UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PARA LA GESTIÓN DEL RIESGO DE LA INFORMACIÓN DE UNA EMPRESA COMERCIALIZADORA DE LUBRICANTES EN LA CIUDAD DE CHICLAYO

TESIS PARA OPTAR EL TÍTULO DE
INGENIERO DE SISTEMAS Y COMPUTACIÓN

AUTOR
MARIO IVAN PEREZ SANDOVAL

ASESOR
MARLON EUGENIO VILCHEZ RIVAS
https://orcid.org/0000-0003-2979-0731

Chiclayo, 2021

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PARA LA GESTIÓN DEL RIESGO DE LA INFORMACIÓN DE UNA EMPRESA COMERCIALIZADORA DE LUBRICANTES EN LA CIUDAD DE CHICLAYO

PRESENTADA POR:

MARIO IVAN PEREZ SANDOVAL

A la Facultad de Ingeniería de la
Universidad Católica Santo Toribio de Mogrovejo
para optar el título de

INGENIERO DE SISTEMAS Y COMPUTACIÓN

APROBADA POR:

Consuelo Ivonne Del Castillo Castro
PRESIDENTE

Jury Yesenia Aquino Trujillo
SECRETARIO

Marlon Eugenio Vilchez Rivas
VOCAL

Dedicatoria

Dedico esta tesis con todo el amor a mi esposa Olga Victoria, por haberme apoyado siempre por creer y confiar en mí, por brindarme comprensión, cariño y amor.

A mis amados Hijos José María e Ian Rafael por ser mi motivo de superación e inspiración para poder luchar cada día.

A mis padres, hermanos y suegros, quienes con sus palabras de aliento me ayudaron a culminar este gran sueño, hoy en día hecho realidad.

Agradecimientos

Agradezco a Dios por permitirme estar con salud y vida. Gracias a mi hermosa familia por apoyarme en cada decisión y proyecto, por permitirme cumplir con excelencia esta tesis.

Gracias por creer en mí y sobre todo estar en las buenas y malas; no ha sido sencillo el camino, pero gracias a sus aportes, su amor, a su inmensa bondad y apoyo, ahora puedo decir lo he logrado.

Índice

Resumen

La presente investigación se dio a partir de la situación problemática identificada en la empresa en cuestión, generada a partir de las deficiencias identificadas en cuanto a la capacidad de resguardar la seguridad de la información que posee la empresa, la cual comparte con sus proveedores y sobre todo con sus clientes. Este estudio tuvo como principal objetivo el de diseñar una propuesta de una herramienta de seguridad de la información para la casa comercializadora de lubricantes en la ciudad de Chiclayo, se realizó una investigación proyectiva y descriptiva. Se aplicaron como instrumentos de recolección de datos una guía de entrevista, guía de observación y un cuestionario compuesto por 20 ítems, el cual fue aplicado a 51 colaboradores, dentro de la presente investigación se consideró el análisis teórico tanto de la variable dependiente como independiente. Esta investigación está sujeta a los criterios éticos y será tomada como referencia en futuros estudios. Dentro de los resultados de la presente investigación está a deficiente gestión del riesgo identificada en la empresa en estudio a partir de la falta de capacitaciones al personal en temas relacionados a la seguridad de la información, además del elevado nivel de incidentes en cuanto a partir de la falta de partir de la falta de capacitaciones al personal en temas relacionados a la seguridad de la información, además del elevado nivel de sucesos sobre el cuidado de los datos.

Palabras clave: gestión comercial, ventas, salud ocupacional

Abstract

The present investigation was given from the problematic situation identified in the company in question, generated from the deficiencies identified in terms of the ability to safeguard the security of the information that the company has, which it shares with its suppliers and especially with its customers. The main objective of this study was to design a proposal for an information security tool for the lubricant trading company in the city of Chiclayo, a projective and descriptive research was carried out. An interview guide, an observation guide and a questionnaire composed of 20 items, which was applied to 51 collaborators, were used as data collection instruments. Theoretical analysis of both the dependent and independent variables was considered in this research. This research is subject to ethical criteria and will be taken as a reference in future studies. Among the results of this research is the deficient risk management identified in the company under study due to the lack of training of personnel on issues related to information security, in addition to the high level of incidents due to the lack of training of personnel on issues related to information security, in addition to the high level of events on the care of data.

Keywords: commercial management, sales, occupational health

Introducción

Según la Revista Ibérica de sistemas y tecnología de información (RISTI), [1] en la actualidad las tecnologías de información y comunicaciones conocidas como (TIC), vienen siendo fundamentales en la competitividad y la productividad de muchas estructuras, no obstante, como cualquier recurso con que cuenta una empresa, esta propenso a diferentes amenazas las cuales se pueden convertir en peligro con reacciones diversas. Las amenazas del tipo tecnológico son hechos cotidianos en el desarrollo empresarial, las cuales se presentan como ataques cibernéticos, virus, y otro tipo de amenazas que vulneran la seguridad de las empresas, todo esto requiere el implementar diversos controles los cuales deben ser gestionados mediante un enfoque adecuado de cuidado de datos.

El fin es el que los niveles de riesgo de la información se mantengan en niveles aceptables dentro de la empresa, esto incluye a los dispositivos tecnológicos que logran el recolectar, procesar, acceder, intercambiar, almacenar, transformar y presentar la información interna de la empresa. La adaptación temprana de la ISO 27001, a nivel mundial en contraparte con otros tipos de estándares de gestión muestra en evidencia lo importante que es la seguridad de la información pues dicha certificación ha crecido de manera exponencial según informe de la Organización Internacional para la Estandarización (ISO) [1].

Conforme a lo mencionado en el artículo de Cárdenas, Martínez y Becerra [2], mencionan que la seguridad de la información ha venido evolucionando desde la seguridad física la cual es orientada solo a la protección de ordenadores y dispositivos de almacenamiento de información, pasando por la seguridad de los sistemas y las redes tecnológicas de información, a centrarse en la gestión del alto nivel a través de políticas, procedimientos y controles basados en las personas.

La gestión del riesgo se encarga de buscar el evitar las pérdidas de la diferente información que manejan las organizaciones, que ese puede producir ante fallas en los sistemas de diferentes tipos es decir naturales, accidentales u intencionales, además del considerar los fraudes internos y externos lo cual implica a su vez un riesgo legal. La gestión del riesgo es necesario que se entienda como un proceso, pues esta permite la reducción del riesgo existente con el fin de poder evitar el que se generen nuevas vulnerabilidades [3].

La gestión del riesgo es la aplicación de un método lógico y sistemático dentro y fuera de la organización que se da con el fin de la identificación, análisis, procesamiento, monitoreo, comunicación y evaluación de los riesgos que se asocian con algún tipo de actividad, función o proceso con la finalidad de que las organizaciones minimicen sus pérdidas y logren maximizar sus beneficios, es por ello que la gestión del riesgo debe de estar incorporada en la filosofía de la organización, en sus prácticas, procesos es decir debe de formar parte de su cultura de gestión organizacional [3].

Considerando la realidad a nivel internacional según Gianese [4] en su artículo menciona que el hecho de que las certificaciones aseguran que tanto los productos como los servicios que brinda una empresa, sean conformes a las expectativas de los clientes, en el caso de la seguridad en la información la certificación ISO 27001, permite el asegurar a los clientes el uso de las mejores y buenas prácticas en concerniente a seguridad. Pues estas garantizan la legalidad, disponibilidad, integridad, confidencialidad de todo tipo de información que estas organizaciones gestionan, es por ello que las certificaciones ISO 27001, han aumentado alrededor del mundo, con un ritmo acelerado superior al 20% anual, en España si bien es cierto solo unas 800 empresas poseen esta certificación, en el año 2017 se encontraba dentro de los 10 países en el mundo con mayores certificaciones.

Tomando en cuenta la información de la Revista Observatorio RH [5], brinda información de que países como el caso de España posee el décimo puesto entre países a nivel mundial en cuanto al número de certificaciones de seguridad de la información ISO 27001, pues hasta el momento posee poco más de 800 reconocimientos, pues en este país europeo, la certificación les ha ayudado a la protección y reforzamiento de los sistemas de información de sus compañías, realizando la implementación de controles adecuados con el fin del asegurar que su sistema de información tenga confidencialidad, disponibilidad e integridad.

A nivel global se estima en el mundo un crecimiento del 45% en el número de certificados de ISO 27001 emitidos, no obstante, en Sudamérica había un crecimiento exponencial, ya que considerando que en el año 2006 solo existían 18 certificados, en el año 2010 paso a 117 y en el año 2016 esta cifra llego a 564, lo cual genero un crecimiento del 1.7% en 10 años. Los países en Sudamérica más representativos en cuanto a este tipo de certificación están Argentina (88) Brasil (117) y Colombia (221) [6].

Dentro de los sectores empresariales en donde se han generado este tipo de certificaciones con mayor repunte, se encuentra el sector textil, con un total de 132 certificaciones de ISO 27001, lo cual permite apreciar el interés de este sector en el compromiso que tiene con la seguridad de la información, como es lógico pensar el sector de la tecnología a nivel mundial cuenta con 6578 certificaciones, pues más que todo para ellos este tipo de certificación es una necesidad primordial [6]

Según el Instituto Europeo de Posgrado [7], la gestión del riesgo en el mundo se basa en un análisis eficiente del costo beneficio, lo cual se vincula a los objetivos estratégicos de las organizaciones. Fue en Estados donde la gestión de riesgos estableció funciones claves dentro de la estructura organizacional de muchas empresas, lo cual incentivo la implementación de la gestión de riesgos poniendo como principales responsables a los directivos financieros, generales y gestores del capital humano, todo ello permitió el poder integrar diversas políticas y distintos procedimientos considerando los diversos riesgos dentro del plan estratégico de estas entidades.

Considerando la seguridad de la información tenemos que en Europa según información publicada por el INCIBE (Instituto Nacional de Ciberseguridad), quienes consideran que la vulnerabilidad de la seguridad de la información es considerada como un fallo en un sistema de información lo cual compromete la integridad, disponibilidad o confidencialidad de las organizaciones, a su vez mencionan que las vulnerabilidades son las condiciones y características propias de los sistemas de una organización lo cual las hace susceptible a una amenaza, fallo, error informático, virus, o algún programa que aprovecha un fallo en seguridad existente en un determinado protocolo [8].

Este instituto da a conocer un estudio de la compañía de seguridad de software VERACODE que analizó más de 85,000 aplicaciones en poco más de 2,300 empresas a nivel mundial, como resultados mencionan que muy a pesar que en el 56% de las empresas estudiadas los fallos en seguridad de la información se han logrado solucionar, la vulnerabilidad de la seguridad de la información sigue siendo uno de los principales problemas, puesto que el tiempo que estás empresas se han tomado en solucionarlas asciende a una media de 147 días en regiones como Europa, Oriente Medio y África; no obstante en la región de América el tiempo es de 56 días, finalmente en Asia y Pacífico el tiempo es de 42 días. Además, el estudio muestra que los fallos en el software resultan ser de condición grave en un 32% de las compañías de Europa, Oriente Medio y África; un 37% en América y un 40% en Asia y Pacífico. Este estudio también menciona que las aplicaciones de las empresas en estudio sufren filtración de información en un 64% de ellas y de errores criptográficos representados por el 62% de las mismas [8].

La empresa Vodafone realizó un estudio de ciberseguridad a escala mundial, para lo cual entrevisto a 1,434 responsables de seguridad de países como Alemania, India, Italia, Irlanda, Reino Unido, Singapur, Estados Unidos y España. Este estudio analiza como las empresas toman decisiones en cuanto a la seguridad de la información, especialmente en lo referente a ciberseguridad. Se muestra como conclusiones que el 89% de estas consideran que la seguridad de la información que manejan es una oportunidad y no un obstáculo, pues permite mejorar la confianza y fidelidad de sus clientes, pues en este contexto mencionan que cuentas más nuevas tecnologías implementen las empresas esto es mejor [9].

Otro dato importante de este estudio es que en cuanto a la preocupación que tienen las empresas de los países en estudio sobre la seguridad de la información, Alemania es el país en donde las empresas se encuentran menos preocupadas por ataques informáticos pues el 53% de las empresas lo consideran así mientras que Estados Unidos y Singapur lideran el ranking superando el 70% [9].

En América Latina, en cuanto a seguridad de la información, según un estudio que toma en cuenta las tendencias con relación a la gestión de Ciber Riesgos y Seguridad de la información en América Latina y Caribe (AL&C), cuyo objetivo principal fue el analizar tendencias en ascenso como consecuencia de la transformación y además de la digitalización de diversos negocios, estudio que considero a 150 organizaciones participantes de 12 países y considerando 07 sectores industriales, dentro de las principales tendencias identificadas tenemos que de un total de diez empresas u organizaciones, cuatro de estas han sufrido algún tipo de incidente de ciber seguridad en los últimos veinticuatro meses, pues se apreció que el 70% de estas no tienen la evidencia de cuan efectivo es su respuesta mediante los procesos que posee ante algún incidente con respecto a su ciber seguridad, pues solo el 3% lleva a cabo algún tipo de simulación en cuanto a posibles fallas, incidentes a suscitarse con el objetivo de que sus capacidades efectivas ante este tipo se situaciones sean probadas [10].

También vemos que las organizaciones en América Latina se encuentran realizando el incremento de sus presupuestos a cuidar la data que se encuentra vulnerable, pues el 89% de estas consideran el nivel de importancia de estos factores como muy alta. Además, este estudio muestra que el 31% de estas organizaciones comparte información con otras entidades, identificando las amenazas de manera inteligente, esto hace ver que estas se encuentran en un estadio inicial referente a este tipo de capacidades de inteligencia de amenazas pues solo cuentan con un proceso de monitoreo de seguridad básico e insuficiente [10].

En el Perú, empresas del sector de servicios electrónicos, han alcanzado la tan ansiada certificación ISO 27001, esto significa un avance muy importante a nivel de empresa, pues fortalece su nivel de estandarización de procesos y de seguridad de la información en los procesos. Además, que va de la mano con la evolución de la forma de trabajo, la estandarización de procesos, sumado a ello con la generación de confianza con los clientes y partes interesadas [11].

Empresas como Telefónica del Perú obtuvo esta certificación internacional, pues se presenta como una empresa de gran y mayor alcance en cuanto al manejo de servicios móviles y centro de datos, pues es la única que se encuentra certificada [12].

