UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac, Callao

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTOR:

Br. Edwin Samuel Arias Quispe (ORCID: 0000-0001-9389-9665)

ASESOR:

Dr. Edwin Alberto Martínez López (ORCID: 0000-0002-1769-1181)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LIMA – PERÚ

2020

Dedicatoria:

El presente trabajo lo dedico a mis padres y familia que siempre me ha brindado el apoyo necesario y a las personas que no dudaron en apoyarme y estar pendiente cuando más fue necesario.

Agradecimiento:

Agradecer en primer lugar a Dios por continuar guiando mi vida y brindándome la fuerza necesaria para seguir con los anhelos más preciados en mi vida profesional, a mis padres por regalarme siempre sus mejores consejos y a mi familia por regalarme el apoyo necesario, las ganas de continuar adelante y ser una parte fundamental en seguir creciendo profesionalmente.

PÁGINA DEL JURADO

Declaratoria de autenticidad

Yo, Edwin Samuel Arias Quispe estudiante de la Escuela de Posgrado, del programa Maestría en Ingeniería de Sistemas con mención en Tecnologías de Información, de la Universidad César Vallejo, Sede Lima Norte; presento mi trabajo académico titulado: "Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac, Callao", en 80 folios para la obtención del grado académico de Maestro(a) en Ingeniería de Sistemas con mención en Tecnologías de Información, es de mi autoría.

Por tanto, declaro lo siguiente:

- He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajos académicos.
- No he utilizado ninguna otra fuente distinta de aquellas expresamente señaladas en este trabajo.
- Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o título profesional.
- Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.
- De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinen el procedimiento disciplinario.

Lima, 01 de Agosto de 2020

Edwin Samuel Arias Quispe

Índice

Página

Dedicatoria ii

Agradecimiento iii

Página del jurado iv

Declaratoria de autenticidad v

Índice vi

Índice de Figuras vii

Índice de Tablas vii

RESUMEN viii

ABSTRACT ix

I. INTRODUCCIÓN 1

II. MÉTODO 17

2.1. Tipo y diseño de la investigación 17

2.2. Escenario de estudio 18

2.3. Participantes 19

2.4. Técnicas e Instrumentos de recolección de datos 19

2.5. Procedimiento 20

2.6. Método de análisis de información 20

2.7. Aspectos éticos 20

III. RESULTADOS 22

IV. DISCUSIÓN 30

V. CONCLUSIONES 37

VI. RECOMENDACIONES 38

REFERENCIAS 39

ANEXOS 43

Índice de Figuras

Página

Figura 1. Escenario del Departamento de Tecnología de Información. 18
Figura 2. Organigrama del Departamento de Tecnología de Información. 19
Figura 3. Triangulación de las entrevistas a profundidad. 22
Figura 4. Triangulación de antecedentes, marco teórico y los resultados. 25
Figura 5. Triangulación de observación de la unidad de estudio 26
Figura 6. Triangulación de las técnicas utilizadas. 28
Figura 7. Ciclo PDCA. 60
Figura 8. Estructura de la norma ISO 27001 60
Figura 9. Análisis de Riesgo TI 61
Figura 10. Proceso para la gestión de incidentes de seguridad 69
Figura 11. Definición de proceso para la gestión de incidentes de seguridad 71

Índice de Tablas

Página

Tabla 1. Dominios y controles basados en la norma ISO 27001 68
Tabla 2. Resumen de la situación actual de los dominios 69
Tabla 3. Políticas y controles definidos 70

RESUMEN

En la presente investigación se describirá la importancia y beneficios que agregará la implementación de la norma ISO 27001 en el departamento de Tecnología de Información de la empresa ESVICSAC, basados en la metodología de mejora continua dividido en las 4 fases establecidas, planificación, implementación, verificar y actuar, que se usará para todos los procesos de la institución.

La presente investigación se realizará mediante el método cualitativo, tipo de investigación aplicada y diseño de investigación de acción, por lo que se ha considerado a los usuarios del Departamento de Tecnología de la Información de la empresa Esvicsac, considerando a 3 especialistas, y se ha desarrollado los instrumentos de investigación que permitirán recoger la actualidad del departamento, como la guía de entrevista, guía de observación y ficha de análisis documental de la seguridad de información de los servicios de TI.

La implementación de la norma ISO 27001, permitirá al departamento de TI conocer de manera adecuada sus riesgos y vulneraciones así reducirlos y poder mitigarlos, a través de un sistema de gestión de seguridad, que permita administrar las ocurrencias y tenerlo controlado, así promover la mejora continua a la implementación y logre su estado de madurez requerido sumando nuevos procesos que ayuden a resguardar la información de la institución.

Palabras claves: TI, ISO27001, Seguridad de la información, PDCA.

ABSTRACT

This research will describe the importance and benefits that the implementation of the ISO 27001 standard will add in the Information Technology department of the ESVICSAC company, based on the continuous improvement methodology divided into the 4 established phases, planning, implementation, verification and act, which will be used for all the processes of the institution.

The present investigation will be carried out by means of the qualitative method, type of applied investigation and design of action investigation, for which the users of the Department of Information Technology of the ESVICSAC company have been considered, considering 3 specialists, and it has been developed the research instruments that will allow collecting the latest news from the department, such as the interview guide, observation guide and documentary analysis sheet on information security for IT services.

The implementation of the ISO 27001 standard will allow the IT department to adequately know its risks and breaches, thus reducing them and being able to mitigate them, through a security management system that allows managing occurrences and having it controlled, thus promoting improvement. Continue to implement and achieve your required state of maturity by adding new processes that help safeguard the institution's information.

Keywords: IT, ISO27001, Information security, PDCA.

I. INTRODUCCIÓN

En la actualidad las empresas desafían muchos riesgos exponiendo sus vulnerabilidades, precedentes de diversos puntos, siendo los activos de información uno de los más importantes y el activo que se debe custodiar de la mejor manera, aguardando los principios de disponibilidad, confidencialidad e integridad. Es por lo cual toda empresa debería hoy en día poder contemplar un sistema de gestión de seguridad de la información (SGSI), basándose en la norma ISO 27001, ya que de esa manera es posible asegurar sus activos de información. La norma es una solución, la cual, evaluará todo tipo de riesgo dispuestos que amenazan la información de toda empresa. En el departamento de tecnología de información de la empresa Esvicsac, no cuenta con un SGSI, y se plantea esta implementación teniendo en cuenta que nos toparemos con una actualidad, ya que, la empresa trabaja con sistemas, cultura de empresa, empleados que tienen su forma de trabajar, sin embargo, trabajaremos para fortificar los sistemas, las personas y los procesos de la empresa, reduciendo la vulnerabilidad, contando con el apoyo de la alta dirección.

En esta era digital, el avance de las tecnologías de la información y comunicación llamadas TIC´S es de gran relevancia. En la actualidad las empresas e instituciones, hacen uso de las nuevas tecnologías y lo convierten de gran utilidad, porque, les facilitan el acceso a la información de manera rápida y efectiva, ejecutándose por equipos electrónicos de comunicación, que están transformando los trabajos de una manera más clara, apoyando y soportando los trabajos realizados por el usuario el cual procesa, transmite o almacena información y de manera inconsciente aumenta un grado llamado riesgo, el cual se deja de lado por falta de conocimiento de las empresas. Es en aquel momento donde se vuelve expuesto la información en un sinfín de números de ataques y amenazas sustancialmente, por lo cual, ahora ya se necesidad de forma obligatoria poder garantizar la confidencialidad, integridad y disponibilidad de la información que se maneja.

La información es el activo más importante para todas las empresas, y hablando de la empresa ESVICSAC, está entidad maneja y administra información a nivel nacional de cerca de 2000 trabajadores, al revelarse información manejado por las distintas áreas administrativas, el riesgo sería muy costoso, lo describe Yupanqui, Ore (2017) cerciora que las empresas generarían grandes pérdidas económicas si es que no cuenta con políticas de seguridad de información, y en la actualidad la empresa no cuenta con un sistema de gestión de seguridad de la información, haciendo que la empresa, no conozca sus riesgos y

vulnerabilidades. La seguridad informática no es un bien que puede ser comprado, sino más bien son normas, guías y pasos que deben realizarse para poder mantenerlo. Siendo uno de sus objetivos el de lograr adecuados niveles de seguridad. En el transcurso del camino de la seguridad informática se han venido creado distintos modelos, estándares, recomendaciones y regulaciones, el cual permite poder mitigar los riesgos, la norma ISO 27001, propone la realización de un número importante de controles, para lograr reducir el riesgo de probabilidad de poder ser vulnerables a los distintos ataques informáticos y fuga de información.

Contar con un nivel de seguridad en la empresa genera confianza en los servicios que se implementan, la experiencia con los clientes al ser visibles digitalmente y seguros, podrán observar mejores experiencias, los procesos obtendrá una mayor capacidad de respuestas y la empresa aumentaría su ventaja competitiva, mostrar fallas de seguridad es muy lamentable, aunque a veces pase desapercibido, nos volvemos dispuestos y vulnerables pues cualquier información tiene valor. Internet no fue diseñado para ser seguro, sino fue diseñado para funcionar, Fernández (2017) así que la responsabilidad depende de todos, la complejidad del mundo tecnológico donde nos movemos merece soluciones complejas para implementarlas, buscando conseguir el nivel de integridad, confidencialidad y disponibilidad, que se necesita alcanzar un riesgo aceptable, asumiendo siempre que podemos ser atacados, sin embargo, debemos ser capaz de poder responder al ataque cumpliendo con las regulaciones implementadas.

Debido a la coyuntura que atravesamos, nos encontramos aguardando en casa por motivos de una pandemia, y ha sido casi obligado a muchas empresas a depender de la tecnología y ha abierto más la brecha en el uso del ciberespacio, unos para beneficiar el teletrabajo y dar continuidad con las labores operacionales de la empresa, y otros para el uso de desarrollo de otras habilidades donde ha causado y de nuevo puesto de moda en todas las noticias los Fraudes delictivos Espinoza (2016) mencionó que las empresas hayan ganado habilidades y conocimientos para mejorar la seguridad, ataques cibernéticos y las muestras de muchas entidades que han sido vulnerables y sus servicios se hallan vistos comprometidos siendo grandes empresas y por otro lado un grupo lucrando con la información obtenida o el simple hecho de ocio.

AT&T Cybersecurity Insights (2017), augura que los perjuicios producidos por estos cibercrimenes, pueda alcanzar los 6 trillones de dólares anual en el 2021. Pues hoy en día

cometer estos actos se ha vuelto cada vez más fácil y es por lo cual ha despertado el interés de las empresas de poder resguardar su información de manera segura , siendo así como se presenta la norma ISO 27001, siendo el principal estándar de seguridad a nivel mundial, el cual genera un sistema de gestión de seguridad de la información que permite que la información de la empresa u organización, se maneje de manera eficaz, así la empresa podría conocer y clasificar sus riesgos, la empresa también podrá adatar controles y procedimientos necesarios, protegerá la reputación de la empresa, aumentara la ventaja competitiva y como resultado se tendrá una empresa fortalecida tecnológicamente. Chilan (2017), mencionó que un SGSI garantizará el establecimiento de controles efectivos.

Entre las investigaciones realizadas a nivel internacional en el desarrollo de nuestra investigación, resalto a Henttinen (2018), que en su investigación utilizó estrategias para mejorar el sistema de gestión de seguridad de la información en la empresa Media X Corporation, la cual, se encuentran basados en el estándar ISO 27001, usó el método cuantitativo, para poder recopilar información de encuestas y realizar un cuestionario, también utilizó la herramienta de evaluación para realizar su medición y probarlas con otras investigaciones existentes, ya que sus objetivos era poder realizar un análisis de brechas para mejorar la seguridad existente. Henttinen concluyó que al realizar un estudio a su empresa existen niveles y factores que no están vistos, ya que no existen procedimientos coherentes para la evaluación de riesgos, proporcionando agujeros para un filtrado de información, sin embargo, propone el de poder mitigar este riesgo, ya que fue identificado por su proceso.

En la investigación realizada por Restrepo (2019), describió sobre la gestión de la seguridad, en la cual, observó el comportamiento de los protagonistas en la empresa NETHESA S.A.S, se apoyó usando el método cualitativo para observar los resultados obtenidos y usa herramientas de evaluación de los resultados de las entrevistas. Además, Restrepo instó en mejorar los procesos desarrollados, mostrando como objetivo el aprendizaje de la empresa en sus constantes procesos que adquiere sus sistemas, por la que propuso un orden en la administración de la seguridad, que para implementarla uso estrategias que ayudó al personal a cambiar procesos y rediseñarlos, también uso controles de evaluación para medir su gestión de seguridad implantada. Concluye diseñando una metodología para las copias de seguridad y la continuidad del negocio, además contó con el apoyo de su alta gerencia para lograr la certificación O-ISM3 que es un estándar para la creación de sistemas de gestión de la seguridad de la información, dejando diseñado la base

del sistema de gestión integral obteniendo un nivel de seguridad de riesgo aceptable para brindar una mejor seguridad a la información.

También Seclen (2016) en su investigó sobre los factores que sufrieron las implementaciones de los sistemas de gestión de seguridad en las instituciones del estado, basándose en la norma ISO 27001, por lo que su objetivo principal fue analizar los problemas que tenían el sector público para poder implementar un SGSI y las estrategias de las entidades que ya habían completado la ejecución y los beneficios que se obtendría, por lo que realizó un análisis observando las manera de implementar correctamente identificando beneficios obtenidos. Para lo que uso el método cualitativo, haciendo uso de herramientas como entrevistas, observación y el análisis de estudio documental, concluyendo que logró encontrar los factores que afectaron la implementación y define que para desarrollar un SGSI basado en la norma ISO 27001 debe ser usando la metodología PDCA para implementarla, además definir que es necesario la formalización del Puesto Oficial de seguridad de la información.

En la investigación realizada por Morales (2019), utilizó la norma ISO 27001, para incrementar la seguridad al trabajar atreves de la metodología de gestión Balanced Scorecard para la toma de decisiones que permita la continuidad del negocio. Usó el método cuantitativo para recopilar información atreves de recopilación de datos mediante cuestionarios y guías de observación realizadas a los usuarios del sistema, usándolo para crear y establecer lineamientos y criterios, para tratar los riesgos de los activos y procesos de información que puede verse afectado, manejando las probabilidades y midiendo el riesgo, concluye generando un plan de seguridad para valorar las políticas, el cual permite crear un plan de acción que califica en media y alta, haciendo que el sistema sea capaz de analizar los activos y valorar el riesgo del activo de la empresa financiera.

En la investigación realizada por Laura (2017), desarrolló una propuesta de diseñar, implantar e implementar, en las entidades del gobierno en el país vecino de Bolivia, un sistema de mejora continua para el uso de la aplicación de comunicación, la cual, permitió poder gestionar la seguridad de la información, de la misma manera basándose en la norma ISO 27001, buscando establecer la mejora en los procesos, además de proponer que su diseño sea un controlador de vulnerabilidades. En el trayecto de su desarrollo, usa el método cualitativo, el cual le permite hacer uso de las herramientas como la observación de los procesos y análisis documental, con los resultados puestos en funcionamiento, su primer

trabajo es de empoderar a los usuarios para poder sostener los controles necesarios para identificar los activos, amenazas y vulnerabilidades, además de poder integrar a la directiva de la empresa para generar sinergia con los usuarios finales para influenciar en el trabajo colectivo con el comité de seguridad formado en la investigación, logrando cumplir el diseño del control y la planificación, y a la vez genera la política de seguridad que define los procesos para tratar y evaluar los riesgo y mejora el sistema de seguridad en su entidad.

En su investigación Crespo (2018), usó la norma ISO 27001 y 27002, la cual trata de aplicar para revisar las incidencias de seguridad en las bases de datos de las instituciones superiores del país de Ecuador, analizando la seguridad de los activos de información, integrando controles de seguridad, el investigador hace uso de un enfoque cuali-cuantitativo, el defiende su estrategia de investigación indicando que necesita del uso de los dos métodos, utiliza el cuantitativo para medir y determinar el estado de la seguridad en las base de datos y la cualitativa para modificar el proceso de la eficiencia en la seguridad de la base de datos. Su investigación utiliza instrumentos de cuestionario para elaborar encuestas, guía de entrevistas y documentación del análisis y mide el grado de seguridad en la actualidad con lo que propone, llegando a concluir que la entidad debería de contar con los procesos formales que detalla, además, encuentra un sistema con carencias de seguridad de información y es de necesidad poder mejorar los procesos de esta entidad.

En su investigación Changoluisa (2017), propuso optimizar el proceso de alta y baja de los usuarios de la industria petrolera, ya que encuentra que es un proceso muy crítico y propuso que es de necesidad hacer uso de la norma ISO 27001, generando un sistema de seguridad para modificar el proceso esperado. Utiliza el método cualitativo, la cual, les permite una gran vista a los escenarios de cada acción en el transcurso esperado, haciendo uso de las herramientas de observación, para llegar a realizar un análisis documental y aplicar los controles necesarios para garantizar la debida seguridad en todo el proceso de alta y baja de los usuarios, concluye desarrollando una medición de tiempo basándose en el conocimiento que se registra gradualmente la reducción de los sub procesos y mejora los tiempos de ejecución de los procesos, una vez implementado los controles de seguridad, para cada proceso que realiza el sistema de la entidad.

Además, considero la investigación de Macanela (2016), buscó garantizar la seguridad mediante un modelo de continuidad de negocio. Usa como método para la investigación el modelo cualitativo para analizar y buscar los controles necesarios mediante

una evaluación de resultados y define estrategias de mejoras para brindar la continuidad de negocio. Macanela (2016) propuso implementar un modelo de SGSI que le garantice continuidad de negocio a su entidad, por lo que define COBIT como su modelo a implementar para dar control a la seguridad y en su observación implica mucho al usuario por la falta de compromiso para usar los procesos de manera correcta en la entidad financiera CACPE, que hace que sea totalmente opuesto a la que la entidad requiere que es el de brindar confianza garantizando continuidad de su operatividad. Los usuarios muestran su poco interés, ya que, no conocen o hace caso omiso a las recomendaciones, además a los controles ya establecidos que por alguna interrupción se dejaron de usar y ya no han sido tomados en cuenta, ocasionando una mala administración de usuarios, claves, accesos bajo perfiles de manera auditada, entre otros, la cual pone en peligro con mucha facilidad la información financiera en la empresa, además el plan de contingencia que tienen no realizan las pruebas periódicamente, provocando que las actividades corran con mucho más peligro en caso se presente una interrupción y la actividad no responda.

En las investigaciones realizadas a nivel nacional, referimos a Niño (2018), por la manera que uso un modelo de sistema de gestión de seguridad de información fortaleciendo, madurando y monitoreando los activos de la institución nacional de estadísticas. Utilizó el método cuantitativo, haciendo uso de herramientas de encuestas y checklist, la cual usa para medir el grado de madures con la que cuenta la institución, por lo que observo un alto índice de vulnerabilidades después de las observaciones a los resultados de la encuesta realizada a la organización. Niño, describió un sistema de gestión de seguridad el cual permitirá poder reducir las vulnerabilidades de la filial, sin embargo, concluye en que se debe de evaluar la implementación de la ISO 27001, para poder mejorar los procesos de la organización, ya que contemplan muchos procesos la cual son riesgosos y no sería posible mitigar rápidamente, pues se requiere un tratamiento y la entidad no cuenta con recurso humano con conocimientos en seguridad, por tal insta a que la empresa pueda contactar con un personal especializado.

También en su investigación Coaguila (2020), diseñó un plan de SGSI basado en la norma ISO 27001 en la universidad de Moquegua, poniendo en práctica la metodología cuantitativa para realizar encuestas y conocer el estado situacional, siendo su objetivo general poder diseñar un plan de SGSI basado en la norma, implementar un SGSI, llegando a la conclusión que la implementación realizada, ha encajado de manera directa y

proporcional a la empresa, y de igual manera recibió la aprobación positiva al culminar la evaluación de los evaluadores, por lo que le permitió elaborar de manera adecuada su plan para poder implementar el SGSI.

También considero a Caballero (2017), en su investigación el uso del PMBOK para proyectar la implementación de la oficina de Gestión de Proyectos bajo la norma ISO 27001, siendo sus objetivos de poder implantar una estructura orgánica además de presentar un modelo metodológico para gestionar proyectos, promover lineamientos de la organización y promover los procedimientos normativos, además de poder usar un método cuantitativo, concluyendo en el modelo encargado de gestionar los proyectos, aportes de la organización y atreves de la guía pmbok para implementar los pilares de la gestión.

En su investigación Flores (2017), que realizó un estudio para poder implantar en la Oficina de Gestión de Proyectos de TI basado en la ISO 27001, de los ministerios del estado peruano para obtener información si es que se usa la norma ISO 27001 y si ha permitido mejorar la seguridad de la información, por lo que hace uso del método cuantitativo, ya que para el estudio es de necesidad poder realizar análisis y obtener estadísticas y medir causa efecto, para lo cual utiliza herramientas como encuestas y cuestionarios a todo el personal especializado en los sistemas de las distintas entidades del estado, trabajando en mejorar la estrategia de seguridad en las infraestructuras críticas, reduciendo el crimen cibernéticos, sin embargo, al realizar el estudio que todas las entidades el manejo y planificación de la norma no ha sido las adecuadas, por lo que su es considerado por el enfoque de implementación lo hace mayor al poder solicitar que se formen órganos de control para supervisar la implementación en las instituciones del estado.

También en su investigación Cueva, Mercado (2017), implementó un sistema de gestión de historia clínica del hospital de Cajamarca, utilizó la verificación de cumplimientos basado en la norma ISO 27001, en la actualidad, el estado a través de sus entidades públicas, tienen la obligación de tener implementado políticas que gestión la seguridad de la información, por lo que es de necesidad poder implementar normas que permitan la evaluación y control de estas actividades. Puso en práctica la metodología cualitativa para desarrollar su investigación, además de usar herramientas como entrevista y el análisis documental que necesita para desarrollar de manera adecuada implementación, por lo que realiza observación directo del entorno y el desarrollo de los procedimientos, y realiza las entrevista al personal especializado y encargados de los procesos, por lo concluye

implementando controles de mejoras para lograr alcanzar la implementación completa de todos los criterios que se requiere en el proceso de resguardar la información.

En la actualidad los problemas del mundo giran bajo el ciberespacio, y los ataques en cibernéticos vienen siendo de uso diarios, por ejemplo el ciberataque en el país de Estonia en el 2007, la cual produjo inhabilitación pasajera de muchas instalaciones militares, también podemos nombrar el ciberataque de Rusia al país de Georgia 2008, el cual trajo como consecuencia la invasión terrestre, otro caída de sistema de ataques informáticos que sufrió EEUU, descubriendo que una de sus bases de ataques se encontraban en china. En el año 2017 la empresa telefónica España fue atacado por un malware rasonware, la cual secuestro miles de información de la compañía y llego a perjudicar a sus clientes que podían estar conectados en sus redes. En el presente año, al inicio de la cuarentena la empresa zoom una de las empresas que brinda una plataforma en la nube para realizar videollamadas, fue vulnerado y poniendo a disposición una lista de información de usuarios, la cual, propago un impacto fuerte a nivel comercial.

