más simples y accidentales pueden darse con el extravío de una computadora portátil (laptop), o un teléfono inteligente (Smartphone) o una memoria externa (conocida como memoria USB), software de contenido malicioso instalados enlas computadoras personales, o casos forzados como un empleado descontento o el empleado-infractor, o la violación de las medidas de protección para que los datos

importantes de los socios de negocios o clientes vayan a las manos equivocadas. Esto puede redundar en costos directos sustanciales, y más aún se pueden traducir en pérdidas indirectas, pérdida de negocio y dañar la reputación de la institución que es un activo de valor incalculable.

Por estas razones, se hace imprescindible e impostergable el desarrollo e implementación de políticas, buenas prácticas y procedimientos adecuados que sean compatibles con la legislación aplicable en materia de seguridad de la información, privacidad y protección de datos personales con una metodología o marco de trabajo que no solo permita disminuir las posibilidades de amenaza latentes, sino también actuar de manera proactiva para evitar brechas que posibiliten la violación de la seguridad de los datos y que en el futuro permitieran allanar el camino a la supervisión por parte de los órganos reguladores competentes, contribuyendo a su vez con una mejora de los procesos institucionales y la adaptación cultural requerida, convirtiendo a la institución en un referente del sector.

3.2 Delimitación del estudio

Para la realización del presente trabajo se están tomando en consideración las siguientes acotaciones:

Delimitación espacial:

El trabajo se realiza en una institución del sector cooperativo, ubicada en la ciudad de Lima, región de Lima, Perú.

Delimitación temporal:

Se considera desde el 2014 como inicio de las implementaciones realizadas en materia de seguridad de la información hasta el 2022.

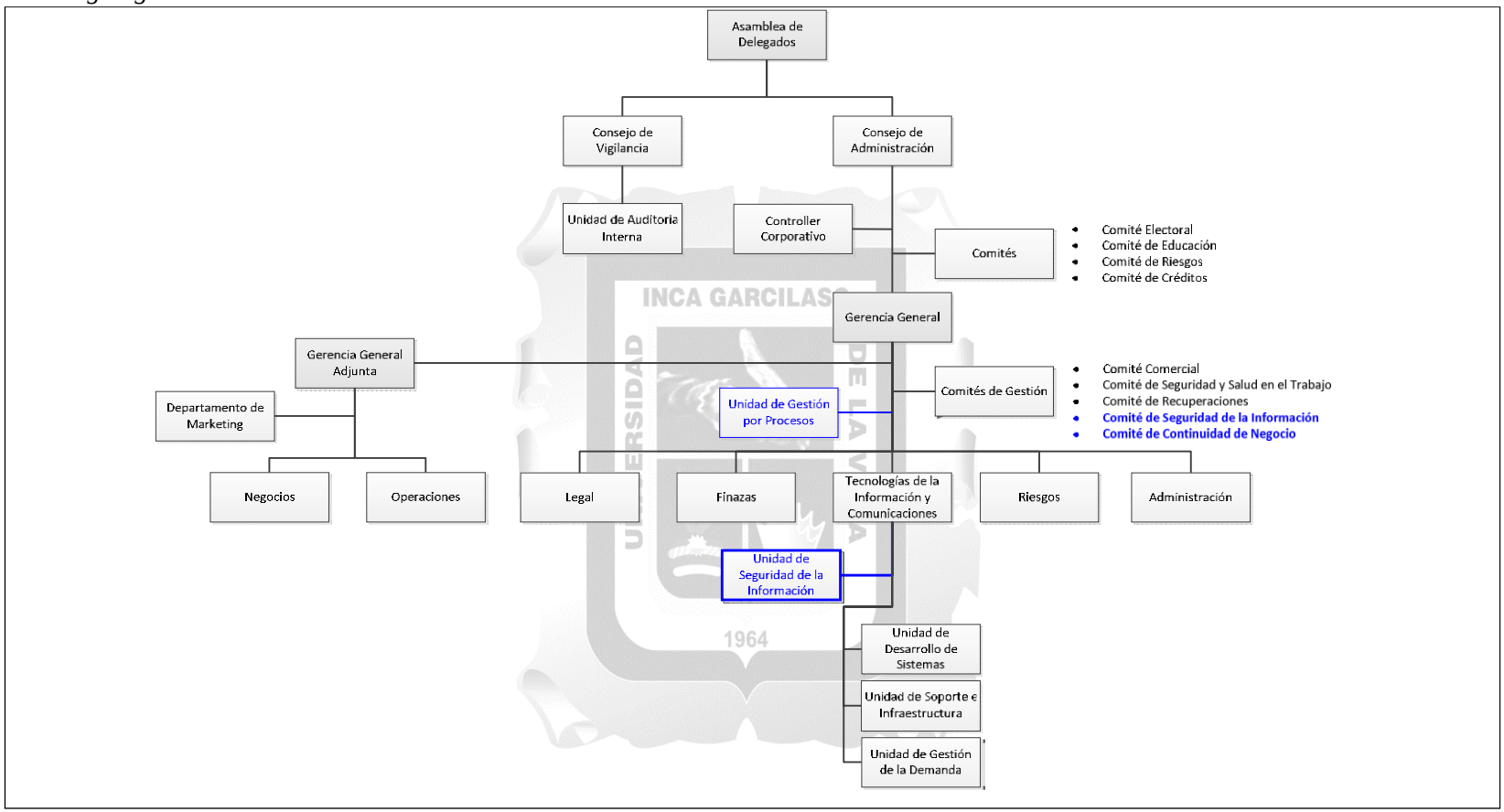
CAPÍTULO IV: FORMULACIÓN DEL DISEÑO

4.1 Diseño esquemático

Para la implementación del SGSI en la institución cooperativa se contemplaron distintos ejes o campos de acción, los mismos que podrían ser de fácil intervención y otros con mayor complejidad. La puesta en marcha de un SGSI es un camino de largo plazo, no obstante, se buscaba que se tuviesen resultados que marcaran la diferencia en el primer año de ejecución.

Todo lo relacionado a la seguridad de la información y la transformación digital estaba cobrando mayor relevancia, de tal manera que las clasificadoras de riesgo exigíana las instituciones del sector financiero que presentaran un informe de situación sobre inversiones en materia de seguridad de la información y continuidad de negocio. Esto mismo ocurría con las entidades fondeadoras (tanto nacionales como internacionales) que en su proceso de *due diligence* también requerían de dicho informe. Debido a todos estos aspectos, la implementación del SGSI era vital para la institución.

Figura 5. *Organigrama de la institución al 2015*



Fuente: Elaboración propia adaptada a partir del organigrama de la institución al 2015.

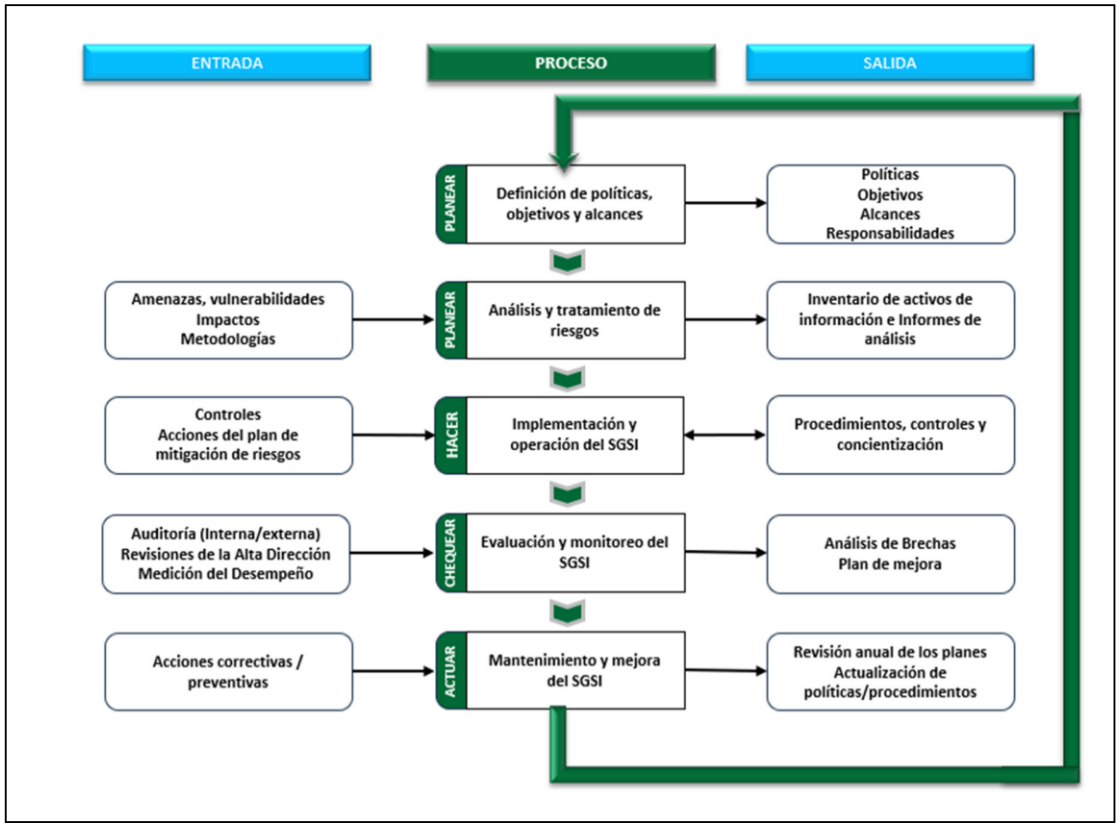
En la figura 5 se muestra el organigrama adaptado de la institución para reflejar el estado al 2015, en el cual se aprecia las incorporaciones iniciales propuestas a nivel de organización y funciones, estableciendo los cambios para la implementación del SGSI.