En el Perú los retos de la gestión de riesgos en las organizaciones dirigen esfuerzos a ser cada día más conscientes, integrales o influyentes, todo ello permite la generación de nuevos negocios que relacionen los tipos de riesgos con sus necesidades particulares, pues estos tienen influencia directa en su capacidad de toma de decisiones [13].

También tenemos que nivel nacional en cuanto a la seguridad de la información, realizando un comparativo relacionado al presupuesto que las organizaciones destinan a realización de acciones de ciber seguridad y seguridad de la información vemos que en América Latina el 63% asigna entre el 1 y 5% del presupuesto asignado a tecnología de la información mientras que en el Perú el 65% de las organizaciones asigna los mismos porcentajes. También a nivel de América Latina solo un 17% de las organizaciones asigna un 11% a más de su presupuesto a ciber seguridad y seguridad de la información, con respecto al Perú esta cifra corresponde al 18% de las organizaciones. Además, en el Perú un 32% de las organizaciones tuvieron ciberataques en los últimos 02 años [10].

Si bien es cierto actualmente el Perú no cuenta con una estrategia nacional de Ciberseguridad, posee la mayoría de los elementos que resultan necesarios para combatir las diferentes amenazas que se suscitan en el ciberespacio pues cuenta por ejemplo con la División de Investigación de Delitos de Alta Tecnología, entidad especializada en la lucha contra los delitos informáticos, cuenta con el Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional de la Administración Pública Peruana y ha establecido leyes como la que permite la protección de datos personales y para la lucha contra los delitos informáticos, todo ello contribuye a la consideración de la seguridad de la información como un factor vital no solo en la defensa del Estado Peruano sino también de las entidades privadas [14].

Un paso importante suscitado en los últimos años por parte del Gobierno Peruano, es que el Congreso de la República aprobó la propuesta del Poder Ejecutivo de la adhesión del Perú al Convenio contra la Ciberdelincuencia o Convenio de Budapest, pues este convenio tiene como finalidad la protección de la sociedad de cara a la ciberdelincuencia todo ello a través de la generación de una legislación óptima y adecuada mediante la cooperación internacional. Según lo mencionado por la Secretaria de Gobierno Digital de la Presidencia del Consejo de Ministros menciono que la incorporación a este convenio constituye un gran avance al desarrollo de una sólida economía digital la cual promueva la competitividad, productividad, bienestar social y el desarrollo de la economía en un entorno digital de confianza digital tanto para las empresas que realizan sus operaciones en el Perú como para los ciudadanos [15].

En Chiclayo podemos identificar la problemática encontrada en la empresa en estudio, empresa que, si bien es cierto esta cuenta con los sistemas necesarios para el desarrollo y operatividad de su negocio, estos resultan deficiente en cuanto a la capacidad de resguardar la data, proveedores y sobre todo clientes. Además de ello la existencia de una deficiente planificación en el área de sistemas, debido a los recursos insuficientes que posee esta área de la empresa, lo que obstaculiza la realización de proyectos que permitan gestionar el riesgo de pérdida de información que posee.

La tesis que abarca el cuidado de la data de una organización en la ciudad de Chiclayo justificó su estudio de manera científica debido a que contribuye para futuros estudios, pues esta investigación siguió una secuencia lógica basada en el método científico, lo cual permitió el poder obtener información veraz y confiable que podrá ser tomada en cuenta por otros investigadores, sumado a ello el uso de fuentes teóricas confiables permitió tener un producto final que puede ser considerado por diversos investigadores.

La justificación financiera y económica se dio por el beneficio tangible que obtuvo la empresa en estudio con el desarrollo de la presente investigación, pues los resultados pudieron ser tomados en cuenta para su futura aplicación, lo cual permitió mejorar su capacidad de seguridad de la información que posee, generando como empresa un impacto positivo que se espera ver reflejado en la generación de nuevas oportunidades de generar ingresos a partir de la captación de mayor cantidad de clientes, los cuales cifraran su

confianza en una empresa ya certificada que cumpla con todos los estándares de calidad que el mercado exige.

La justificación de tipo social radicó en el beneficio que se obtuvo no solo para el personal de la empresa en estudio, sino para los clientes, proveedores y todos los grupos de interés relacionados con la empresa en estudio, ya que no solo el poder mejorar la gestión de riesgos de la empresa obtuvo un beneficio directo para ella como tal, sino para quienes participaron dentro de todo el proceso. Obteniendo beneficios que permitieron la mejora y la reducción del riesgo pues esto conlleva a la perdida de información esencial e importante para la entidad; contribuyendo a la generación de políticas que permitan la revisión continua de los riesgos, implementación de medidas de seguridad, reducción de costos y un mejor funcionamiento de procesos, entre otros beneficios que brinda la certificación ISO 27001.

La justificación tecnológica de la presente investigación, estuvo dada por el cambio de los procesos de cuidado informático que posee la empresa, la cual se consideró como referente dentro de las empresas relacionadas en el giro de negocio donde se desarrolla la empresa en estudio, la mejora de las herramientas tecnológicas que esta empresa posee, generó en el entorno donde se desarrolla la necesidad de poder contar y aplicar este tipo de certificaciones en empresas del sector, lo cual generó un ambiente más competitivo y brindó mejores condiciones a los clientes.

Ante esta realidad, es importante formular la siguiente pregunta ¿Cómo el diseño de una propuesta de un sistema de gestión de seguridad de la información, mejora la gestión del riesgo en una empresa comercializadora de lubricantes en la ciudad de Chiclayo?

Frente a esta pregunta y con el fin de profundizar en el problema, se realizó la investigación de tipo proyectiva, no experimental, descriptiva cuya población la conformaron 51 trabajadores de la empresa en estudio.

Para tal fin se determinó como Objetivo General: Diseñar una propuesta de un sistema de gestión de seguridad de la data para una empresa comercializadora de lubricantes en la ciudad de Chiclayo; con la finalidad de lograr el fin general, se propuso los objetos específicos: Diagnosticar la situación actual de la seguridad en la información en una empresa comercializadora de lubricantes en la ciudad de Chiclayo; determinar cómo se desarrolla actualmente la gestión de riesgos en una empresa comercializadora de lubricantes en la ciudad de Chiclayo; establecer planes de acción basados en la seguridad en la información que permitan la disminución de los niveles de riesgo respecto a los activos de la información de una empresa comercializadora de lubricantes en la ciudad de Chiclayo; validar la propuesta de un sistema de gestión de seguridad de la información para la gestión del riesgo en una empresa comercializadora de lubricantes en la ciudad de Chiclayo.

Revisión de literatura

Análisis de los sistemas de gestión de seguridad de la información

Actualmente, empresas que realizan o desarrollan diversos tipos de actividad, enfrentan con mayor frecuencia a una serie de inseguridades y riesgos los cuales provienen de un sinnúmero de circunstancias y contingencias, que ocasionan daños considerables a sus sistemas de información, así como a la información que haya sido procesada y almacenada en un determinado periodo de tiempo [25].

En este escenario, las organizaciones, para proteger su información derivada de sus actividades, deben establecer adecuados controles y estrategias que hagan segura la gestión de los procesos del negocio.

Para lograr lo señalado, de una manera coherente y eficaz, se hace necesario la implementación de un SGSI, que forma parte del sistema global de gestión, y se basa en el análisis de los riesgos a los que está y estaría expuesto el negocio, asegurando a la información ante la posibilidad de pérdida de:

• Confidencialidad: cuando el acceso a la información es solo para el personal autorizado.
• Integridad: cuando la información es exacta y completa.
• Disponibilidad: cuando los usuarios autorizados tienen acceso a la información cuando ellos lo requieran.

La seguridad total en las organizaciones es inalcanzable, pero teniendo en cuenta un proceso de mejora continua del Sistema de seguridad a implementar, es posible conseguir niveles satisfactorios de seguridad, para lograr la minimización del impacto que ocasionaría si se llegaran a concretar los riesgos a los que está expuesta [25].

Con referencia a la seguridad informática, es la que se encarga de la protección del sistema informático, todo ello con el fin del aseguramiento de la integridad y de la privacidad de toda la información que esta contiene, es decir se encarga de la implementación de medidas de tipo técnicas que permitirán la preservación de la infraestructura y de la comunicación dentro de la operatividad de la empresa, es decir tanto el software como el software que esta emplea.

Este concepto refiere al análisis de los riesgos, amenazas, análisis de los escenarios, esquemas normativos y buenas prácticas las cuales exigen ciertos niveles que aseguren los procesos que se dan en una empresa, además de la tecnología con la que ésta cuenta, con el fin de elevar los niveles de confianza en el crear, utilizar, almacenar, trasmitir, recuperar y disponer de la información que poseen [26].

Fases de un SGSI

Con el fin de lograr la realización de un proyecto para implementar un SGSI, se consideran un conjunto de fases secuenciales las cuales cuentan con una serie de actividades que se describen a continuación [27].

• Analizar el contexto de la organización: Lo cual implica el saber y conocer cuáles son las circunstancias actuales de la organización en cuanto al tipo de funcionamiento, dependencias, implicaciones, además de los requisitos internos y externos que poseen, sumando al conocer cuál es la motivación principal que la motiva a implementar un SGSI.
• Definir el alcance: Que consiste en determinar cuáles son los elementos que formarán parte y serán considerados en el SGSI, lo cual concierne el identificar los procesos de la empresa en los cuales se aplicara el sistema.
• Definir los objetivos y la política de seguridad: Conlleva a la fijación de un marco organizativo, en el cual se determinan cuáles son las funciones y las diferentes responsabilidades para gestionar la seguridad de la información, además es necesario considerar los diversos aspectos de la seguridad ya sea física, lógica y personal, adaptándose a los recursos y necesidades particulares de la organización.
• Evaluar riesgos de la organización: Que implica la caracterización de tanto los trabajadores, como las intimidaciones y debilidades de la organización conforme al siguiente detalle:
o Desarrollar el catálogo de existencias informáticas, mediante la cuantificación de su valor todo ello en términos de confidencialidad, integridad y de disponibilidad.
o Identificar y valorar amenazas, las cuales podrían afectar a la organización para lo cual se les asigna un valor de probabilidad de que esto ocurra o se degrade el activo si este se concreta.

o Calcular el impacto, esto se realiza por cada activo y dimensiones de seguridad de la organización, el impacto identificado se dará como resultado del activo y su valor, además de la degradación como consecuencia de la amenaza.

o Calcular el riesgo, en función del impacto identificado se procede a calcular el riesgo de cada activo, además de cuan probable es la materialización de una amenaza.

o Identificar a los propietarios de los riesgos, que consiste en la determinación del colaborador o colaboradores que son responsables de tomar una decisión en cuanto al riesgo identificado.

o Tratamiento de los riesgos, una vez calculado el riesgo e identificados sus propietarios se procede a la determinación de las estrategias necesarias y oportunas a aplicar sobre cada uno de los riesgos que se identificaron.

o Determinar las medidas de seguridad a implementar, que consiste en el establecimiento de un conjunto de controles de tipo organizativo y técnico que contribuyan a la reducción en un nivel aceptable del riesgo identificado.

o Evaluar los riesgos residuales, los cuales quedaran como resultado de la implantación de las medidas tomadas para minimizar los riesgos que posee la empresa, los cuales deberán ser calculados ya que este valor nunca será 0, es decir nunca se eliminara el riesgo totalmente.

o Plan de tratamiento de riesgos, que consiste en el detalle de las actividades oportunas y necesarias para implementar las medidas identificadas y seleccionadas.

o Elaboración de la información documentada prescindible para implementar las medidas seleccionadas.

o Implementación de los controles y los procedimientos, para lo cual resulta muy conveniente iniciar la implementación realizando aquellas acciones que con un mínimo esfuerzo puedan aportar un valor sustancial y significativo para la organización.

o Formar y concienciar al personal, la formación y capacitación de los usuarios serán de acuerdo al tipo de funciones que estos realicen.

o Realización de una auditoría de carácter interna y revisión por parte de la dirección del SGSI [27].

La Norma ISO/IEC 27001:2017

En el mes de octubre de 2013 se realizó la publicación las normas ISO, las cuales sustituirían a las versiones anteriores normadas en el año 2005.

Respecto a las versiones anteriores se considera lo siguiente:

• Se enfatiza el manejo de las oportunidades y activos.

• Se considera la identificación de los riesgos que se asocian a la pérdida de la data.

• Se considera la información documentada, en lugar de referencias a documentos y registros.

• Se determinan los controles considerados como necesarios y posteriormente compararlos con otros relacionados en los anexos de la norma

• Se disminuyeron las acciones preventivas, aunque se pueden manejar aún como en versiones anteriores

• Se actualizó el conjunto de controles a 114 repartidos en 14 secciones.

En 2014 y 2015 se hicieron algunas modificaciones, no muy sustanciales, a mencionar:

• El objetivo del control A.8.1.1 “Inventario de activos” pasa de hablar de “activos asociados a la información” a hablar de “la información y otros activos asociados a la información”.

• Se modifica la presentación del apartado 6.1.3.d) de ISO/IEC 27001:2013 en relación a la “Declaración de aplicabilidad” para mostrarla como una lista de requisitos.

• Se corrige un error, en la guía de implantación del control 14.2.8 “Pruebas funcionales de seguridad de sistemas” de ISO/IEC 27002:2013, por el que se hacía referencia al control 14.1.9 en lugar de al 14.2.9 [27].

Objetivo y campo de aplicación de la norma

Independientemente del sector, naturaleza o tamaño de la organización la Norma UNE-EN ISO/IEC 27001, es aplicada a diferente tipo de organizaciones, tal como sucede con otros sistemas de gestión. Tomando en cuenta los objetivos y riesgos que las organizaciones poseen, esta norma muestra de manera específica los diferentes requisitos necesarios para el establecimiento, la implementación, mantenimiento y la mejora de forma continua del SGSI. Muy a pesar de que la norma no contempla de manera concreta el cómo deben desarrollarse los procesos, existen una variedad de posibilidades que permiten su cumplimiento. Un ejemplo claro de estos es que, por ejemplo, la norma establece cuales son las formas de evaluar al momento de cumplir los requisitos, pues pueden ajustarse a su capacidad y naturaleza propia de la organización.

Para que esto se cumpla, se requiere principalmente tener factores como el contexto de la empresa, el liderazgo, la planificación, las operaciones, el soporte, la evaluación y la mejora.