Las caídas de las redes sociales, la red social llamada tik tok, la cual, por no usar un protocolo seguro (https), formo parte de secuestro de información, caída de los DNS en EEUU, servicio de comunicación por radios de la policía de Chicago, entre otros. En la actualidad podemos decir que se ha convertido muestras para hacer prevalecer ideales, motivos de protestas, secuestro de información para luego lucrar y además por ocio, pues conociendo todos estos antecedentes, se debe de generar un buen sistema de seguridad reduciendo la vulnerabilidad de posibles ataques en nuestros sistemas, bajo estos argumento se llega a conclusiones que en caso que no se use un buen sistema que nos permita gestionar la seguridad en nuestra empresa podemos ser blancos fáciles frente a cualquier ataque o fuga de información, sin poder reaccionar y evitar hasta el quiebre de la empresa, por tal, se convierte ya no un lujo sino una necesidad para salvaguardar la información.

Recursos disponibles: Se debe de buscar el compromiso de la alta dirección, así facilitaría el acceso a lo más importante el recurso económico, el cual nos abriría la brecha necesaria para poder tener el presupuesto debido y se obtendrá el recurso económico, las oficinas, las herramientas de trabajo, lo tangible, lo cual obtendremos el recurso físico, el capital humano es muy importante, ya que conocen los procesos, sin embargo, es necesario la capacitación de cursos debidos, así se podrá resolver problemas y gestionar los cambios en el equipo, para mejor el desempeño del proyecto fortaleciendo el recurso humano.

Competencia del personal: Es poder determinar la competencia necesaria para llevar acabo, asegurando que sean personal altamente competente en la educación, preparación y experiencias referente a seguridad de la información, se deberá usar métodos sobre requisitos o habilidades mínimas para calificar aun personal que reúna los requisitos y habilidades necesarios que cumpla lo descritos en las primeras líneas de este concepto. Cabe mencionar que, el departamento siempre deberá de mantener capacitado a su personal debido a las normativas y sistemas que se tienen desplegados, por lo cual, el personal siempre deberá estará relacionado con las políticas y controles que se deben de ejecutar.

Norma: Son un conjunto de reglamentos que se establecen con el propósito de poder regular comportamientos procurando mantener orden, el cual permite a sentar las bases de una conducta aprobado, para así conservar un orden. Las normas es el conocimiento, la sabiduría, la cual destiló de la gente con experiencia en el tema y quienes conocen las necesidades de las organizaciones en las que representan. El punto de una norma es proporcionar una base confiable para que los especialistas puedan compartir las mismas expectativas acerca de un producto o servicio, esto ayudará a poder proporcionar un marco de referencia para lograr economías, eficiencia e interoperabilidad, poder mejorar la protección y la confianza del interesado.

ISO 27001: Es una norma internacional de seguridad de la información, publicado en el 2005 por dos organizaciones mundiales, la International Organization for Standardization y International Electrotechnical Commission. El cual especifica los requisitos necesarios para poder implantar, mantener y mejorar, un sistema de seguridad de la información, esta permite ser implementada en cualquier tipo de organización con o sin fines de lucro, privada o pública, pequeña o grande empresa. La cual ha sido desarrollada por los mejores especialistas del mundo en el tema, proporcionando una metodología para implementar la seguridad de la información en una organización obteniendo resultados de riesgos aceptables.

La norma ISO 27001, tiene como propósito poder proteger los tres pilares de la seguridad que son: la confidencialidad, integridad y disponibilidad de la información en la organización. Pues revisa las distintas complicaciones que podrían perturbar a la información y luego precisar cómo evitar que estos inconvenientes puedan ser mitigados por el riesgo, por lo tal se afirma que la ISO 27001, apoyada en la gestión de riesgo, investiga en donde pueden ser captado los riesgos para inmediatamente trabajarlo de manera

sistemática. Si es implantada correctamente no se vuelve burocrático, sino más bien en una herramienta eficiente buscando objetivos comerciales. La ISO 27001, tiene familias que ayudan a mejorar la seguridad, evaluación de riesgo y reducción de vulnerabilidades, y para su continuidad apoyándose en la norma ISO 27002 – Implementa controles, ISO 27004 – Evalúa la seguridad de la información, ISO 27005 – Gestión de riesgo, ISO 27017 – Controles de seguridad para los servicios cloud.

La implementación de la ISO 27001, es basarse en el uso de la metodología que permite una mejora continua llamado el ciclo de Deming o PDCA, basados en cuatro pasos de manera sistemática (Planificar, Hacer, Verificar y Actuar) para lograr la mejora continua y la calidad de los servicios, siendo cuatro etapas cíclicas, que permite mejorar volviendo a la primera y repetir el ciclo de manera que todas las actividades pueda ser reevaluadas periódicamente y permite añadir nuevas mejoras que refuercen la eficacia y eficiencia de la implementación de forma continua.

Información: Es denominado como al conjunto de datos procesados para brindar un conocimiento, concepto o idea, el cual es generado para mostrar un mensaje. Para entender un concepto sobre información informática, primero derivamos y encontramos el dato, el cual es un carácter, símbolo, o representación, que se encuentran aisladas sin ningún conocimiento entre sí, quien designa y ordena a estos datos se le denomina conjunto de datos, encargándose de ordenar y procesar los datos, mediante la una unidad central de procesamiento, obteniendo la cantidad de variedad datos organizados, por lo cual este ya puede ser interpretado. Conella (1995), en su libro de recurso de información, explica que la información es un recurso y se presenta eminentemente metodológicos que si es bien tratada la información este se convierte en un factor favorable si es que se conduce de manera apropiada, muestra empresas como Benetton, Zardoya-Otis y American Airlines, las cuales muestran características de triunfo por el buen uso y manipulación de la información.

Seguridad de la Información: La seguridad de la información persigue el resguardo atreves de un acumulado de técnicas y medidas anticipadas y reactivas de la empresa y los sistemas tecnológicos que lo resguardan, así poder inspeccionar todos los datos que maneja la institución y asegurar que no sea expuesto, alcanzando el objetivo de la preservación de la confidencialidad, integridad y disponibilidad de la información, minimizando los daños a la organización y ayudando a maximizar el retorno de inversiones.

Según López (2010), en su libro seguridad informática, da un concepto que debe estar claro, el cual, menciona que todo lo que no esté permitido, debe estar prohibido. Existen 2 tipos de seguridad, activa, la cual comprende el conjunto de defensas, técnicas, reglas o medidas usadas para evitar o reducir el riesgo que amenazan los sistemas y pasiva, son los métodos y/o medidas que se constituyen para una vez producido el incidente, se pueda minimizar su repercusión, facilitando la recuperación del sistema. También Bertolinín (2008) en su libro de seguridad de la información, menciona que el objetivo general de la seguridad de la información debe ser una disciplina continua de evolución, para así llegar a la meta que es, que toda la empresa pueda cumplir el objetivo del negocio cuidando y considerando los riesgos relativos de los sistemas y procesos de tecnologías de información de la empresa.

Riesgo Informático: Es la contingencia o cercanía de un daño, cuya probabilidad de ocurrencia puede ser eventual y se mide mediante su factible manifestación y el impacto que llegara a causar, pasa por un conjunto de escenarios que pueden disminuir el beneficio, siendo un riego potencial, como la carencia de control de los dispositivos, control sobre los accesos a la información y su protección a usuarios ajenos Diéguez (2019), también es la posibilidad de que una amenaza explote una vulnerabilidad en un activo y pueda causar daños y pérdidas. Pues trabajar en el riesgo nos ayuda a tener la contingencia para el posible daño. Los lugares principales para medir los riesgos deben ser: la seguridad física, control de acceso, protección de datos, seguridad en redes, así evitar el cumplimiento de un objetivo ante una eventualidad, por tal se debe considerar tener una administración del riesgo, ya que debe ser necesario la evaluación periódicamente de los riesgos definidos y es en esta situación donde Sena (2004) en su catedra de introducción al riesgo, define los pasos estructurales para la evaluación de los riesgos y controles que se debe de realizar utilizando la metodología COBIT para ayudar a desarrollar, organizar e implementar las estrategias.

Amenazas: Las amenazas son aquellas situaciones que se convierten en incidentes en la empresa, dañando lo material o experimentando perdidas de activos de información. Por lo cual, cabe mencionar que, es un potencial evento, que puede suceder en cualquier momento, que esta presto para ocurrir sin que esté previsto, o se puede desencadenar sin previo aviso, por ende, la amenaza es un incidente que altera la seguridad de los activos de información de la empresa o cualquier cosa que puede salir mal y es necesario tenerlo en

cuenta y examinar el impacto, ya que puede afectar a la disponibilidad, confidencialidad o integridad.

Existen amenazas no humanas, de origen industrial, que pueden ser incendios, explosiones, inundaciones, contaminación, accidentes naturales, como temblores, terremoto, interrupción de suministros esenciales, como fluido eléctrico, agua, telecomunicaciones, además de los accidentes mecánicos o electromagnéticos. Amenazas humanas, errores en el proceso de recolección y transmisión de datos, errores en los diseños en los procesos, errores en la entrega de datos de los procesos, errores de monitoreo y tráfico de información. Amenazas humanas intencionales con presencia físico y amenazas intencionales de origen remoto.

Vulnerabilidad: Es una debilidad o fallo en un activo de información, es la posibilidad que se materialice una amenaza poniendo en riesgo la seguridad de la información, también engloba cualquier debilidad en los sistemas o procesos dejando expuesto a una amenaza, los fallos más comunes que se ven a diarios son las contraseñas débiles, software y sistemas comprometidos, falta de restricciones a sitios no confiables. Las vulnerabilidades de día cero, la cual es un fallo no conocido, facilitando al atacante cumplir con su cometido, también existe la vulnerabilidad de diseño, la cual son debido al mal diseño de las redes y seguridad perimetral, vulnerabilidad de implementación, la cual son derivado de la programación de los sistemas o descuidos de fabricantes, las vulnerabilidades por falta de mantenimiento y también las vulnerabilidades por uso las cuales ha sido debido al factor humano. Además, Zambrano (2017) en su artículo de seguridad en informática, define como vulnerabilidad a los posibles ataques que se realice por dejar puestas abiertas en un sistema e insta en poder tener en cuenta que cualquier proceso no bien definido puede ser aprovechado que podrían causar daños a los sistemas.

Análisis de riesgo: También conocido como evaluación de riesgo, pues es el estudio que se realizar para evaluar las causas de las posibles amenazas y probables eventos que pueden causar daños a la información, además de determinar los recursos de un sistema que requiere protección. Su objetivo es poder llegar a un nivel razonable de consenso para implementar indicadores operacionales la cual se pueda medir y evaluar, se debe tener en cuenta que existen varios métodos para evaluar los riesgos, como Itil, Cobit, Margerit, Octave, entre otros.

Inventario de activos de información: Es un control de la norma, pues exige su realización, pues es necesario conocer con lo que se cuenta para dar inicio a los trabajos a realizar, evitando complicaciones para gestionarlos correctamente, además se debe tener claro que este inventario debe actualizarse periódicamente y cada cambio que hubiese debería ser comunicado, podemos además decir que, los activos son los recursos que usa todo sistema de gestión de seguridad de la información para que los procesos de la empresa puedan conseguir su objetivo. Los activos se separan en tangibles e intangibles, los tangibles son los activos que contienen información, como los servidores, equipos informáticos, equipos de red local, periféricos, y se debe proteger de los riesgos físicos como golpes, fuego, humedad, etc, y los intangibles son los activos que soportan la información, como las aplicaciones, sistemas, procesos, suministros.

Manual de seguridad: Es el documento en donde se define el procedimiento de cómo debe ser implementado y como dar continuidad a la gestión de seguridad, pues en el documento se deberá instaurar los lineamientos básicos, información sobre los responsables, las políticas, objetivos, alcances y otras actividades, las cuales ayudará a proteger de manera eficaz y eficiente, mediante un enfoque preventivo y reactivo, además de definir la importancia de custodiar los servicios críticos a las posibles fallas.

Manual de Procedimientos: Es el documento, el cual se implementa para poder describir cada procedimiento que se necesita atender y efectuar en las tareas que desarrolla el departamento de tecnología de información, el cual cumple con uno de sus objetivos de poder orientar al personal del departamento y las otras jefaturas de la empresa, sobre los pasos que deberán de realizad para tener acceso a los servicios informáticos; así como para la planificación, administración de los recursos informáticos, por la cual deberá de contener los diagramas de flujos, los procedimientos y los formularios debidamente explicado detalladamente, buscando así a contribuir y prestar servicios de calidad tanto para la empresa como para sus clientes.

Manual de riesgos: Es el documento, el cual se implementará para describir las políticas y metodologías de los procedimientos que se trabajará para mejorar una adecuada gestión del riesgo, en donde se detallará además el objetivo, el alcance, en la que se deberá describir las responsabilidades, con el propósito de cumplir con las normativas y disposiciones acogidas por la entidad, mejorando el desempeño y la capacidad de respuestas frente a un riesgo detectado o vulnerado.

Auditoría Interna ISO 27001: Es el control vital e importante que se realiza al SGSI para revisar el cumplimiento de la norma ISO 27001 en todos los procesos definidos, además de medir su calidad, su eficacia, eficiencia y suficiencia, también sirve para medir el alcance de la norma en la institución, por lo cual tiene en consideración todas áreas involucradas en el proceso y cada uno de los usuarios que son parte del proceso, para encontrar puntos de mejora, usando como medida o alarma a los usuarios de cuán importante y cuán prioritario es el cumplimiento de las obligaciones de la seguridad .

Para implementar la norma ISO 27001, se es de necesidad considerar 4 fases, las cuales ayudarán en el completo desarrollo de la implementación y produce una implementación exitosa, al iniciar con el diagnostico, la cual, es la primera fase esencial que nos permitirá obtener la aprobación de la dirección general, en la que se deberá medir la competencia del personal y realiza el análisis de riesgo que puedan afectar la implementación. Segunda fase la planificación, en esta etapa se deberá hacer la entrega las actividades, fijando las políticas y determinando los procesos y controles, por lo que cada actividad pasa a ser compromisos. Como tercera fase de implementación, se deberá usar un método de gestión de proyectos el cual permita desarrollar el manual de seguridad, manual de procedimiento y el manual de riesgo, el cual permitirá implantar el desarrollo en todos los procesos. Cuarta fase la evaluación, el cual nos permitirá poder medir los indicadores de la implementación y los riesgos si es que persisten y establecer las acciones de mejora y la elaboración de los resultados para ser presentado a los altos funcionarios.

La justificación de la presente tesis radica en poder realizar la propuesta de implementación de la norma ISO 27001 que permita minimizar los riesgos de los procesos que adquiere la empresa bajo el departamento de Tecnología de Información, ya que estaría comprometido toda la empresa en caso de alguna caída de los sistemas y o perdidas de información de áreas críticas, por el solo hecho de no contar con un sistema de gestión de seguridad de la información en la empresa, definimos que es necesario poder apoyarnos en una metodología que nos brinde los ítems necesarios para brindar mayor seguridad, reduciendo la escala de vulnerabilidad, en la empresa, definiendo los términos necesarios para que la implementación pueda ser exitosa, cuidando los procesos y los sistemas, para lo cual se estará utilizando como base la norma ISO 27001, así poder fortalecer y mitigar los riesgos, siendo capaz de poder mantener continuidad en los servicios y procesos, brindando la contingencia necesaria para la disponibilidad, confidencialidad e integridad de la información.

Desde la intencionalidad práctica, es necesario poder reducir los riesgos y vulnerabilidades de la empresa, teniendo en conocimiento que no estaremos seguros a un 100% ya que no existe tal concepto, sin embargo, si es posible reducir el grado más mínimo el riesgo o las vulnerabilidades que podemos ser víctimas frente a los ataques o fuga de información. En consecuencia, la norma ISO 27001 en la empresa ESVICSAC, mejorará los procesos y servicios informáticos, se trabajará bajo un sistema de gestión de seguridad de la información para poder trabajar de manera adecuada y segura los ítems que observemos por los resultados obtenidos y así implementar la ISO 27001, por lo cual, no ayudará a estar preparados para accionar en cualquier momento brindando posibles acciones correctivas para dar solución a posibles incidentes de seguridad.

En la investigación presentada, se define el problema general que nos insta en poder defenderlo y ponerlo en investigación para revisar y evidenciar los resultados concebidos, siendo el enunciado lo siguiente: ¿Cómo la implementación la norma ISO 27001 en el departamento de Tecnología de Información de la empresa Esvicsac, Callao, mejorará la seguridad de la información? obteniendo los siguientes problemas específicos: ¿Cómo planificar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?, ¿Cómo ejecutar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?, ¿Cómo verificar la implementación de la norma ISO 27001 en el departamento de

Tecnología de Información en la empresa Esvicsac, Callao?, ¿Cómo actuar en la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?.

La presente investigación tiene como objetivo general describir la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao, las cuales establece los siguientes objetivos específicos: Describir la planificación para implementar la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac. Callao. Describir la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao. Determinar la verificación de la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao y Determinar la actuación para mejorar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao.

II. MÉTODO

El problema que tiene la empresa en la actualidad es no conocer lo critico que es no contar con un SGSI, para tomar decisiones inmediatas a un posible fallo, fuga de información o incidentes que generen la perdida de la información. El departamento de Tecnología de la Información de la empresa Esvicsac, no maneja una estructura bajo normas de trabajo, por lo que no mide el riesgo y las vulnerabilidades que puede existir en cada proceso que tiene a su cargo y es la falta de interés de la alta dirección de poder contar con un sistema de seguridad. Esta investigación busca implementar la norma ISO 27001 en el departamento de TI, para garantizar la confidencialidad, disponibilidad e integridad que los sistemas requieren fomentando la mejora continua, logrando reducir sus riesgos y vulnerabilidades.

Por tal sentido se define el enfoque cualitativo, ya que observamos de manera directa a los trabajadores en su entorno analizando y estudiando sus particularidades y experiencias. Solarte (2015), en su libro sobre metodología de la investigación cualitativa, describe las características de este método, haciendo uso de la entrevista a profundidad la cual le sirve, para recoger información y brinda la alternativa de ser flexible y desestructurado, la cual se necesita para esta investigación. También Gonzales (2016), se basa en el paradigma interpretativo y utiliza dicho enfoque para transmitir su investigación, observando los resultados y dar inicio, para luego planificar la implementación de la ISO 27001 en su empresa.

2.1. Tipo y diseño de la investigación

Tipo de Investigación

El propósito de la siguiente investigación, persigue según la finalidad un tipo de investigación aplicada, porque la presente se basa en un conocimiento científico y tecnológico que busca analizar la actualidad de los procesos en la empresa para perfeccionarla, además, nos basaremos en los procesos tecnológicos para serlos más eficaces con los cambios propuestos, la cual estallaremos brindando un alto nivel de seguridad en la información, teniendo en cuenta que lo esencial es promover un cambio en la seguridad de la información en el departamento de TI, por lo cual al ser implementada se estará brindando mayor seguridad, reduciendo las vulnerabilidades encontradas que en la actualidad se adolece.

Diseño de Investigación

La siguiente investigación, mantiene un diseño de investigación de acción, la cual busca mejorar los procesos para a través de la implementación a realizar, además de ver que se manifiesten mejoras en los procesos, siendo mucho más seguros y menos vulnerables a los riesgos existentes para la implementación. Se trabajará en los tres pasos necesarios observando, pensando y actuando, por lo cual generaremos mejoras permanentes en cada proceso que tratemos. Según Bell (2005) indica que este diseño es usado comúnmente para investigadores que han encontrado problemas en sus empresas y tienen la necesidad de estudiarlo para contribuir en la mejora.

2.2. Escenario de estudio

Se promueve implementar la presente investigación en la empresa Esvicsac, en el departamento de Tecnología de Información (figura 2), ubicada en el distrito del callao. Se eligió este escenario, ya que, el ambiente físico (Figura 1) brindará el apoyo emocionar y las interacciones entre el personal fluye de manera adecuada y se está dispuesto para el acorde trabajo de investigación, pues no brinda un mejor escenario al problema de seguridad en los procesos, es necesario poder implementar la norma ISO 27001 que ayude a mejorar y reducir los riesgos en el departamento de sistemas, causando un impacto de mejoría en toda la organización, a través de sus procesos, bajo el sistema de gestión implantado la cual deberá de cumplir eficientemente, demostrando la capacidad de protección de su información.

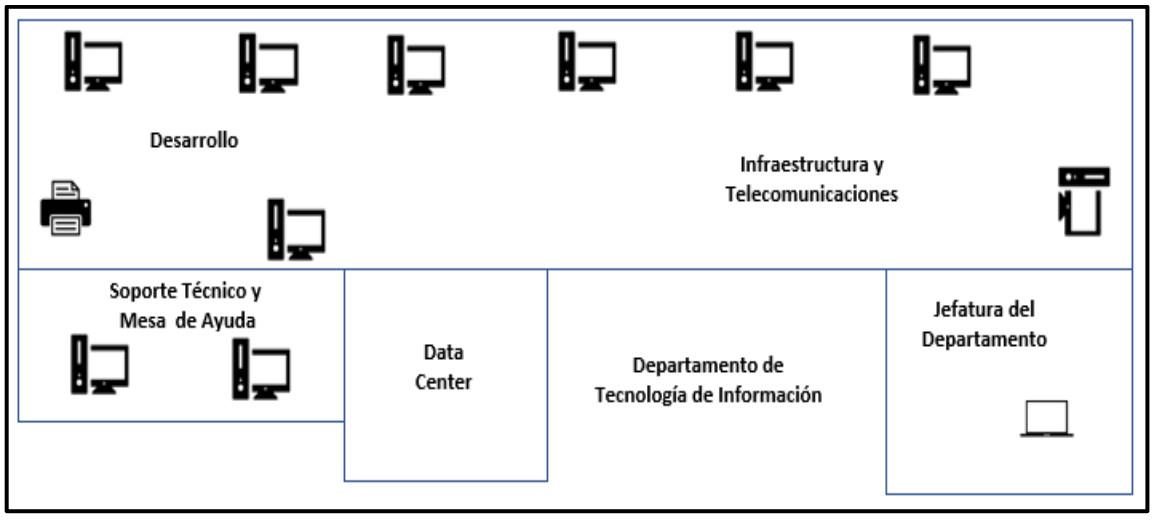

Figura 1. Escenario del Departamento de Tecnología de Información.