Figura 6. *Ejes de ejecución del SGSI*

Fuente: Elaboración propia.

En la figura 6 se observa el esquema de trabajo general para la implementación del SGSI, el cual se encuentra alineado a la norma ISO 27001, considerando su posterior integración a otros sistemas de gestión.

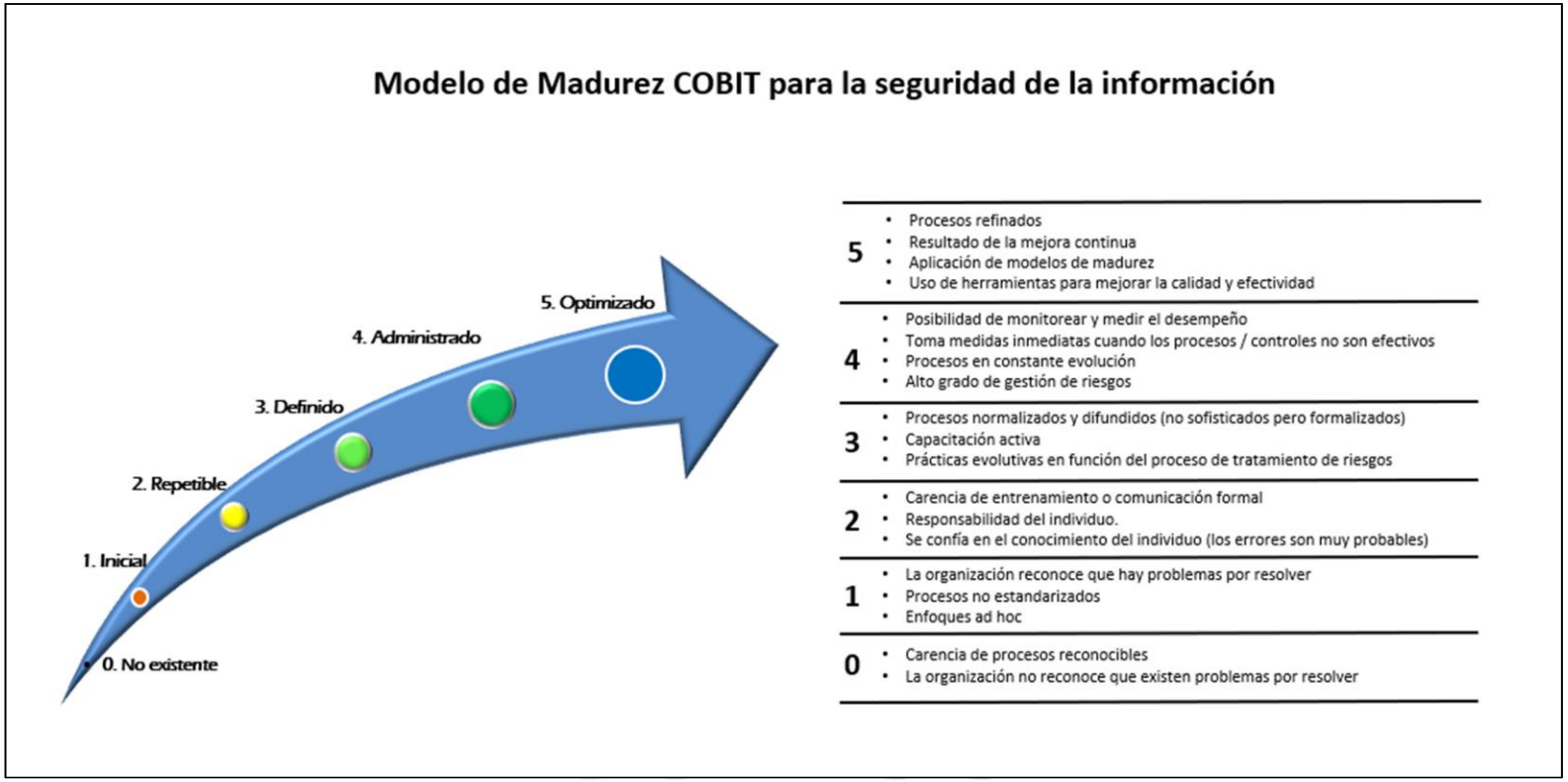
Figura 7. Proceso de implementación del SGSI



Fuente: Elaboración propia adaptada de los procesos de mejora continua.

En la figura 7 se puede observar el flujo procedimental en que se realizaron las implementaciones del SGSI, considerando una metodología de mejora continua con las entradas y salidas generales de cada proceso.

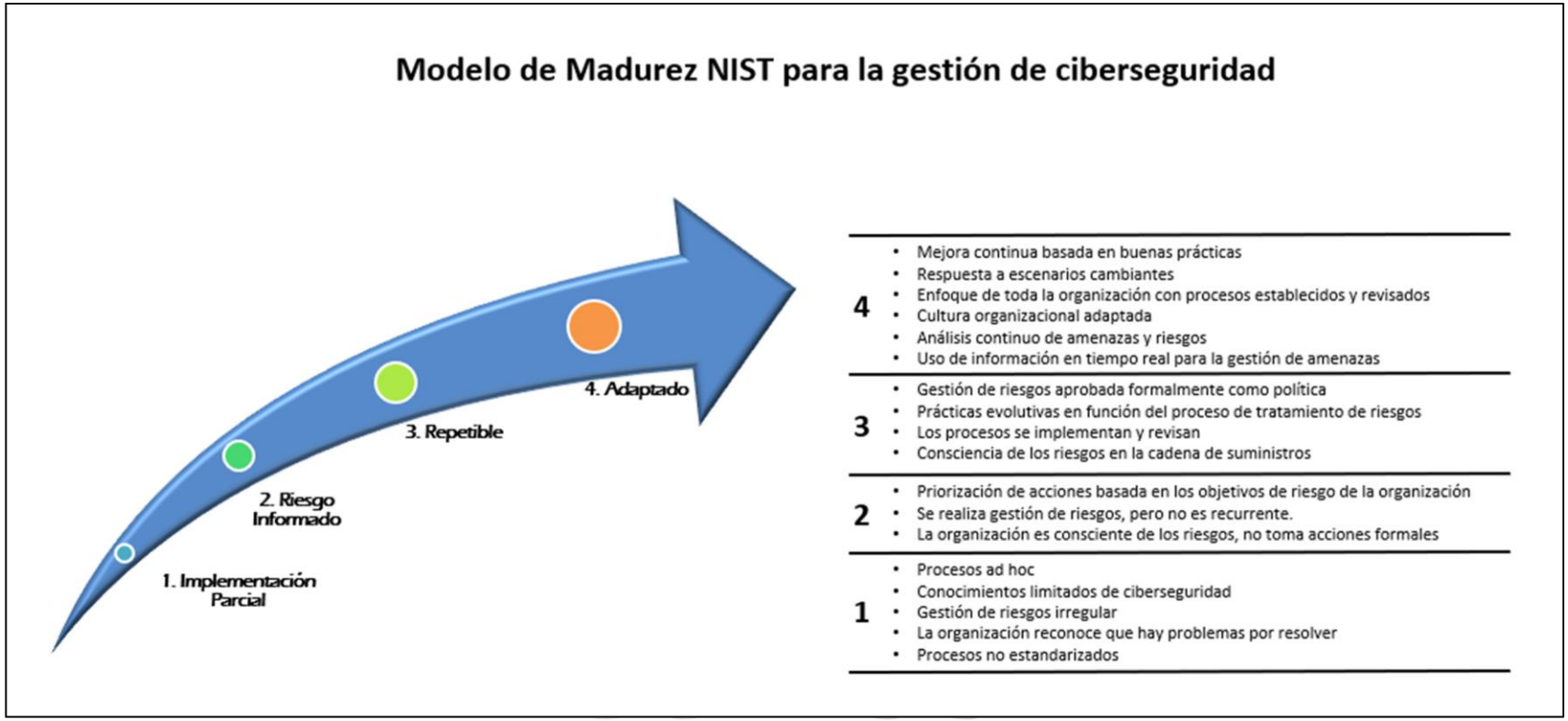
Figura 8. *Modelo de madurez para el Sistema de Gestión de Seguridad de la Información*



Fuente: Elaboración propia basada en el modelo de madurez de COBIT.

En la figura 8 se describen las escalas del modelo de madurez basado en COBIT de ISACA con el cual se realiza la medición de la efectividad de la implementación del SGSI en la institución. Su aplicación permite conocer el alineamiento constante del SGSI con los objetivos de la organización en un proceso de mejora constante.