La información a documentar que el sistema contendrá en diferentes niveles son:
• Políticas, las cuales proporcionaran las líneas de carácter general para actuar en cada caso particular.
• Información documentada sobre procesos, los cuales muestran los procedimientos al detalle de las actividades a realizar.
• Información documentada sobre evidencias, lo que previamente se denominaban registros, lo cual evidencia que las actividades previstas se hayan llevado a cabo [25].

El ciclo de mejora continua

Consiste en un proceso el cual está basado en el trabajo en equipo, además que se encuentra orientado hacia la acción, todo ello conlleva hacia un camino de mejora hacia la perfección la cual es guiada y conducida por quienes conforman una determinada organización. La mejora continua está inmersa tanto en el implantar una filosofía de gestión y el que los miembros de una organización tengan una participación activa [28].

Considerando que el ciclo PDCA viene de las siglas de las palabras en inglés: Plan, Do, Check, Act que en castellano es conocido como PHVA (Planificar, Hacer, Verificar y Actuar); este ciclo es considerado como la sistémica más empleada para implementar un sistema de mejora continua [28]; tenemos que la norma ISO 27001:2017 con respecto a las versiones anteriores trae la novedad de la exclusión del ciclo PDCA como escenario de carácter obligatorio en la gestión de la mejora continua, pues señala que toda organización debe buscar la mejora de forma continua de la eficacia, adecuación e idoneidad del sistema de gestión de seguridad de la información [27].

Sin embargo, se puede apreciar que el ciclo PDCA vive sobreentendido en la estructura personal.

Este modelo consta de las siguientes fases:
• Plan: Se realiza la planificación del SGSI, pues es necesario la determinación del contexto de la organización, es aquí donde se realiza la definición de tanto los objetivos como de las políticas que permitirán el poder alcanzarlos.

• Do: Es aquí donde se realiza la implementación y funcionamiento del SGSI, pues se ponen a la práctica las diferentes políticas y controles que han sido seleccionadas para cumplirlas basadas en el análisis del riesgo realizado. Es por ello que deben de tenerse claros cuales son los procedimientos y quien o quienes deben de hacer las tareas y actividades necesarias, tomando en consideración la capacitación oportuna y necesaria para ello.

• Check: Se da el monitoreo y la revisión del SGSI, ya que es necesario la realización de controles que permitan evidenciar que los procesos se han ejecutado y se están ejecutando de la manera prevista, todo ello con el fin del logro de lo planteado.

• Act: Permite el mantener y mejorar el SGSI, mediante la definición y la ejecución de todo tipo de acciones de carácter correctivo, pues estas son necesarias y oportunas para la rectificación de los falles que se han podido identificar en la anterior fase. Esta fase corresponde con ello.

Al momento del diseño del SGSI, se debe de tener en cuenta que sobre éste será aplicado un proceso de mejora continua. Por ello resulta necesario el inicio con una versión que se adapte a los recursos, necesidades y operatividad de la organización, generando mínimas acciones de seguridad que permitan la protección de la información con la finalidad de lograr el cumplimiento de los requisitos y especificaciones de la norma. Por consiguiente, el SGSI se acondicionará en las personas implicadas, teniendo una evolución de manera gradual, no implicando mucho esfuerzo [27].

Gestión del riesgo

Considerando la base teórica de la variable dependiente tomada en cuenta en la presente investigación, tenemos que según lo mencionado por Casares y Lizarzaburu [29], la Gestión de Riesgo está referido al análisis tanto de las amenazas, oportunidades, incertidumbres y los riesgos a los que se encuentran propensas las actividades realizadas en una organización, no importando su tamaño o interés, pero que afectan de manera significativa el logro de los objetivos organizacionales pues alteran sus sistemas de gestión. La gestión del riesgo es considerada como como una etapa importante y fundamental en la evaluación tanto financiera como económica en las empresas, pues se trata de un enfoque documentado y muy riguroso en los diferentes niveles de desarrollo de las actividades que se realizan en la organización, para lo cual resulta oportuno el contar con la información de las diferentes áreas de interés tanto internas como externas. Dentro de los activos más principales que la empresa posee es la información de sus procesos pues son de gran valor para estas, por lo cual es necesario es necesario el implementar mecanismos que aseguren su protección, por tanto, la seguridad de la información de estos procesos organizacionales ha venido cobrando mayor consideración.

Otros autores como son Calder y Watkins [30], definen a la Gestión de Riesgos como un tipo de disciplina existente con el fin de enfrentar a los riesgos que afectan a la organización puesto se generan pérdidas para ella. Dentro de los objetivos de la gestión de riesgos tenemos en primer lugar el eliminar el riesgo, seguido de reducir los riesgos que la organización no puede eliminar a niveles aceptables, convivir con los riesgos mediante el establecimiento de inspecciones que los conservan en horizontes admisibles o en su defecto lograr el transferirlos a alguna otra organización o a entidades aseguradoras.

Según lo mencionado por Imbaquingo, Pusdá y Jácome [31], la Tarea de inseguridades se concibe de la necesidad de la organización e interpretación de datos científicos y otro tipo de información, lo cual hace fácil los acuerdos y toma de decisiones. La Gestión del riesgo para la seguridad de la información se genera como consecuencia del campo de la gestión de seguros donde da inicio a la relación costo-beneficio, lo cual cobra importancia en las empresas para su planificación y estrategias en las décadas de los 80 y 90, no obstante a finales del siglo XX los riesgos informáticos encuentran mayor presencia dentro de las

empresas por lo tanto es necesario tomar acciones necesarias para evitarlos, por ello desde 1995 se establecen estándares.

Con el fin de realizar un análisis del riesgo dentro de una organización es necesario el determinar que activos son los más significativos e importantes para ésta, su interrelación y también su valor; seguido del determinar si estos activos están expuestos a alguna amenaza; también la determinación de qué mecanismos de protección están disponibles y cuan eficaces son ante la presencia del riesgo; estimación del impacto que tendrían los activos a partir de las amenazas identificadas y por último la estimación del riesgo [31].

Con la finalidad de realizar un cálculo del riesgo dentro de una organización es necesaria la identificación y la valoración del riesgo, en el proceso de identificación del riesgo la organización tiene como función específica el encontrar riesgos potenciales sobre cada uno de sus activos, utilizando diversidad de técnicas o métodos secuenciales y sistemáticos como son las entrevistas, encuestas, análisis FODA, entre otros. Una vez identificado el riesgo, se procede a la valoración del riesgo, el cual inicia su proceso en la identificación de los activos, seguido de la identificación de cada amenaza sobre cada activo, culminando en la estimación de la vulnerabilidad de las amenazas sobre cada activo. Con esta información recabada como resultados de la valoración del riesgo, se lleva a cabo una evaluación rápida para esta operación, dividiéndose el nivel de riesgo en cuatro estados: Bajo: donde el nivel de riesgo es bajo y es esencial y necesario la utilización de salvaguardas adicionales; Medio: donde el nivel de riesgo es medio, por lo que se debe de considerar si se deben implementar salvaguardas para evitarlos; Alto: en este nivel es una obligación la implementación de salvaguardas necesarios que disminuyan el riesgo [31].

Uno de los mayores beneficios del análisis del riesgo está relacionado con el motivo de que los resultados son considerados como bases fiables científicas para la toma de decisiones. Además, con la ejecución de las medidas oportunas y necesarias acompañadas del mantenimiento, evolución y adaptación constante como efecto de la revisión de forma periódica de los controles de seguridad establecidos permiten la corrección de fallas de seguridad descubiertos, todo ello para combatir riesgos nuevos, sumado a ello beneficios como la minimización del impacto de los riesgos con el fin de reducir costos, el afianzar la continuidad operativa de la empresa y la adecuada gestión. [31].

Proceso de la gestión de riesgos

Tiene como principal objetivo la identificación y tratamiento de los riesgos potenciales de forma urgente, pues el fin de llegar al conocimiento exacto y realista de las circunstancias que podrán afectar los procesos o servicios, lo cual causa pérdidas y daños lo cual permite el establecimiento de prioridades y la asignación de requisitos de seguridad con el fin de afrontar dichas situaciones de manera conveniente [31].

El proceso de gestión de riesgos es detallado por Imbaquingo, Pusdá y Jácome [31], considerando:

- Determinación del contexto: Que permite la determinación de parámetros y condicionantes internas y externas que delimitan las políticas a seguir para gestionar los riesgos.
- Personalización de los peligros: Proceso el cual busca establecer una relación de los puntos posibles de peligros.
- Análisis de riesgos: Donde se busca la calificación de los riesgos identificados, ya sea analizando cualitativa como cuantitativamente sus consecuencias, todo ello permitirá obtener como resultado del análisis una visión estructurada con el fin de centrarnos en lo verdaderamente importante.

• Evaluación de los riesgos: En esta etapa del proceso se toma en cuenta factores de percepción, de estrategia y de política lo cual permite la toma de decisiones con relación a que riesgos son aceptados y cuáles no, así como en qué circunstancias se puede aceptar un riesgo o en su defecto trabajar en su tratamiento.

• Tratamiento de los riesgos: Que se encarga de la recopilación de las actividades dirigidas y encaminadas a la modificación de la situación de riesgo.

• Comunicación y consulta: Que busca encontrar un equilibrio entre la productividad y la seguridad.

• Seguimiento y revisión: Una vez finalizado el análisis de riesgos los resultados obtenidos deben de ponerse en práctica según lo recomendado con el fin de evitar incidentes dentro del entorno organizacional.

Medición del Nivel de Riesgo

Con el fin de evaluar los riesgos de seguridad en la información, es necesario controlar la situación. Es por ello que se han considerado la metodología Octave Allegro, la cual fue desarrollada por SEI (Software Engineering Institute), pues ayuda a tomar en cuenta las amenazas que afectarían de forma negativa los objetivos que persigue la organización, realizando estudio de impacto.

Octave Allegro puede realizarse en un entorno colaborativo con estilo taller, pues considera elementos como guías, hojas de trabajo y cuestionarios. Octave Allegro en organizaciones que no cuentan con la experiencia suficiente en la gestión, cultura e información de riesgos resulta muy adecuado para el desarrollo del análisis de sus riesgos [32].

El enfoque Allegro de OCTAVE tiene:

Instaurar juicios de cálculo del peligro:

o Como primer paso de esta metodología, es preciso la definición de criterios, con el fin de conocer cuan propensa es la organización a los riesgos, además de conocer su postura actual en cuanto a este aspecto. Esta actividad es la base para la evaluación ya que permite la medición del grado en que una organización puede verse sometida o afectada al momento que una amenaza se materializa. [32].

o Una vez seleccionadas las categorías se procede a que por cada uno de los elementos evalúen el nivel de impacto deberá de ser establecido por los colaboradores o el colaborador encargado de la generación de los criterios de medición del riesgo mediante una hoja de trabajo, lo cual es una de las características ventajosas que posee Octave Allegro, pues permite registrar la información generada durante su aplicación. [32].

Desarrollar un perfil:

o Para realizar la evaluación de riesgos es necesario centrarse en los activos de la información, esto implica tanto los datos como los conocimientos que son valiosos para la organización, es en este paso donde es necesario la documentación de las razones por la que se eligen, realizando una descripción de los mismos.

o Es preciso la asignación de un responsable encargado de la custodia de cada uno de los activos de información, pues éste debe establecer los requisitos de seguridad para los mismos: confidencialidad, integridad y disponibilidad, de acuerdo a su experiencia y criterio.

o Luego de ello se procede a tener un profile el cual será considerado como críticos previa evaluación de los encargados, esto permite tener forjar la base la identificación de amenazas y riesgos en pasos subsecuentes. Esta acción resulta ser primordial con el fin de asegurarse de que los activos se describen de manera consistente y clara, a su vez permite identificar los requisitos de seguridad con el fin de definir que opción en cuanto a su protección se puede aplicar [32].

• Identificar contenedores de activos de la información:

o En este paso se identifican los repositorios en donde es almacenada la información de la organización, todo ello con el fin de identificar sitios en donde a menudo se realizan los ataques contra los datos.

• Identificar áreas de preocupación:

o Es donde se da inicio al proceso del desarrollo de perfiles.

o En este paso se realiza la identificación riesgos evidentes sin necesidad de revisarlos exhaustivamente por lo cual se registra información sobre los actores es decir quien o quienes podrían realizar la amenaza, los medios por los cuales es posible ejecutarla, los motivos y los resultados. [32].

• Identificar escenarios de amenazas:

o Es donde las diferentes partes de la empresa tienen el carácter crítico de la organización y que además no se observan a simple vista.

o Existen árboles de amenaza que también consideran a los problemas de tipo técnico como son los defectos se hardware y software, falla de suministro eléctrico, fallas en telecomunicaciones, incidentes por códigos maliciosos e incluso por algún tipo de desastres naturales los cuales pueden afectar de alguna manera los activos de información.

• Identificar riesgos:

Para lo cual se utiliza la ecuación siguiente:

Riesgo= Amenaza (condición) + Impacto (consecuencia)

o Aquí es necesario utilizar información estadística como el registro de incidencias, considerando que a una probabilidad de ocurrencia alta se le asigna el valor 3, si es medio un valor 2 y un valor 1 para una probabilidad baja [32].

• Analizar riesgos:

o Se mide de forma cualitativa mediante la indicación del grado en que se ve afectada la organización por una amenaza, mediante el cálculo de cada riesgo de cada activo de la información asignándole una puntuación.

• Escoger una dirección de ablandamiento:

o En el último paso es necesario la determinación de las opciones de tratamiento de riesgos tomando como base los resultados de análisis, mediante la utilización de los valores de impacto y la probabilidad que ha sido calculada en los anteriores pasos.

o En Octave Allegro se procede a la categorización en grupos de escenarios de amenazas para su posterior tratamiento tomando como base los resultados.

Los enfoques de tratamiento son el mitigar, postergar, transferir o aceptar, es conveniente el poder priorizar los riesgos para identificar a cuáles deben de dársele prioridad [32].

Materiales y métodos

Tipo proyectiva, pues según lo mencionado por Hurtado [33], esta investigación permitió el proponer una solución a un problema identificado, el cual sigue un proceso desde la indagación hasta la propuesta de alternativas de solución, no obstante, la propuesta no es ejecutada necesariamente.

Nivel de investigación. La finalidad del establecimiento de su comportamiento la hace descriptiva, pero sin influir sobre el de ninguna manera. Esta investigación se encargó de describir un determinado acontecimiento o situación.

El diseño fue no experimental ya que según la teoría de Hernández, Fernández y Baptista [35] este tipo de diseño busca centrarse en el observar determinados fenómenos, los cuales

se dan en un ambiente natural o en situaciones ya existentes que son posteriormente analizadas. En este tipo de diseño no existe manipulación deliberada de las variables, por tanto, no existen condiciones ni estímulos a los cuales los sujetos de estudio sean expuestos.