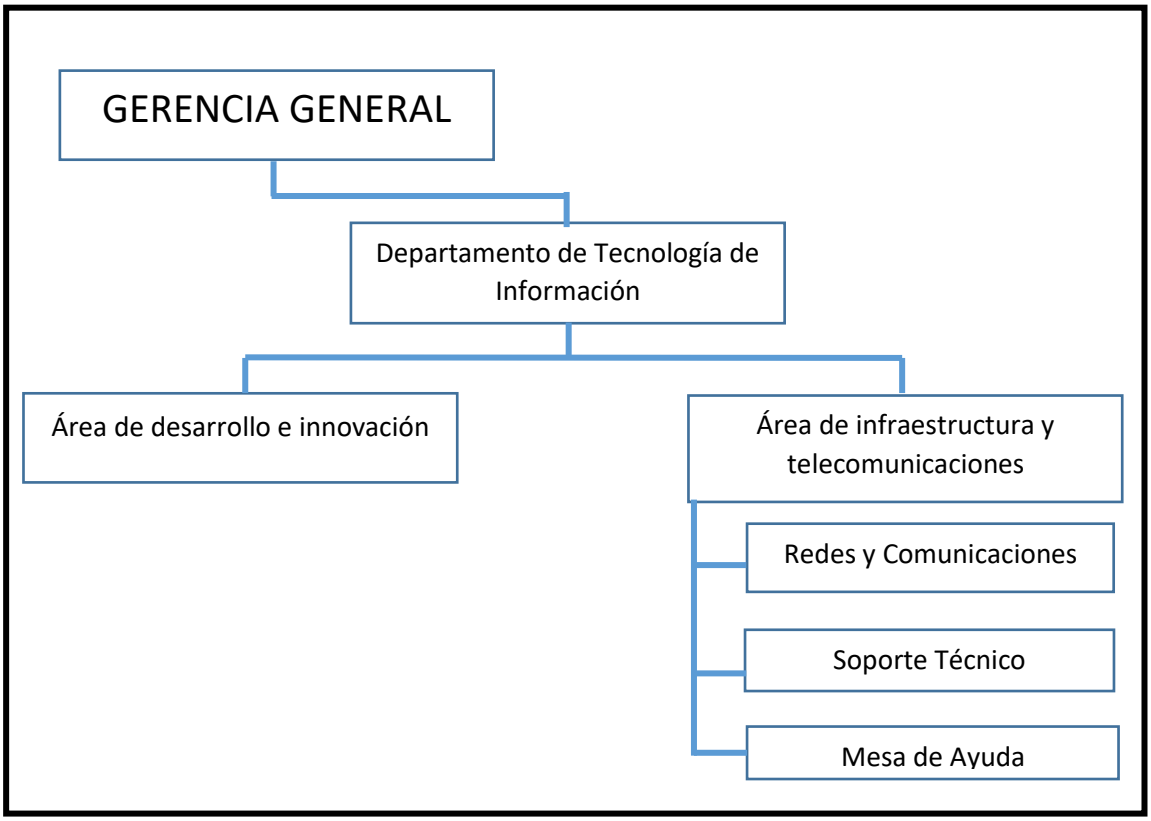

Figura 2. Organigrama del Departamento de Tecnología de Información.

2.3. Participantes

En la presente investigación hemos elegidos a tres (3) personas representativas, los cuales, son los responsables de las áreas que se define en el organigrama del Departamento de Tecnología de Información de la empresa Esvicsac, los cuales han sido elegidos por ser parte fundamental en la presente investigación, ya que brindan las facilidades para contemplar los procesos, examinando a detalle el comportamiento, además, son especialistas y cuentan con experiencia en cada una de las áreas a las que representan, con el fin de poder observarlos y describir cada proceso y las herramientas informáticas que usan para realizar y cumplir con el desempeño de sus labores dentro del ambiente de trabajo.

2.4. Técnicas e Instrumentos de recolección de datos

Existen distintas técnicas para la recolección de datos Mendez (2011), definió que las fuentes y técnicas para recoger información, son los hechos o documentos que se usan para la investigación. En la siguiente investigación se procedió a realizar la recolección de datos usando la técnica de entrevista a profundidad, usando instrumentos como la guía de entrevista semi-estructurada, guía de observación estructurada, ya que se ha elaborado preguntas para proceder con el entrevistado, además se usará la observación con la finalidad de obtener la información del estado situacional y el comportamiento de los participantes en

su misma naturaleza de trabajo, con la finalidad de poder analizarlo de manera individual y colectiva para poder responder las preguntas de la investigación el cual nos da el punto de partida para la investigación así mejorar los procesos internos, además de la ficha de análisis documental, para revisar el estado situacional.

2.5. Procedimiento

En la presente para el desarrollo de la investigación se utilizará los siguientes métodos para realizar la investigación, tales como, la entrevista a profundidad que se está realizando a 3 especialistas del tema y laboran en la empresa y conocen a fondo el negocio, también se cuenta con una guía de entrevista, la cual nos permitirá poder recoger la información valorada de los especialistas de cada área del departamento de Tecnología de Información de la empresa Esvicsac, además, se realizará la observación, con el fin de valorar el comportamiento de cada usuario mediante la guía de observación y por lo siguiente se realizará un análisis documental. Por lo que nos ayudará en poner en marcha el diagnostico, planificación, organización y la evaluación de la implementación de la norma ISO 27001.

2.6. Método de análisis de información

En la presente investigación se usa el método inductivo, por la manera de poder evaluar las características reflejadas en el comportamiento de los participantes, además de poder usar como herramienta la entrevista semi estructurada, basándonos en el problema general y las categorías de nuestra matriz y se realiza una matriz de codificación y la matriz de entrevista la cual nos dará un claro resultado de las diferencias semejanzas y conclusiones que obtengamos por cada pregunta.

2.7. Aspectos éticos

La presente investigación es desarrollada de manera propio y original del investigador respetando cada lineamiento para expresar el contenido, haciendo uso mediante el sistema turnitin, además, se respeta las ideas de los autores citados en el contenido en la tesis, referenciando correctamente los autores. Cabe mencionar que, el investigador tiene una habilidad en el manejo de los métodos y técnicas a poder usar, usando la RRNº 0089 que corresponde a los lineamientos establecidos por la Universidad Cesar Vallejos, en donde se encuentra la estructura de la tesis, la norma de redacciones al estilo APA, además de conservar el anonimato de las personas entrevistadas. De tal manera se logrará demostrar en cada resultado planificado poner todo de sí para demostrar lo que se busca con los objetivos

planteados, llegando a obtener resultados esperados y demostrando con las conclusiones poder terminar con éxitos lo propuesto en el problema general.

III. RESULTADOS

En la presente investigación, se ha trabajado con las herramientas de recolección de datos, la cual, nos permitió trabajar con la entrevista a profundidad, la observación y el análisis documental, para poder llegar a los a alcanzar nuestro objetivo definido, lo que nos permitió poder desarrollar nuestra triangulación para definir nuestras conclusiones, después de las debidas respuestas de los especialistas.

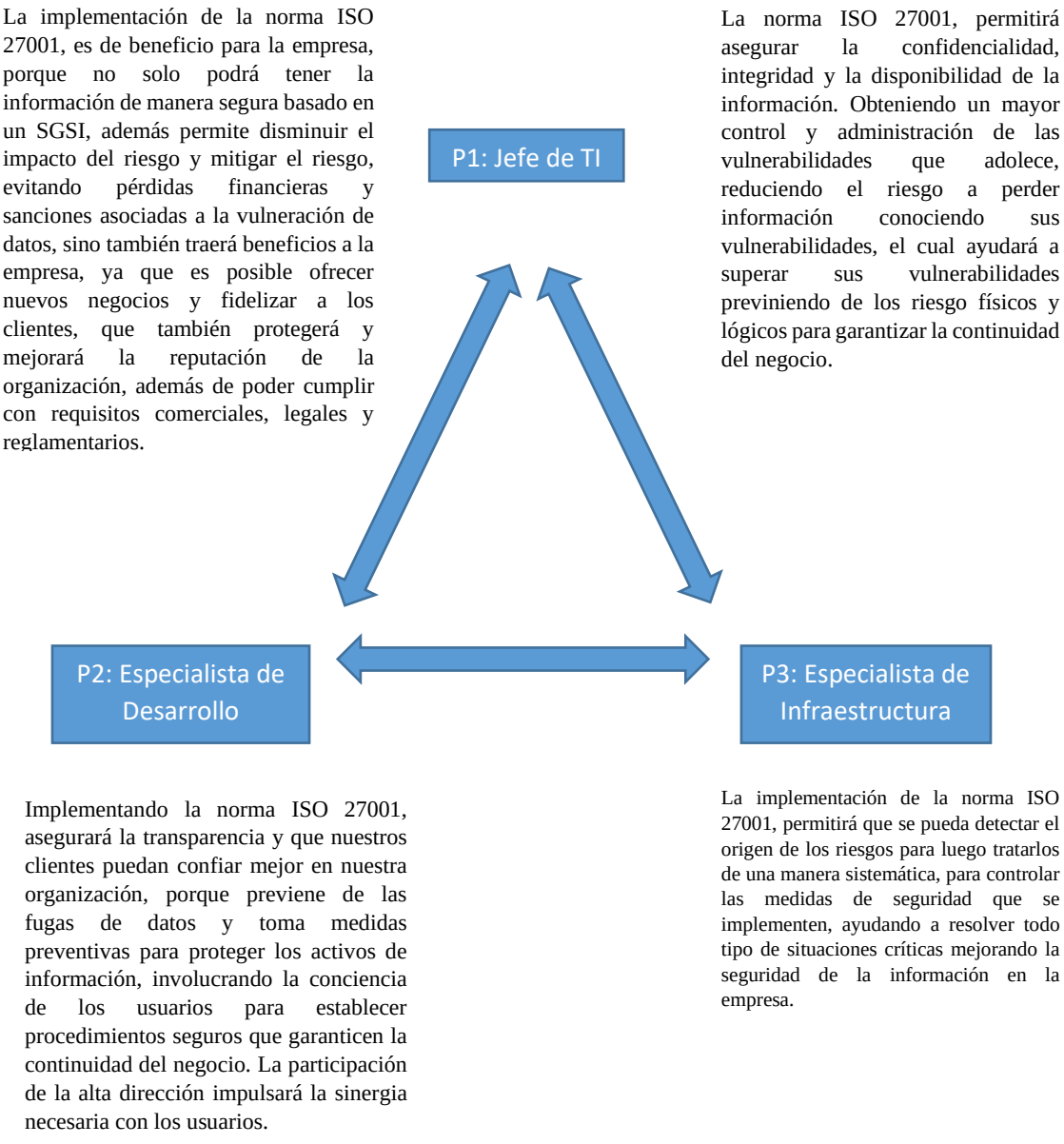

Figura 3. Triangulación de las entrevistas a profundidad.

Según la pregunta relacionada con el objetivo general de la investigación ¿Cómo la implementación la norma ISO 27001 en el departamento de Tecnología de Información de la empresa Esvicsac, Callao, mejorará la seguridad de la información? Especialistas entrevistados concluyeron que la implementación de la norma ISO 27001 mejorará la seguridad de la información, ya que, gracias a sus buenas prácticas, se puede conocer cuáles son los riesgos y vulnerabilidades, que la empresa adolece, previniendo las posibles fugas de información mediante un plan de seguridad, que permita mitigar el riesgo de la información, basándose en la mejora continua logrará siempre mejorar el significado de seguridad informática. Para implementar la norma ISO 27001, es necesarios poder realizarlo en 4 fases de la PDCA, siendo conocidas como el ciclo de Deming o el ciclo de la mejora continua, con respecto a la pregunta que se relaciona con el primer objetivo específico de ¿Cómo se planifica la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao? Se concluye que los especialistas en la planificación consideran trabajar haciendo uso de una metodología de gestión de proyectos, basados en la guía del pmbok, quien brinda sus características necesarias para poder implementar de manera adecuada la implementación, ya que se encargará de administrar todos los recursos y define sus responsables, además de poder definir de manera correcta y practica el alcance del proyecto y el análisis de riesgo para la implementación.

Continuando en orden las etapas, con respecto a la pregunta que hace mención a nuestro segundo objetivo específico: ¿En qué consiste la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao? Los entrevistados concluyeron que la implementación consiste en poner en marcha lo planificado, respetando los tiempos por tareas organizadas y los recursos establecidos, bajo el personal responsable. También la pregunta que hace mención a nuestro tercer objetivo ¿Cómo verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao? Los entrevistados concluyen que se debe de verificar regularmente la efectividad de la implementación, el cual permitirá poder validar correctamente las actividades, por lo que se deberá de realizar auditoría interna que permita comprobar que se cumpla los requisitos y procedimientos en los procesos planteado.

Además, la pregunta que hace mención al cuarto objetivo específico: ¿Cómo se actúa en la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao? En la implementación se actúa estableciendo acciones correctivas que permitan mejorar la implementación, ya que es necesario dar conformidad a una implementación culminada el cual debe de cumplir con el alcance debido mitigando vulnerabilidades y reduciendo los riesgos. Se ha realizado una conclusión general, de acuerdo a los expresado por los especialistas, la implementación de la norma ISO 27001, es de beneficio para la empresa, porque no solo podrá tener la información de manera segura basado en un SGSI, que nos permite disminuir el impacto del riesgo y mitigar el riesgo, evitando pérdidas financieras y sanciones asociadas a la vulneración de datos.

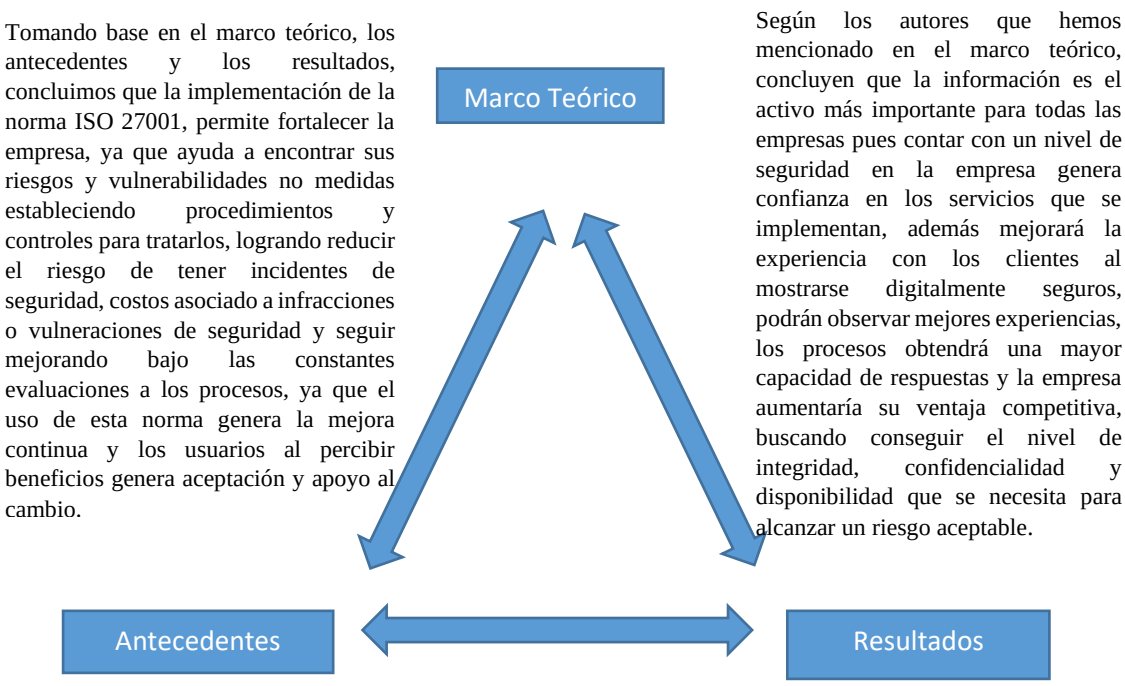

Figura 4. Triangulación de antecedentes, marco teórico y los resultados.

De acuerdo a lo desarrollado y tomando base en el marco teórico, los antecedentes y los resultados, concluimos que la implementación de la norma ISO 27001, permite fortalecer la empresa, ya que ayuda a encontrar sus riesgos y vulnerabilidades no medidas estableciendo procedimientos y controles para tratarlos, logrando reducir el riesgo de tener incidentes de seguridad, costos asociado a infracciones o vulneraciones de seguridad y seguir mejorando bajo las constantes evaluaciones a los procesos, ya que el uso de esta norma genera la mejora continua y los usuarios al percibir beneficios genera aceptación y apoyo al cambio.

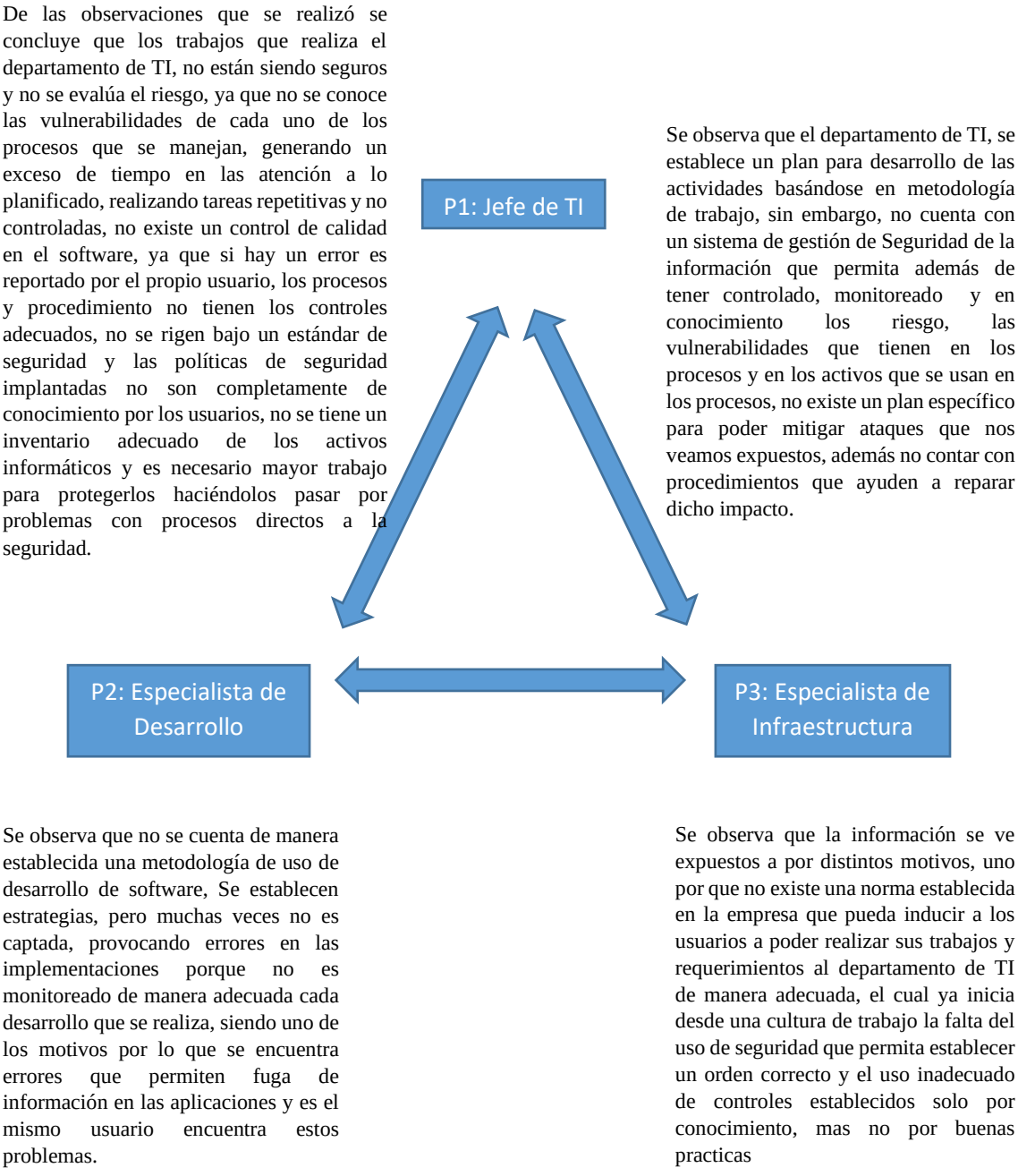

Figura 5. Triangulación de observación de la unidad de estudio

En esta triangulación de observación que se ha realizado los trabajadores que en la actualidad laboran y en la empresa esvicsac en el departamento de Tecnología de Información, han sido los participantes y el objeto del estudio por conocimiento y especialización en las áreas que administran, son los especialistas quienes se hacen

referencia como P1: Jefe del TI, encargado de gestionar el departamento a través de elaboraciones, propuestas y seguimiento a las normativas y políticas en tecnología de información, además de planificar y coordinar las áreas de desarrollo e infraestructura. P2: Especialista de desarrollo, encargado de analizar, desarrollar, coordinar y tener a cargo a los desarrolladores que implementan los sistemas de información de la empresa P3: Especialista de infraestructura, encargado de hacer y estables las políticas y normas de seguridad informática en la empresa.

De las observaciones que se realizó se concluye que los trabajos que realiza el departamento de TI, no están siendo seguros y no se evalúa el riesgo, ya que no se conoce las vulnerabilidades de cada uno de los procesos que se manejan, generando un exceso de tiempo en las atención a lo planificado, realizando tareas repetitivas y no controladas, no existe un control de calidad en el software, ya que si hay un error es reportado por el propio usuario, los procesos y procedimiento no tienen los controles adecuados, no se rigen bajo un estándar de seguridad y las políticas de seguridad implantadas no son completamente de conocimiento por los usuarios, no se tiene un inventario adecuado de los activos informáticos y es necesario mayor trabajo para protegerlos haciéndolos pasar por problemas con procesos directos a la seguridad.