Figura 9. *Modelo de madurez para la Gestión de la Ciberseguridad*



Fuente: Elaboración propia basada en el modelo de madurez de NIST.

En la figura 8 se describen las escalas (*tiers*) del modelo de madurez basado en el marco de trabajo de Ciberseguridad de la NIST con el cual se realiza la medición de la efectividad de la implementación de la gestión de la ciberseguridad en la institución. Su aplicación permite conocer el alineamiento constante con los objetivos de la organización y su mejora continua.

4.2 Descripción de los aspectos básicos del diseño

La metodología usada se enmarca en el proceso de mejora continua de IMS2 de PCEB, como fue descrito en los capítulos anteriores, alineándolos a los marcos de trabajo de los estándares ISO también mencionados previamente.

Los conocimientos aplicados para esta implementación estuvieron de la mano con los cursos, temáticas y expectativas del perfil del profesional de la carrera de Ingeniería de Sistemas y Cómputo, pues lo que se buscada no era la adopción de una herramienta que solucione un tema puntual sino de tener carácter de análisis holístico e interdisciplinario de entendimiento transversal de toda la organización con su interacción con entidades internas y externas, integrando tanto soluciones tecnológicas como normativas y procedimentales, haciendo uso de estándares mundialmente aceptados para incrementar la seguridad de los datos considerando un enfoque de riesgos, alineándolos a los objetivos estratégicos, con impacto favorable en la cultura organizacional, que procuraran la mejora continua de los procesos y que finalmente contribuyeran a la generación de valor para la institución.

El eje central para el diseño se basa en los activos de información que se debían resguardar, recordando que el alcance va más allá de la seguridad informática y que involucra todo aquello que se considera información en todos sus estados y formas, conforme lo señalado en el apartado Materiales (Información) del capítulo 2. Alrededor de este eje es que se diseña la estrategia a seguir para la implementación, iniciando conla creación de algunas unidades organizacionales que le dieran cabida a las funciones especiales que se designaron. Es así como se propone la adición de la Unidad de Seguridad de la Información (USI), cuya jefatura fue asignada al suscrito, y luego algunos comités especializados. Si bien es cierto que la recomendación general es que la USI sea independiente a las áreas de Tecnología o en todo caso que pertenezca a las unidades de Riesgos, se opta por una estrategia conjunta para este punto que abarcara dos aspectos de la Seguridad de la Información: una que estuviera ligada al interior de la División de TIC (de carácter operacional) y otra con un colegiado que tomara las decisiones de alto nivel y marcara la pauta de gestión. Lo primero se logra con la incorporación de la USI que desarrolle acciones a nivel operativo y táctico y lo segundo (meses después) con la propuesta de creación del Comité de Seguridad de la Información – CSI (compuesto porla Gerencia de TIC, la de Riesgos y el Jefe de Seguridad de la Información), y el Comitéde Continuidad de Negocio – CCN (compuesto por la Gerencia General y la Adjunta, las

Gerencias de Negocios, de Riesgos, de TIC, De Finanzas, de Administración, el Controller Corporativo y el Jefe de Seguridad de la Información) ambos a nivel estratégico. Esto se puede observar en la figura 5 en la cual se muestra en retrospectiva el organigrama que se tenía a inicios del 2015. Se ha resaltado en azul la propuesta inicial de donde se ubicaría la USI y adicionalmente se colocan los comités que, el suscrito como gestor a cargo de la Unidad, propuso para el involucramiento de la Alta Dirección; complementariamente la Unidad de Gestión por Procesos que fue incorporada por la Gerencia General. La composición detallada de cada unidad organizacional (aparte de la División de Tecnologías de la Información y Comunicaciones) ha sido omitida por no considerarse relevante para la presente investigación.

Como comentario complementario, la mencionada Unidad de Gestión por Procesos incorporada para la formalización normativa de todas las unidades de la cooperativa, constituyó un elemento clave en el cual se apoyó la institucionalización de los procesos.

Los otros ejes planteados constituyen los pilares de la transformación que se deseaba realizar en la institución, esto comprendido por el bajo control que existía en ese momento para la gestión de la información y los accesos brindados a los usuarios. Según se muestra en la figura 6, cada eje de Procesos, Personas y Tecnología tienen identificados un grupo de áreas, temáticas o dominios que se han trabajo y que alineamos con los estándares ISO mencionados previamente. Cada ítem fue abordado con su evaluación de riesgos y sus posteriores controles de mitigación, siendo los más especiales y sensibles aquellos relacionados con personas por el rechazo natural al cambio del *status quo* en los accesos a las plataformas y las "restricciones" (controles) que se impusieron en salvaguarda de la información.

Todos los ejes se trataron bajo la metodología de mejora continua IMS2 de PECB (como se mostró en la figura 2). Para ello, no solo era suficiente un juicio experto del gestor del SGSI, sino que debía ir acompañado de revisiones independientes y de rendir cuentas de la gestión a un ente superior. Es en este momento en el cual las primeras acciones tomadas para la creación de un comité estratégico cobran relevancia, incluyendo también las revisiones de auditorías tanto internas como externas, aquellas de cumplimiento (supervisión) como aquellas solicitadas por iniciativa propia de la institución, las cuales brindarían la evolución y madurez que requería la gestión. Esto se observa en el flujo de procesos de la figura 7.

Para medir el desempeño y madurez de la gestión realizada se utilizó el marco de trabajo de COBIT, para lo relacionado a la seguridad de la información (figura 8), y el

marco de la NIST para la gestión de ciberseguridad (figura 9). En ambos casos, los planes aprobados estuvieron enfocados en una meta trazada a alcanzar por cada año que significaran una evolución de la madurez de los sistemas de gestión.

Finalmente, cabe mencionar que parte de propuesta del suscrito para la implementación de largo plazo giraba en torno a realizar una gestión holística integrada que cubra todos los aspectos de seguridad de la información, ciberseguridad, protecciónde datos personales, continuidad de negocio y por ende la gestión de crisis, todo ello siguiendo los marcos de trabajo ISO (27001, 27005, 27032, 22301, el de Ciberseguridad de la NIST y las mejores prácticas existentes relacionadas al sector.