El diseño se diagrama como sigue:

M ⟶ O ⟶ P

Donde:

(M) Muestra, la muestra en estudio conformado por el personal de la empresa en estudio
(O) Observación, de la situación y problema diagnosticado
(P) La propuesta del Sistema de Gestión de Seguridad de la información

El método de investigación a emplear es el deductivo que implica la generación de una estrategia para el planteamiento de la propuesta de solución al problema, según Torres [36], este método que lingüísticamente significa conducir o extraer, se basa en el razonamiento, pue permite pasar de principios generales a hechos particulares. Es decir, una vez al comprobar y verificar que un principio es válido, se comienza a aplicarlo en contextos particulares.

La población se considera como el conjunto de todos los casos que tienen concordancia con una serie de especificaciones, sobre la cual se estudia un fenómeno determinado. La población posee características que son compartidas en común por ciertos individuos y estas características son estudiadas dando origen a los datos de la investigación [37].

Tabla 1: Personal de la empresa en estudio

CARGO	**N° DE COLABORADORES**
Personal de ventas	04
Personal administrativo	37
Personal asistencial	03
Jefaturas	04
Gerencia	03
TOTAL	**51**

Fuente: Empresa en estudio

Tamayo [38], indica que la muestra está referida a la a una porción representativa del total de la población en estudio, la cual posee ciertos perfiles que la convierten en una porción de individuos aptos para una determinada investigación. López [39] menciona que una muestra puede ser considerada censal, cuando una porción de ésta representa a toda la población.

En vista a lo mencionado al ser una población pequeña conformada por 51 trabajadores de la empresa en estudio, la muestra empleada fue censal, puesto que se aplicó el instrumento a toda la población que participa en el estudio.

Según Cochran [40], el muestreo que se considero fue el no probabilístico por conveniencia, el cual considera las unidades muestrales conforme al acceso y conveniencia del investigador. Este tipo de muestreo permite la obtención de información de la población de forma rápida.

Criterios de selección. Dentro de las características que delimitaron la población en estudio tenemos que es a partir de la identificación de la misma se identificó una muestra representativa en cuanto a la proporción. Además, se seleccionó como muestra a los colaboradores de la empresa en estudio considerando sus diferentes puestos y niveles jerárquicos lo cual permitió al investigador el poder tomar en cuenta las opiniones del tema investigado en todos los niveles de la empresa estudio. Siendo la unidad de análisis ubicada en la ciudad de Chiclayo, específicamente en una empresa comercializadora de lubricantes.

Dentro de las técnicas a considerar en la presente investigación, tenemos:

• Entrevista, que, según Olsen, [41] consiste en intercambiar diferentes tipos de ideas, opiniones, formas de pensar a través de la interacción de mínimo dos personas con el fin de obtener información de un tema en específico.

Encuesta, que según Fernández, Baptista y Hernández [37], mencionan que es una técnica conformada por un conjunto de interrogantes para una o dos variables en estudio con el fin de detectar la opinión de una determinada muestra de personas.

• Observación, según Bunge [42], consiste en un procedimiento de carácter empírico pero elemental, el cual tiene como objeto de estudio uno a varios hechos, fenómenos, objetos de la realidad actual, siendo este hecho observado verdadero o contundente.

Los instrumentos a aplicar conforme a cada técnica de recolección de datos son:

• Guía de entrevista, considerado por Olsen [41] como un encuentro cara a cara el cual viene respaldado por una serie consecutiva de preguntas, las cuales han sido previamente planeadas de forma cuidadosa, pues deben seguir una serie de pautas con el fin de recopilar las respuestas deseadas. La guía de entrevista será aplicada al Jefe de Sistemas de la empresa en estudio con la finalidad de evaluar el cuidado de la data.

• Cuestionario, que para Fernández, Baptista y Hernández [37], es un instrumento que lo conforman un conjunto de preguntas elaboradas teniendo como base una o más variables, sus dimensiones y sus respectivos indicadores los cuales se van a medir. El cuestionario a aplicar permitirá diagnosticar la situación actual de la empresa estudiada.

• Guía de observación, según Tamayo [43] la define como un formato en el cual que permite la recolección de datos de forma sistemática y uniforme. Es útil para una revisión clara y objetiva de los hechos según necesidades específicas respondiendo a las variables o elementos del problema. La guía de observación a aplicar, permitirá reforzar la evaluación de la seguridad de la información en esta.

A continuación, se presentan las técnicas e instrumentos que serán necesarias:

Tabla 2: Técnicas e instrumentos de recolección de datos

Técnicas	**Instrumentos**	**Elementos de la población**	**Propósito**
Encuesta	Cuestionario (Anexo 05)	Responsables de la gestión informática y alta dirección	Determinar la gestión del riesgo
Entrevista	Guía de entrevista (Anexo 03)	Jefe de Sistemas	Diagnosticar la seguridad en la información
Observación	Guía de observación (Anexo 04)	Áreas de la empresa	Diagnosticar la seguridad en la información

Metodología de desarrollo

Se puede desarrollar de diferentes formas, pero es esencial para poder lograr un resultado aceptable, en cuanto el tomar en cuenta un enfoque que permita de manera secuencial y sistemática su aplicación con el fin de cumplir con cada uno de los elementos que la conforman.

La metodología a utilizar para la presente investigación será contemplada en cinco (5) fases que se darán de forma secuencial, y detallada todo ello con el fin de tener una comprensión de los pasos a desarrollar desde el punto de vista tanto metodológico como conceptual, pues un proyecto de esta envergadura incorpora capital humano, tiempo y recursos así a su vez el respaldo por parte de la alta dirección, considerado un requisito esencial para el cumplimiento de los objetivos previstos [44].

A continuación, se explica cada una de las fases detalladas en esta metodología:

A. Fase 1: Análisis del contexto de la Organización

Considerando que un proyecto de SGSI no solo tiene implicancias en el área de tecnología de la información de la empresa, sino que es un proyecto que considera a toda la organización, por lo que requiere el tener aceptación y sobre todo el ayudar con el fin de una adecuada implementación. Es por ello que se consideran las siguientes actividades:

• Prioridades para un SGSI: Tomando en cuenta elementos como: Objetivos estratégicos de la organización [44].

• Definir el alcance preliminar del SGSI: Definiendo lo que se desea proteger y en base a esto se realiza la determinación de forma preliminar del alcance [44].

• Creación del proyecto [44].

B. Fase 2: Definición del Alcance

Contempla los siguientes elementos:

• Definición del alcance: Este elemento permite establecer la delimitación del proceso de gestión de riesgos, poniendo énfasis a todo el proceso que se da en la implementación del SGSI.

• Axioma de la política y objetivos de seguridad [45]

• Aprobación de la Dirección: Que consiste en la obligación de la Dirección, mediante el refuerzo que ésta realiza del establecimiento de las diferentes políticas y de los objetivos del cuidado de la información.

C. Fase 3: Elaboración de Política y propuesta de Objetivos

Conforme a lo que se establece en la norma ISO 27001 [27], con el objetivo de establecer los requisitos de seguridad de la información es necesario contar con cinco elementos a identificar los cuales son:

a) Conjunto de activos de información importantes que posee la organización.

b) Cuál es la posición de la organización y cuáles son sus consecuencias.

c) Formas recientes y actuales de procesamiento de información como son las redes, aplicaciones y recursos de TI.

d) Los requisitos de tipo legal, reglamentario, obligaciones de tipo contractual, normas que se desarrollan en la industria, acuerdos tanto con clientes como con proveedores.

e) Lo que posee la empresa.

D. Fase 4: Evaluación y Tratamiento de Riesgos

Vemos la existencia de otros modelos que permiten esta evaluación, entre los cuales se encuentran: MAGERIT, OCTAVE, NIST SP 800-30, CRAMM, MEHARI, FAIR, RISK FOR COBIT 5.0. En nuestro trabajo nos apoyaremos en la metodología Octave Allegro [32]. Para ello se debe tener en cuenta:

• Establecimiento de contexto: Mediante la identificación y establecimiento de parámetros de evaluación de riesgo de tipo racional y fácil de utilización durante todo el proceso de implementación del SGSI.

• Parámetros de probabilidad: Mediante el establecimiento de una tabla de frecuencias de las amenazas que posiblemente se susciten e indicando los niveles que se requieren conforma al tipo de organización y las necesidades que esta posea.

• Parámetros de impacto: Generado a partir de las diversas consecuencias que tiene cualquier tipo de amenaza de la información.

• Determinación de la vulnerabilidad: Que identifica cuan sensible se encuentra la organización ante una amenaza materializada relacionada con la información empresarial.

• Criterios de aceptabilidad del riesgo: Que permite determinar si un riesgo es aceptable para la organización conforme a los parámetros previamente establecidos por la misma.

• Valoración del riesgo: La cual incluye fases como el identificar escenarios de riesgo, estimar el riesgo y evaluar el riesgo.

• Evaluación del riesgo: Que se refiere a la comparación entre las vulnerabilidades como resultado.

• Tratamiento del riesgo: Que mediante el establecimiento de acciones mediante controles propuestos permite desplazar al riesgo a un nivel que es aceptable dentro de la organización.

E. Fase 5: Documentar la Información del SGSI

Esta fase, contempla tres componentes que incluye la parte documentaria, el implementar la SI [27].

Resultados y discusión

Los principales resultados encontrados son:

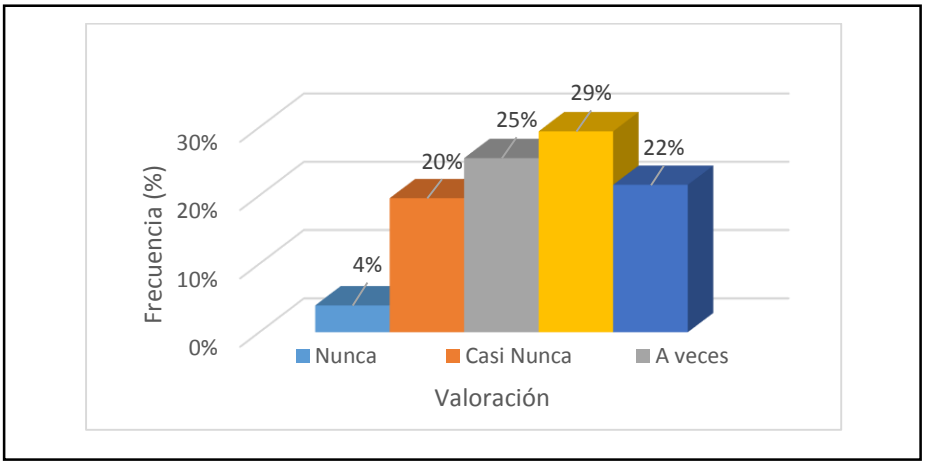

Figura 1: Cifras de incidentes reportados relacionados con la seguridad de la información

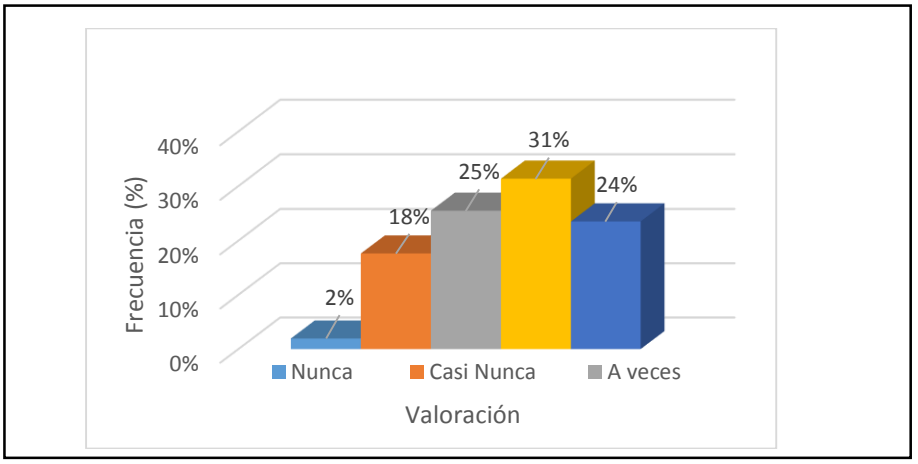

Figura 2: Incidentes reportados relacionados con la seguridad de la información que afectan su área de trabajo

Conforme a los resultados obtenidos y reflejados en la figura 2, tenemos que el 55% de los encuestados consideran que casi siempre y siempre con los problemas de la información dentro de la empresa, afectan de manera directa e indirecta a su área de trabajo. Además, que solo el 20% consideran que nunca y casi nunca estos incidentes afectan a su área de trabajo.

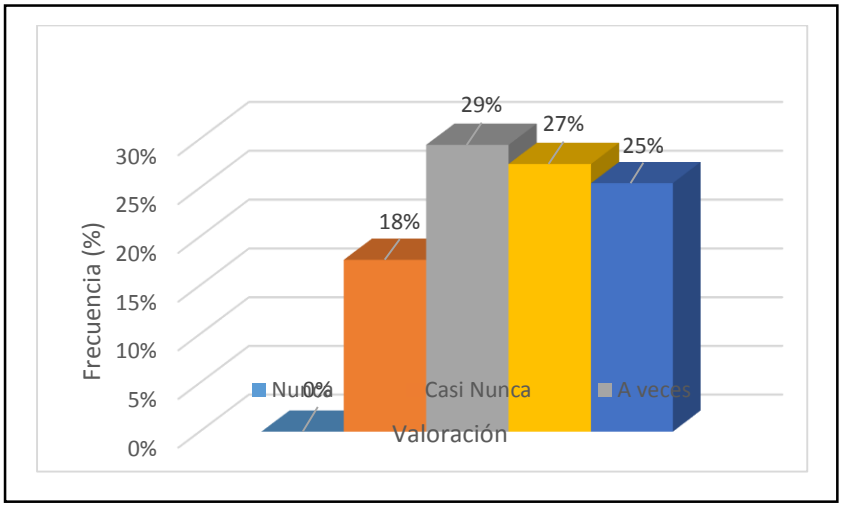

Figura 3: Acciones concretas realizadas para dar solución a un incidente relacionado con la seguridad de la información

La figura 3 nos muestra que el 52% de los encuestados casi siempre y siempre ante la presencia de un incidente relacionado con la seguridad de la información toma algún tipo de acción con el fin de poder solucionarlo. Mientras que el 18% menciona que casi nunca y un 29% indica que a veces lo hace.