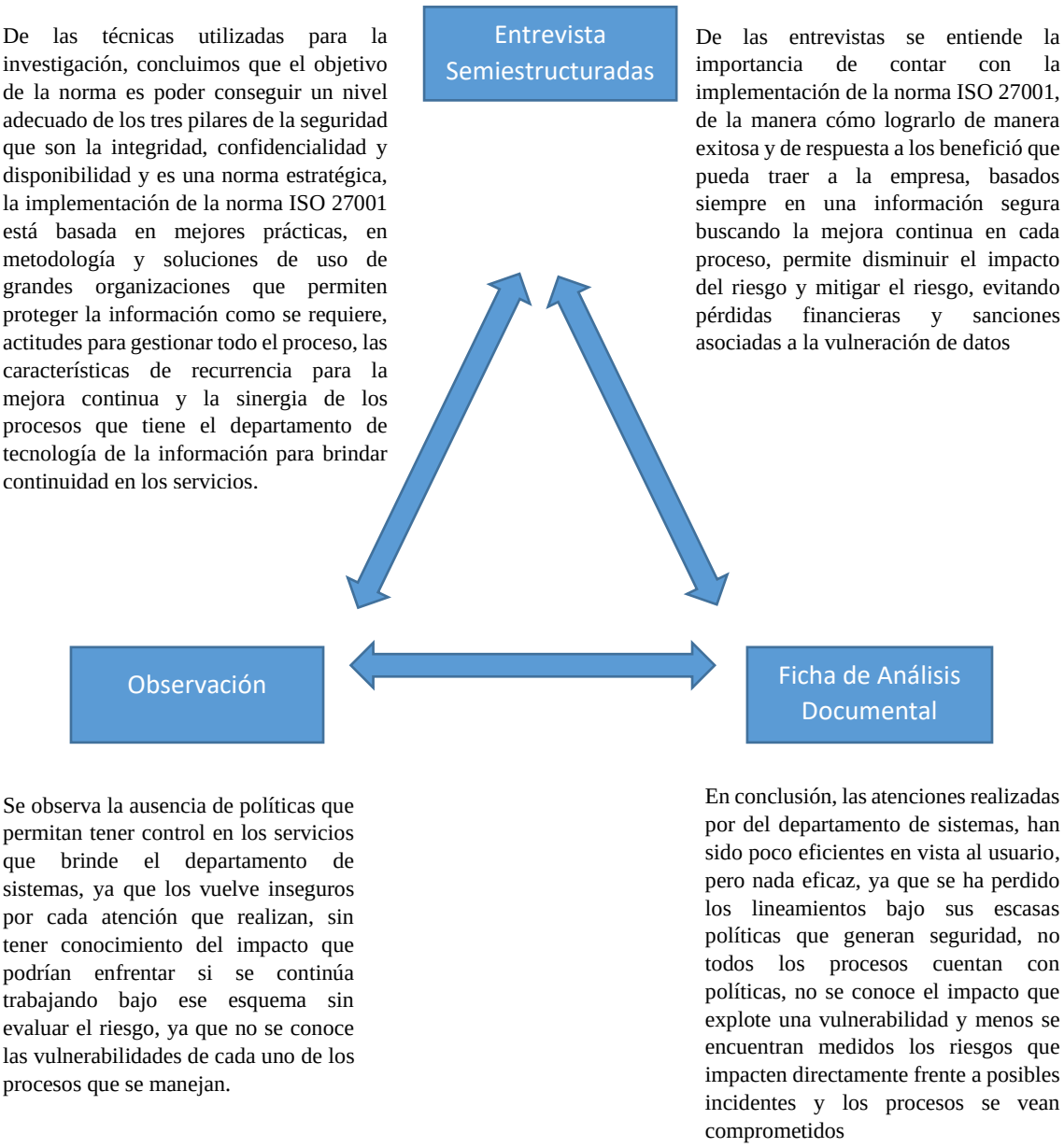

Figura 6. Triangulación de las técnicas utilizadas.

En esta triangulación realizada entre las técnicas usadas, se puede concluir lo importante que resulta tener un SGSI basado en la norma ISO 27001, por lo que el objetivo de la norma es poder conseguir un nivel adecuado de los tres pilares de la seguridad que son: la integridad, confidencialidad y disponibilidad. La norma se estratégica, ya que los altos cargos son los que forman parte de la directiva para su implementación, ofreciendo una visión estratégica de los activos de información que se maneja y las medidas de seguridad

que se debe de contar, la norma ISO 27001 está basada en mejores prácticas, en metodología y soluciones de uso de grandes organizaciones que permiten proteger la información como se requiere, gracias a los datos recogidos, generando mejores actitudes para gestionar todo el proceso, pues ayudará a tomar decisiones, ya que se conocerá todos los riesgos que tiene la organización las características de recurrencia para la mejora continua y la sinergia de los procesos que tiene el departamento de tecnología de la información para brindar continuidad en los servicios y protegerlas por más mínima que sea la información.

IV. DISCUSIÓN

Para la investigación se ha realizado la comparación de los resultados obtenidos mediante las técnicas usadas, por lo que se analiza con las documentaciones que se usó para soportar la investigación, como tesis, artículos, libros, Siendo el objetivo principal describir la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, que mejorará la seguridad de la información, ya que según los entrevistados, mencionan la importancia de poder contar con una norma que ayude a mejorar la seguridad y pueda hacer comprender lo importante que es basarse en el apoyo de la norma ISO 27001, pues ayudará de manera integral a contar con una estructura segura, siendo de beneficio para la empresa, ya que su objetivo principal es proteger la disponibilidad, confidencialidad e integridad ya que se encuentra apoyada con la gestión de riesgos por lo que permitirá ubicarlos y tratarlos.

Los entrevistados coincidieron en que la ISO 27001, ayuda a administrar la información de la empresa de una manera segura basado en un SGSI, que permitirá disminuir el impacto del riesgo y mitigarlo, evitando pérdidas financieras y sanciones asociadas a la vulneración de datos, sino también traerá beneficios a la empresa, ya que es posible ofrecer nuevos negocios y fidelizar a los clientes, que también protegerá y mejorará la reputación de la organización, además de poder cumplir con requisitos comerciales, legales y reglamentarios, por lo que podrá de manera efectiva mejorar procesos de trabajo de la institución, ya que ISO 27001 no es solo antivirus o sistemas que use la institución para poder proteger la información, sino que también influye en los procesos y su gestión,

Henttinen (2018), realizó un estudio en análisis de brechas para mejorar la seguridad, por lo que se tomó como referencia para ayudar a evaluar los riesgos y además brinda un alcance de cómo es el comportamiento de una empresa extranjera y con altos índices de normas certificaciones de seguridad y calidad, existen fuga de información y muestra estrategias para mitigar el riesgo. Trabajar con una metodología y con una norma implementada, ayuda a poder gestionar y optimizar de manera adecuada los recursos, teniendo un orden que permita saber qué plan de acción tomar frente a los distintos escenarios y de acuerdo al negocio. Coaguila (2020), de la misma manera implementa un diseño para implementar un SGSI, obteniendo como resultados una implementación basada en la norma ISO 27001, promoviendo el análisis de riesgo a medida exhaustiva.

Las ventajas de implementar la ISO 27001, es que los procesos sean seguros, equilibrados y estén comunicados entre sí, logrando reducir los riesgos con nuevas metodologías que mitiguen el riesgo y aumente la seguridad, además de poder contar con un plan de acción eficaz frente a posibles riesgos y pueda ser controlado y en caso que vea actividades sospechosas puedan ser alertados, además asegura el cumplimiento legal exigidos por las entidades de control, por lo que ayuda a que se reduzcan los costos por la eficiencia que genera en que pueda suceder incidentes por falta de seguridad, además provocará mayor confianza con los clientes que se sientan protegidos, proveedores y todos los usuarios de la entidad, contribuyendo a mejorar la imagen corporativa.

Para implementar la norma ISO 27001 es necesario poder trabajar en función de las fases por lo que se establece la metodología PDCA (Plan, Do, Check,Act), que en español viene hacer planificar, hacer, revisar y actuar, (Figura 7) el cual nos brinda el uso de la mejora continua para la implementación, la primera fase se basa en la planificación, por lo que se observa el capítulo 4 contexto de la organización, capítulo 5 liderazgo, capítulo 6 planificación y el capítulo 7 soporte (Figura 8). Por lo que ayudará a definir una política de seguridad, se determinará el alcance del SGSI, se procederá a evaluar los riesgos, para esto se debe responder a las medidas de control que brinda la norma de la ISO que permite auditar el riesgo bajo 133 puntos (Anexo 8), también es necesario conocer el inventario de activo, que ayudará a medir.

Restrepo (2019) en su investigación describe el comportamiento de los participantes mediante entrevistas para entender el alcance y los objetivos para la mejora del SGSI basándose en la norma ISO 27001, por lo que el uso podrá ordenar y mejorar los procedimientos y obtener un nivel de riesgo aceptable, Seclen (2016) en su investigación revisó los factores que sufrió las implementaciones y nos ayuda a poder tener en cuenta en la implementación, ya que el análisis conlleva a poder hacer un uso adecuado y basarse en la metodología PDCA.

Los entrevistaron coincidieron en que es necesario poder determinar una guía que apoye la gestión de la planificación, por lo que se hace presente la guía pmbok, el cual nos brinda las acciones necesarias para la elaboración de la planificación de manera adecuada del proyecto, permitiendo un mayor control de los riesgos, por lo que mejorará la calidad, aumentando la eficiencia de la planificación. Realizando un diagrama de Gantt, nos ayudará a orientar y organizar el uso adecuado de los recursos, definiendo las tareas y actividades

necesarias que se realizará en todo el transcurso de la implementación, estableciendo los tiempos realistas. Caballero (2017), en su investigación, demuestra la eficiencia del uso del pmbok para demostrar el correcto control de los procesos bajo esta guía de trabajo, ya que demuestra claramente las obligaciones que se maneja para establecer los procesos que se necesitan para implementar en cada una de las etapas del proyecto.

El análisis de riesgo es la acción clave que determinará los controles que se deben de implementar y las acciones que se deben de considerar, analizando el impacto que puede causar al negocio mediante una ausencia de seguridad, ya que mide de manera realista la probabilidad de que pueda ocurrir fallos por una amenaza, vulnerabilidad o impacto con los activos de información, por lo que es útil este proceso para comparar los resultados, por lo que su desarrollo es uno de los más duraderos (Figura 9), en concordancia con los entrevistados argumentan que un correcto análisis de riesgo podrá tener los mejores resultados en la implementación, ya que se sabrá identificar los controles a usar e implementar un correcto SGSI, por lo que dará resultados del tipo de criticidad como un riesgo aceptable o residual.

Como Morales (2019), realizó un análisis exhaustivo del completo análisis de riesgo para implementar un Balanced Scorecard que mide el riesgo y lo califica para poder crear y establecer lineamientos y criterios para tratar el riesgo en los procesos. Un riesgo aceptable no hay necesidad de eliminarlo, porque llegaría a ser costoso y muchas veces no es posible, además la práctica de revisar este resultado muchas veces no conlleva un nivel perjudicial para la empresa tanto económico, de asistencia logística o de visión de imagen institucional, por lo que la evaluación podrá definir mayor asertividad en el resultado. El riesgo residual, es subsistente ya que después de la implementación realizada medido con los controles definidos y elaborado completamente el SGSI en el proceso, pasa a ser un reflejo de que posiblemente pueda ocurrir, pese a haberse reducido el riesgo inherente.

En la segunda fase llega la etapa de la implementación por lo que el departamento de TI de la empresa esvicsac reconoce el funcionamiento eficiente, efectivo y estratégico de esta norma para aguardar la seguridad de su información, y lo aterriza en la implantación del plan de tratamiento del riesgo, donde se deberá fijar las políticas de control de acuerdo al negocio de la institución, donde se describirá los objetivos de la seguridad, los compromisos a cumplir y el compromiso de la mejora continua, en la documentación se plasmará el objetivo del correcto uso de los activos informáticos, de que todo el personal deba saber la

responsabilidad de sus tareas para el cuidado, así como brindar el alcance la cual es aplicada para todo el personal y normado para el control del cumplimiento y del no cumplimiento.

Los entrevistados coincidieron en que la implementación consiste en poner en marcha lo planificado, respetando los tiempos por tareas organizadas y los recursos establecidos, bajo el personal responsable. Fijando las políticas necesarias que permiten tener los resultados esperados, además es necesario redactar dos entregables para la guía y gestión del uso que vienen hacer el manual de procedimientos, el documento que pone en función los nuevos procedimientos y su uso y el manual de riesgo, por lo que es necesario estudiar de manera detallada los requisitos y las políticas, los resultados de la evaluación de riesgos determinará el contenido de los documentos, y la clasificación de los resultados.

Seclen (2016), investigó cuales son los factores que principales para que una implementación fracase y una de las más comunes también fueron la parte de la implementación, ya que muchas veces las políticas no son diseñadas de manera exacta generando una carga al usuario más que un apoyo. Por lo definir tanta documentación con demasiada información o repetitiva, por lo que llevaría al fracaso, ya que no será entendida y el lector no querrá usar la lectura en ello, es mejor tener documentos optimizados y haciendo referencia a las mismas, los documentos deben contener una estructura la cual necesita la aprobación de los procedimientos y la distribución. Es importante la capacitación que se tendrá que brindar a los empleados que ayudará a concientización de las nuevas normas y políticas o procedimientos definidos.

Laura (2017), desarrollo en su investigación propuesta de implementación, el cual permite poder realizar una gestión adecuada, para lo cual genera los controles necesarios lo que se basa mucho en el análisis de riesgo que fueron identificados en la primea tapa y la correcta implantación, desarrollando como entregables el manual de seguridad y manual de procedimiento debidamente diseñados para la institución y enfocado a la organización. El manual de seguridad debe ser clara y coherente, por lo que los dueños del proceso deben formar parte del diseño para comprometer el cumplimiento de la implantación. El manual de procedimientos, es para definir el paso a paso del proceso definiendo las acciones correctas preventivas y oportunas para prevenir de manera oportuna cualquier incidente visible y no visible, por lo que es de necesidad que el área dueño del proceso tenga el correcto conocimiento y pueda definir alcances que permita ser evaluado para corregir los

procedimientos antes que se lleve a cabo con el fin de resguardar la seguridad de la información y promover la mejora continua de los procesos.

Como en toda implementación y proponiendo en la mejora continua, es necesario esta etapa para dar continuidad a la etapa de actuar, ya que es necesidad de auditar la implementación para analizar y describir la eficiencia y eficacia de la implementación, esta etapa es llamada verificar, por lo que se demuestra de importancia poder realizarlo, se llegó a la conclusión en las entrevista que es importante la verificación, ya que es necesario poder de establecer los controles para asegurar, tratar y minimizar el impacto, ayudará a estar preparados para las auditorias que se realicen ya que se puede en esta fase identificar y corregir los procedimientos antes de que se lleve a cabo.

Es importante y se deberá de verificar regularmente la efectividad de la implementación, el cual permitirá poder validar de manera adecuada y correctamente las actividades destinadas a cada proceso, por lo que se deberá de realizar auditoría interna que permita comprobar que se cumpla los requisitos y procedimientos en los procesos planteados en el caso que se dé, poder comunicar a las partes interesadas para proponer una solución y mejorar el proceso. Es necesario poder evaluar a las personas específicas y que se encuentren autorizadas, además es necesario poder difundir el conocimiento al personal nuevo que ingrese a formar parte del área y conlleve ser parte de los procedimientos, brindando las facilidades para aclarar las dudas, dando como beneficio que el proceso sea eficiente y eficaz.

Crespo (2018), en su investigación analizó los activos de información de manera adecuada y para él fue su actividad más importante para poder realizar una correcta implementación y parte fundamental a la hora de la verificación, ya que demuestra la integración de su implementación contemplando todos los activos de información en sus procesos, por lo que la evaluación utiliza piezas importante como los activos, el cual le permitió poder mejorar los procesos de su entidad, cuando Changoluisa (2017) usa la norma ISO 27001, lo utiliza para optimizar procesos y es una de las acciones más evaluadas, dentro de la actividad de auditar, ya que la importancia de un proceso no es serlo cargada, sin embargo, es de necesidad que deberá de contar con la respectiva seguridad requerida.

De la misma manera Niño (2018), demostró el fortalecimiento de la implementación asegurando en este proceso una medición realizada por un adecuado monitoreo que permite verificar a través de un checklist, el cual permitirá la correcta toma de información actual y

podrá medir la importancia de cada proceso, el analizar es la herramienta más usada por lo que demuestra la manara de medir el grado de madures y el comportamiento que lleva la implementación y como es el avance continuo, por lo que ayuda a evidenciar y se propone un tratamiento para mitigar el daño realizado.

La auditoría interna tiene como objetivo poder identificar, las carencias o actividades ausentes en el sistema de implementación, ya que se debe dar que la implementación realizada cumple con las normas legales del reglamento de requisitos de la norma y conocer que la norma a cumplidos con los requisitos de seguridad definidos de manera correcta, ya que en caso de una no conformidad se podrá corregir antes de que se lleve a cabo, ya que una correcta auditoria identificará las oportunidades de mejora y las auditorias habituales proporciona madurez a la implementación. Por lo que se debe de considerar un auditor interno con buenos conocimientos de los procesos y los requisitos de la ISO 27001.

Flores (2017), a través de su investigación realizó un estudio para la implantación de la norma, enfocando la necesidad del apoyo y en la supervisión y control de la evaluación identificando que esta tarea es importante para generar la mejora continua del SGSI, que permitirá poder contener los controles necesarios para la correcta evaluación. Por lo que en una auditoria es necesario definir de manera adecuada los criterios y el alcance por lo que cada proceso debe ser evaluado de manera individual con todos lo que conforman el proceso, estas auditorias deberá de realizarse de manera objetiva y debe contener evidencia para proceder con la siguiente fase.

En esta Fase de actuar, los especialistas encuestados llegan a la conclusión de que como pone en marcha la mejora continua, en lo que se estable las acciones correctivas que permiten la mejora de la implementación, ya que es necesario poder dar la conformidad a una implementación culminada el cual debe de cumplir con el alcance debido mitigando vulnerabilidades y reduciendo los riesgos, por lo que en esta fase se da el ciclo de mejora continua atendiendo y rectificando las no conformidades, la cuales son reconocidas por no cumplir o tener el comportamiento de los procesos internos de la organización, por lo general es causa de una implementación no realizada correctamente, no cumple o cumple parcialmente los requisitos legales, es revelado conductas que infringen los procedimientos y políticas definidas en la planificación, procesos que no muestren resultados que se esperen, por lo que después de poder analizar la causa de la no conformidad, se establece la causa

raíz, se establece la acción correctiva y se verifica la eficacia de la acción correctiva generando.

Cueva, mercado (2017), en su investigación implementan basándose en la ISO 27001 la verificación de los cumplimientos para su sistema de gestión el cual le brindarían la acción de poder mejorar los procesos de su SGSI, logrando mejorar sus controles y dando mayor robustez a sus procesos y procedimientos que permiten resguardar la información de su entidad. Toda implementación requiere de una mejora continua, toda implementación necesita conocer para madurar, el cual permite que la implementación se segura, sin embargo es un proceso que se realiza mediante el aprendizaje del SGSI y de los nuevos procesos que se involucren y de los nuevos activos que formen parte de los procesos y los procedimiento que se usen y así crece poco a poco provocando un mejor SGSI provocando un mayor beneficio para la empresa y se podrá definir una sistema más seguro.

V. CONCLUSIONES

Primera:

Del objetivo general, se describe que la implementación de norma ISO 27001 en el departamento de TI de la empresa esvicsac, mejorará eficientemente los procesos actuales y reducirá el riesgo de la información ayudando a cumplir con los tres pilares de la seguridad como la confidencialidad, disponibilidad e integridad, brindando continuidad de los servicios y mejorando las experiencias con los clientes y con el apoyo de los miembros de la alta dirección la implementación tendrá un peso crucial, para el uso y cumplimiento de la norma.

Segunda:

Del primer objetivo específico se describe que la planificación de la norma ISO 27001, se debe establecer el Sistema de Gestión de Seguridad de Información bajo la guía de fundamentos del pmbok y definir el alcance, que servirá para instaurar correctamente los recursos asociados a la implementación, analizando los riesgos para determinar los controles a aplicar, las acciones y tratamientos que se realizará para demostrar la utilidad del SGSI y no carga laboral para el usuario.

Tercera:

Del segundo objetivo específico se describe la implementación de la norma ISO 27001, fijando políticas que permitan establecer los lineamientos fundamentales de amanera adecuada y medida a la institución, además se determinará el manual de seguridad que establezca las medidas de seguridad, asegurando el cumplimiento de las garantías de confidencialidad, disponibilidad e integridad, también el manual de procedimientos que será una guía para indicar los procedimientos paso a paso del desarrollo de los procesos y las acciones a tomar en caso suceda un incidente.

Cuarto:

Del tercer objetivo específico se determina la verificación de la implementación de la norma ISO 27001, mediante la auditoría interna que permitirá comprobar que el SGSI que se ha implementado de manera correcta y cumpla con la norma, identificando las oportunidades de mejora, antes que suceda.

Quinto:

Del cuarto objetivo específico se determina la manera de actuar para realizar las acciones correctivas de las no conformidades identificando, analizando y eliminando las cosas reales, para la eficacia de la implementación buscando la mejora continua.

VI. RECOMENDACIONES

Primero:

Se recomienda a los miembros de la alta dirección ejecutar el proceso de la implementación, y de formar parte del comité de seguridad para el despliegue, obteniendo el respaldo y patrocinio que esta implementación requiere, aumentando los beneficios a la hora de centrar los objetivos de la organización que se requiere.

Segundo:

Se recomienda al especialista de planificación considerar y planificar correctamente los recursos y realizar el análisis de brechas que permita conocer de manera correcta el desempeño actual y lo que se necesita en la organización, para definir el alcance de la implementación.

Tercero:

Se recomienda al Gerente de TI, implantará los cambios en todos los sistemas y procesos manuales que intervienen, y delegará la revisión del inventario de los activos, para lograr los objetivos planificados, por lo que se debe de considerar los controles para identificar las métricas e indicadores de seguridad.

Cuarto:

Se recomienda al auditor interno medir el desempeño del SGSI, para demostrar que la implementación haya sido de manera correcta y acorde a las necesidades de la institución, además de almacenar un histórico de soluciones, permitiendo adoptar una base de conocimientos, para analizar y diseñar soluciones al tamaño y complejidad de las no conformidades de los procesos.

Quinto:

Se recomienda a todos los jefes de las áreas involucradas en el proceso para ser parte principal en las revisiones y las acciones correctivas dando la conformidad para mejorar el proceso.

REFERENCIAS

AT&T Cybersecurity Insights (2017). Protect your data through innovation, The CEO's Guide to Data Security, Volume 5, (pp. 1-20), recuperado a partir de https://www.business.att.com/cybersecurity/docs/vol5-datasecurity.pdf.

Barragán Quizhpe, C. F. (2017). Adaptación de las normas ISO 27001 e HIPPA para la reducción de riesgos en la seguridad en hospitales nivel I del IESS. (Tesis de maestría, Escuela Superior Politécnica de Chimborazo).

Bell, J. (2005). *Cómo hacer tu primer trabajo de investigación*. (Roc Filella Escolá, trad.). Gedisa.

Bertolín, J. A. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Editorial Paraninfo.

Caballero Macavilca, D. J. (2017). Implantación de la Oficina de Gestión de Proyectos PMO de TI en una empresa de Telecomunicaciones bajo el enfoque metodológico PMI–PMBOK.

Cardona Londoño, A., & Carvajal Portilla, D. L. (2018). Diseño del sistema de gestión de seguridad de la información basado en la familia de normas de la serie ISO/IEC 27000 para una entidad pública colombiana.

Carlino, P. (2004). Diario de tesis y revisión entre pares: análisis de un ciclo de investigación-acción en talleres de tesis de posgrado. In Jornadas Latinoamericanas de Investigación y Práctica en Psicología Educacional. Facultad de Psicología de la Universidad de Buenos Aires.

Changoluisa Criollo, W. F. (2017). Optimización del proceso de alta y baja de usuarios a través de la implementación de gestión de seguridad de la información, basado en la norma ISO 27001: 2013 en una empresa de consultoría para la industria petrolera (Bachelor's thesis, Pontificia Universidad Católica del Ecuador-Facultad de ciencias administrativas y contables).

Chilán-Santana, E. I., & Pionce-Pico, W. F. (2017). *Apuntes teóricos introductorios sobre la seguridad de la información*. Dominio de las Ciencias, 3(4), 284-295.