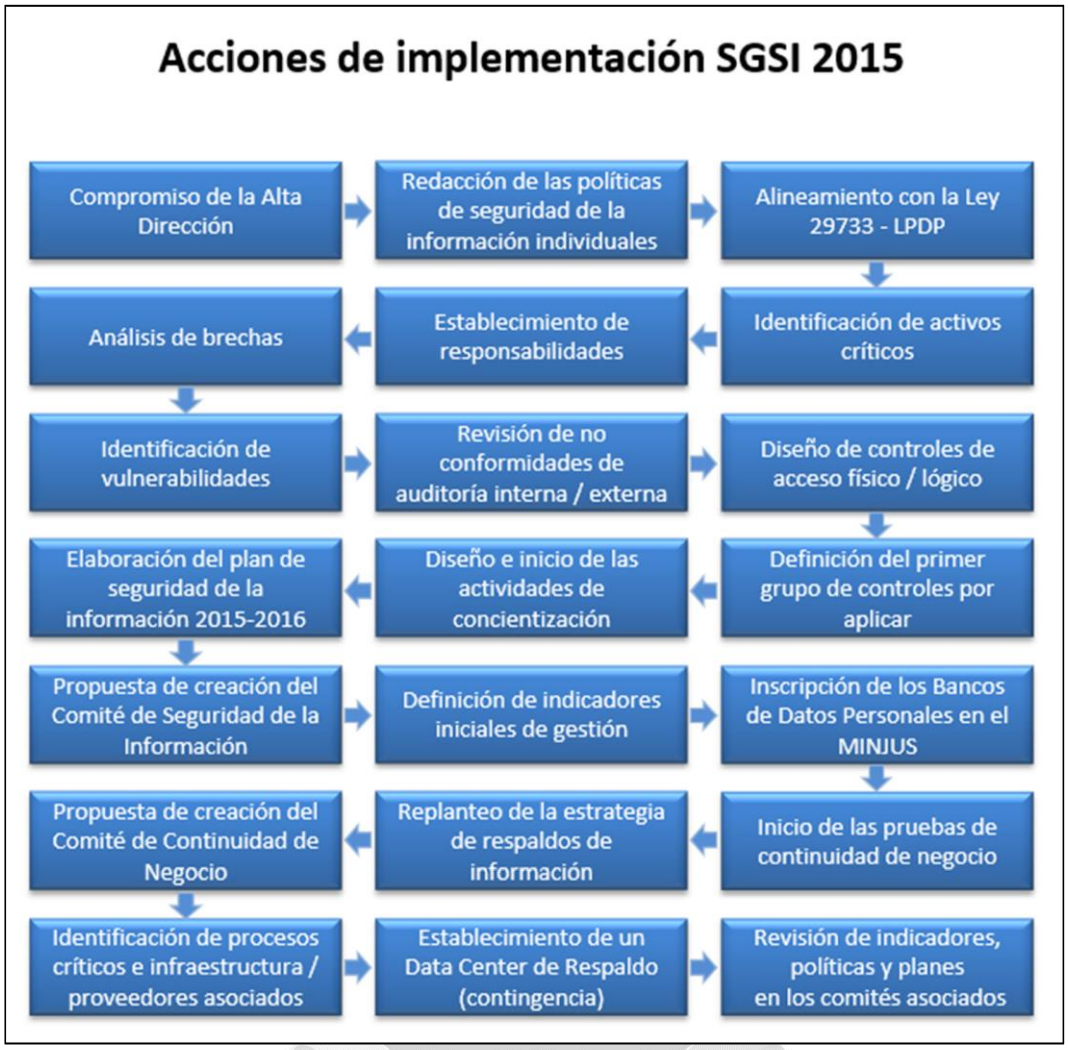
CAPÍTULO V: PRUEBA DE DISEÑO

5.1 Aplicación de la propuesta de solución

Para el logro del objetivo general, en efecto se procedió con el inicio de la implementación del SGSI en la institución tomando como marcos de trabajo los estándares y buenas prácticas internacionales, siendo el principal la ISO 270001 relacionada al SGSI, además de otros como son el ISO 27032 (Guía de Ciberseguridad), ISO 27005 Riesgos de Seguridad de la Información y el *framework* de Ciberseguridad de la NIST. Todos estos, en conjunto con la ISO 22301 (Continuidad de Negocio) han permitido cubrir también completamente los requisitos de la Ley de Protección de Datos Personales. Esto se realizó siguiendo una gestión evolutiva a lo largo de los últimos años, incrementando el nivel de madurez estratégica de la institución en estos aspectos.

Para el caso del primer objetivo específico, sobre describir como el compromiso de la Alta Dirección en asignar los recursos y respaldar las acciones de implementación de la cultura de seguridad contribuirán al éxito de la implementación del sistema de gestión, en el primer año (2015) se llevaron a cabo grandes implementaciones sobre toda la organización, los cuales se pueden observar a continuación.

Figura 10. *Acciones de implementación SGSI 2015*

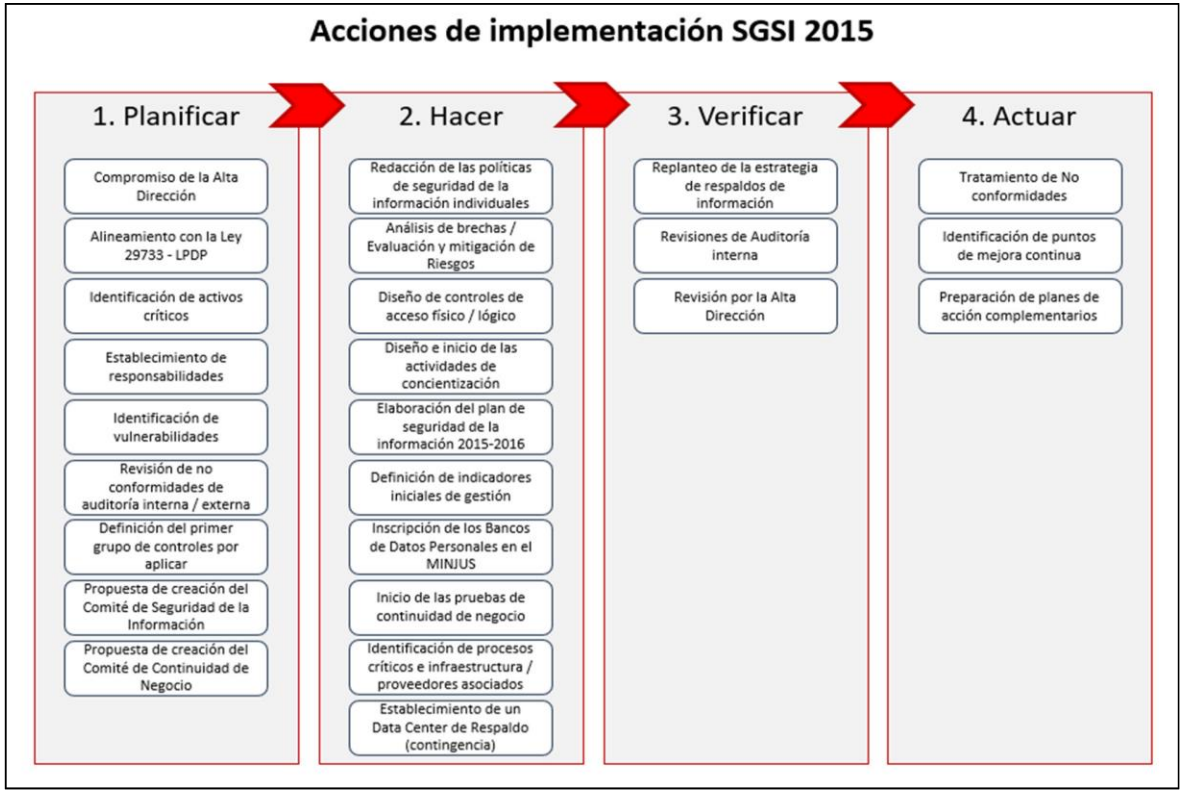


Fuente: Elaboración propia.

La figura 10 muestra en detalle las acciones de implementación realizadas durante el 2015, las cuales buscaban instituir las bases de todo el SGSI y más aún de tener un impacto real en bien de la institución.

Estas fueron las acciones iniciales marcaron el derrotero de la gestión en la cual se concentraron los esfuerzos en cubrir las principales falencias detectadas, conforme se había descrito en el diagrama de Ichikawa (figura 3). Se implementaron los planes de acción siguiendo un enfoque de riesgos y de medición de resultados de manera iterativa siguiendo la metodología IMS2 de PECB conforme se muestra a continuación.

Figura 11. *Acciones de Implementación SGSI 2015 - IMS2*



Fuente: Elaboración propia.

En la figura 11, para una mejor observación del seguimiento de la metodología IMS2 para el ciclo de implementación y mejora continua, se han trasladado el conjunto de procesos descrito en la figura 10. En esta parte del documento solo se muestran las actividades del 2015, no obstante, lo realizado desde el 2016 al 2022 ha sido ubicado en los anexos del presente trabajo.

Para la explicación del desarrollo de los otros objetivos específicos también se apoyará en la estructura mostrada en la figura 11 para que se tenga un mejor entendimiento de lo aplicado.

Unos puntos saltantes en lo que comprende al desarrollo de este objetivo esta referido a que, por iniciativa y solicitud propia del suscrito, la Alta Dirección contrató en el 2017 a Price Waterhouse Coopers para realizar una auditoría sobre el estado de la gestión de seguridad de la información. En el mismo año, se realizó la primera prueba de penetración (Hacking Ético) por una empresa especializada para también acompañar los planes de acción con miras al 2018. Adicionalmente, en el 2019 se contrataron los servicios de otra firma auditora para revisar todos nuestros aspectos de alineamiento de la Ley de Protección de Datos Personales. En todos los casos los informes de resultados fueron alentadores en cuanto a que los temas y controles principales se encontraban funcionando adecuadamente además que los otros hallazgos sirvieron como insumo para laelaboración de los planes de trabajo siguientes.

En el segundo objetivo específico, sobre describir como la sensibilización de todas las unidades organizacionales permitirá realizar los cambios requeridos considerando un enfoque basado en riesgos, el factor humano es considerado el más elevado en las causas de los incidentes de seguridad de la información, estadísticamente mayor al 90%, por lo cual no solo bastaba con la puesta a punto de las soluciones automatizadas o la adquisiciónde las más avanzadas herramientas tecnológicas, sino que se realizó un plan detallado que cubriera todas las temáticas de sensibilización de los colaboradores, más aún cuando esto involucraba cambios y/o reforzamientos de la cultura organizacional.

En lo relacionado a las sesiones de capacitación y concientización, se iniciaron únicamente con material preparado a la interna hasta el 2017, luego de lo cual se intercalaban con sesiones realizadas por terceros hasta el 2020. Luego de ellos se buscó una plataforma en línea especializada en seguridad de la información cuyo lema era “el error humano conquistado”, el cual se alineaba completamente con nuestros objetivos en este aspecto, llegando a tener indicadores de riesgo no solo de la institución sino de cada uno de los colaboradores de acuerdo con su conducta e interacción con la plataforma.

Complementariamente a las charlas, el plan incluyó comunicaciones dentro de la red social interna, incentivos para los que identificaban posibles incidentes o reportaban amenazas potenciales (como por ejemplo correos *phishing*), ejercicios simulados de ataques para observar las reacciones, todo lo cual ha reforzado el grado de alerta y de reconocimiento de posibles eventos maliciosos (gestión de incidentes).

Figura 12. *Temática actual de los planes de capacitación y concientización*

Fuente: Elaboración propia.