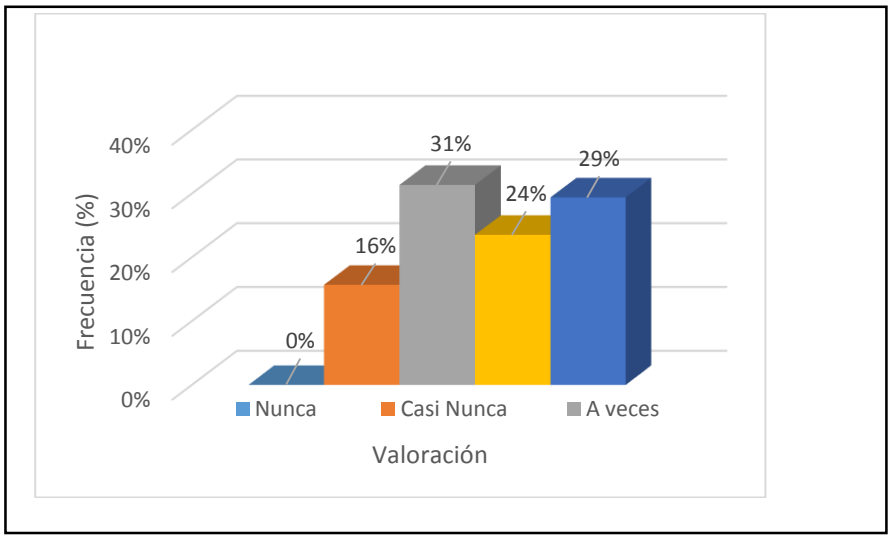

Figura 4: Cumplimiento de las políticas y directivas establecidas por la empresa en cuanto a seguridad de la información

La figura 4, nos indica que en cuanto al cumplimiento por parte del personal de las políticas y directivas que la empresa ha establecido en cuanto a seguridad de la información, tenemos que el 53% de los encuestados menciona que casi siempre y siempre cumple con estas políticas y directivas, mientras que el 16% menciona que casi nunca y un 31% menciona que a veces las cumple.

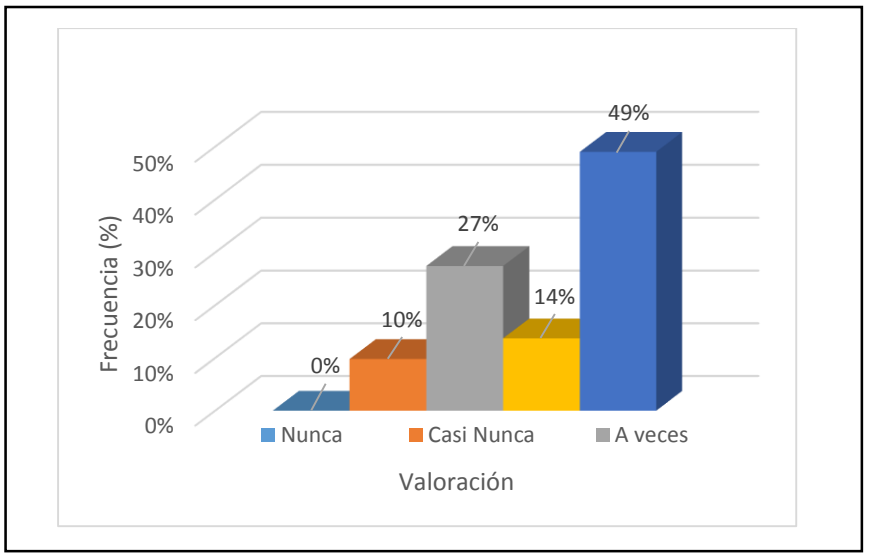

Figura 5: Herramientas brindadas por la empresa para salvaguardar sus bienes en cuanto a la seguridad de la información

La figura 5 muestran que el 63% de los encuestados considera que casi siempre y siempre es necesario recibir por parte de la empresa todas las herramientas necesarias para salvaguardar los bienes de la empresa en cuanto a seguridad de la información. Mientras que un 10% menciona que nunca es necesario recibir estas herramientas.

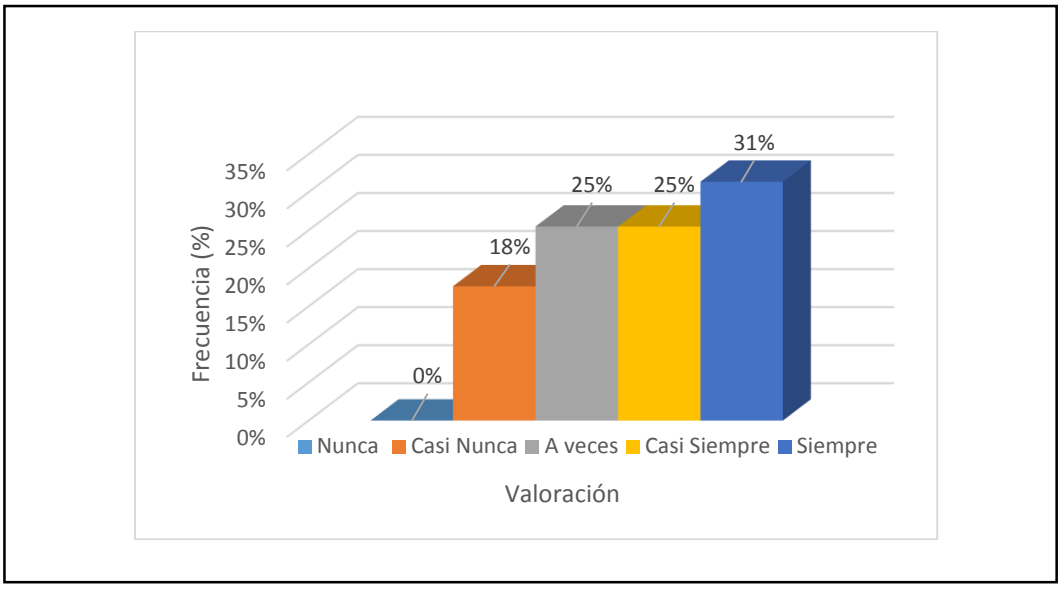

Figura 6: Existencia de niveles de riesgos en la información que pueda ser vulnerada

Los resultados de la figura 6 nos muestra que el 56% de los encuestados menciona que dentro de la empresa existe un alto nivel de riesgo en que la información que posee sea vulnerada, mientras que un 25% menciona que a veces existe este alto nivel de riesgo, además solo el 18% menciona que casi nunca se da.

Propuesta

Actualmente las organizaciones son, cada vez, más dependientes de las Tecnologías de la Información, teniéndose en ese contexto, que cualquier problema que se suscite, por mínimo que sea, llega a comprometer los procesos y operaciones de dichas organizaciones, que, por ende, se traduciría en pérdidas económicas y financieras. Ante este escenario, la Seguridad de la Información llega a convertirse en una labor a nivel institucional y no solamente del área de sistemas o tecnologías de la información.

La Gerencia de la organización, gerencias de área, de sucursales y la Alta Dirección han considera optar por esta propuesta de un sistema de Gestión de Seguridad de la Información en Empresa Comercializadora de Lubricantes. Dicho sistema formará parte de los sistemas de gestión institucionales (Comercial) y se ha fundamentado en la norma ISO 27001, que establece el marco de referencia acerca de las buenas prácticas en seguridad de la información de las organizaciones.

"Este Sistema de Gestión de Seguridad de la Información cubre once dominios de la norma ISO/IEC 27001 con la finalidad de salvaguardar la información, sistemas de información, procesos y personas de la Empresa Comercializadora de Lubricantes", siendo estos:

1) Política de Seguridad: Es donde se estipulan las políticas con respecto a la seguridad de la Información para la organización.

2) Organización de la seguridad de la información: Busca administrar la seguridad dentro de la organización (Roles, compromisos, autorizaciones, etc.).

3) Gestión de activos: Referido al mantenimiento y protecciones apropiadas de todos los activos de información.

4) Control de accesos: Busca controlar el acceso a la información, así como el acceso no autorizado a los sistemas de información y computadoras. De igual forma, detecta actividades no autorizadas.

5) Seguridad física y ambiental: Destinado a prevenir accesos físicos no autorizados (perímetro), daños o interferencias a las instalaciones de la organización y a su información.

6) Asegurar las operaciones.

7) Mantenimiento de sistemas y soporte

8) Relación con los proveedores: Para asegurar la protección de los activos de la organización que son accesibles a los proveedores, dentro de las actividades y relaciones comerciales propias de la gestión.

9) Gestión de incidentes en la seguridad de información: Permitir que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, sean comunicadas de tal manera que se tome una acción correctiva adecuada en el momento indicado.

10) Aspectos de seguridad de información en la gestión de continuidad del negocio: Dominio enfocado en reaccionar en contra de interrupciones a las actividades de la organización y en proteger procesos críticos de los efectos de fallas mayores en los sistemas de información o desastres, y asegurar que se resuelvan a tiempo.

11) Cumplimiento: Destinado a prevenir el incumplimiento total o parcial de cualquier ley, norma, regulación u obligación contractual de los requerimientos de seguridad.

Se excluyó el dominio de "A.7. Seguridad de los Recursos Humanos", ya que actualmente la organización cuenta con sus propios controles para obtener la información referente al personal actual y nuevo (a ingresar), así como los procesos de capacitación y procesos disciplinarios, gestionando lo necesario ante el cese de cualquier colaborador, respecto a sus accesos a los sistemas de información de la organización.

Se excluyó el dominio de "A.10. Criptografía", ya que actualmente la organización cuenta con sus propios controles para proteger y no divulgar la información confidencial que maneja (uso de claves y contraseñas); es por ello que por el momento no es necesario utilizar controles criptográficos en la información confidencial, aunque más adelante sería lo más apropiado implementarlos con mayor complejidad.

Se excluyó el dominio de "A.13. Seguridad de las comunicaciones", ya que la organización cuenta con controles que aseguran la información transferida a través de las redes tanto internas como externas, hacia sucursales y proveedores.

Como el Sistema de Gestión de la Seguridad de la Información (SGSI), es de aplicación a toda organización, en este caso, se enfocará en las áreas cuyos procesos son críticos.

Las siguientes áreas están incluidas dentro del alcance del SGSI por su interacción con el sistema y el nivel de criticidad de los procesos que se desarrollan dentro de ellas:

- Gerencia de Comercialización.
- Gerencia de Administración
- Gerencia de Sistemas
- Gerencia General

Política del Sistema:

a. Generalidades

Para la Empresa Comercializadora de Lubricantes existe una serie de valores que se relacionan con la seguridad, además garantiza la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la organización.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional. Para esto, se debe asegurar un compromiso manifiesto de la alta Dirección de la organización y de las áreas y/o divisiones para la difusión, consolidación y cumplimiento de la presente Política.

b. Objetivo.

 Proteger los recursos de información de la organización y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

 Mantener la Política de Seguridad de la Información actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

c. Responsabilidad

Todos los Gerentes, Jefes de Áreas y personal operativo y sea cual fuere su nivel jerárquico son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Empresa Comercializadora de Lubricantes, cualquiera sea su situación en la misma, el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

d. Base legal

 "Resolución Ministerial Nº 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del sistema nacional de informática".

e. Cumplimiento obligatorio

El cumplimiento de las políticas y estándares definidos en el presente documento de Información es obligatorio y debe ser considerado como una condición en los contratos del personal.

La organización (Empresa Comercializadora de Lubricantes) puede obviar algunas de las políticas de seguridad definidas en este documento, únicamente cuando se haya demostrado claramente que el cumplimiento de dichas políticas no tendría un impacto significativo e inaceptable para el negocio. Toda excepción a las políticas debe ser documentada y aprobada por el Área de Sistemas, detallando el motivo que justifica el no cumplimiento de las políticas establecidas en el presente plan.

f. Definiciones

Para la mejor comprensión de los términos y contenido del plan, se detallan las siguientes definiciones:

 Factor de autenticación: Información utilizada para verificar la identidad de una persona. Pueden clasificarse de la siguiente manera:

 Algo que el usuario conoce (por ejemplo: una clave de identificación o una tarjeta)

 Jefe de Sistemas: Es la persona encargada de coordinar los esfuerzos de administradores de sistemas, administradores de seguridad y dueños de información.

 Encargado de Soporte: Es la persona encargada del sistema y día a día coordina el correcto funcionamiento de servidores y medios de almacenamiento.

 Dueño de la información (usuarios): Es la persona que se encargada de definir cuáles son las formas de uso de información y los comportamientos que se esperan de las personas que tienen acceso a la misma.

 Usuario Final: Persona que recibe y utiliza la información para producir un resultado esperado o no, tiene acceso tanto a la información como a los sistemas que la procesan.

 Política de seguridad de TI: Normas aprobadas por el Directorio para establecer la gestión de seguridad de TI, sus metas y responsabilidades; reglas de seguridad específicas a sistemas particulares.

 Evaluación de riesgos: Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de la entidad.

 Incidente de Seguridad: Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o amenaza de romper los mecanismos de seguridad existentes.

La Empresa Comercializadora de Lubricantes, inicia sus operaciones en la ciudad de Chiclayo en el año 1995, su giro de negocio es la comercialización y distribución de neumáticos Goodyear y lubricantes de la marca Repsol, tiene movimiento comercial en las siguientes ciudades: Trujillo, Chimbote, Jaén, Cajamarca y Chiclayo.

Dentro de este contexto la Empresa Comercializadora de Lubricantes adoptará, aceptará, aprobará, cumplirá, revisará y actualizará el plan de gestión en seguridad de información el mismo que será acorde con los lineamientos y objetivos de la entidad.

Dicho plan se encuentra basado en un enfoque de riesgo operativo; para establecer, monitorear, revisar, mantener y mejorar la seguridad de la información con la finalidad de buscar mantener la confidencialidad, integridad y disponibilidad sobre los activos de información propiedad de la Empresa Comercializadora de Lubricantes.

Es importante resaltar las siguientes definiciones basadas en el estándar NTP ISO/IEC 27001.