Coaguila Mamani, M. E. (2020). Diseño de un plan de gestión de seguridad de información alineado a la norma ISO/IEC 27001: Caso Universidad Nacional de Moquegua. (Tesis de maestría, Universidad Nacional de Moquegua).

Cornella, A., & Vega, A. M. (1995). *Los recursos de información. Ventaja competitiva de las empresas.* Revista Española de Documentación Científica, 18(1), 113.

Crespo Chávez, N. J. (2018). La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior (Bachelor's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Maestría en Gestión de Bases de Datos).

Cueva Araujo, P. O., & Ríos Mercado, J. A. (2018). Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca-ESSALUD bajo la NTP-ISO/IEC 27001: 2014. (Tesis de maestría, Universidad Privada del Norte).

Diéguez, M., & Cares, C. (2019). *Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información.* RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, (32), 113-128.

Espinoza, W.(2016). *La tecnología de la información como herramienta construccionista para el auditor financiero hibrido*. Fitdes Et Ratio, 11, 17-35

Fernández, D. A. A., & Casas, X. C. (2017). *Auditoría informática: un enfoque efectivo*. Dominio de las Ciencias, 3(3), 157-173.

Flores Solís, F. R., & Guerra Farfán, J. A. (2017). Relación de la NTP ISO/IEC 27001: 2008 EDI y la seguridad de la información en los Ministerios del Estado Peruano al 2015. (Tesis de maestría, Universidad Nacional del Callao).

García León, E. A. (2019). Diseño e implementación del modelo de gestión en los procesos de servicios de la Municipalidad Provincial de Trujillo.

Gutiérrez, G. V. R., Jaime, J. A. B., & González, I. A. D. (2018). *Gestión de seguridad de la información en las organizaciones*. Investigación e Innovación, 111.

Henttinen, H. (2018). Improvement of Information Security Management System in Media X Corporation. (Master ‘s Thesis, JAMK University of Applied Sciences.

Hernández-Sampieri, R., & Torres, C. P. M. (2018). *Metodología de la investigación* (Vol. 4). México eD. F DF: McGraw-Hill Interamericana.

Jaramillo, C., Jácome, L., Ordóñez, Á., Gaona, M., Carrión, J., & Palma, M. (2017). *Auditoría de gestión de seguridad informática, en entidades públicas y privadas en Loja*. Maskana, 8, 149-162.

Laura Zurita, N. A. (2017). Propuesta de Diseño, implantación e Implementación de un Sistema de Gestión de Seguridad de la Información para Entidades Gubernamentales de Bolivia Basado en la Norma NB/ISO/IEC-27001; 2013 (Doctoral dissertation,

Universidad Mayor de San Andrés. Facultad de Ciencias Económicas. Carrera de Contaduría Pública. Instituto de Investigaciones en Ciencias contables, Financieras y Auditoria. Unidad de Postgrado.

López, P. A. (2010). *Seguridad informática*. España: Editex.

Macancela Macero, D. P. (2016). Modelo de gestión de la seguridad informática para garantizar la continuidad del negocio en la Cacpe Pastaza. (Master's thesis, Universidad Regional Autónoma de los Andes).

Maddu, C. S. (2018). Project implementation of Information Security Management System in Wilmington Pharmaceuticals (Doctoral dissertation, Instytut Organizacji Systemów Produkcyjnych).

Mazorra Olmedo, E. R. (2019). Metodología para la implementación de un sistema de gestión de seguridad de la información iso/iec 27001: para soporte de áreas de admisión y atención de un hospital público (Master's thesis, Universidad Espíritu Santo).

Mendez Rosemary y Sandobal Franco (2011). *Investigación. Fundamentos y metodología 2da Edición*. Editorial Pearson Educación de Mexico.

Morales Alomoto, L. R. (2019). Balanced ScoreCard para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito (Master's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Maestría en Sistemas de información).

Morante, N., & Rogger, N. (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 de maestría, Universidad Nacional Pedro Ruiz Gallo).

Niño Benitez, Y., & Silega Martínez, N. (2018). *Requisitos de Seguridad para aplicaciones web*. Revista Cubana de Ciencias Informáticas, 12, 205-221.

Restrepo Marin, S. (2019). Sistema de gestión integral de seguridad informática en servicios web de e-learning y telefonía IP en Grupo Nethexa SAS. (Master's thesis), Universidad Pontificia Bolivariana, Escuela de Ingenierías)

Rivas Plata Arredondo, Z. M. (2018). Diseño de un sistema de gestión de la seguridad de la información de acuerdo a la norma ISO/IEC 27001: 2013. Caso de estudio:

Oficina de informática de la sede descentralizada de una entidad pública. (Tesis de maestría, Universidad Nacional de San Agustín de Arequipa).

Rivera-Guerrero, C. B., Felipe-Redondo, A. M., & Nuñez-Cárdenas, F. J. (2019). *Esquema de ISO 27001 Sistema de Gestión de la Seguridad de la Información*. Ciencia Huasteca Boletín Científico de la Escuela Superior de Huejutla, 7(13), 28-29.

Samaniego Zanabria, A. L. (2018). Evaluación de Algoritmos Criptográficos para mejorar la Seguridad en la Comunicación y Almacenamiento de la Información. (Tesis de Maestría, Universidad Ricardo Palma).

Seclén Arana, J. A. (2016). Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001. (Tesis de Maestría, Universidad Nacional Mayor de San Marcos).

Sena, L., & Tenzer, S. M. (2004). *Introducción a Riesgo informático.* Cátedra Introducción a la Computación. Universidad de la República, Facultad de Ciencias Económicas y de Administración.

Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001*. Revista Tecnológica-ESPOL, 28(5).

Vallejo, M. R. L. (2017). *Hacking ético. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas.* Revista Publicando, 4(10 (1)), 31-51.

Yupanqui, J. R. A., & Oré, S. B. (2017). *Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento*. RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, (25), 112-134.

Zambrano, S. M. Q., & Valencia, D. G. M. (2017). *Seguridad en informática: consideraciones*. Dominio de las Ciencias, 3(3), 676-688.

ANEXOS

Anexo 1: Matriz de Categorización

Título: Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información en la empresa Esvicsac, Callao.
Nombre: Edwin Samuel Arias Quispe.

Problema General	**Objetivo General**	**Categoría**	**Subcategoría**	**Técnicas**	**Instrumentos**
¿Cómo la implementación la norma ISO 27001 en el departamento de Tecnología de Información de la empresa Esvicsac, Callao, mejorará la seguridad de la información?	Describir la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao, que mejorará la seguridad de la información.	Planificar	• Establecer SGSI. • Analizar riesgos.	Entrevista a profundidad	Guía de entrevista
Problemas Específico	**Objetivo Específico**				
• ¿Cómo planificar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	• Describir la planificación para implementar la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac. Callao.	Implementar	• Fijar Políticas. • Determinar manual de seguridad. • Determinar manual de procedimientos.	Observación	Guía de observación
• ¿Cómo ejecutar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	• Describir la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao.				
• ¿Cómo verificar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	• Determinar la verificación de la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao.	Verificar	• Auditoría interna.	Análisis documental	Ficha de análisis documental
• ¿Cómo actuar en la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	• Determinar la actuación para mejorar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao.	Actuar	• Realizar acciones correctivas.		

Fuente: ISO 27001

Anexo 2:

Instrumento de recolección de datos

Guía de entrevista

"Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información en la empresa Esvicsac, Callao"

1. ¿Cómo la implementación la norma ISO 27001 en el departamento de Tecnología de Información de la empresa Esvicsac, Callao, mejorará la seguridad de la información?

2. ¿Cómo planificar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?
    a. ¿Cómo establecer el SGSI para implementar la norma ISO 27001?
    b. ¿Cómo analizar los riesgos para implementar la norma ISO2001?

3. ¿En qué consiste la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?
    a. ¿Cuál es el objetivo de fijar las políticas de seguridad para implementar la norma ISO 27001?
    b. ¿Cómo se determina el manual de seguridad en la implementación de la norma ISO 27001?
    c. ¿Cómo se determina el manual procedimientos para la implementación de la norma ISO 27001?

4. ¿Cuál es la importancia de verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?

5. ¿Cómo verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?
    a. ¿Cómo auditar la implementación de la norma ISO 27001?

6. ¿Cómo se actúa en la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?
    a. ¿Cómo se debe realizar las acciones correctivas en la norma ISO 27001?

Anexo 3:

Matriz de desgravación de la entrevista

N°	Preguntas	Entrevistado 1 – Jefe del Departamento de TI
1	¿Cómo la implementación de la norma ISO 27001 en el departamento de Tecnología de Información de la empresa Esvicsac, Callao, mejorará la gestión del sistema de seguridad de la información?	La norma ISO 27001, es una solución de mejora continua, en la que se puede basar un sistema de gestión de seguridad de la información, que permita asegurar la confidencialidad, integridad y disponibilidad de la información de la empresa, permitiendo evaluar todo tipo de riesgos y amenazas. Por lo que su uso, ayudará a la empresa tener un mayor control y administración de sus vulnerabilidades que adolece y reducir el riesgo de la perdida de información, ya que su implementación no solo protege contra riegos lógicos y previsibles, sino que también evalúa los riesgos físicos que puede comprometer la seguridad de la información de los datos informáticos y el software, garantizando la continuidad del negocio.
2	¿Cómo planificar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	La planificación debe de consistir en identificar y analizar de que la idea principal del proyecto pase a una fase posterior cumpliendo con los objetivos que se necesite analizar, y así reducir los riesgos sobre la implementación, por lo que me enfoco al uso del pmbok, que permite determinar el alcance, el tiempo y el costo, siendo necesarios para planificar con atención las actividades de seguridad de manera adecuada, así como establecer los objetivos de seguridad de la información eligiendo controles correctos. Para establecer el SGSI, es necesario poder realizar un estudio de la empresa desde el punto de vista de seguridad, que permita determinar el alcance, redactar una política. Se sabe que no toda la información que se maneja en la empresa tiene el mismo valor o tienen los mismos riesgos, para analizar el riesgo, se debe de valorar los activos de información identificando los procesos de negocios más críticos, clasificar las amenazas, estimar las vulnerabilidades y de los resultados de la valoración de alto, medio o bajo, considerar los tipos de respuestas.
3	¿En qué consiste la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	En esta etapa del ciclo, se genera la documentación necesaria e identifica los controles para implementar de manera adecuada el SGSI que fueron identificados en la etapa de la planificación mediante los resultados del análisis de riesgo, por lo que se deberá establecer los roles y las responsabilidades de las tareas. El principal objetivo de fijar las políticas es poder indicar el propósito del SGSI, de cómo conseguir el resultado esperado, como ha sido aprobado, como realizar su seguimiento, ya que debe de revisarse de manera continua. El manual de procedimientos, consiste en establecer todos los controles que se va a implementar dentro de los procesos respecto a la seguridad de la información. Manual de seguridad consiste en identificar todo aquel riesgo que debes de tratar y hacerle seguimiento y minimizar tanto su probabilidad como su impacto.
4	¿Cuál es la importancia de verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	Es importante la verificación de la implementación, ya que es necesario poder medir los tiempos, lo errores generados, ya que, de los resultados obtenidos, se podrá tomar acciones para coordinar y a ayudar a la dirección de la empresa a determinar las actividades desarrolladas y las personas responsables de los procesos a mejorar para volver más eficiente y eficaz la implementación, por lo que se deberá detectar y prevenir reduciendo lo más mínimo posibles los incidentes de seguridad que han sido implantadas.
5	¿Cómo verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	Para verificar es necesario poder revisar regularmente la efectividad del SGSI implementado, mediante el uso de indicadores, que es la gestión del tiempo, la gestión de la calidad, que aterriza en el control de calidad de cada producto intermedio y la gestión de costos. Por lo que se debe determinar las acciones que fueron realizados para resolver un proceso, mediante auditorias, revisión de incidentes, medición de eficacia, y observaciones o sugerencias realizadas de las partes interesadas, por lo que permita satisfacer los requisitos especificados al iniciar la implementación. La auditoría debe ser comunicado a todas las partes interesadas, usando los canales de comunicación externos internos establecidos, debe definirse los objetivos, alcance, criterios de la auditoría.
6	¿Cómo actuar en la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	De los resultados obtenidos en la fase de verificación, se debe de estudiar los resultados, y confrontar con el funcionamiento de los procesos antes de implementar la mejora, acá se tomará la decisión si es que es satisfactoria deberá establecerse la mejora de forma definitiva, de lo contrario deberá de realizase los cambios para ajustar los resultados, es así que terminado este paso es necesario volver al paso uno para poder estudiar mejoras nuevas a implementar. Para realizar las acciones correctivas, se debe tener en cuenta los parámetros esperados, los comportamientos de los procedimientos y políticas, la eficiencia esperada, y la conformidad por la alta dirección.

N°	Preguntas	Entrevistado 2 – Especialista en desarrollo
1	¿Cómo la implementación de la norma ISO 27001 en el departamento de	Es importante para poder contar con un sistema de gestión de seguridad de la información adecuada para asegurar así la transparencia y que nuestros clientes puedan confiar mejor en nuestra organización. También involucra la conciencia de los usuarios para poder tener establecidos procedimientos seguros para garantizar la continuidad del negocio. Debe estar de

	Tecnología de Información de la empresa Esvicsac, Callao, mejorará la gestión del sistema de seguridad de la información?	la mano con la alta dirección quien será la cabeza necesaria para poder impulsar y dar la sinergia necesaria con los usuarios que son reacios al cambio. Por lo que una adecuada implementación de la ISO 27001, ayudará a mejorar los tres puntos esenciales en la seguridad, la confidencialidad, la integridad y la disponibilidad de la información.
2	¿Cómo planificar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	Un Sistema de Gestión de Seguridad de la Información comienza con su correcto diseño. Para ello deberemos definir cuatro aspectos fundamentales, el alcance del sistema, la Política de Seguridad a seguir, la organización de la seguridad y los programas de concienciación y formación del personal. Estos puntos tratados podrán asegurar el alcance, el tiempo y el costo de la implementación, por lo que se debe de contar con el apoyo y respaldo de la alta dirección. Por lo que es necesario el uso de metodologías que ayuden a la implementación, como PMP o pmbook. Para establecer el SGSI, es necesario conocer los procesos de la empresa, por lo que nos permitirá poder definir el alcance, el cual, se debe describir la extensión y los límites del SGSI, por lo que es el punto donde se definirá los elementos críticos que se deben de proteger teniendo en claro todo lo que es de interés para el sistema de gestión determinado por las actividades que se encuentren alineados con la misión de la empresa y mejore los objetivos de la empresa. Se debe analizar los riegos para evaluar las consecuencias y probabilidades de la implementación.
3	¿En qué consiste la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	La implementación del sistema consiste en definir las acciones, recursos responsabilidades y prioridades de los resultados que se obtuvo del análisis del riesgo, por lo que en esta fase se debe de alcanzar los objetivos de control identificados en la que se deben de estar incluidos los recursos, los responsables y las prioridades. Definir un control de métricas, bajo una metodología de trabajo como el pmbok que nos permita manejar y medir los recursos y poder comparar la eficacia de la implementación, es quien nos permitirá que el SGSI implementado se mantenga. El objetivo de fijar las políticas de seguridad es poder delimitar que se debe de proteger, cuáles son los límites aceptables, cuáles son los riesgos y cuál es la respuesta si sobrepasan, para conseguir el resultado esperado. El manual de seguridad es el documento que indica lo que debe hacer de forma general, señala las acciones como las operaciones que deben seguirse para llevar a cabo las funciones generales de la empresa, además, permite realizar un seguimiento adecuado y secuencial de las actividades anteriormente programadas en orden lógico y en un tiempo definido. El manual de procedimientos es una colección de procedimiento que detallan las acciones de a seguir en cada una de las situaciones, identificadas como eventos de riesgo, la cual se puede decir que es el actuar paso a paso.
4	¿Cuál es la importancia de verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	Es importante la verificación regularmente, ya que es necesario poder detectar a tiempo los errores posibles en el procesamiento de la información. Por lo que se debe de identificar los incidentes de seguridad y proponer la solución para mitigarlo, lo que es posible detectar y prevenir para reducir las ocurrencias de podrían poner en riesgo la seguridad, ya que necesario poder resolver grietas que has sido dejados en la implementación realizada, por lo que es necesario medir la eficacia del sistema de gestión.
5	¿Cómo verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	La verificación de la implementación debe ser realizada mediante un checklist establecido en el plan de auditoria el cual permite evaluar la eficacia de la implementación y la gestión realizada a los recursos que se dispuso para la implementación, atreves de auditorías internas el cual permita cumplir con la estructura de la norma ISO 27001. La implementación debe ser auditada para validar su eficacia de la implementación, para lo cual se debe de comprobar que el SGSI cumpla con los requisitos y proceso de la norma establecida atreves de una lista de verificación de los puntos a tratar, se debe identificar el no cumplimiento de los procedimientos establecidos para tomar las medidas correctivas que se requieran y la frecuencia con la que se debe de realizar para medir los resultados adecuados y efectivos, por lo que se debe revisar los problemas identificados y los riegos de la organización, por lo que se enfoca en evaluar los resultados
6	¿Cómo actuar en la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	En esta etapa es de necesidad establecer las acciones correctivas para las mejoras identificas en el SGSI, aplicar las acciones correctivas y preventivas de la seguridad, se debe de comunicar a los interesados sobre los resultados obtenidos en los procesos, asegurando que las mejoras puedan lograr sus objetivos. Es la fase para corregir el proceso en coso no se tenga los resultados esperados y puedan llegar a cumplir con el comportamiento deseado.

N°	Preguntas	Entrevistado 3 – Especialista de Infraestructura
1	¿Cómo la implementación de la norma ISO 27001 en el departamento de Tecnología de Información de la	La implementación de la ISO 27001, es importante porque formaliza la gestión de la seguridad, establece los objetivos de seguridad que pueda ser medibles bajo un criterio de mejora continua, además de brindar conciencia a la organización sobre la importancia de la seguridad y puede hacer cumplir los requisitos legales y la superveniencia frente a los errores y/o desastres, por lo que permitirá que se pueda detectar el origen de los riesgos para luego tratarlos de una manera sistemática, esto ayudará gradualmente a resolver todo tipo de situaciones críticas de los

	empresa Esvicsac, mejorará la gestión del sistema de seguridad de la información?	procesos de información que hasta el momento son inciertas, ya que no se tienen implementado un sistema de gestión de seguridad, siendo una herramienta de utilidad para mejorar la seguridad de la información en la empresa.
2	¿Cómo planificar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	En la fase de Planificación, Se trabajará bajo una metodología de gestión del proyecto que es posible hacer uso del pmbok, para poder administrar los recursos necesario para la implementación e iniciar con un estudio de la situación de la organización desde el punto de vista de la seguridad, para estimar las medidas que se van a implantar en función de las necesidades detectadas, como la mejora de procesos y los procesos que intervienen, los datos recogidos, el objetivo de mejora a los procesos, definiendo las políticas y los objetivos de seguridad, definiendo el alcance del SGSI y la elaboración del análisis de riesgo ya que no toda la información de la que disponemos tiene el mismo valor o está sometida a los mismos riesgos. Por ello, es importante realizar un Análisis de Riesgos que valore los activos de información y vulnerabilidades a las que están expuestas. Así mismo, es necesaria una Gestión de dichos riesgos para reducirlos en la medida de lo posible. Con el resultado obtenido en el Análisis y la Gestión de Riesgos estableceremos unos controles adecuados que nos permitan minimizar los riesgos.
3	¿En qué consiste la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	Consiste en la implementación del SGSI mediante la metodología de trabajo planteada, que es capaz de clasificar y priorizar la implementación gestionando el proyecto, además deberá de implementar los controles y administrar de manera eficiente, los recursos y los tiempos necesarios para trabajar en las distintas tareas propuestas planificadas de manera adecuada, siendo como su objetivo la continuidad del negocio, el control del sistema de acceso. El objetivo de fijar las políticas de seguridad es que pueda ser adaptable, debe ser basada basándose en la organización, por lo que debe ser aprobado y comunicado a todas las partes y siempre estar actualizados. El manual de seguridad debe ser clara y coherente para que elementos que conformen la política sean conocidas, acatadas y sea del cumplimiento de todos los usuarios bajo el liderazgo del área que lo implanta. El manual de procedimientos debe ser definida el paso a paso de cada proceso y la responsabilidad de cada departamento implicado en el SGSI, por lo que se debe de emitir las acciones correctas y preventivas oportunas en los casos que sean afectados.
4	¿Cuál es la importancia de verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	La verificación juega un papel muy importante en el aseguramiento y tratamiento de la información y los activos que lo soportan que permite establecer e identificar cuáles son los riesgos que como empresa está expuesto, así mismo permite establecer los controles necesarios para asegurar, tratar y minimizar el impacto (técnico, económico, reputacional) de que se explote una vulnerabilidad y concrete un evento de perdida, poder verificar la implementación ayudará a estar preparados para certificación permitiendo poder identificar y corregir los procedimientos antes de que se lleve a cabo.
5	¿Cómo verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	Para verificar se deben de realizar la auditoría interna, para poder medir la eficacia del SGSI por medios de los indicadores. Validando correctamente las actividades y propuestas revisadas en el proceso y validar el cumplimento de todos los objetivos. Para auditar la implementación, debe de comprobarse el SGSI cumpla con los requisitos de la norma, por lo que debe ser revisado el alcance del SGSI, las políticas, el manual de seguridad y el manual de procedimientos. Ya que el plan del tratamiento de riesgo debe estar documentado y debe ser aceptable a los principios de los sistemas seguros y a los procedimientos que se haya implementado para mejorar la gestión.
6	¿Cómo se actúa en la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	En esta fase es poner el plan la rectificación de las posibles no conformidades normativas de los procesos evaluados que fueron encontradas en la fase anterior, por lo que en esta fase se trabajará para garantizar que las acciones correctivas sean apropiadas, para evitar las no conformidades encontradas, por lo que trabajamos en la mejora continua. Las acciones correctivas deberán ser realizadas ante una no conformidad, debe evaluar la necesidad de acciones a eliminar la cuasa de la no conformidad, para evitar que vuelva a ocurrir, implantar nuevos procedimientos o acciones y hacer los cambios necesarios en los procesos y en el SGSI

Anexo 4:

Matriz de codificación de la entrevista

N°	Preguntas	Entrevistado 1 – Jefe del Departamento de TI	Entrevista 1 Codificada
1	¿Cómo la implementación de la norma ISO 27001 en el departamento de Tecnología de Información de la empresa Esvicsac, mejorará la gestión del sistema de seguridad de la información?	La norma ISO 27001, es una solución de mejora continua, en la que se puede basar un sistema de gestión de seguridad de la información, que permita asegurar la confidencialidad, integridad y disponibilidad de la información de la empresa, permitiendo evaluar todo tipo de riesgos y amenazas. Por lo que su uso, ayudará a la empresa tener un mayor control y administración de sus vulnerabilidades que adolece y reducir el riesgo de la perdida de información, ya que su implementación no solo protege contra riegos lógicos y previsibles, sino que también evalúa los riesgos físicos que puede comprometer la seguridad de la información de los datos informáticos y el software, garantizando la continuidad del negocio.	La norma ISO 27001, permitirá asegurar la confidencialidad, integridad y la disponibilidad de la información. Obteniendo un mayor control y administración de las vulnerabilidades que adolece, reduciendo el riesgo a perder información conociendo sus vulnerabilidades, el cual ayudará a superar sus vulnerabilidades previniendo de los riesgo físicos y lógicos para garantizar la continuidad del negocio.
2	¿Cómo planificar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	La planificación debe de consistir en identificar y analizar de que la idea principal del proyecto pase a una fase posterior cumpliendo con los objetivos que se necesite analizar, y así reducir los riesgos sobre la implementación, por lo que me enfoco al uso del pmbok, que permite determinar el alcance, el tiempo y el costo, siendo necesarios para planificar con atención las actividades de seguridad de manera adecuada, así como establecer los objetivos de seguridad de la información eligiendo controles correctos. Para establecer el SGSI, es necesario poder realizar un estudio de la empresa desde el punto de vista de seguridad, que permita determinar el alcance, redactar una política. Se sabe que no toda la información que se maneja en la empresa tiene el mismo valor o tienen los mismos riesgos, para analizar el riesgo, se debe de valorar los activos de información identificando los procesos de negocios más críticos, clasificar las amenazas, estimar las vulnerabilidades y de los resultados de la valoración de alto, medio o bajo, considerar los tipos de respuestas.	La planificación consiste en identificar y analizar la idea principal del proyecto reduciendo el riesgo de la implementación, por lo que es necesario el uso de una metodología para la gestión del proyecto, como el uso del pmbok, que permite guiar y orientar, para poder avanzar y conseguir los resultados y objetivos propuestos, eligiendo los controles correctos. Por lo que se tendrá que realizar un estudio de la empresa y determinar el alcance para establecer el SGSI. Además, es necesario poder valorar los riesgos que permitirá realizar un correcto análisis del riesgo para implementar de manera correcta la norma ISO 27001.
3	¿En qué consiste la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	En esta etapa del ciclo, es necesario desarrollar todas las actividades planificadas, se genera la documentación necesaria e identifica los controles para implementar de manera adecuada el SGSI que fueron identificados en la etapa de la planificación mediante los resultados del análisis de riesgo, por lo que se deberá establecer los roles y las responsabilidades de las tareas. El principal objetivo de fijar las políticas es poder indicar el propósito del SGSI, de cómo conseguir el resultado esperado, como ha sido aprobado, como realizar su seguimiento, ya que debe de revisarse de manera continua. El manual de procedimientos, consiste en establecer todos los controles que se va a implementar dentro de los procesos respecto a la seguridad de la información. Manual de riesgo consiste en identificar todo aquel riesgo que debes de tratar y hacerle seguimiento y minimizar tanto su probabilidad como su impacto.	La implementación consiste en poder desarrollar todas las actividades planificadas, generar toda la documentación haciendo el uso de los controles correctos para una implementación adecuada estableciendo los roles y las responsabilidades de las tareas. Se fijarán las políticas para indicar el propósito del SGSI, también el manual de procedimientos para establecer todos los controles que se va a implementar dentro de los procesos y el manual de riesgo para identificar el riesgo que se debe de tratar, hacerle seguimiento y minimizar tanto su probabilidad como su impacto.
4	¿Cuál es la importancia de verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	Es importante la verificación de la implementación, ya que es necesario poder medir los tiempos, lo errores generados, ya que, de los resultados obtenidos, se podrá tomar acciones para coordinar y a ayudar a la dirección de la empresa a determinar las actividades desarrolladas y las personas responsables de los procesos a mejorar para volver más eficiente y eficaz la implementación, por lo que se deberá detectar y prevenir reduciendo lo más mínimo posibles los incidentes de seguridad que han sido implantadas.	Es importante la verificación, porque medirá los tiempos, los errores generados de los resultados obtenidos y así poder tomar las acciones para coordinar y determinar las actividades para mejorar el proceso, generando el procesos más eficiente y eficaz.
5	¿Cómo verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la	Para verificar es necesario poder revisar regularmente la efectividad del SGSI implementado, mediante el uso de indicadores, que es la gestión del tiempo, la gestión de la calidad, que aterriza en el control de calidad de cada producto intermedio y la gestión de costos. Por lo que se debe determinar las acciones que fueron realizados para resolver un proceso, mediante auditorias, revisión de incidentes, medición de	Para verificar se debe de revisar regularmente la efectividad del SGSI implementado, mediante el uso de indicadores, que son el tiempo, la calidad, y los costos. Por lo que es necesario medir mediante auditorias, revisión de incidentes, medición de

	empresa Esvicsac, Callao?	eficacia, y observaciones o sugerencias realizadas de las partes interesadas, por lo que permita satisfacer los requisitos especificados al iniciar la implementación. La auditoría debe ser comunicado a todas las partes interesadas, usando los canales de comunicación externos internos establecidos, debe definirse los objetivos, alcance, criterios de la auditoría.	eficacia y resolver las observaciones. Y para auditar la implementación se debe de comunicar a las partes interesadas, definir los objetivos, alcance y criterios de la auditoria.
6	¿Cómo se actúa en la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	De los resultados obtenidos en la fase de verificación, se debe de estudiar los resultados, y confrontar con el funcionamiento de los procesos antes de implementar la mejora, acá se tomará la decisión si es que es satisfactoria deberá establecerse la mejora de forma definitiva, de lo contrario deberá de realizase los cambios para ajustar los resultados, es así que terminado este paso es necesario volver al paso uno para poder estudiar mejoras nuevas a implementar. Para realizar las acciones correctivas, se debe tener en cuenta los parámetros esperados, los comportamientos de los procedimientos y políticas, la eficiencia esperada, y la conformidad por la alta dirección.	En actuar se debe de estudiar los resultados, y confrontar con el funcionamiento de los procesos antes de implementar la mejora, para decidir si es que es satisfactoria o establecer la mejora de forma definitiva. Para realizar las correcciones correctivas,

N°	Preguntas	Entrevistado 2 – Especialista de desarrollo	Entrevista 2 Codificada
1	¿Cómo la implementación de la norma ISO 27001 en el departamento de Tecnología de Información de la empresa Esvicsac, mejorará la gestión del sistema de seguridad de la información?	Es importante para poder contar con un sistema de gestión de seguridad de la información adecuada para asegurar así la transparencia y que nuestros clientes puedan confiar mejor en nuestra organización. Ya que la ISO 27001 previene de las fugas de datos y toma medidas preventivas para proteger los activos de información. También involucra la conciencia de los usuarios para establecer procedimientos seguros que garanticen la continuidad del negocio. Debe estar de la mano con la alta dirección quien será la cabeza necesaria para poder impulsar y dar la sinergia necesaria con los usuarios que son reacios al cambio. Por lo que una adecuada implementación de la ISO 27001, ayudará a mejorar los tres puntos esenciales en la seguridad, la confidencialidad, la integridad y la disponibilidad de la información.	Implementando la norma ISO 27001, asegurará la transparencia y que nuestros clientes puedan confiar mejor en nuestra organización, porque previene de las fugas de datos y toma medidas preventivas para proteger los activos de información, involucrando la conciencia de los usuarios para establecer procedimientos seguros que garanticen la continuidad del negocio. Permitirá que se trabaje de la mano con la alta dirección quien impulsará la sinergia necesaria con los usuarios, ayudando a respetar los tres puntos esenciales en la seguridad, la confidencialidad, la integridad y la disponibilidad de la información.
2	¿Cómo planificar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	Un Sistema de Gestión de Seguridad de la Información comienza con su correcto diseño. Para ello deberemos definir cuatro aspectos fundamentales, el alcance del sistema, la Política de Seguridad a seguir, la organización de la seguridad y los programas de concienciación y formación del personal. Estos puntos tratados podrán asegurar el alcance, el tiempo y el costo de la implementación, por lo que se debe de contar con el apoyo y respaldo de la alta dirección. Por lo que es necesario el uso de metodologías que ayuden a la implementación, como PMP o pmbook. Para establecer el SGSI, es necesario conocer los procesos de la empresa, por lo que nos permitirá poder definir el alcance, el cual, se debe describir la extensión y los límites del SGSI, por lo que es el punto donde se definirá los elementos críticos que se deben de proteger teniendo en claro todo lo que es de interés para el sistema de gestión determinado por las actividades que se encuentren alineados con la misión de la empresa y mejore los objetivos de la empresa. Se debe analizar los riegos para evaluar las consecuencias y probabilidades de la implementación.	Se planificará definiendo cuatro aspectos fundamentales, el alcance del sistema, la Política de Seguridad a seguir, la organización de la seguridad y los programas de concienciación y formación del personal, que podrán asegurar el alcance, el tiempo y el costo de la implementación, siempre contando con el apoyo y respaldo de la alta dirección, siendo necesario usar PMP o pmbook para gestionar el proyecto. Para establecer el SGSI, es necesario conocer los procesos de la empresa, por lo que nos permitirá poder definir el alcance y los límites del SGSI y es necesario analizar los riegos para evaluar las consecuencias y probabilidades de la implementación.
3	¿En qué consiste la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	La implementación del sistema consiste en definir las acciones, recursos responsabilidades y prioridades de los resultados que se obtuvo del análisis del riesgo, por lo que en esta fase se debe de alcanzar los objetivos de control identificados, en la que se deben de estar incluidos los recursos, los responsables y las prioridades. Definir un control de métricas, bajo una metodología de trabajo como el pmbok que nos permita manejar y medir los recursos y poder comparar la eficacia de la implementación, es quien nos permitirá que el SGSI implementado se mantenga. El objetivo de fijar las políticas de seguridad es poder delimitar que se debe de proteger, cuáles son los límites aceptables, cuáles son los riesgos y cuál es la respuesta si sobrepasan, para conseguir el resultado esperado. El manual de seguridad es el documento que indica lo que debe hacer de forma general, señala las acciones como las operaciones que deben seguirse para llevar a cabo las funciones generales de la empresa, además, permite realizar un	La implementación del sistema consiste en definir las acciones, recursos responsabilidades y prioridades de los resultados que se obtuvo del análisis del riesgo, los objetivos de control identificados, incluidos los recursos, los responsables y las prioridades mediante un control de métricas. El objetivo de fijar las políticas es poder delimitar que se debe de proteger, cuáles son los límites aceptables, cuáles son los riesgos y cuál es la respuesta si sobrepasan, para conseguir el resultado esperado. El manual de seguridad es el documento que indica de forma general, las acciones que deben seguirse de forma

		seguimiento adecuado y secuencial de las actividades anteriormente programadas en orden lógico y en un tiempo definido. El manual de procedimientos es una colección de procedimiento que detallan las acciones de a seguir en cada una de las situaciones, identificadas como eventos de riesgo, la cual se puede decir que es el actuar paso a paso.	adecuado y secuencial en el tiempo definido. El manual de procedimientos es una colección de procedimiento que detallan las acciones de a seguir en cada una de las situaciones, identificadas como eventos de riesgo
4	¿Cuál es la importancia de verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	Es importante la verificación regularmente, ya que es necesario poder detectar a tiempo los errores posibles en el procesamiento de la información. Por lo que se debe de identificar los incidentes de seguridad y proponer la solución para mitigarlo, lo que es posible detectar y prevenir para reducir las ocurrencias de podrían poner en riesgo la implementación del SGSI, ya que necesario poder resolver grietas que has sido dejados en la implementación realizada, por lo que es necesario medir la eficacia del sistema de gestión.	La verificación es importante, ya que es necesario poder detectar a tiempo los errores posibles en el procesamiento de la información identificando los incidentes de seguridad y propone la solución para mitigarlo, lo que es posible detectar y prevenir para reducir las ocurrencias de podrían poner en riesgo implementación del SGSI.
5	¿Cómo verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	La verificación de la implementación debe ser realizada mediante un checklist establecido en el plan de auditoria el cual permite evaluar la eficacia de la implementación y la gestión realizada a los recursos que se dispuso para la implementación, atreves de auditorías internas el cual permita cumplir con la estructura de la norma ISO 27001. La implementación debe ser auditada para validar su eficacia de la implementación, para lo cual se debe de comprobar que el SGSI cumpla con los requisitos y proceso de la norma establecida atreves de una lista de verificación de los puntos a tratar, se debe identificar el no cumplimiento de los procedimientos establecidos para tomar las medidas correctivas que se requieran y la frecuencia con la que se debe de realizar para medir los resultados adecuados y efectivos, por lo que se debe revisar los problemas identificados y los riegos de la organización, por lo que se enfoca en evaluar los resultados	La verificación de la implementación debe ser realizada mediante un checklist establecido en el plan de auditoria, evaluar la eficacia de la implementación. La implementación debe ser auditada para validar su eficacia de la implementación, para lo cual se debe de comprobar el SGSI y cumpla con los requisitos y proceso de la norma se debe identificar el no cumplimiento de los procedimientos establecidos para tomar las medidas correctivas.
6	¿Cómo se actúa en la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	En esta etapa es de necesidad establecer las acciones correctivas para las mejoras identificas en el SGSI, aplicar las acciones correctivas y preventivas de la seguridad, se debe de comunicar a los interesados sobre los resultados obtenidos en los procesos, asegurando que las mejoras puedan lograr sus objetivos. Es la fase para corregir el proceso en caso no se tenga los resultados esperados y puedan llegar a cumplir con el comportamiento deseado, por lo que se debe de corregir la desviación, mitigar las consecuencias, evaluar la necesidad y diseñar las acciones e implementar los cambios.	En el actuar, es necesario establecer las acciones correctivas para las mejoras identificas en el SGSI y aplicar las acciones correctivas y preventivas de la seguridad que se debe de corregir la desviación, mitigar las consecuencias, evaluar la necesidad y diseñar las acciones e implementar los cambios

N°	**Preguntas**	**Entrevistado 3 – Especialista de Infraestructura**	**Entrevista 3 Codificada**
1	¿Cómo la implementación de la norma ISO 27001 en el departamento de Tecnología de Información de la empresa Esvicsac, Callao, mejorará la gestión del sistema de seguridad de la información?	La implementación de la norma ISO 27001, es importante ya que se basa en la gestión de riesgo, el cual permitirá que se pueda detectar el origen de los riesgos para luego tratarlos de una manera sistemática, esto ayudará gradualmente a controlar las medidas de seguridad que se implementen, ayudando a resolver todo tipo de situaciones críticas de los procesos de información que hasta el momento son inciertas, ya que no se tienen implementado un sistema de gestión de seguridad, siendo una herramienta de utilidad para mejorar la seguridad de la información en la empresa, cabe mencionar que, una implementación de estas características es muy costosa y si se desea proponer una implementación, deberá ser de la mano de la alta dirección, ya que depende mucho el factor económico.	La implementación de la norma ISO 27001, permitirá que se pueda detectar el origen de los riesgos para luego tratarlos de una manera sistemática, para controlar las medidas de seguridad que se implementen, ayudando a resolver todo tipo de situaciones críticas mejorando la seguridad de la información en la empresa.
2	¿Cómo planificar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	En la fase de Planificación, Se trabajará bajo una metodología de gestión del proyecto que es posible hacer uso del pmbok, para poder administrar los recursos necesario para la implementación e iniciar con un estudio de la situación de la organización desde el punto de vista de la seguridad, para estimar las medidas que se van a implantar en función de las necesidades detectadas, como la mejora de procesos y los procesos que intervienen, los datos recogidos, el objetivo de mejora a los procesos, definiendo las políticas y los objetivos de seguridad, definiendo el alcance del SGSI y la elaboración del análisis de riesgo ya que no toda la información de la que	La planificación bajo una metodología de gestión del proyecto para poder administrar los recursos a través del pmbok que permitirá administrar los recursos e iniciar con un estudio de la situación de la organización desde el punto de vista de la seguridad para estimar las medidas que se van a implantar en función de las necesidades detectadas, como la mejora de procesos y los procesos que

		disponemos tiene el mismo valor o está sometida a los mismos riesgos. Por ello, es importante realizar un Análisis de Riesgos que valore los activos de información y vulnerabilidades a las que están expuestas. Así mismo, es necesaria una Gestión de dichos riesgos para reducirlos en la medida de lo posible. Con el resultado obtenido en el Análisis y la Gestión de Riesgos estableceremos unos controles adecuados que nos permitan minimizar los riesgos.	intervienen, los datos recogidos. Se establece el SGSI basándose en los objetivos de seguridad y en el el alcance definido. Análisis y la Gestión de Riesgos estableceremos unos controles adecuados para minimizar los riesgos.
3	¿En qué consiste la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	Consiste en la implementación del SGSI mediante la metodología de trabajo planteada, que es capaz de clasificar y priorizar la implementación gestionando el proyecto, además deberá de implementar los controles y administrar de manera eficiente, los recursos y los tiempos necesarios para trabajar en las distintas tareas propuestas planificadas de manera adecuada, siendo como su objetivo la continuidad del negocio, el control del sistema de acceso. El objetivo de fijar las políticas de seguridad es que pueda ser adaptable, debe ser basada basándose en la organización, por lo que debe ser aprobado y comunicado a todas las partes y siempre estar actualizados. El manual de seguridad debe ser clara y coherente para que elementos que conformen la política sean conocidas, acatadas y sea del cumplimiento de todos los usuarios bajo el liderazgo del área que lo implanta. El manual de procedimientos debe ser definida el paso a paso de cada proceso y la responsabilidad de cada departamento implicado en el SGSI, por lo que se debe de emitir las acciones correctas y preventivas oportunas en los casos que sean afectados.	La implementación del SGSI, para clasificar y priorizar la implementación, implementando los controles que administre de manera eficiente los recursos y los tiempos, siendo como su objetivo la continuidad del negocio, el control del sistema de acceso. fijar las políticas de seguridad es que pueda ser adaptable, debe ser basada basándose en la organización y siempre estar actualizados. El manual de seguridad debe ser clara y coherente. El manual de procedimientos debe ser definida el paso a paso de cada proceso y la responsabilidad de cada departamento implicado
4	¿Cuál es la importancia de verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	La verificación juega un papel muy importante en el aseguramiento y tratamiento de la información y los activos que lo soportan que permite establecer e identificar cuáles son los riesgos que como empresa está expuesto, así mismo permite establecer los controles necesarios para asegurar, tratar y minimizar el impacto (técnico, económico, reputacional) de que se explote una vulnerabilidad y concrete un evento de perdida, poder verificar la implementación ayudará a estar preparados para certificación permitiendo poder identificar y corregir los procedimientos antes de que se lleve a cabo.	La verificación permite que los activos que lo soportan puedan establecer e identificar cuáles son los riesgos que como empresa está expuesto, además de establecer los controles necesarios para asegurar, tratar y minimizar el impacto, ayudará a estar preparados para certificación permitiendo poder identificar y corregir los procedimientos antes de que se lleve a cabo
5	¿Cómo verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	Para verificar se deben de realizar la auditoría interna, para poder medir la eficacia del SGSI por medios de los indicadores. Validando correctamente las actividades y propuestas revisadas en el proceso y validar el cumplimento de todos los objetivos. Para auditar la implementación, debe de comprobarse el SGSI cumpla con los requisitos de la norma, por lo que debe ser revisado el alcance del SGSI, las políticas, el manual de seguridad y el manual de procedimientos. Ya que el plan del tratamiento de riesgo debe estar documentado y debe ser aceptable a los principios de los sistemas seguros y a los procedimientos que se haya implementado para mejorar la gestión.	En la verificación, se deben de realizar la auditoría interna, para poder medir la eficacia del SGSI por medios de los indicadores, también validar correctamente las actividades y propuestas revisadas. Para auditar la implementación, debe ser revisado el alcance del SGSI, las políticas, el manual de seguridad y el manual de procedimientos, por lo que debe ser aceptable a los principios de los sistemas seguros y a los procedimientos que se haya implementado.
6	¿Cómo se actúa en la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	En esta fase es poner el plan la rectificación de las posibles no conformidades normativas de los procesos evaluados que fueron encontradas en la fase anterior, por lo que en esta fase se trabajará para garantizar que las acciones correctivas sean apropiadas, para evitar las no conformidades encontradas, por lo que trabajamos en la mejora continua. Las acciones correctivas deberán ser realizadas ante una no conformidad, debe evaluar la necesidad de acciones a eliminar la causa de la no conformidad, para evitar que vuelva a ocurrir, implantar nuevos procedimientos o acciones y hacer los cambios necesarios en los procesos y en el SGSI	En la actuación viene la rectificación de las posibles no conformidades normativas de los procesos evaluados, para garantizar que las acciones correctivas sean apropiadas. Las acciones correctivas deberán ser realizadas ante una no conformidad por lo que debe evaluar la necesidad y eliminar la causa para evitar que vuelva a ocurrir.