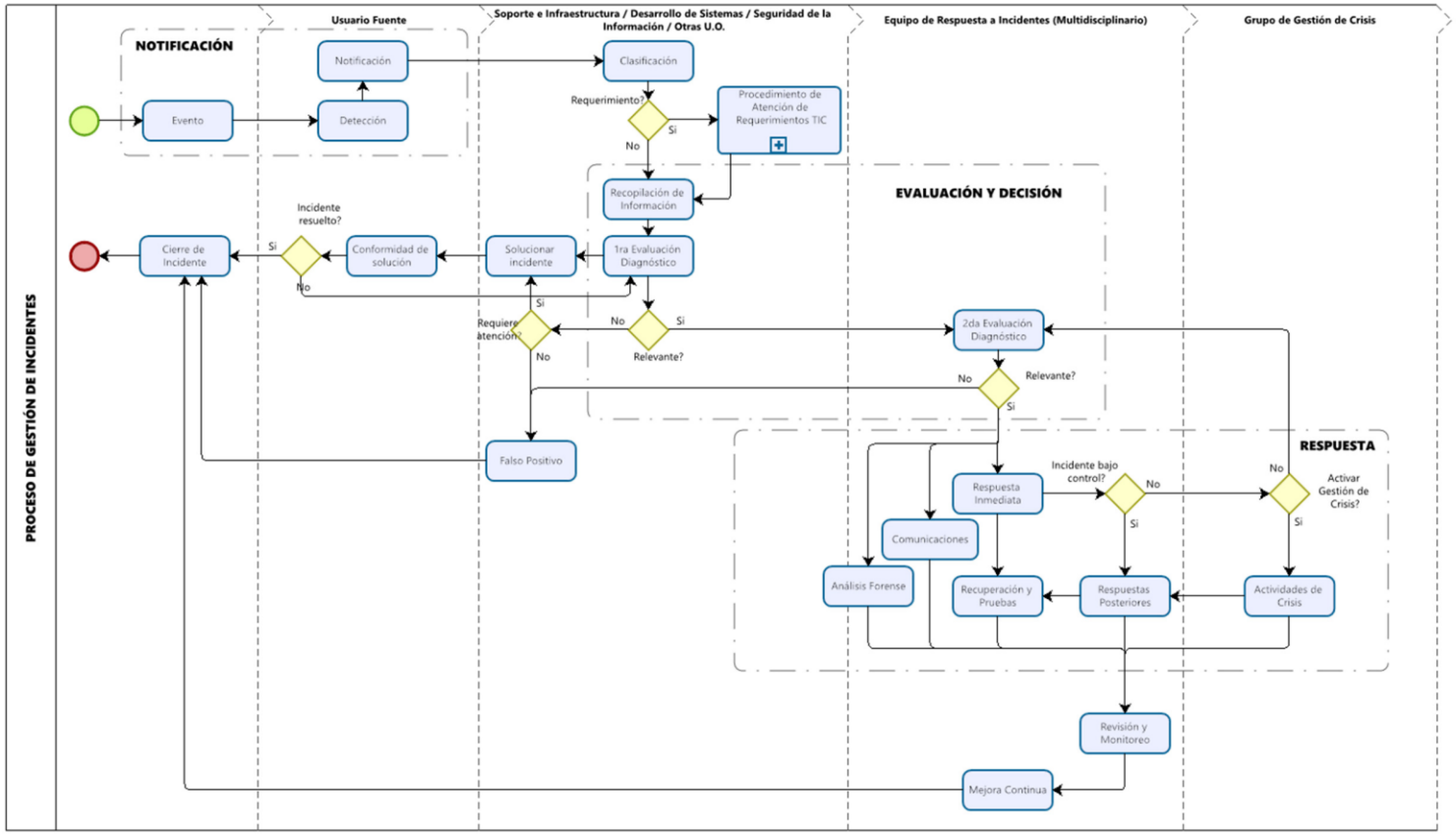
En la figura 12 se muestra la temática de las sesiones, las cuales habían sido evolutivas, llegando a este punto óptimo de temas a cubrir.

La evolución mencionada se basa en varios aspectos: la implementación de controles, las nuevas normativas, los cambios en la plataforma tecnológica, las necesidades de la organización y las acciones de mejora de los planes de seguridad de la información, ciberseguridad, protección de datos personales, continuidad y de crisis, todos ellos derivados de la gestión de riesgos que también cubrían todos estos aspectos de manera integral.

Un evento clave que puso a prueba la implementación fue cuando en el marzo del 2020 se inicia el estado de emergencia por el COVID-19. La preparación iniciada con la implementación del SGSI y de los sistemas de gestión afines desde el 2015 representaron un gran reto para la organización con miras no solo al cumplimiento de la normativa vigente de la SBS, sino de establecer una cultura de seguridad de la totalidad de susactivos de información y la continuidad de todos los servicios que brinda la institución,sin dejar de lado el factor humano como ente canalizador de estos. En este marco, las implementaciones realizadas acompañadas de las consiguientes pruebas anuales ejecutadas sobre los planes establecidos prepararon a la cooperativa para la complicada coyuntura que significó afrontar la pandemia del COVID-19, en la que podemos afirmar que la institución mantuvo la continuidad de sus operaciones en un 99.96%.

Para el tercer objetivo específico, sobre describir como la institucionalización de todos los procesos asociados al sistema de gestión permitirán un entorno evolutivo, se afirma que la normativa interna y su revisión anual permiten establecer un base decumplimiento y por ende de madurez de la gestión. Los procesos o planes que se realizan sin un sustento normativo son acciones *ad hoc* que no necesariamente garantizan que se vayan a repetir y mucho menos evolucionar en el tiempo. La estrategia seguida en este caso fue la documentación normativa de toda la gestión, esto es de las políticas, los procesos, procedimientos, guías, formatos, etc., los cuales estuvieron bajo revisiones anuales. Los controles a los que se hicieron referencia en la normativa se evaluaban bajoel marco de la gestión de riesgos, alineada no solo con la de seguridad de la información (ISO 27005) sino también con los objetivos de riesgo operacional, han permitido primero que en el 2018 se haga la integración de los comités de Seguridad de la Información (CSI) y el de Continuidad de Negocio (CCN), pasando a constituirse el Comité de Seguridad y Continuidad de Negocio, y segundo, que se pueda establecer un proceso de gestión de incidentes unificada, a cargo de un grupo multidisciplinario enlazado con la gestión de crisis como se muestra en la figura 13.

Figura 13. *Proceso Integral de Gestión de Incidentes*



Fuente: Elaboración propia.

La figura 13 muestra el diagrama de procesos en el cual la gestión de incidentes se abarca transversalmente a los sistemas de gestión de la institución de manera holística.

Bajo esta nueva instancia del CSCN, se implementó la integración y unificación también de las estrategias de los sistemas de gestión cumpliendo con una de las metas personales que era tener una visión holística en la que se prevea que un incidente de seguridad de la información puede impactar en la continuidad del negocio (o viceversa) y que, a su vez, si la situación continúa escalando puede generar una crisis que afecte gravemente la reputación de la institución. El diagrama de flujo de este proceso se observa de manera detallada en la figura 13 considerando también su ciclo de mejora continua.

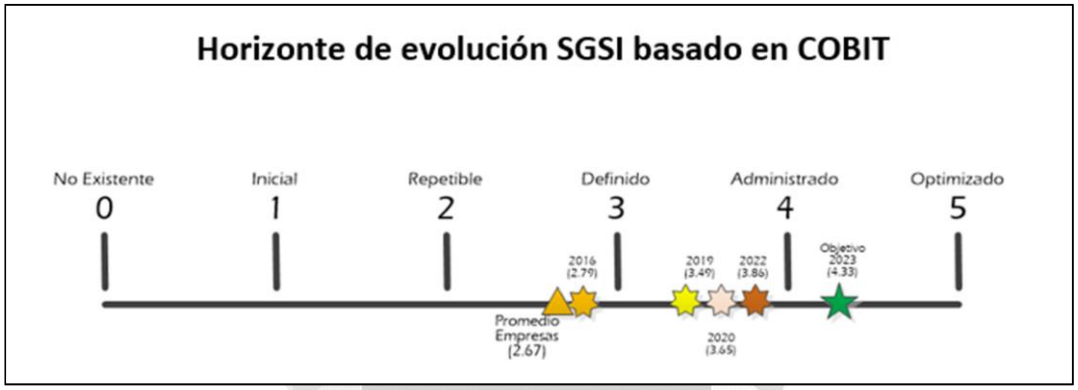
Para el año 2019 se implementó el manual de gestión de crisis, al cual lo siguieron dos simulacros de escalamiento de incidentes (tanto de respuesta procedimental rápida como también para casos de ciberataques) en el cual participaron desde colaboradores de diversas unidades organizacionales, la Alta Dirección e inclusive miembros del Consejo de Administración (CAD). Estas simulaciones también sirvieron de preparación para el escenario de crisis ocasionado por el COVID-19, lo cual se afrontó de manera satisfactoria según lo comentado previamente.

En el año 2020, se otorgó un manejo especial a los temas de ciberseguridad, por lo cual se crearon políticas, planes e inversiones específicas para cubrir el escenario creciente de amenazas, las mismas que se acentuaron durante el tiempo de la pandemiaen que parte del mundo pasó a entornos virtuales en modalidad de trabajo remoto. El Comité de Seguridad y Continuidad de Negocio (CSCN) también absorbió la implementación de la gestión de ciberseguridad que, si bien es cierto que se realizaba como parte de la seguridad de la información, debía tener un protagonismo equivalente. Cabe mencionar en este punto que los planes de capacitación también se realinearon taly como se explicó en el sustento del segundo objetivo específico. Esta misma alineación se realizó en el marco de todas las políticas, planes, procedimientos y protocolos de los sistemas de gestión mencionado para que pudieran interactuar entre sí.