La Empresa Comercializadora de Lubricantes declara:

1. El compromiso por parte de todos los niveles de la entidad en adoptar, aceptar, aprobar, cumplir, revisar y actualizar las políticas, lineamientos y controles que forman parte del Sistema de gestión de Seguridad de Información.
2. El compromiso de identificar claramente en el ámbito de la seguridad los roles, responsabilidades y sanciones por incumplimiento por parte del personal y terceros.
3. El compromiso de conformar el Comité de gestión de seguridad de información el mismo que mantendrá una participación activa de acuerdo a sus roles y responsabilidades.
4. El compromiso de adoptar, aceptar, aprobar, ejecutar y revisar periódicamente una o varias metodologías formales de análisis.
5. El compromiso en implantar, monitorear y gestionar el riesgo operativo y de información mediante los controles administrativos y tecnológicos que la Empresa
6. El compromiso de elaborar, mantener y ejecutar periódicamente programas de capacitación, concientización y entrenamiento en temas de seguridad de información dirigido al personal y terceros.
7. El compromiso de auditar periódicamente.
8. Entender que es necesario mantener un compromiso diario con las actividades relacionadas con la seguridad de información.

Por lo expuesto:

La Empresa Comercializadora de Lubricantes en todos sus niveles de Organización declara su firme compromiso en adoptar, aceptar, aprobar, cumplir, monitorear, revisar y actualizar el plan de gestión de seguridad de información en conformidad al marco de referencia NTP ISO/IEC 27001. Chiclayo, XX de setiembre 2020.

Definición del alcance y límites del proceso de Gestión del Riesgo en Seguridad de la Información.

Consideraciones Generales

a). Marco estratégico institucional

El Plan estratégico de la organización detalla el siguiente marco estratégico:

Visión:

Brindar calidad en todos los productos y servicios que ofrecemos en nuestras estaciones, sucursales y establecimientos, con la finalidad de satisfacer eficientemente las necesidades de nuestros clientes y ser la mejor representación de nuestros socios estratégicos.

Misión:

Ser la empresa líder en la comercialización minorista de combustible y lubricantes en la región norte y principal referente de excelencia del rubro, expandiendo operaciones comerciales a nivel macro regional en los próximos tres años mediante alianzas estratégicas

Valores:

- Compromiso con nuestros clientes.
- Eficiencia.
- Respeto.
- Responsabilidad.
- Trabajo en equipo.

Diagnóstico institucional

i. Estructura y Organización

Detalle según MOF

ii. Modelo de Gestión

Empresa Comercializadora de lubricantes, utiliza dentro de su Modelo de Gestión: Estrategias Competitivas y Estrategias de Crecimiento.

Su estrategia competitiva, es la de ser la empresa líder en cada uno de sus unidades de negocio con respecto a sus competidores, por ese motivo busca que sus clientes le perciban como la empresa comercializadora más óptima y eficiente.

Para lograr esta estrategia es necesario identificar quienes ofrecen los productos y servicios en el mercado, analizar sus precios y descubrir cuál es valor agregado de la competencia, que les genera ventaja y cuáles son sus factores críticos de éxito, después del análisis, tomar decisiones para establecer actividades de diferenciación.

La estrategia de crecimiento adoptado por Empresa Comercializadora de lubricantes en la región norte se da gracias a las sólidas alianzas con reconocidas empresas como: Repsol y GoodYear quienes nos ofrecen el prestigio de sus marcas y la red de contactos de sus principales clientes.

El plan de acción es mantener excelentes relaciones con nuestros socios, alineados a sus objetivos y buscando la mejora continua.

iii. Documentos de Planeamiento

En DSD Representaciones SAC, los documentos de planeamiento se centran en su cadena de valor, considera macro proceso al nivel 0 o nivel inicial, que agrupa a los procesos misionales, estratégicos y de soporte.

Los procesos misionales son los procesos Core del negocio es decir la razón de ser de la empresa. Para DSD Representaciones SAC es la gestión comercial DSD (lubricantes y neumáticos).

Los procesos estratégicos son los procesos que necesariamente deben existir para el desempeño eficiente de los procesos misionales. En DSD Representaciones SAC son: la gestión administrativa, que realiza el planeamiento estratégico de la organización, la gestión de marketing que propone campañas, promociones y es el canal principal de comunicación, la gestión de calidad, que a través del diseño de procesos y planes para la mejora continua permite el crecimiento de la empresa y por último la gestión de control, que a través de auditoría permite identificar y evitar las vulnerabilidades de la empresa.

iv. Instrumentos de Gestión

La empresa cuenta con instrumentos de gestión tales como:

- MOF (Manual de Organización y Funciones
- Reglamento Interno de Trabajo (RIT)
- Reglamento Interno de Seguridad y Salud en el Trabajo (RISST)
- Organigrama

"Este Sistema de Gestión de Seguridad de la Información cubre doce dominios de la norma NTP-ISO/IEC 27001:2014 con la finalidad de salvaguardar la información, sistemas de información, procesos y personas de la Empresa Comercializadora de Lubricantes".

Del mismo modo el Sistema de Gestión de la Seguridad de la Información (SGSI), es de aplicación a toda la organización, pero, se enfocará en las áreas críticas de la misma.

Las siguientes áreas están incluidas dentro:

- Gerencia de Comercialización
- Gerencia de Administración
- Gerencia de Sistemas
- Gerencia General

Lista de restricciones que afectan a la organización

Se muestra las restricciones que afectan a la organización (empresa comercializadora de lubricantes) y que determinan su orientación en lo que a seguridad de la información se refiere. Las fuentes de estas restricciones pueden ser internas (que se pueden controlar de cierta manera) y externas, las cuales no serían controlables por la organización.

a) Restricciones de naturaleza política

Cuando éstas provienen de organismos gubernamental a través de normas y/u ordenanzas de índole municipal, regional o nacional.

b) Restricciones estructurales

Podría ser que la organización no cuente, dentro de su estructura, con el área responsable de la gestión de la seguridad de la información.

c) Restricciones funcionales

Cuando las tareas acerca de la seguridad de la información no han sido definidas correctamente.

d) Restricciones respecto al personal

No se han establecido mecanismo de capacitación y/o evaluación del conocimiento del personal de la organización acerca de sus actividades en lo que a seguridad de la información se refiere.

e) Restricciones de naturales cultural

Se generan cuando se tiene hábitos incompatibles con los controles en la seguridad de la información. Estar acostumbrado a realizar actividades que no son las habituales en este ámbito.

f) Restricciones presupuestales

Lista de referencias legislativas y regulatorias aplicables a la organización

a) Regulación a la que se somete

Ley general de sociedades (Ley 26887)

Ley orgánica de Hidrocarburos (Ley 26221)

Leyes tributarias (SUNAT y Municipalidad)

Directivas y Normas de la organización

b) Estándares internacionales

Se recomienda que la organización pueda tener el conocimiento, a través de las áreas correspondientes, acerca de los siguientes documentos:

COBIT (Objetivos de Control para la Información y Tecnología relacionada): Buenas prácticas para el trabajo de dominios y procesos.

ITIL (Biblioteca de Infraestructura de Tecnologías de la Información): Mejores prácticas destinadas a facilitar entrega de servicios de TI de alta calidad.

c) Estándares y regulaciones nacionales

i. Norma Técnica Peruana ISO/IEC 27001:2014. Constituye la norma principal de la serie y contiene los requisitos del SGSI. En su Anexo A, detalla de manera resumida los objetivos de control y controles que desarrolla la ISO 27002:2013, que pueden ser seleccionados por las organizaciones para el desarrollo del SGSI.

ii. ISO/IEC 27002:2013. Constituye una guía de buenas prácticas que detalla los objetivos de control y controles recomendables en lo que a seguridad de la información se refiere. Contiene 35 objetivos de control y 111 controles, agrupados en 14 dominios.

Lista de restricciones que afectan el alcance

También se han considerado las restricciones que tienen un nivel de impacto en el alcance del SGSI. Éstas se añadirán a las restricciones de la organización que se han considerado anteriormente y que pueden incluso reformarlas. Se presentan:

Restricciones técnicas:

• Por ejemplo, las Redes de comunicación que no se adecuan a los estándares establecidos.

• Problemas en el fluido eléctrico, de acuerdo a la zona de ubicación de la organización, puede ser con mayor o menor frecuencia.

• Estructura del área de TI inadecuada, cuando se ha considerado, posiblemente desde que inició actividades la organización, una estructura de TI que no se adapta al crecimiento organizacional o no lo contempló en sus inicios.

Restricciones temporales

• El tiempo es considerado un factor determinante para tomar las decisiones respecto a las soluciones y prioridades. Si los tiempos de implementación son muy extensos, los riesgos para los que se ha diseñado el control pueden haber variado.

Criterios básicos

Criterios de evaluación del riesgo

Los criterios de evaluación del riesgo se desarrollaron para evaluar el riesgo de seguridad para la información en la organización, teniendo en consideración lo siguiente:

• El valor estratégico del proceso de información institucional.
• Las expectativas y percepciones de los grupos de interés.
• Las consecuencias negativas para el buen nombre y la reputación, ante cualquier eventualidad.

Adicionalmente se utilizan tablas y mapas de riesgos para formar los criterios de evaluación del riesgo con la finalidad de dar prioridades para el tratamiento del mismo (riesgo).

Criterios de impacto

Consiste en cuantificar el valor de impacto en términos del grado de daño (principalmente en costos) para la organización causados por un evento en contra de la seguridad de la información. Para ello, se tendrá en consideración lo siguiente:

• Nivel de clasificación del activo de información impactado.
• Infracciones a la seguridad de la información (por ejemplo, pérdida de confidencialidad, integridad y disponibilidad)
• Operaciones impedidas (internas o de terceros)
• Lucro cesante y valor financiero.
• Perturbación de los planes y plazos.
• Daño a la reputación.
• Infracciones de estipulaciones legales, regulatorias o contractuales.

Criterios de aceptación del riesgo

Los criterios de aceptación del riesgo dependen de los intereses, políticas, metas, objetivos de los interesados en la organización. Por lo que la empresa Comercializadora de lubricantes ha definido sus propias escalas para los niveles de aceptación del riesgo. El criterio de aceptación del riesgo obedecerá a la matriz de riesgos relativos (que se detalla a continuación) y donde quede ubicado después del análisis respectivo.

Requisitos de seguridad: Son los que determinan cómo debe estar protegido un activo de información. Estos también se denominan a menudo "objetivos de seguridad": confidencialidad, integridad y disponibilidad.

La metodología OCTAVE Allegro toma en cuenta los activos de información de la organización, por eso, en este paso comienza el proceso de crear un perfil para esos activos. Un perfil es una representación de un activo de información que describe sus características únicas, cualidades y valor. El proceso de creación de perfiles garantiza que un activo se describa de forma clara y coherente, que existe una definición inequívoca de los límites del activo y que los requisitos de seguridad para los activos están adecuadamente definidos.

Los activos que se identificaron dentro de la empresa investigada son:

 Base de datos (Gestor de Base de Datos SQL Server 2008 R2 y 2014, con un tamaño aproximado de 5GB)
 Correo electrónico (Cuentas ilimitados HostDime)
 Sistema de Información Comercial (Sistema principal del negocio)
 Documentación (Generados por los diversos sistemas y que son almacenados en diversos dispositivos físicos y lógicos por su importancia)
 Directorio (Manejo de cuentas de cuentas principales, Contactos de proveedores e información personal de los colaboradores)
 Control de acceso
 Servidor de aplicaciones (Servidor HP Proliant ML350 Gen9)
 Servidor de pruebas (Servidor virtual para testeos de desarrollos)

Identificación de amenazas

En la metodología utilizada se determinan las áreas de preocupación que es una declaración descriptiva.

Para identificar las áreas de preocupación se comienza con elaborar los perfiles de riesgos de los activos de información, los cuales contendrán un componente denominado amenaza a través de una ecuación de riesgo.

Amenaza (condición) + Impacto (Consecuencia) = Riesgo

DISCUSIÓN

Para realizar la discusión de la presente investigación se consideraron tanto los resultados obtenidos, los antecedentes consultados y las bases teóricas expuestas dentro de esta investigación.

Iniciando la discusión tenemos los resultados obtenidos en la tabla XII y figura 18 con relación a que, si los colaboradores reciben por parte de la empresa capacitaciones constantes que permita brindarles conocimiento y tomar conciencia en cuanto a la seguridad de la información dentro de su empresa, los resultados muestran que el 32% de los encuestados nunca y casi nunca las reciben, mientras que el 29% menciona que a veces la empresa lo realiza, podemos relacionar estos resultados con lo mencionado por Ararat [16], quien concluye en que las principales amenazas detectadas en cuanto a la seguridad de la información tienen estrecha relación con las decisiones tomadas e inversiones realizadas por los directivos de la empresa en estudio, sumada a la falta de capacitaciones en temas que consideren los riesgos de la información, lo cual ocasiona que los usuarios no conozcan el cómo deben de actuar frente a una amenaza en la seguridad de la información de la empresa; esto tiene relación de la teoría mencionada por Rivero y Gómez [27], quienes mencionan dentro de las fases del SGSI es necesario el formar y concienciar al personal de la empresa y está formación se da mediante la capacitación frecuente de los usuarios acuerdo al tipo de funciones que estos realicen.

Según los resultados obtenidos en la Tabla VI y Figura 12 vemos que el 51% de los encuestados consideran que casi siempre y siempre dentro de su empresa se generan cifras elevadas de incidentes relacionados con la seguridad de la información, mientras que un 25% menciona que esas incidencias suceden a veces. Este resultado lo podemos relacionar con la investigación de Yañez [17] quien concluye que es necesario que dentro del desarrollo de los software que realicen las empresas, sean considerados aspectos relacionados a la seguridad de la información, pues le permite a la empresa hacer frente a los posibles incidentes y amenazas los cuales es necesario a medida de los recursos que posee la empresa el que sean los menos frecuentes, lo mencionado tiene el respaldo de la teoría considerada por Imbaquingo, Pusdá y Jácome [26], quienes en su teoría manifiestan que la seguridad de la información, se refiere al análisis de los riesgos, amenazas y buenas prácticas las cuales exigen ciertos niveles que aseguren los procesos que se dan en dentro una empresa, además de la tecnología con la que ésta cuenta, todo ello con el fin de elevar los niveles de confianza en el manejo de la información dentro de la empresa.