Anexo 5:

Matriz de entrevistados y conclusiones

N°	Pregunta	E1 – Jefe de TI	E2 – Especialista de Desarrollo	E3 – Especialista de Infraestructura	Similitud	Diferencias	Conclusión
1	¿Cómo la implementación la norma ISO 27001 en el departamento de Tecnología de Información de la empresa Esvicsac, Callao, mejorará la seguridad de la información?	La norma ISO 27001, permitirá asegurar la confidencialidad, integridad y la disponibilidad de la información. Obteniendo un mayor control y administración de las vulnerabilidades que adolece, reduciendo el riesgo a perder información conociendo sus vulnerabilidades, el cual ayudará a superar sus vulnerabilidades previniendo de los riesgo físicos y lógicos para garantizar la continuidad del negocio.	Implementando la norma ISO 27001, asegurará la transparencia y que nuestros clientes puedan confiar mejor en nuestra organización, porque previene de las fugas de datos y toma medidas preventivas para proteger los activos de información, involucrando la conciencia de los usuarios para establecer procedimientos seguros que garanticen la continuidad del negocio. Permitirá que se trabaje de la mano con la alta dirección quien impulsará la sinergia necesaria con los usuarios, ayudando a respetar los tres puntos esenciales en la seguridad, la confidencialidad, la integridad y la disponibilidad de la información.	La implementación de la norma ISO 27001, permitirá que se pueda detectar el origen de los riesgos para luego tratarlos de una manera sistemática, para controlar las medidas de seguridad que se implementen, ayudando a resolver todo tipo de situaciones críticas mejorando la seguridad de la información en la empresa.	E1, E2 y E3: Coinciden que la implementación de la norma ISO 27001, podrá ayudar a conocer los riegos y sus vulnerabilidades que la empresa tiene y así poder reducir sus riesgos de manera sistemática y mejorará gradualmente la seguridad de los sistemas de información en la empresa.	E1: Adiciona la implementación busca poder asegurar los tres pilares de la seguridad confidencialidad, integridad y disponibilidad. E2: Adiciona que implementando la norma podrá asegurar la transparencia y que nuestros clientes puedan confiar mejor en nuestra organización. E3: Adiciona que la implementación podrá detectar el origen de los riesgos.	La implementación de la norma ISO 27001 mejorará la seguridad de la información, ya que, gracias a sus buenas prácticas, se puede conocer cuáles son los riesgos y vulnerabilidades, que la empresa adolece, previniendo las posibles fugas de información mediante un plan de seguridad, que permita mitigar el riesgo de la información, por lo que será controlado y evidenciado, basándose en la mejora continua logrará siempre mejorar el significado de seguridad informática.
2	¿Cómo planificar la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	La planificación consiste en identificar y analizar la idea principal del proyecto reduciendo el riesgo de la implementación, por lo que es necesario el uso de una metodología para la gestión del proyecto, como el uso del pmbok, que permite guiar y orientar, para poder avanzar y conseguir los resultados y objetivos propuestos, eligiendo los controles correctos. Por lo que se tendrá que realizar un estudio de la empresa y determinar el alcance para establecer el SGSI. Además,	Se planificará definiendo cuatro aspectos fundamentales, el alcance del sistema, la Política de Seguridad a seguir, la organización de la seguridad y los programas de concienciación y formación del personal, que podrán asegurar el alcance, el tiempo y el costo de la implementación, siempre contando con el apoyo y respaldo de la alta dirección, siendo necesario usar PMP o pmbok para gestionar el proyecto. Para establecer el	La planificación bajo una metodología de gestión del proyecto para poder administrar los recursos a través del pmbok que permitirá administrar los recursos e iniciar con un estudio de la situación de la organización desde el punto de vista de la seguridad para estimar las medidas que se van a implantar en función de las necesidades detectadas, como la mejora de procesos y los procesos que intervienen, los datos recogidos. Se establece el	E1 y E3: Coinciden en poder hacer uso de una metodología de gestión de proyecto para poder planificar de manera adecuada la implementación, basándose en el uso de la metodología pmbok, quien ayudará a poder administrar de manera adecuada los recursos, teniendo en	E2: Adiciona que no solo es posible usar el pmbok, sino que existen otras metodologías para planificar de manera adecuada el proyecto como haciendo uso del PMP.	En la planificación se deberá trabajar haciendo uso de una metodología de gestión de proyectos, basados en la guía del pmbok, quien brinda sus características necesarias para poder implementar de manera adecuada la implementación, ya que se encargará de administrar todos lo recursos y define sus responsables, además

		es necesario poder valorar los riesgos que permitirá realizar un correcto análisis del riesgo para implementar de manera correcta la norma ISO 27001.	SGSI, es necesario conocer los procesos de la empresa, por lo que nos permitirá poder definir el alcance y los límites del SGSI y es necesario analizar los riegos para evaluar las consecuencias y probabilidades de la implementación.	SGSI basándose en los objetivos de seguridad y en el alcance definido. Análisis y la Gestión de Riesgos estableceremos unos controles adecuados para minimizar los riesgos.	cuenta el alcance del SGSI con el análisis de riesgo.		de poder definir de manera correcta y practica el alcance del proyecto y el análisis de riesgo para la implementación.
3	¿En qué consiste la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	La implementación consiste en poder desarrollar todas las actividades planificadas, generar toda la documentación haciendo el uso de los controles correctos para una implementación adecuada estableciendo los roles y las responsabilidades de las tareas. Se fijarán las políticas para indicar el propósito del SGSI, también el manual de procedimientos para establecer todos los controles que se va a implementar dentro de los procesos y el manual de riesgo para identificar el riesgo que se debe de tratar, hacerle seguimiento y minimizar tanto su probabilidad como su impacto.	La implementación del sistema consiste en definir las acciones, recursos responsabilidades y prioridades de los resultados que se obtuvo del análisis del riesgo, los objetivos de control identificados, incluidos los recursos, los responsables y las prioridades mediante un control de métricas. El objetivo de fijar las políticas es poder delimitar que se debe de proteger, cuáles son los límites aceptables, cuáles son los riesgos y cuál es la respuesta si sobrepasan, para conseguir el resultado esperado. El manual de seguridad es el documento que indica de forma general, las acciones que deben seguirse de forma adecuado y secuencial en el tiempo definido. El manual de procedimientos es una colección de procedimiento que detallan las acciones de a seguir en cada una de las situaciones, identificadas como eventos de riesgo	La implementación del SGSI, para clasificar y priorizar la implementación, implementando los controles que administre de manera eficiente los recursos y los tiempos, siendo como su objetivo la continuidad del negocio, el control del sistema de acceso. fijar las políticas de seguridad es que pueda ser adaptable, debe ser basada basándose en la organización y siempre estar actualizados. El manual de seguridad debe ser clara y coherente. El manual de procedimientos debe ser definida el paso a paso de cada proceso y la responsabilidad de cada departamento implicado	E1 y E2: Coinciden que en esta fase se debe desarrollar todas las actividades planificadas, generar toda la documentación haciendo el uso de los controles correctos para una implementación adecuada. Además de poder indicar el propósito del SGSI, el manual de procedimiento y el manual de riesgo	E3: Considera que se debe de clasificar y priorizar la implementación basado en controles y que pueda ser parte fundamental la mejora continua dentro de la implementación.	La implementación consiste en poner en marcha lo planificado, respetando los tiempos por tareas organizadas y los recursos establecidos, bajo el personal responsable. Fijando las políticas necesarias que permiten tener los resultados esperados, además es necesario redactar dos entregables para la guía y gestión del uso que vienen hacer el manual de procedimientos, el documento que pone en función los nuevos procedimientos y su uso y el manual de riesgo, definidos como eventos.
4	¿Cuál es la importancia de verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa	Es importante la verificación, porque medirá los tiempos, los errores generados de los resultados obtenidos y así poder tomar las acciones para coordinar y determinar las actividades para mejorar el proceso, generando el procesos más eficiente y eficaz.	La verificación es importante, ya que es necesario poder detectar a tiempo los errores posibles en el procesamiento de la información identificando los incidentes de seguridad y propone la solución para mitigarlo, lo que es posible detectar y prevenir para reducir las ocurrencias de podrían poner	La verificación permite que los activos que lo soportan puedan establecer e identificar cuáles son los riesgos que como empresa está expuesto, además de establecer los controles necesarios para asegurar, tratar y minimizar el impacto, ayudará a estar preparados para certificación permitiendo poder identificar y corregir los	E1, E2 y E3: Coinciden que la verificación es importante, ya que es necesarios poder medir los tiempos y los errores generados en la implementación, pues ayudará a poder dar solución a los incidentes ocurridos, proponiendo su	E2: Manifiesta que es importante en poner la solución porque pondría en riesgo la implementación.	Es importante la verificación, ya que es necesario poder de establecer los controles para asegurar, tratar y minimizar el impacto, ayudará a estar preparados para las auditorias que se realicen ya que se puede en esta fase identificar y

	Esvicsac, Callao?		en riesgo implementación del SGSI.	procedimientos antes de que se lleve a cabo.	atención para la corrección antes que puedan llevarse a cabo.		corregir los procedimientos antes de que se lleve a cabo.
5	¿Cómo verificar la implementación de la norma ISO 27001, en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	Para verificar se debe de revisar regularmente la efectividad del SGSI implementado, mediante el uso de indicadores, que son el tiempo, la calidad, y los costos. Por lo que es necesario medir mediante auditorias, revisión de incidentes, medición de eficacia y resolver las observaciones. Y para auditar la implementación se debe de comunicar a las partes interesadas, definir los objetivos, alcance y criterios de la auditoria.	La verificación de la implementación debe ser realizada mediante un checklist establecido en el plan de auditoria, evaluar la eficacia de la implementación. La implementación debe ser auditada para validar su eficacia de la implementación, para lo cual se debe de comprobar el SGSI y cumpla con los requisitos y proceso de la norma se debe identificar el no cumplimiento de los procedimientos establecidos para tomar las medidas correctivas.	En la verificación, se deben de realizar la auditoría interna, para poder medir la eficacia del SGSI por medios de los indicadores, también validar correctamente las actividades y propuestas revisadas. Para auditar la implementación, debe ser revisado el alcance del SGSI, las políticas, el manual de seguridad y el manual de procedimientos, por lo que debe ser aceptable a los principios de los sistemas seguros y a los procedimientos que se haya implementado.	E1, E2 y E3: Coinciden en poder realizar una auditoría interna para medir la implementación, ya que el resultado debería de mostrar la eficacia de la implementación planteada, por lo que debe ser contrastado con el alcance de la implementación.	E3: Agrega que debe ser revisado el manual de seguridad y procedimientos, para poder verificar de manera adecuada bajo los principios de los sistemas seguros.	Se deberá de verificar regularmente la efectividad de la implementación, el cual permitirá poder validar correctamente las actividades, por lo que se deberá de realizar auditoría interna que permita comprobar que se cumpla los requisitos y procedimientos en los procesos planteado en caso no que se dé, poder comunicar a las partes interesadas para proponer una solución.
6	¿Cómo se actúa en la implementación de la norma ISO 27001 en el departamento de Tecnología de Información en la empresa Esvicsac, Callao?	En actuar se debe de estudiar los resultados, y confrontar con el funcionamiento de los procesos antes de implementar la mejora, para decidir si es que es satisfactoria o establecer la mejora de forma definitiva. Para realizar las correcciones correctivas,	En el actuar, es necesario establecer las acciones correctivas para las mejoras identificas en el SGSI y aplicar las acciones correctivas y preventivas de la seguridad que se debe de corregir la desviación, mitigar las consecuencias, evaluar la necesidad y diseñar las acciones e implementar los cambios	En la actuación viene la rectificación de las posibles no conformidades normativas de los procesos evaluados, para garantizar que las acciones correctivas sean apropiadas. Las acciones correctivas deberán ser realizadas ante una no conformidad por lo que debe evaluar la necesidad y eliminar la causa para evitar que vuelva a ocurrir.	E1 y E2: Coinciden en poder estudiar los resultados obtenidos en la verificación y aplicar las acciones correctivas, definiendo a través de la implementación mejoras diseñadas para eliminar la causa.	E3: Agrega que la rectificación de las posibles no conformidades normativas de los procesos evaluados, deben ser bajo una evaluación de la necesidad.	En la implementación se actúa estableciendo acciones correctivas que permitan mejorar la implementación, ya que es necesario dar conformidad a una implementación culminada el cual debe de cumplir con el alcance debido mitigando vulnerabilidades y reduciendo los riesgos, por lo que en esta fase se da el ciclo de mejora continua atendiendo las no conformidades.

La implementación de la norma ISO 27001, es de beneficio para la empresa, porque no solo podrá tener la información de manera segura basado en un SGSI, que nos permite disminuir el impacto del riesgo y mitigarlo, evitando pérdidas financieras y sanciones asociadas a la vulneración de datos, sino también traerá beneficios a la empresa, ya que es posible ofrecer nuevos negocios y fidelizar a los clientes, que también protegerá y mejorará la reputación de la organización, además de poder cumplir con requisitos comerciales, legales y reglamentarios.

Anexo 6:

Guía de Observación

Empresa:	ESVICSAC
Ubicación:	Ca. Beta 147 Urb. Parque de la industria y Comercio - Callao
Área:	Departamento de Tecnología de TI
Observador:	Edwin Samuel Arias Quispe

Redacción de lo observado sobre las (03) tres personas que trabajan dentro de la unidad de estudio, donde P1: Jefe de TI, P2: Especialista en Desarrollo y P3: Especialista en infraestructura.

P1: Se observó que después de la recepción de un requerimiento y/o solicitud al departamento de TI, coordina una reunión con el o los especialistas referente a lo solicitado y el encargado del departamento que realizó la solicitud de darse el caso y aproximadamente entre 20 a 60 min dura la coordinación que usa para identificar cada fase de la realización de la solicitud y/o requerimiento definiendo el grado de atención, según sus requerimientos pendientes mediante el uso de un Gantt para realiza y prioriza actividades especificando los recursos más importantes, delega a los especialistas poder agregar en sus actividades diarias y coordinar las atenciones al entregable. Se identifica que existe una buena relación en el grupo de trabajo y gestión de proyecto, sin embargo, las atenciones no son trabajados en el tiempo debido, las atenciones no son medidas bajo un término de seguridad de la información.

P2: Se observó que después de la designación, elabora un plan de atención y completa el Gantt con funciones específicas para realizar las atenciones, envía correo de las atenciones a seguir y las coordinaciones que sebe de tener en cuenta con las actividades más importantes. En el proceso llegan atenciones de incidentes en el sistema actual, que debe ser atendido por el mismo, causando que en ocasiones no se complete el flujo del cierre de actividades, además se observa errores en los detalles de análisis y puesta en producción, que ocasiona que las tareas sean repetitivas por no pasar por un análisis de calidad de software. Las atenciones que brindó atención son más de las que puede evidenciar, dejando abierto el tiempo de atención a las tareas analizadas en la coordinación.

P3: Se observa que después de la designación de las tareas, elabora su plan de atención, sin embargo no es regular en la elaboración de las actividades, realiza las atenciones y coordina atenciones para soluciones inmediatas, no lleva un control de las atenciones y soluciones

que brinda para dar atención y seguridad, las atenciones lo realiza directamente no se tiene en conocimiento los usuarios o los responsables con la que da solución a los campos o atenciones que usa para coordinar atenciones. Genera políticas sin embargo no es suficiente para la total gestión realiza.

De las observaciones que se realizó se concluye que los trabajos que realiza el departamento de TI, no están siendo seguros y no se evalúa el riesgo, ya que no se conoce las vulnerabilidades de cada uno de los procesos que se manejan, generando un exceso de tiempo en las atención a lo planificado, realizando tareas repetitivas y no controladas, no existe un control de calidad en el software, ya que si hay un error es reportado por el propio usuario, los procesos y procedimiento no tienen los controles adecuados, no se rigen bajo un estándar de seguridad y las políticas de seguridad implantadas, no son completamente de conocimiento por los usuarios, no se tiene un inventario adecuado de los activos informáticos y es necesario mayor trabajo para protegerlos haciéndolos pasar por problemas con procesos directos a la seguridad.

Anexo 7:

Ficha de Análisis Documental

Empresa:	ESVICSAC
Ubicación:	Ca. Beta 147 Urb. Parque de la industria y Comercio - Callao
Área:	Departamento de Tecnología de TI
Observador:	Edwin Samuel Arias Quispe

El departamento de Tecnología de la Información de la empresa Esvicsac, tienen a cargo distintas tareas en su cartera de servicio gestionados pero no ordenados, existen ausencias de políticas y las pocas que hay no son completamente cumplidos de manera que en el proceso se pierde la estructura para los que fueron creadas e implantadas, por lo que se genera duplicación de tareas e inversión de tiempo de manera innecesaria y muchos de los servicios no son gestionados de manera adecuada, provocando riesgos críticos y que no se tienen registrado ni controlado y ni se tienen una planificación bajo supuestos incidentes que puedan suceder en el proceso del desarrollo de estas actividades. Además, se ha observado que las vulnerabilidades se vuelven más críticos cuando por atender al usuario lo más rápido posible y en algunas oportunidades por demostrar atención no es revisado por el especialista a cargo de la actividad produciendo ambigüedades de solución que involucra inestabilidad en el proceso por no cumplir correctamente la forma de realizarlo, sino que es realizado empíricamente.

En base a lo analizado, la implementación de la norma ISO 27001, permitirá analizar la empresa, revisar los objetivos, determinando el alcance, para buscar los controles necesarios, figando políticas, determinando manual de seguridad y manual de procedimientos, realizando auditorías internas y actuando con las acciones correctivas, se buscará la mejora continua de los procesos implementados que traerá el beneficio de reducir los riesgos tantos físicos como lógicos del departamento y por ende se verá beneficiado la empresa.

En conclusión, las atenciones realizadas por del departamento de sistemas, han sido poco eficientes en vista al usuario, pero nada eficaz, ya que se ha perdido los lineamientos bajo sus escasas políticas que generan seguridad, no todos los procesos cuentan con políticas, no se conoce el impacto que explote una vulnerabilidad y menos se encuentran medidos los riesgos que impacten directamente frente a posibles incidentes y los procesos se vean

comprometidos, por lo cual, implementando la norma ISO 27001, se logrará poder mejorar cada proceso de gestión de servicios que realice el departamento, se conocerá los riesgos, su impacto, se fijaran políticas de control, contará con manual de seguridad, manual de procedimientos debidos que puedan dar apoyo a los procesos y se muestre seguridad para resolver impactos que afecten e involucren a la empresa generando riesgo de confianza y reputación.

Anexo 7: Otras evidencias

Autorización

Lima, 20 de julio de 2020

Señores
Universidad Cesar Vallejo
Escuela de Post Grado - UCV Filial Lima
Presente. -

De nuestra consideración:

Por medio de la presente, tenemos el agrado de dirigirnos a Ustedes, a fin de informarles sobre la solicitud para el uso de información no confidencial de mi representada, requerido por vuestro alumno de post grado Br. Edwin Samuel Arias Quispe, identificado con DNI: 43768024, para el desarrollo de su Tesis titulada "Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información en la empresa Esvicsac, Callao".

Al respecto, de manera expresa autorizamos que la información recogida en la presente investigación pase a ser de carácter pública dentro de los fines académicos que son propios de la naturaleza de este tipo de trabajos, entre los cuales está su publicación, una vez concluido el mismo, en el repositorio de la Universidad.

Sin otro particular, nos despedimos de Ustedes, expresándole las muestras de nuestra mayor consideración.

Atentamente,

Juan Carlos Paz Cárdenas
Gerente General

- Ciclo de vida la implementación de la norma ISO 27001

Figura 7. Ciclo PDCA.

- Estructura del estandar ISO 27001

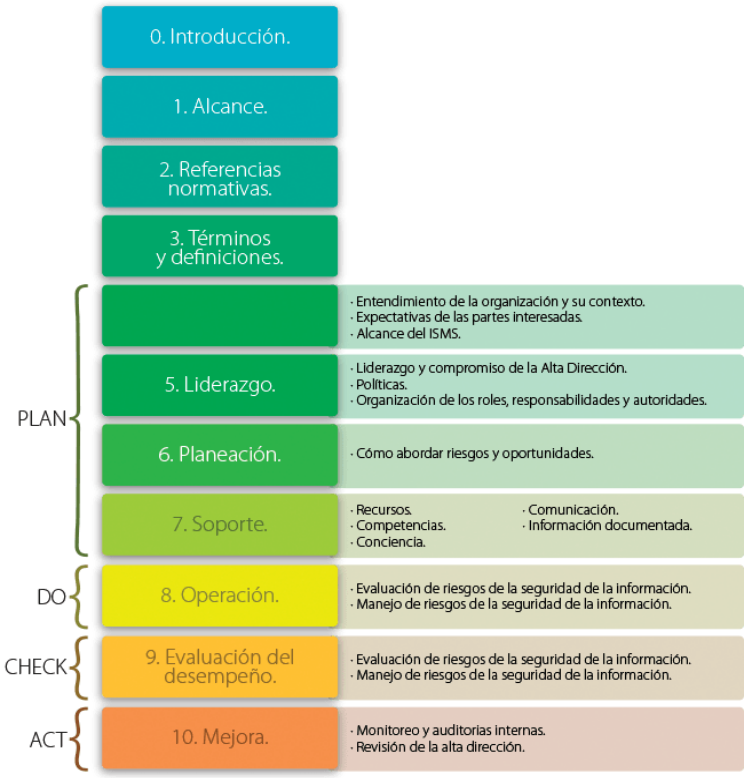

Figura 8. Estructura de la norma ISO 27001

- Estructura para realizar un análisis de riesgo en el departamento de TI

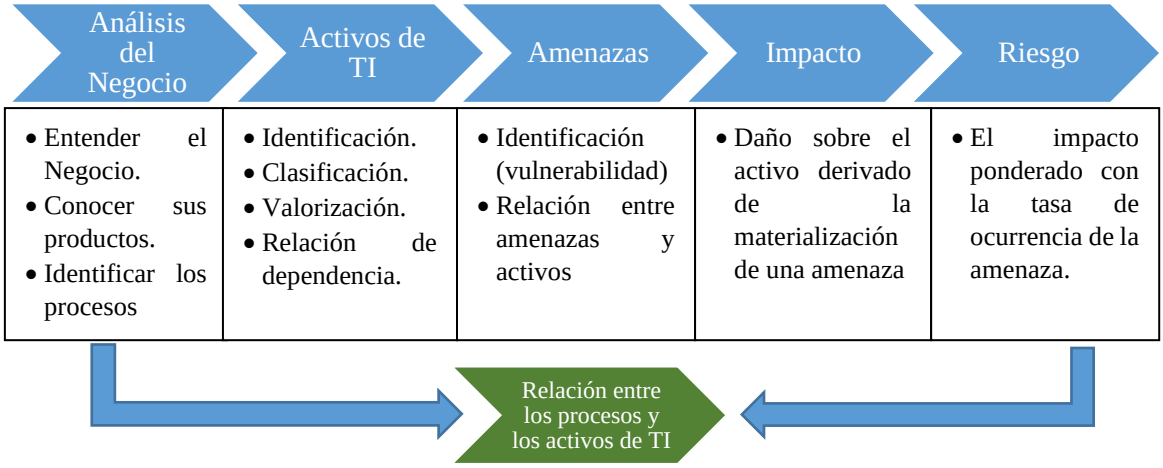

Figura 9. Análisis de Riesgo TI

Anexo 8: Propuesta de implementación realizada

- Conjunto de medidas y acciones que permitan implementar control y controles de seguridad de la información que permiten auditar cierto riesgo, basados en 133 puntos.