Finalmente, para el cuarto objetivo específico, sobre describir como la medición y evaluación constante del desempeño de los planes planteados alineados con los objetivos estratégicos permitirán no solo una implementación evolutiva sino también generar valor para la institución, la presentación de los planes operativos anuales (POA), los informes trimestrales al CSCN (de los que personalmente el suscrito se encarga de preparar y sustentar) además del seguimiento de las observaciones y/o recomendaciones de las auditorías internas / externas han permitido realizar las mejoras al SGSI de manera holística, así como detectar algunos hallazgos no contemplados o que necesitaban controles más específicos para su mitigación.

Al cierre de cada año, luego de la actualización de las políticas y el resultado de la ejecución del plan, se realiza la medición de la madurez alcanzada y con ello se promueven las acciones que formarán parte del nuevo plan a desarrollar el siguiente período anual.

Figura 14. *Madurez del SGSI basado en COBIT*

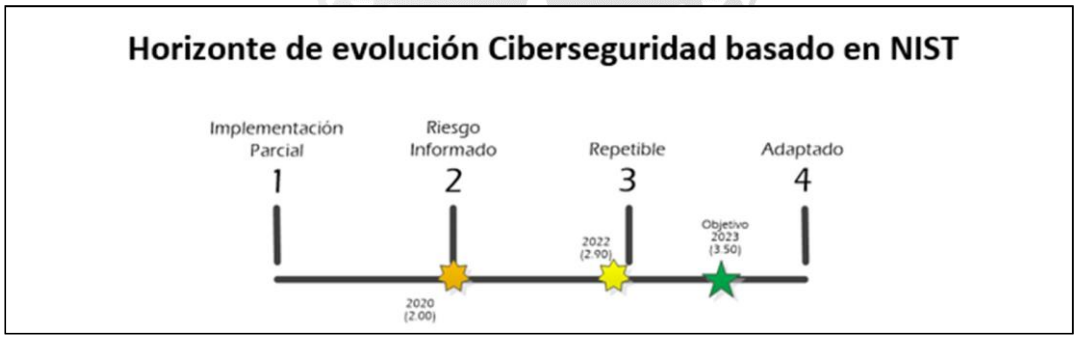


Fuente: Elaboración propia basado en el marco COBIT.

Conforme se muestra en la figura 14, se puede observar la evolución que ha tenido el SGSI desde que se iniciaron las mediciones en el que se reportó un índice de madurez de 2.79, pasando en la actualidad a tener un objetivo de 4.33. Para el caso de la seguridad de la información se utiliza el marco de trabajo COBIT.

En cuanto a la gestión de ciberseguridad se utiliza el marco de trabajo de la NIST, el cual comprende la toma de una línea base (perfil actual) y sobre esta medir la evolución que se espera alcanzar (perfil objetivo).

Figura 15. *Madurez de la Gestión de Ciberseguridad basado en la NIST*



Fuente: Elaboración propia basado en el marco de trabajo de ciberseguridad de la NIST.

Conforme se muestra en la figura 15, la ciberseguridad como un sistema de gestión específico se inició en el 2020 y a la fecha tiene un perfil objetivo al 2023 de 3.50.

Una experiencia especial del suscrito fue la de haber sustentado el estado del SGSI y

de los otros sistemas de gestión asociados (continuidad de negocio y ciberseguridad) ante representantes del Banco Interamericano de Desarrollo (BID) que se encontraba llevando a cabo un *due diligence* a la cooperativa para la realización de un convenio de fortalecimiento institucional, lo cual se llegó a concretar.

Progresivamente desde el 2015 se ha incrementado cada año los recursos para el SGSI y los otros sistemas de gestión asociados, lo cual iba de la mano con las inversiones necesarias descritas en los planes anuales sustentados y aprobados.

Durante el 2019 se recibió la visita de fiscalización por parte de la Autoridad Nacional de Protección de Datos Personales del MINJUS para constatar las medidas tomadas en el marco de la adaptación obligatoria de la Ley 29733, la cual también tuvo resultados positivos.

Para el 2020 se completó el alineamiento holístico no solo de los sistemas de gestión mencionados, sino de cómo el SGSI apoya activamente los objetivos estratégicos de la institución cooperativa (como se aprecia en la figura 13), con beneficio tanto para las unidades organizacionales, los socios de la cooperativa y todas las partes interesadas entre las que se encuentran las entidades regulatorias como la SBS, el Ministerio de Justicia y Derechos Humanos entre otros, así como también a los fondeadores, clasificadoras de riesgos, firmas auditoras y entidades del sector cooperativo tanto nacionales como internacionales, sumando valor al negocio y generando espacios de referencia sobre la implementación realizada.

Todo esto cobró mayor relevancia desde el 2020 en que la institución decidió incluir en su memoria anual el resumen de la gestión que se hace sobre los sistemas de gestión a cargo del suscrito, constituyéndose como un importante hito asociado a la evaluación, medición e impacto de lo realizado dentro de los objetivos estratégicos de la organización.

Adicionalmente se apuntalaron los planes a mediano plazo para el acompañamiento a la institución en los procesos de transformación digital en todos sus niveles y de manera transversal. Todo lo antes mencionado permite afirmar que la implementación evolutivay holística del SGSI, el cual era el objetivo principal de la investigación, ha contribuido no solo en el resguardo de los activos de información, el cumplimiento de las leyes, normas y expectativas de partes interesadas, sino que fehacientemente también ha generado valor para la institución cooperativa.

Figura 16. *Alineamiento institucional cooperativo del SGSI*

Fuente: Elaboración propia.

En la figura 16 se observa el alineamiento holístico de los sistemas de gestión siempre en apoyo de los objetivos estratégicos de la cooperativa y también acorde a las expectativas de las partes interesadas, conformando todo un ciclo de retroalimentación y de mejora continua.

CONCLUSIONES

La aplicación de estándares internaciones y buenas prácticas como marcos de referencia han permitido implementar un SGSI robusto, evolutivo y sobre todo holístico han preparado a la institución para poder evitar e inclusive afrontar incidentes inesperados. Evitando la materialización de eventos adversos se está contribuyendo al indicador de retorno de las inversiones realizadas en el SGSI y por ende a los objetivos estratégicos de la institución.

El éxito de la implementación de un SGSI depende directamente del grado de involucramiento de la Alta Dirección, no solo en proveer los recursos necesarios sino también en ser los promotores, impulsores y evangelizadores del cumplimiento de los objetivos plantados dentro de cada uno de sus equipos, más aún cuando éstos involucran cambios inclusive a nivel cultural.

Las evaluaciones de riesgo han permitido establecer las brechas entre el estado actual de los controles y las metas de madurez periódica que se van proponiendo anualmente,en la cual la concientización y entrenamiento del usuario (en todos sus niveles y especialidades) en el reconocimiento proactivo de amenazas/vulnerabilidades viene jugando un rol fundamental en la gestión de incidentes para evitar la materialización de eventos de gran impacto.

La formalización de las normativas internas (políticas, procesos, procedimientos, guías y otros) han permitido también establecer un marco interno de cumplimiento, las cuales se han sometido a revisiones anuales obligatorias para su adaptación a la realidad cambiante en contextos de incertidumbre, volatilidad y complejidad. La integración con otros sistemas de gestión (como los de continuidad, ciberseguridad y de crisis) han impactado también favorablemente en la madurez de la institución.

Finalmente, la inclusión de los planes operativos de seguridad de la información dentro de los planes estratégicos institucionales (y por consiguiente en el *Balanced Scorecard* de la institución), las revisiones trimestrales en el Comité especializado (CSCN), los exámenes tanto de auditoría tanto interna como externa, la medición y control de brechas han permitido darle vida y evolución al SGSI, convirtiéndolo en un factor de generación de valor para la institución, para las partes interesadas y en convertirse en un referente en el sector cooperativo. Los resultados satisfactorios de las mediciones incentivan el compromiso de la organización con el SGSI en la asignación de recursos y refuerzo de políticas (primer objetivo específico), lo cual promueve y robusteceel ciclo iterativo de mejora continua.

RECOMENDACIONES

La sensibilización de todos los colaboradores y terceros directamente relacionados con la institución es un proceso que no se detiene: el objetivo es continuar con la instauración de una cultura de seguridad y que esto forme parte del ADN de la organización para que lo implemente en todos sus procesos y adicionalmente que cada integrante lo aplique en su vida personal, familiar y profesional.

Los entornos y contextos son cambiantes y llenos de incertidumbre, por lo que mantener una estrategia proactiva, evolutiva y en constante revisión son la clave para que todo sistema de gestión de la seguridad de la información tenga éxito y que más aún genere valor a las organizaciones. Es aquí donde se debe realizar un análisis detallado que fortalezca los controles, y que interactúen positivamente, para que el *core* del negocio no los tome como trabas y limitantes, sino que sean los que garanticen y complementen el flujo de información de manera confidencial, integra y segura entre la institución y lasaltas expectativas de sus partes interesadas.