Los resultados de la tabla XVIII y la figura 24 muestran que el 27% de los encuestados consideran que la empresa donde laboran casi nunca realiza un control riguroso en cuanto a acceso a la información que ésta posee. Además, un 27% de los encuestados menciona que solo a veces la empresa realiza algún tipo de control en cuanto a este tipo de acceso, esto nos permite ver la investigación de Casadesús [18] donde concluyo que la gestión del riesgo implica el anticiparse a lo que puede salir mal y prevenirlo mediante acciones de tratamiento, además de llevar un control adecuado y riguroso de la información que esta posee. El tratar la gestión del riesgo influye en otros ámbitos de la organización contribuyendo a la mejora

global de la misma pues es necesario estudiar la gestión del riesgo de perspectivas diferentes que se puedan complementar, esto podemos relacionarlo con la base teórica mencionada por Gómez [25], quien menciona que las organizaciones, para proteger su información derivada de sus actividades, deben establecer adecuados controles y estrategias que hagan segura la gestión de los procesos del negocio.

En cuanto a los resultados de la siguiente tabla XVI y figura 22 se muestra que el 30% de los encuestados menciona que la empresa nunca y casi nunca comunica a sus colaboradores cuales son los controles que deben de tomar en cuenta para no poner en riesgo tanto el software como el hardware que utilizan, mientras que un 24%considera que a veces existe este tipo de comunicación, esto es evidenciado por la investigación de Santos [19], quien concluye que un SGSI tiene beneficio para toda la organización, puesto que varias de las actividades y controles gestionados tiene un alcance de forma general dentro de la empresa, para ello es necesario identificar los puntos críticos o sensibles según la información que la organización maneja, con el fin de poderlas comunicar a los colaboradores a fin de que tomen acciones que puedan hacer frente a los posibles riesgos a suscitarse, todo ello lo podemos respaldar con lo mencionado por Imbaquingo Pusdá y Jácome [31], en relación al cálculo del riesgo dentro de una organización pues es necesaria la identificación y la valoración del riesgo, utilizando diversidad de técnicas o métodos secuenciales y sistemáticos como son las entrevistas, encuestas, análisis FODA, todo ello permite que las empresas puedan tomar acciones para controlar los posibles riesgos que se puedan dar dentro de estas, además de que esto sea transmitido a sus colaboradores.

Los resultados de la tabla X y figura 16, nos muestran que el 16% de los encuestados manifiesta que casi nunca la empresa donde labora establece políticas y directivas necesarias y oportunas que permitan mantener la seguridad de la información en todos los procesos de la empresa, mientras que un 37% menciona que a veces las establece de manera oportuna; esto es corroborado por lo investigado por García [22] quien concluyo de que muchas empresas no cuentan con políticas y controles de seguridad definidos con el fin de proteger su información, además es necesario proponer un modelo de seguridad de la información basados en metodologías adaptadas a la situación, giro y tamaño de la empresa, permitiendo establecer medidas de mejora en cada uno de sus procesos a través de las políticas y directivas generadas por quienes dirigen la empresa, esto es corroborado por la teoría planteada por Deming [28], con relación a la mejora continua que se debe de establecer en el desarrollo de los procesos de la empresa, pues se basa en el trabajo en equipo, además que se encuentra orientado hacia la acción, dirigiendo los esfuerzos de quienes la componen a la perfección, la mejora continua está inmersa tanto en el implantar un sistema como el aprendizaje continuo de la organización, esto implica que los miembros de una organización tengan una participación activa en todo el proceso de implementación de un SGSI.

Los resultados de la tabla VIII y figura 14, nos muestran que el 22% de los encuestados considera que casi nunca la empresa donde labora atiende de manera oportuna los incidentes relacionados con la seguridad de la información que se presentan, todo ello con el fin de realizar una gestión del riesgo efectiva, mientras que un 37% considera que a veces estos incidentes solo son atendidos oportunamente, podemos relacionar estos resultados con la investigación de Moscoso, Peña y Soto [24], quienes indican que la gestión del riesgo permite mejorar la efectividad en cuanto a la toma de decisiones de la empresa, pues es necesario que esta tome decisiones de carácter proactivo a fin de evitar un comportamiento de tipo reactivo , esto nos permite ver lo importante que es para la empresa él tomar medidas oportunas, esto es corroborado por la teoría sobre gestión del riesgo según Casares y Lizarzaburu [29], quienes indican que ésta es considerada como como una etapa importante y fundamental en la evaluación tanto financiera como económica en las empresas, pues se trata de un enfoque documentado y muy riguroso en los diferentes niveles de desarrollo de las actividades que se realizan en la organización, para lo cual resulta oportuno el contar con la información de las diferentes áreas de interés tanto internas como externas de la empresa,

por tanto es necesario realizar de manera oportuna la evaluación del riesgo dentro de la organización.

Conclusiones

1. Ante el diagnóstico realizado a la situación actual de la seguridad en la información de la empresa en estudio, se ha podido concluir que ésta no se da de la manera adecuada, pues no se tienen protocolos formales establecidos, si bien es cierto la empresa aplica algunas medidas que permiten en cierta manera salvaguardar su información, esta no resulta suficiente para hacer frente a los posibles riesgos a generarse.

2. En cuanto a la determinación de cómo se desarrolla actualmente la gestión de riesgos dentro de la empresa en estudio, se tiene que existen altos índices de incidencias relacionados a la seguridad de la información, lo cual afecta las operaciones de la empresa y el desempeño del personal, además al momento de que estas se generan no son atendidas de manera oportuna por los encargados de tomar las decisiones importantes dentro de la misma, no habiendo acciones por parte de la empresa como capacitaciones en cuanto a cómo deben de gestionar el riesgo. Todo ello permite evidenciar un nivel de riesgo alto lo cual pone a la empresa en un estado de vulnerabilidad.

3. En cuanto al establecimiento de planes de acción en la seguridad en la información los cuales permitan la disminución de los niveles de riesgo con relación a los activos de la información, se ha considerado la presentación de una propuesta de un Sistema de Gestión de seguridad de la información la cual se encuentra basada en el ISO 27001, que establece el marco de referencia acerca de las buenas prácticas en seguridad de la información de las organizaciones, ésta propuesta que ha sido realizada a partir de los datos obtenidos en la presente investigación, los cuales servirán como referente para los directivos de la empresa con el fin de que tomen decisiones que permitan mejorar su gestión del riesgo.

4. En cuanto a la validación de la propuesta que plantea la investigación, ésta será realizada por expertos en la materia, lo cual permitirá tener una propuesta fiable, confiable y con sustento teórico necesario para ser presentado a los directivos de la empresa en investigación.

Recomendaciones

1. Es importante se defina un protocolo inmediato para salvaguardar la información de la empresa, es por ello que la propuesta aplicada permitirá se ejecute esta acción; por tanto, se sugiere su inmediata adaptación para hacer frente a los riesgos de pérdida de datos.

2. Debe aplicarse un programa de prevención de situaciones de riesgo que permita atender de manera inmediata cualquier situación con el personal y los sistemas, los responsables deben de prevenir mediante capacitaciones al personal sobre la gestión del riesgo, así se puede reducir el nivel de vulnerabilidad que tenga la empresa.

3. Implementar la propuesta del Sistema de Gestión de seguridad de la información que se ha establecido sobre el ISO 27001, esto asegurará las buenas prácticas en la empresa, para ello se debe de tomar la información y datos obtenidos para que pueda entregarse de forma constante a los directivos de la empresa.

4. Es importante se realice una prueba inicial antes de poder lanzar del todo la propuesta, debe ejecutarse por etapas e ir midiendo el impacto de su aplicación dentro de la empresa.

Referencias

[1] F. Valencia y M. Orozco, «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000,» Revista Ibérica de Sistemas e Tecnologias de Informação, vol. 22, pp. 73-88, 2017.

[2] L. Cárdenas, H. Martinez y L. Becerra, «Gestión de la seguridad de la información: Revisión Bibliográfica,» El profesional de la información, vol. 25, nº 6, pp. 931-948, 2016.

[3] M. Corda, M. Viñas y M. Coria, «Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje,» Palabra clave, vol. 7, nº 1, pp. 1-18, octubre 2017.

[4] N. Gianese, «6 ventajas de tener una certificación ISO 27001,» Empresa Actual, 07 marzo 2019.

[5] Observatorio de RRHH, «España, en el top ten mundial de certificaciones ISO 32010354 - pixelated acronym iso made from cubes, mosaic pattern,» OHR Grupo Editorial de conocimiento y gestión S.L, 31 octubre 2018.

[6] SGSI, «¿Cuál es la situación de la norma ISO 27001 en Sudamérica?,» SSI, 2017.

[7] Instituto Europeo de Posgrado, «Conócemos noticias,» Summa, s.f.

[8] C. Otero, «Europa tarda 147 días en resolver fallos peligrosos en aplicaciones, Asia sólo 42,» MeriStation, 2019.

[9] Cámara de Valencia, «La ciberseguridad en cifras: los datos muestran incremento en la preocupación empresarial,» Tecnología para los negocios, 2017.

[10] Risk Advisory, «Ciber Riesgos y Seguridad de la Información en América Latina & Caribe Tendencias 2019,» Deloitte, Mayo 2019.

[11] América Sistemas, «Empresas de AECE logran certificación ISO – 27001,» Julio 2018.

[12] Gestión, «Telefónica del Perú obtiene la certificación ISO 27001,» Diario Gestión, 2020.

[13] Andina, agencia Peruana de noticias, «Nuevos retos para la gestión de riesgos en las empresas,» Andina, 13 septiembre 2019.

[14] C. Guerrero, «¿Y qué pasó con la Ciberseguridad en Perú?,» Hiperderecho, 24 Octubre 2016.

[15] Presidencia del Consejo de Ministros, «Perú se adhiere al Convenio de Budapest para luchar contra la ciberdelincuencia,» 01 Febrero 2019.

[16] J. Ararat, «Diseño de un SGSI basado en la norma ISO 27001 para la empresa MA PEÑALOSA CÏA. S.A.S. sede principal Cúcuta.,» Cúcuta, 2018.

[17] N. Yañez, «Sistema de Gestión de seguridad de la información para la Subsecretaría de Economía y empresas de menor tamaño.,» Santiago de Chile, 2017.

[18] A. Casadesús, «La gestión del riesgo aplicada a la gestión de documentos y su impacto en la rendición de cuentas pública,» Barcelona, 2018.

[19] D. Santos, «Establecimiento, Implementación, Mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software.,» Lima, 2016.

[20] L. Bayona y L. Palacios, «Diseño e implementacion de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica Medcam Perú S.A.C.,» Lima, 2017.

[21] F. Cáceres, «La gestión de riesgos y su impacto en la rentabilidad de las empresas de Telecomunicaciones ubicadas en Lima Metropolitana,» Lima, 2018.

[22] S. García, «Modelo se seguridad de la información para contribuir en la gestión de las unidades ambientales de la región Lambayeque,» Chiclayo, 2018.

[23] L. Celis, «Plan de seguridad de la información aplicado a la central hidroeléctrica de Carhuquero,» Chiclayo, 2018.

[24] L. Moscoso, E. Peña y M. Soto, «Modelo de Gestión de riesgos de TI que contribuye a la operación de los procesos de gestión comercial de las empresas del sector saneamiento del norte del Perú,» Chiclayo, 2018.
[25] L. Gómez Fernández, Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes, Madrid: AENOR - Asociación Española de Normalización y Certificación, 2012.
[26] D. Imbaquingo Esparza, M. Pusdá Chulde y J. Jácome León, Fundamentos de Auditoría Informática basada en Riesgos, Ibarra, Ecuador: UTN, 2016.
[27] P. P. Rivero Fernández y L. Gómez Fernández, Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad, Madrid: AENOR - Asociación Española de Normalización y Certificación, 2018.
[28] E. Deming, Calidad, productividad y competitividad. La salida de la crisis, Madrid: Diaz de Santos, 1989.
[29] I. Casares y E. Lizarzaburu, Introducción a la Gestión Integral de Riesgos Empresariales Enfoque: ISO 31000, V. M. Saenz, Ed., Lima: Platinium Editorial S.A.C, 2016, p. 27.
[30] A. Calder y S. Watkins, A Manager´s Guide to Data Security and ISO 27001/ISO 27002, 4 ta ed., Kogan Page, 2008.
[31] D. Imbaquingo, M. Pusdá y J. Jácome, Fundamentos de auditoría informática basada en riesgos, Ibarra: Editorial UTN, 2016, pp. 113, 114, 127, 128, 130, 131, 132, 133, 134.
[32] M. Mendoza, «8 pasos para hacer una evaluación de riesgos,» Welive Security, 30 09 2014.
[33] J. Huartado, El proyecto de investigación. Comprensión holística de la metodologia y la investigación, 7 tma ed., Caracas: Ediciones Quiron, Sypai, Servicios y proyecciones para Latinoamerica, 2012.
[34] F. Arias, El proyecto de investigación, introducción a al metodología cientifica, 6 ta ed., Caracas: Editorial Episteme, 2012.
[35] R. Hernandez, C. Fernandez y P. Baptista, Metodología de la Investigación, 4ta. ed., México D.F: McGraw Hill, 2006.
[36] C. Bernal, Metodología de la investigación: para la administración, economía, humanidades y ciencias sociales, Mexico D.F: Pearson Educación, 2006.
[37] C. Fernandez, P. Baptista y R. Hernandez, Metodología de la Investigación, Mexico D.F.: Mc Graw Hill, 2014.
[38] M. Tamayo, Disccionario de investigación científica, 2da ed., Mexico DF: Limusa, 2004.
[39] J. Lopez, Proceso de investigación, 1 era ed., Caracas: Panapo, 1998.
[40] W. Cochran, Técnicas de muestreo, Mexi D.F: Editorial Continental S.A., 1972.
[41] W. Olsen, Data collection. Key debates and methods in social research., First publisehd ed., Los Angeles: Sage Publications Ltd, 2012.
[42] M. Bunge, La investigación científica, Mexico D.F: Siglo XXI, 2007.
[43] M. Tamayo, El proceso de la investigación científica, Mexico D.F: Limusa, 2004.
[44] F. Valencia, «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000,» Revista lbérica de Sistemas y Tecnologías de Información, vol. 22, pp. 73-88, 2017.
[45] A. Diaz, «Sistema de Gestión de la Seguridad de la Información,» Revista Calidad, pp. 18-20, 2010.

Anexos

ANEXO N° 01. Guía de entrevista Seguridad de la Información

Fecha: / /

Nombre del entrevistado: Empresa Comercializadora de Lubricantes

Objetivo: Diagnosticar la seguridad de la información de una empresa comercializadora de lubricantes en la ciudad de Chiclayo

Entrevista con Ingeniero de Área de Sistemas

1. ¿DSD cuenta con políticas de seguridad de información?

2. ¿Las políticas de la información revisadas, publicadas, y comunicadas al personal?