N°	Dominio - Control		#Ctrls	Cumplimiento
A5	Política de seguridad de la información		2	
	Dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requisitos institucionales, leyes y reglamentos pertinentes.			
A.5.1.1	Política de seguridad de la información	Se dispone de una política de SI aprobada por la dirección, publicada y comunicada a todos los empleados y partes externas pertinentes.		
A.5.1.2		La política de seguridad de información se revisa a intervalos planificados, y si ocurren cambios significativos se asegura su conveniencia, adecuación y eficacia continua.		
A6	Organización de la seguridad de la información		11	
	Gestionar la organización de la seguridad de información.			
A.6.1.1	Organización interna	La Alta Dirección apoya (dirige, se compromete, demuestra y reconoce responsabilidades) activamente la SI en la Institución.		
A.6.1.2		En las actividades de SI participan representantes de todas las UU.OO. Tienen roles y funciones.		
A.6.1.3		Los roles y responsabilidades en SI están bien definidos.		
A.6.1.4		Está establecido el proceso de autorización para nuevos activos de información (AI).		
A.6.1.5		Están definidos acuerdos de confidencialidad y se revisa con regularidad.		
A.6.1.6		Se mantiene los contactos apropiados con las autoridades pertinentes.		
A.6.1.7		Se mantiene los contactos apropiados con entidades especializadas en SI.		
A.6.1.8		El enfoque de la organización para gestionar la SI se revisa de manera independiente y periódica.		
A.6.2.1	Entidades externas	Se gestiona (identifica e implementa) los riesgos de acceso a la información de entidades externas.		
A.6.2.2		Se trata todos los requerimientos de SI antes de dar acceso a los clientes.		
A.6.2.3		Se establece acuerdos con terceros, que involucran acceder, procesar, comunicar o gestionar la información de la entidad, que abarcan los requerimientos de SI relevantes.		
A7	Gestión de activos de información (AI)		5	
	Lograr y mantener la protección apropiada de los activos de información			

A.7.1.1	Responsabilidad por los activos	Se mantiene un inventario de AI.		
A.7.1.2		Todo AI tiene asignado un responsable (propietario).		
A.7.1.3		Se dispone de una normativa de uso de los AI		
A.7.2.1	Clasificación de la información	La información está clasificada según su valor, requisitos legales, sensibilidad y criticidad		
A.7.2.2		Se dispone del procedimiento de rotulado y manejo de la información.		
A8	Seguridad de los recursos humanos		9	
	Asegurar que todo el personal involucrado entienda sus responsabilidades, sean apropiados para sus roles y así reducir el riesgo de robo, fraude o mal uso de los activos de información.			
A.8.1.1	Antes del empleo	Se tiene documentado (de acuerdo a la política) los roles y responsabilidades de SI, de todo el personal.		
A.8.1.2		Se verifica antecedentes de todo candidato a empleado o contratista.		
A.8.1.3		Se firman contratos donde se incluye las responsabilidades de SI.		
A.8.2.1	Durante el empleo	Se procura que todos los empleados apliquen la SI según la política.		
A.8.2.2		Se sensibiliza, capacita y educa en SI pertinente a su función de trabajo.		
A.8.2.3		Se tiene establecido un proceso disciplinario ante el incumplimiento de SI.		
A.8.3.1	Terminación o cambio del empleo	Están definidas las responsabilidades para el término o cambio de empleo.		
A.8.3.2		Se procura la entrega de activos al término de contrato.		
A.8.3.3		Se retira los derechos de acceso al término del contrato.		
A9	Seguridad física y medioambiental		13	
	Prevenir el acceso físico no autorizado, daño e interferencia en las instalaciones y activos de información.			
A.9.1.1	Áreas seguras	Se utiliza mecanismos de protección perimétrica (muros, vigilantes, etc.) a las áreas que contienen información e instalaciones que procesan información.		
A.9.1.2		Se utiliza mecanismos de control de acceso en entradas críticas.		
A.9.1.3		Se utiliza mecanismos de seguridad en oficinas, habitaciones e instalaciones.		
A.9.1.4		Se utiliza mecanismos de protección ante amenazas externas y ambientales.		
A.9.1.5		Se aplica medidas de seguridad física y directrices para trabajar en áreas seguras.		
A.9.1.6		Se aplica medidas de seguridad en áreas de acceso público (entrega/descarga).		

A.9.2.1	Seguridad del equipo	Los equipos están ubicados en salas con protección física ante un posible acceso no autorizado.		
A.9.2.2		Los equipos están protegidos frente a fallas de servicios públicos.		
A.9.2.3		El cableado eléctrico y de comunicaciones está protegido frente a interceptación o daños.		
A.9.2.4		Los equipos son mantenidos en forma periódica.		
A.9.2.5		Se aplica seguridad a los equipos fuera del local		
A.9.2.6		Antes de dar de baja un equipo se elimina la información		
A.9.2.7		Todo equipo requiere autorización para ser retirado de la Institución		
A10	Gestión de operaciones y comunicaciones		32	
	Asegurar la operación correcta y segura de los activos de información.			
A.10.1.1	Procedimientos y responsabilidades operacionales	Procedimientos de operación documentados y disponible a los usuarios.		
A.10.1.2		Gestión del control de cambios en los recursos de procesamiento de información.		
A.10.1.3		Segregación de responsabilidades para reducir el mal uso de los activos.		
A.10.1.4		Separación de los recursos de desarrollo, prueba y producción.		
A.10.2.1	Gestión de la entrega de servicios de terceros	Procurar que los terceros implementen, operen y mantengan los controles de seguridad.		
A.10.2.2		Monitoreo y auditoría regular de los servicios e informes de terceros.		
A.10.2.3		Gestionar los cambios en servicios de terceros, considerando criticidad de sistema de negocio, así como procesos involucrados y la evaluación de riesgos.		
A.10.3.1	Planeación y aceptación del sistema	Monitorear, afinar y realizar proyecciones de uso de recursos para asegurar buen desempeño.		
A.10.3.2		Establecer los criterios de aceptación de sistemas y realizar las pruebas antes de la aceptación.		
A.10.4.1	Protección contra software malicioso y código móvil	Implementar controles de prevención, detección y recuperación ante software malicioso, así como controles adecuados para la toma de conciencia.		
A.10.4.2		Asegurar que el código móvil autorizado opere de acuerdo a las políticas de seguridad.		
A.10.5.1	Copias de respaldo (back-up)	Se realiza copias de respaldo de información y software, y se prueba regularmente.		
A.10.6.1	Gestión de seguridad de redes	Manejar y controlar adecuadamente las redes para proteger la información e infraestructura.		
A.10.6.2		Las características de seguridad, los niveles del servicio, y los requisitos de gestión de todos los servicios en red están identificados e incluido en cualquier acuerdo de servicio de red, ya sea que estos servicios sean proporcionados en la empresa o subcontratos.		

A.10.7.1	Gestión de medios (activos de almacenamiento)	Se dispone de procedimientos para la gestión de medios removibles.		
A.10.7.2		Se dispone de procedimientos formales para la eliminación de medios.		
A.10.7.3		Se dispone de procedimientos para el manejo de información de manera confidencial.		
A.10.7.4		La documentación de los sistemas es protegida del acceso no autorizado.		
A.10.8.1	Intercambio de información (transferencia)	Se dispone de normativa para proteger la información durante su intercambio en cualquier medio de comunicación.		
A.10.8.2		Se firma acuerdos para el intercambio de información y software con entidades externas		
A.10.8.3		Se protege los medios en tránsito contra acceso no autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de la institución.		
A.10.8.4		Se protege adecuadamente la información involucrada en los mensajes electrónicos.		
A.10.8.5		Se dispone de normativa para proteger la información asociada con la interconexión de los sistemas de información de la institución.		
A.10.9.1	Servicios de comercio electrónico	Se protege la información de comercio electrónico que se trasmite en redes públicas, contra actividades fraudulentas, litigios contractuales y divulgación o modificación.		
A.10.9.2		Se protege la información de las transacciones en línea: De transmisión incompleta, pérdida de rutas, alteración, divulgación y duplicidad.		
A.10.9.3		Se protege la integridad de la información disponible públicamente.		
A.10.10.1	Monitoreo (de actividades no autorizadas)	Se registra pistas de auditoria, excepciones y eventos de seguridad.		
A.10.10.2		Se dispone de procedimientos de monitoreo del uso de recursos y se revisa regularmente.		
A.10.10.3		Se protege la información y los medios de registro frente a acceso manipulado o no autorizado.		
A.10.10.4		Se registra las actividades del administrador y operador del sistema.		
A.10.10.5		Se registran las fallas, se analizan y se toma la acción apropiada.		
A.10.10.6		Los relojes de los sistemas de procesamiento de información se mantienen sincronizados.		
A11	Control de acceso (lógico)		25	
	Controlar el acceso lógico a los activos de información			
A.11.1.1	Requerimientos	Se dispone de una política de control de acceso con base en requerimientos del negocio y de seguridad para el acceso.		
A.11.2.1	Gestión de acceso de usuarios	Se dispone de procedimiento de registro y baja de concesión de acceso a los sistemas y servicios de información.		
A.11.2.2		Se dispone de procedimiento para la gestión (restricción, control y asignación) de privilegios.		
A.11.2.3		Se dispone de procedimiento para la gestión de contraseñas.		

A.11.2.4		Se audita los derechos de acceso de manera regular.		
A.11.3.1	Responsabilidades de usuarios	Se promueve las buenas prácticas de seguridad para la selección y uso de contraseñas seguras.		
A.11.3.2		Se promueve que los usuarios deben asegurar la protección de los equipos desatendidos.		
A.11.3.3		Se promueve la práctica de escritorio limpio para documentos y dispositivos de almacenamiento removibles, y una política de pantalla limpia.		
A.11.4.1	Control de acceso a la red	Los usuarios solo tienen acceso a los servicios que están autorizados.		
A.11.4.2		Se utiliza mecanismos apropiados de autenticación para acceso de usuarios externos.		
A.11.4.3		La identificación del equipo forma parte de la autenticación.		
A.11.4.4		Se controla el acceso para el diagnóstico y configuración de puertos.		
A.11.4.5		Se segrega en la red, los usuarios y sistemas de información.		
A.11.4.6		Se restringe la capacidad de conexión de usuarios a redes compartidas.		
A.11.4.7		La red se configura de modo que no se infrinja los controles de acceso.		
A.11.5.1	Control de acceso al sistema operativo	Se controla el acceso al SO en las estaciones o terminales (procedimiento de conexión segura).		
A.11.5.2		Todo usuario dispone de una cuenta de acceso única.		
A.11.5.3		El sistema de gestión de claves asegura su calidad.		
A.11.5.4		Se restringe el uso de utilidades (software) no autorizadas, que podrían eludir las medidas de control del sistema.		
A.11.5.5		Las sesiones inactivas se cierran luego de un tiempo de inactividad.		
A.11.5.6		Se restringe el horario de acceso a las aplicaciones de alto riesgo.		
A.11.6.1	Control de acceso a las aplicaciones e información	Se restringe el acceso a los usuarios y al personal de TI.		
A.11.6.2		Los sistemas sensibles están en un ambiente aislado.		
A.11.7.1	Computación móvil y teletrabajo	Se dispone de política de protección de equipos móviles.		
A.11.7.2		Se dispone de política y procedimiento para teletrabajo.		
A12	Adquisición, desarrollo y mantenimiento de sistemas de información		16	
	Procurar que la seguridad sea una parte integral de los sistemas de información.			
A.12.1.1	Requerimientos de seguridad de los sistemas	Se especifican los requerimientos para nuevos sistemas o mejoras, incluyendo los controles de seguridad.		
A.12.2.1		Se validan los datos de entrada a las aplicaciones para asegurar que esta sea correcta y apropiada.		

A.12.2.2	Procesamiento correcto en las aplicaciones	Se incorpora mecanismos de validación en las aplicaciones para detectar corrupción de la información.		
A.12.2.3		Se identifican los requisitos para asegurar la autenticidad e integridad de los mensajes en las aplicaciones.		
A.12.2.4		Se valida la data de salida de las aplicaciones.		
A.12.3.1	Controles criptográficos	Se dispone de una política de uso de controles criptográficos para proteger la información.		
A.12.3.2		Se realiza gestión de claves para dar soporte al uso de las técnicas criptográficas.		
A.12.4.1	Seguridad de los archivos del sistema	Se dispone de procedimientos para la instalación del software de los sistemas.		
A.12.4.2		Se selecciona, protege y controla los datos de prueba del sistema.		
A.12.4.3		Se controla el acceso al código fuente del sistema.		
A.12.5.1	Seguridad en los procesos de desarrollo y soporte	Los cambios se controlan mediante el uso de procedimientos de control de cambios.		
A.12.5.2		Las aplicaciones se revisan después de haber hecho cambios en el sistema operativo, para observar el impacto generado.		
A.12.5.3		Se limita a los cambios necesarios (no se fomenta las modificaciones a los paquetes).		
A.12.5.4		Se procura evitar las fugas o filtraciones de información.		
A.12.5.5		Se supervisa y monitorea el desarrollo tercerizado de software.		
A.12.6.1	Gestión de vulnerabilidades técnicas	Se procura minimizar la explotación de vulnerabilidades de los sistemas.		
A13	Gestión de incidentes de seguridad de información		5	
	Asegurar que los eventos y debilidades de seguridad de información sean comunicados de manera tal que, permita una acción correctiva oportuna.			
A.13.1.1	Reporte de incidentes y debilidades	Los incidentes de SI se reportan por los canales apropiados tan rápido como sea posible.		
A.13.1.2		Se promueve que todo el personal reporte las debilidades de SI, que observe o sospeche.		
A.13.2.1	Gestión de incidentes y mejoras	Se dispone de procedimiento para respuesta rápida, eficaz y ordenada ante incidentes de SI.		
A.13.2.2		Se dispone de mecanismos para aprender a resolver incidentes, que permitan cuantificar y realizar el seguimiento de los tipos, volúmenes y costos de los incidentes de SI.		
A.13.2.3		Se recolecta y mantiene evidencias (para fines de auditoría).		
A14	Gestión de continuidad de operaciones		5	
	Contrarrestar las interrupciones de las actividades del negocio y proteger los procesos críticos, de los efectos de fallas significativas o desastres, y asegurar su reanudación oportuna.			

A.14.1.1	Gestión de la continuidad operativa	Se dispone de un proceso de gestión de continuidad de operaciones.		
A.14.1.2		Se realiza gestión de riesgos.		
A.14.1.3		Se dispone de un Plan de Continuidad de Operaciones (PCO).		
A.14.1.4		Se maneja un único marco referencial de PCO.		
A.14.1.5		El PCO se prueba y actualiza en forma regular.		
A15	Cumplimiento regulatorio		10	
	Evitar el incumplimiento de cualquier ley, estatuto, obligación, reglamento o contractuales, y de cualquier requisito de seguridad.			
A.15.1.1	Con los requerimientos legales	Se ha definido, documentado y mantiene actualizado todos los requisitos legales, reglamentarios, contractuales pertinentes.		
A.15.1.2		Se dispone de procedimientos para respetar la propiedad intelectual.		
A.15.1.3		Se protege los registros importantes de la organización.		
A.15.1.4		Se protege la privacidad de la información personal, según las regulaciones.		
A.15.1.5		Se sensibiliza al personal para evitar usos no autorizados.		
A.15.1.6		Se hace uso de cifrado, según las regulaciones.		
A.15.2.1	Con las políticas y estándares de S.I.	Se procura el cumplimiento de los procedimientos de SI.		
A.15.2.2		Se procura el cumplimiento de la normativa de SI en los sistemas de información.		
A.15.3.1	Auditoría de los sistemas de información	Se planifica las auditorías internas de sistemas de información.		
A.15.3.2		Se protege el acceso a las herramientas de auditoría de sistemas de información.		
			133	

Tabla 1. Dominios y controles basados en la norma ISO 27001

- Tabla de Resumen de la situación de la institución con respecto a los controles basados en la norma ISO 27001

Dominios y Controles de la ISO 27001	Situación Actual	Objetivo	Óptimo
Política de seguridad de la información	0.00%	85.00%	100.00%
Organización de la seguridad de la información	0.00%	85.00%	100.00%
Gestión de activos de información (AI)	0.00%	85.00%	100.00%
Seguridad de los recursos humanos	0.00%	85.00%	100.00%
Seguridad física y medioambiental	0.00%	85.00%	100.00%
Gestión de operaciones y comunicaciones	0.00%	85.00%	100.00%
Control de acceso (lógico)	0.00%	85.00%	100.00%
Adquisición, desarrollo y mantenimiento de sistemas de información	0.00%	85.00%	100.00%
Gestión de incidentes de seguridad de información	0.00%	85.00%	100.00%
Gestión de continuidad de operaciones	0.00%	85.00%	100.00%
Cumplimiento regulatorio	0.00%	85.00%	100.00%

Tabla 2. Resumen de la situación actual de los dominios

- Representación de la auditoria de cumplimiento por niveles basados en la ISO 27001

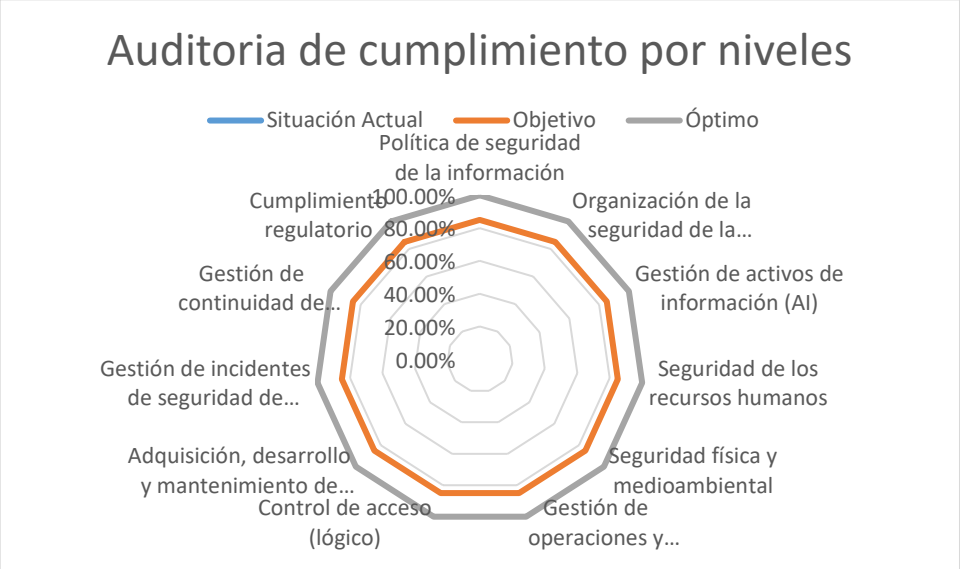

Figura 10. Proceso para la gestión de incidentes de seguridad

- Desarrollo de las políticas y controles para la empresa Esvicsac.

POLÍTICAS	CONTROLES
Mantener definiciones claras sobre la dirección y administración de la seguridad de información	• Políticas y procedimientos de seguridad de información
Contar con recursos humanos y logísticos que permita administrar la seguridad de información en forma efectiva y eficiente	• Funciones y responsabilidades del Departamento de TI para la seguridad de información.
Asegurar que los activos de información de la empresa Esvicsac sean claramente identificados y permitan efectuar un análisis de riesgos y definir niveles de protección	• Procedimiento de clasificación de activos de información. • Inventario de activos de información.
Reducir los riesgos de error humano, robo, hurto, fraude o mal uso de recursos de computo	• Funciones y responsabilidades de los usuarios. • Procesos de revisión de antecedentes de los empleados de Esvicsac. • Acuerdos de confidencialidad y código de conducta • Pólizas de seguro
Prevenir accesos no autorizados, daños o interrupción en las actividades de negocio de la empresa Esvicsac	• Identificación de áreas criticas • Procedimientos de control de acceso a las áreas criticas • Instalación de controles ambientales
Minimizar los riesgos de falla en los sistemas, perdida de información, daños a los equipos e interrupciones en el procesamiento de información	• Procedimientos documentados de operación de computadoras. • Control de cambios en la infraestructura de cómputo. • Procedimientos de administración de incidentes de seguridad. • Segregación de funciones • Separación de ambientes de desarrollo y producción • Planificación de la capacidad de procesamiento • Control contra software malicioso • Respaldo de información • Log de auditoria • Log de fallas • Control de la red
Evitar accesos y modificaciones no autorizados a la información de la empresa Esvicsac	• Políticas y procedimientos de control de acceso
Asegurar que los sistemas de información tengan controles de seguridad.	• Requerimientos y especificaciones de seguridad en los sistemas • Políticas y procedimientos de control de cambios a los programas
Minimizar riesgos que afecten la disponibilidad de los recursos de computo	• Plan de recuperación del centro de cómputo.

Tabla 3. Políticas y controles definidos

- Proceso de Incidencia frente un incidente de seguridad

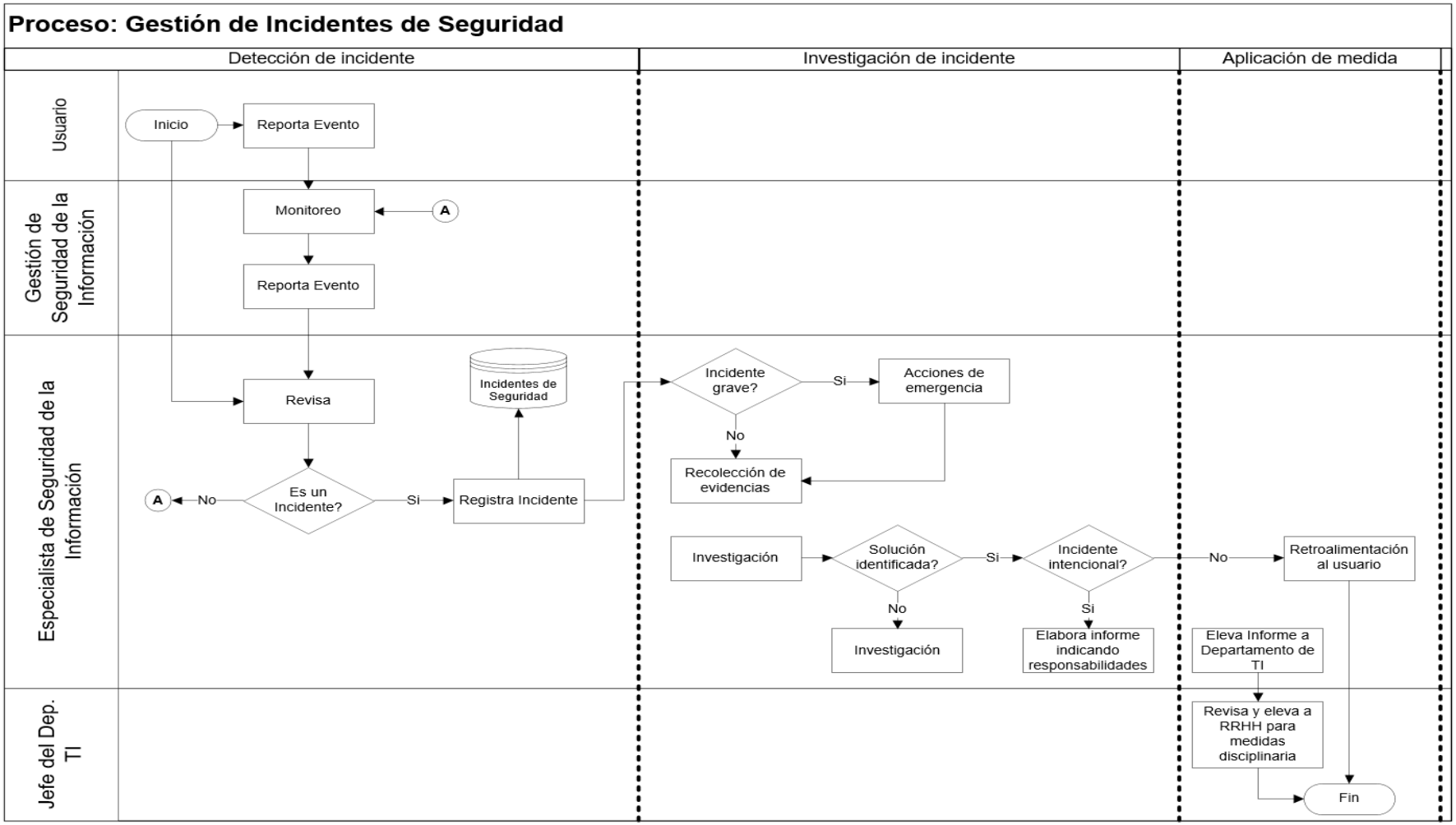

Figura 11. Definición de proceso para la gestión de incidentes de seguridad