REFERENCIAS BIBLIOGRÁFICAS

Ashkenas, R. (8 de mayo de 2012). *Harvard Business Review*. Obtenido de https://hbr.org/2012/05/its-time-to-rethink-continuous

CEPAL. (18 de diciembre de 2020). *Comisión Económica para América Latina y el Caribe*. Obtenido de https://biblioguias.cepal.org/c.php?g=495473&p=4398118

Congreso de la República del Perú. (3 de julio de 2011). Obtenido de Ley Nº 29733 - Ley de Protección de Datos Personales: https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf

Congreso de la República del Perú. (19 de 7 de 2018). *Ley N. ª 30822 – Ley que modifica la Ley 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, y otras normas concordantes, respecto de la Regulación y Supervisión de Cooperativas de Ahorr*. Obtenido de https://www.mef.gob.pe/es/por-instrumento/ley/17927-ley- 30822/file

Farinango Pabón, L. E., & Negrete Ricci, E. P. (2022). *Desarrollo del Programa del Sistema de Gestión de Seguridad de la Información de una Cooperativa de Ahorroy Crèdito.*

Farinango, L. E., & Negrete, E. P. (2022). *Desarrollo del Programa del Sistema de Gestión de Seguridad de la Información de una Cooperativa de Ahorro y Crèdito.*

FENACREP. (2023). Obtenido de https://www.fenacrep.org/es/conocenos/historia

GDPR. (2016). *General Data Protection Regulation (GDPR) - Official Legal Text*. Obtenido de https://gdpr-info.eu/

ISACA. (2023). *COBIT - Control Objectives for Information Technologies*. Obtenido de https://www.isaca.org/resources/cobit

ISO. (2015). *Sistemas de Gestión de Calidad - Fundamnetos y Vocabulario*. Obtenido de https://www.iso.org/standard/45481.html

ISO. (2018). *Lineamientos para la Gestión de Riesgos*. Obtenido de https://www.iso.org/standard/65694.html

ISO. (2019). *SIstema de Gestión de la Continuidad de Negocio*. Obtenido de https://www.iso.org/standard/75106.html

ISO. (2022). *Sistema de Gestión de Seguridad de la Información.* Obtenido de https://www.iso.org/standard/27001

ISO. (2023). *ISO 27032 - Ciberseguridad - Lineamientos para la Seguridad en Internet*. Obtenido de https://www.iso.org/standard/76070.html

ISOTOOLS.US. (20 de febrero de 2015). Obtenido de https://www.isotools.us/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/

Morales Alomoto, L. R. (2019). *Balanced ScoreCard para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito.* Valencia - España: Universidad Técnica de Ambato.

Morales, L. R. (2019). *Balanced ScoreCard para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito.* Valencia - España: Universidad Técnica de Ambato.

Moscaiza, O. I. (2018). *Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013.* Lima.

Niño Morante, N. R. (2019). *Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI filial Lambayeque.* Universidad NacionalPedro Ruiz Gallo.

Niño, N. R. (2019). *Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI filial Lambayeque.* Universidad Nacional Pedro Ruiz Gallo.

NIST. (2023). Obtenido de https://www.nist.gov/cyberframework

PECB. (2020). Obtenido de https://www.pecb.com

PRESTAMYPE. (2023). Obtenido de https://www.prestamype.com/articulos/que-es-el-sistema-financiero-peruano-y-como-funciona

Silva Guerrero, A. R. (2021). *Implementación de un Sistema de Gestión de Seguridad de la Información para mejorar la Seguridad de la Información en una empresa MYPE - 2021*. Universidad Tecnológica del Perú.

Silva, A. R. (2021). *Implementación de un Sistema de Gestión de Seguridad de la Información para mejorar la Seguridad de la Información en una empresa MYPE - 2021*. Universidad Tecnológica del Perú.

Superintendencia de Banca, Seguros y AFP. (2022). Obtenido de Portal SBS: https://www.sbs.gob.pe/coopac

Toro Moncada, J. A. (2021). *Modelo de Políticas Estrategias y Controles que Permitan Minimizar los Riesgos para la Seguridad de la Información en la Nube Híbrida Existente en las Organizaciones.* Medellín: Tecnológico de Antioquia I.U.

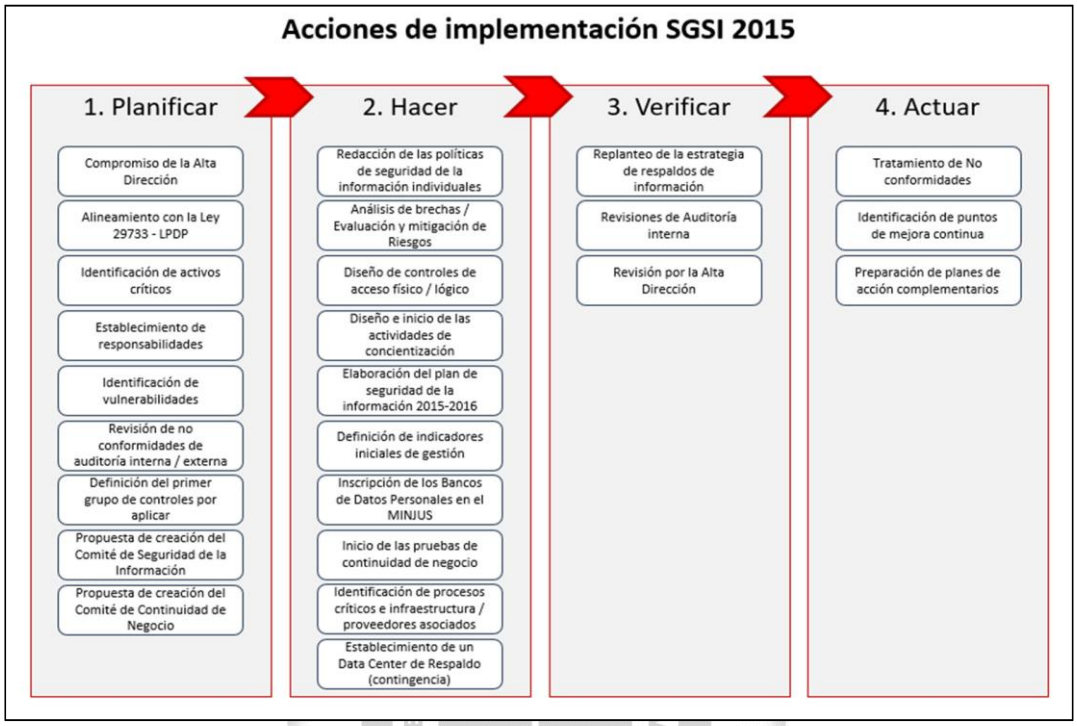
Toro, J. A. (2021). *Modelo de Políticas Estrategias y Controles que Permitan Minimizar los Riesgos para la Seguridad de la Información en la Nube Híbrida Existente en las Organizaciones.* Medellín: Tecnológico de Antioquia I.U.

Wikin , E. (junio de 2023). *Sweden Data Protection Overview*. Obtenido de https://www.dataguidance.com/notes/sweden-data-protection-overview

WOCCU. (2014). *World Council of Credit Unions*. Obtenido de https://www.woccu.org/documents/2013_Informe_Estadistico

ANEXOS

Acciones de Implementación SGSI 2015 - IMS2



Fuente: elaboración propia.

Acciones de Implementación SGSI 2016 - IMS2

Fuente: elaboración propia.

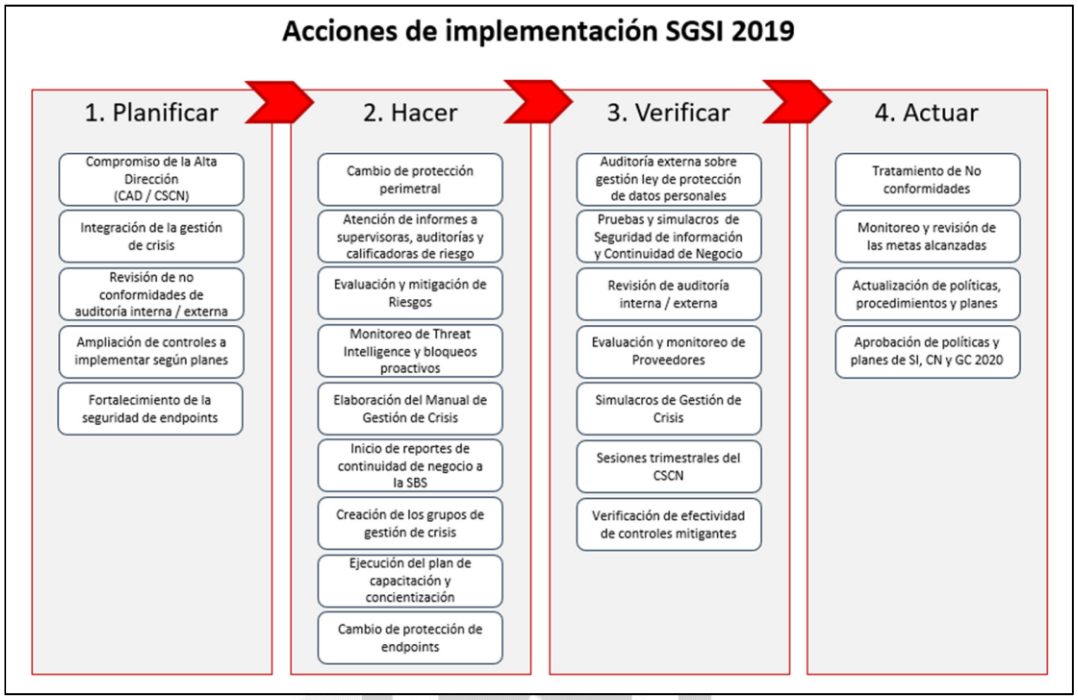
Acciones de Implementación SGSI 2017 - IMS2

Fuente: elaboración propia.

Acciones de Implementación SGSI 2018 - IMS2

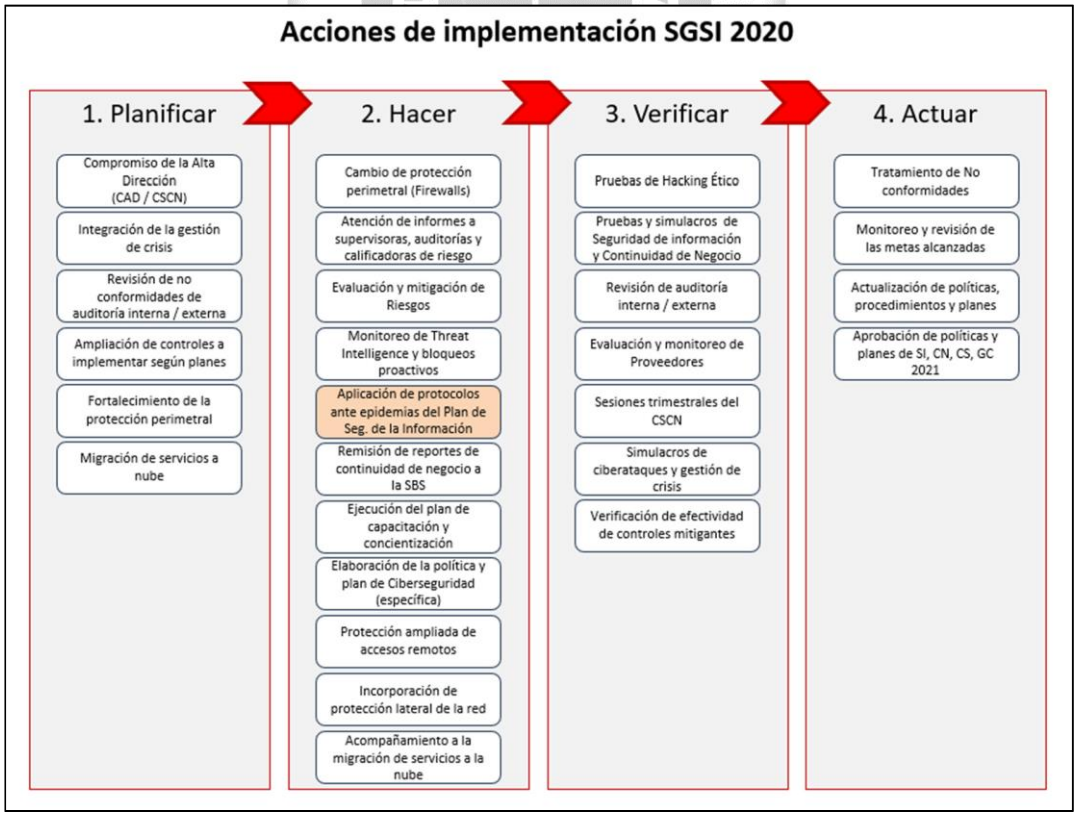
Fuente: elaboración propia.

Acciones de Implementación SGSI 2019 - IMS2



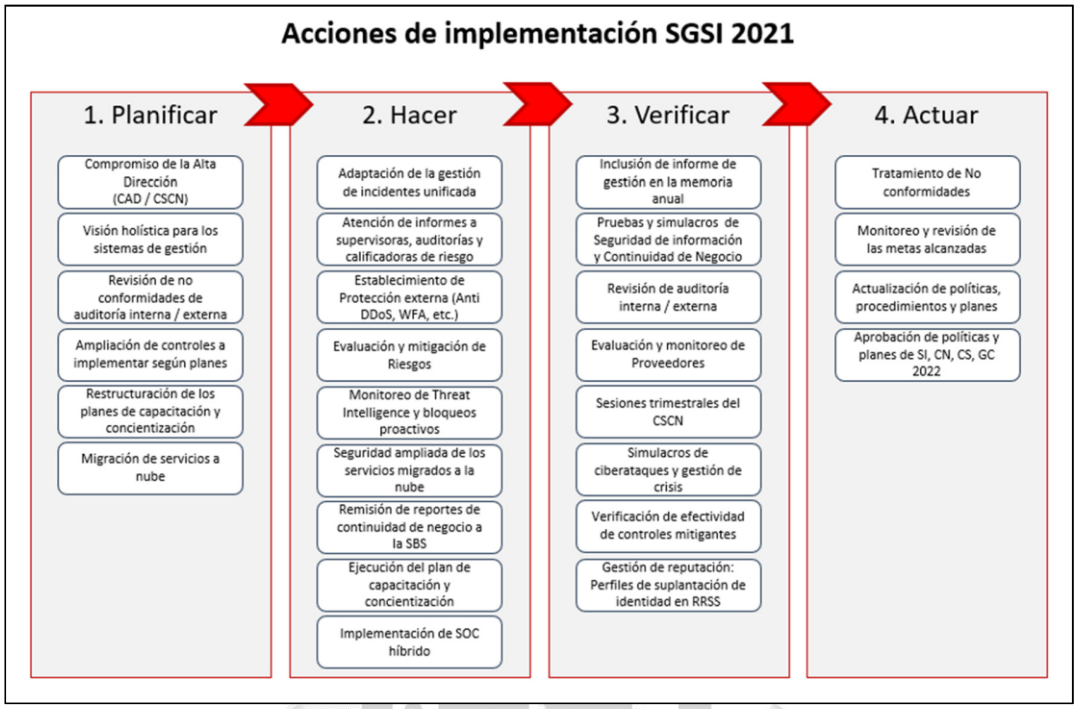
Fuente: elaboración propia.

Acciones de Implementación SGSI 2020 - IMS2



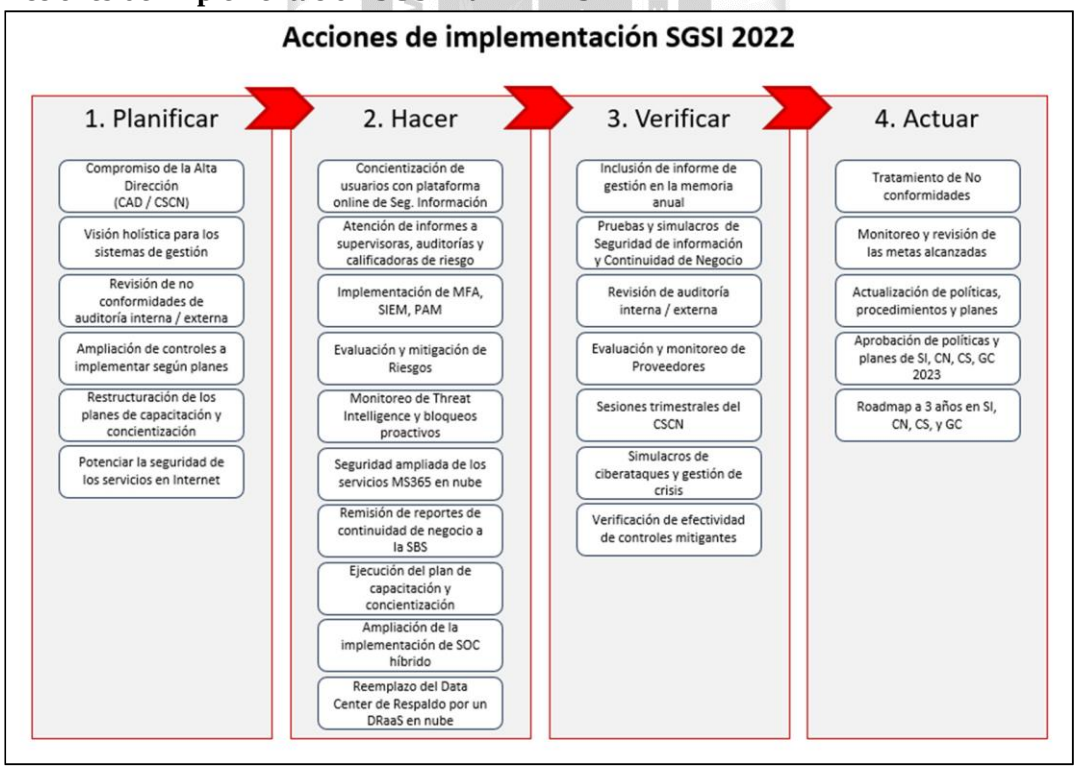
Fuente: elaboración propia.

Acciones de Implementación SGSI 2021 - IMS2



Fuente: elaboración propia.

Acciones de Implementación SGSI 2022 - IMS2



Fuente: elaboración propia.