3. ¿Se realizan revisiones de las políticas y con qué regularidad?

4. ¿Existen procedimientos para la revisión de las políticas de seguridad y con qué regularidad realizan esta actividad?
5. ¿Las actividades de seguridad de la información son coordinadas por alguna persona responsable?
6. ¿Se realiza verificación de antecedentes de los candidatos al empleo?

7. ¿Se firman contratos de confidencialidad?

8. ¿Existen procesos para los cambios de cargo del personal?

9. ¿Manejan algún inventario de todos los activos de información?

10. ¿DSD cuenta con políticas en cuenta al uso de los equipos?

11. ¿Existen políticas del uso aceptable para cada tipo de información?

12. ¿Existen políticas para el uso de medios extraíbles?

13. ¿Existen controles para asegurar el acceso a páginas que no son utilizadas para las actividades diarias?
14. ¿DSD cuenta políticas para el control de acceso?

15. ¿Existen políticas para asegurar la eliminación de los accesos de los usuarios que finalizan contrato?

16. ¿Existen políticas para el uso de encriptación?

17. ¿Se han diseñado medidas de protección física para prevenir desastres naturales, ataques maliciosos o accidentes

18. ¿Tiene sistemas de control de acceso adecuados para las zonas de acceso restringido?

19. ¿Existen procesos para mantener la seguridad de bloquear, limpiar escritorios?

20. ¿Hay un sistema UPS o un generador de respaldo?

21. ¿Están documentados los procedimientos operativos?

22. ¿Están los procedimientos disponibles para todos los usuarios que los necesitan?

23. ¿Se mantienen los registros de eventos apropiados y se revisan periódicamente?

24. ¿Existe un proceso de gestión de la red?

25. ¿Existen procedimientos para la transferencia de datos a todos los empleados?

26. ¿Los empleados, contratistas y agentes firman acuerdos de confidencialidad o no divulgación?

27. ¿Están sujetos a revisión periódica estos acuerdos?

28. ¿Se incluye la seguridad de la información en los contratos establecidos con proveedores y proveedores de servicios?

29. ¿Se controla el acceso de los proveedores a los activos y la infraestructura de la información?

30. ¿Las responsabilidades de gestión están claramente identificadas y documentadas en los procesos de gestión de incidentes?

31. ¿Existe un proceso para la información oportuna de los eventos de seguridad de la información?

32. ¿Existe un proceso para revisar y tratar los informes de manera oportuna?

33. ¿Existe un proceso para asegurar que los eventos de seguridad de la información sean debidamente evaluados y clasificados?

34. ¿Está incluida la seguridad de la información en los planes de continuidad de la organización?

35. ¿El enfoque de las organizaciones para gestionar la seguridad de la información está sujeto a una revisión independiente regular?

ANEXO N° 02. GUIA DE OBSERVACIÓN

NOMBRE DE LA EMPRESA: EMPRESA EN INVESTIGACIÓN

NOMBRE DEL OSERVADOR: Pérez Sandoval, Mario Iván

GIRO DE LA EMPRESA: COMERCIALIZADORA DE LUBRICANTES

OBJETIVO: Diagnosticar la seguridad en la información

ID	Dominio	CS	CP	NC	Ítems evaluados
A5	**Política de Seguridad**	**0**	**2**	**0**	**2**
	Conjunto de políticas para la seguridad de la información		x		
	Revisión de las políticas para la seguridad de la información		x		
A6	**Organización de la seguridad Informática**	**0**	**6**	**1**	**7**
	Asignación de responsabilidades para la segur. de la información.		x		
	Segregación de tareas.		x		
	Contacto con las autoridades.		x		
	Contacto con grupos de interés especial.			x	
	Seguridad de la información en la gestión de proyectos		x		
	Política de uso de dispositivos para movilidad.		x		
	Teletrabajo		x		
A7	**Seguridad de los Recursos Humanos**	**2**	**4**	**0**	**6**
	Investigación de antecedentes.	x			
	Términos y condiciones de contratación	x			
	Responsabilidades de gestión.		x		
	Concienciación, educación y capacitación en segur. de la información		x		
	Proceso disciplinario		x		
	Cese o cambio de puesto de trabajo		x		
A8	**Gestión de Activos**	**1**	**8**	**1**	**10**
	Inventario de activos.		x		
	Propiedad de los activos.		x		
	Uso aceptable de los activos.		x		
	Devolución de activos.		x		
	Directrices de clasificación.		x		
	Etiquetado y manipulado de la información.		x		
	Manipulación de activos		x		
	Gestión de soportes extraíbles.	x			
	Eliminación de soportes.			x	
	Soportes físicos en tránsito		x		
A9	**Control de Accesos**	**6**	**7**	**1**	**14**
	Política de control de accesos.		x		
	Control de acceso a las redes y servicios asociados		x		
	Gestión de altas/bajas en el registro de usuarios.	x			
	Gestión de los derechos de acceso asignados a usuarios.	x			

	Gestión de los derechos de acceso con privilegios especiales.	x			
	Gestión de información confidencial de autenticación de usuarios.		x		
	Revisión de los derechos de acceso de los usuarios.	x			
	Retirada o adaptación de los derechos de acceso	x			
	Uso de información confidencial para la autenticación			x	
	Restricción del acceso a la información.		x		
	Procedimientos seguros de inicio de sesión.		x		
	Gestión de contraseñas de usuario.	x			
	Uso de herramientas de administración de sistemas.		x		
	Control de acceso al código fuente de los programas.		x		
A10	**Criptografía**	**0**	**2**	**0**	**2**
	Política de uso de los controles criptográficos.		x		
	Gestión de claves.		x		
A11	**Seguridad física y ambiental**	**5**	**8**	**2**	**15**
	Perímetro de seguridad física.		x		
	Controles físicos de entrada.		x		
	Seguridad de oficinas, despachos y recursos.		x		
	Protección contra las amenazas externas y ambientales.		x		
	El trabajo en áreas seguras.			x	
	Áreas de acceso público, carga y descarga.	x			
	Emplazamiento y protección de equipos.		x		
	Instalaciones de suministro.	x			
	Seguridad del cableado.	x			
	Mantenimiento de los equipos.		x		
	Salida de activos fuera de las dependencias de la empresa.	x			
	Seguridad de los equipos y activos fuera de las instalaciones.		x		
	Reutilización o retirada segura de dispositivos de almacenamiento.	x			
	Equipo informático de usuario desatendido.		x		
	Política de puesto de trabajo despejado y bloqueo de pantalla			x	
A12	**Seguridad de la Operaciones**	**3**	**8**	**3**	**14**
	Documentación de procedimientos de operación.			x	
	Gestión de cambios.		x		
	Gestión de capacidades.		x		
	Separación de entornos de desarrollo, prueba y producción.			x	
	Controles contra el código malicioso		x		
	Copias de seguridad de la información.	x			
	Registro y gestión de eventos de actividad.		x		
	Protección de los registros de información.	x			

	Registros de actividad del administrador y operador del sistema.	x			
	Sincronización de relojes		x		
	Instalación del software en sistemas en producción.		x		
	Gestión de las vulnerabilidades técnicas.		x		
	Restricciones en la instalación de software		x		
	Controles de auditoría de los sistemas de información			x	
A13	**Seguridad de las Comunicaciones**	**5**	**2**	**0**	**7**
	Controles de red.	x			
	Mecanismos de seguridad asociados a servicios en red.	x			
	Segregación de redes.	x			
	Políticas y procedimientos de intercambio de información.		x		
	Acuerdos de intercambio.		x		
	Mensajería electrónica.	x			
	Acuerdos de confidencialidad y secreto.	x			
A14	**Adquisición de Sistemas, Desarrollo y Mantenimiento**	**2**	**9**	**2**	**13**
	Análisis y especificación de los requisitos de seguridad.		x		
	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	x			
	Protección de las transacciones por redes telemáticas.	x			
	Política de desarrollo seguro de software.		x		
	Procedimientos de control de cambios en los sistemas.		x		
	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.			x	
	Restricciones a los cambios en los paquetes de software.			x	
	Uso de principios de ingeniería en protección de sistemas.		x		
	Seguridad en entornos de desarrollo.		x		
	Externalización del desarrollo de software.		x		
	Pruebas de funcionalidad durante el desarrollo de los sistemas.		x		
	Pruebas de aceptación.		x		
	Protección de los datos utilizados en pruebas		x		
A15	**Relación con proveedores**	**1**	**2**	**2**	**5**
	Política de seguridad de la información para suministradores.		x		
	Tratamiento del riesgo dentro de acuerdos de suministradores.			x	
	Cadena de suministro en tecnologías de la información y comunicaciones.			x	
	Supervisión y revisión de los servicios prestados por terceros.	x			
	Gestión de cambios en los servicios prestados por terceros		x		
A16	**Gestión de los incidentes de seguridad**	**2**	**4**	**1**	**7**
	Responsabilidades y procedimientos.	x			
	Notificación de los eventos de seguridad de la información.	x			
	Notificación de puntos débiles de la seguridad.		x		

	Valoración de eventos de seguridad de la información y toma de decisiones.		x		
	Respuesta a los incidentes de seguridad.		x		
	Aprendizaje de los incidentes de seguridad de la información.			x	
	Recopilación de evidencias.		x		
A17	**Continuidad del negocio**	**0**	**2**	**2**	**4**
	Planificación de la continuidad de la seguridad de la información.		x		
	Implantación de la continuidad de la seguridad de la información.			x	
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.			x	
	Disponibilidad de instalaciones para el procesamiento de la información		x		
A18	**Cumplimiento con Requerimientos Legales y Contractuales**	**0**	**5**	**3**	**8**
	Identificación de la legislación aplicable.			x	
	Derechos de propiedad intelectual (DPI).			x	
	Protección de los registros de la organización.		x		
	Protección de datos y privacidad de la información personal.		x		
	Regulación de los controles criptográficos		x		
	Revisión independiente de la seguridad de la información.			x	
	Cumplimiento de las políticas y normas de seguridad.		x		
	Comprobación del cumplimiento.		x		

ANEXO N° 03. Cuestionario

CUESTIONARIO PARA LA MEDICIÓN DE LA GESTIÓN DEL RIESGO DE LA INFORMACIÓN EN EL PERSONAL DE UNA EMPRESA COMERCIALIZADORA DE LUBRICANTES EN LA CIUDAD DE CHICLAYO

OBJETIVOS DE LA INVESTIGACIÓN:

GENERAL:

Determinar la gestión del riesgo de la información en el personal de una empresa comercializadora de lubricantes en la ciudad de Chiclayo

INSTRUCCIONES

Estimado colaborador, a continuación, tiene 20 ítems, con escala de puntuación de 1 a 5 en donde:

(Nunca =1 Casi Nunca =2 A veces = 3 Casi Siempre =4 Siempre =5).

Responda con la verdad y marque con una "x" la alternativa seleccionada

N°	ÍTEMS	1	2	3	4	5
1	¿Considera que dentro de su empresa se generan cifras elevadas de incidentes reportados relacionados con la seguridad de la información que esta posee?					
2	¿Los incidentes reportados que se encuentran relacionados con la seguridad de la información afectan de manera directa o indirecta a su área de trabajo?					
3	¿Diría que su empresa atiende de manera oportuna los incidentes relacionados con la seguridad de la información que se presentan?					
4	¿Ante la presencia de un incidente relacionado con la seguridad de la información considera que usted toma algún tipo de acción concreta para poder solucionarlo?					
5	¿La empresa establece políticas y directivas necesarias y oportunas para mantener la seguridad de la información en todos los procesos que lleva a cabo?					
6	¿Considera que cumple a cabalidad con las políticas y directivas que actualmente la empresa ha establecido en cuánto seguridad de la información?					
7	¿Recibe por parte de la empresa capacitaciones constantes que le permitan a usted tener conocimiento y tomar conciencia de lo importante que es la seguridad de la información en su centro de trabajo?					

8	¿Considera que para salvaguardar los bienes de la empresa en cuanto a la seguridad de la información es necesario recibir por parte de la empresa todas las herramientas necesarias para su cumplimiento?					
9	¿Dentro de su empresa considera que existe un alto nivel de riesgo en que la información que posee sea vulnerada?					
10	¿Las acciones y actividades que usted realiza dentro de su centro de trabajo contribuyen a que exista un alto nivel de riesgo en la seguridad de la información de la empresa?					
11	¿La empresa le comunica cuales son los controles establecidos que usted debe de tomar en cuenta para no poner en riesgo tanto el software como el hardware que esta utiliza?					
12	¿En el desarrollo de sus actividades y labores diarias toma en cuenta algún tipo de control o realiza alguna actividad o procedimiento para hacer frente al posible riesgo de vulnerabilidad que puede generarse en la información que maneja?					
13	¿Considera que la empresa donde usted labora posee un control riguroso en cuanto a acceso a la información que ésta posee?					
14	¿Cuándo usted realiza sus actividades dentro de la empresa tiene acceso rápido y fácil a toda la información que la empresa posee?					
15	¿Ante la presencia de algún tipo de riesgo en la seguridad de la información que posee su empresa realiza algún tipo de actividad o acción para mitigarlo?					
16	¿Considera que existe una relación directa entre la productividad que posee su empresa y la seguridad de la información que esta brinda?					
17	¿Con frecuencia su empresa le brinda y transmite recomendaciones en cuanto a los posibles riesgos en la seguridad de la información que se pueden suscitar en su área?					
18	¿Toma en cuenta al momento de realizar sus labores diarias las recomendaciones que la empresa le brinda en cuanto a la mitigación del riesgo existente en la información que usted maneja?					
19	¿Percibe que la empresa donde usted labora posee los procedimientos y documentos estandarizados para gestionar el riesgo de la información dentro de su empresa?					
20	¿Considera suficiente la cantidad de colaboradores capacitados por parte de su empresa en cuanto a la gestión del riesgo de la seguridad de la información?					

ANEXO N° 03. Validaciones de Propuesta

VALIDACIÓN DE PROPUESTA

Estimado: Doctora Ing. María Aurora Gonzales Vigo

Solicito apoyo de su sapiencia y excelencia profesional para que emita juicios sobre la Propuesta que se ha elaborado en el marco de la ejecución de la tesis titulada **"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PARA LA GESTIÓN DEL RIESGO DE LA INFORMACIÓN DE UNA EMPRESA COMERCIALIZADORA DE LUBRICANTES EN LA CIUDAD DE CHICLAYO"**

Realizado por: MARIO IVAN, PÉREZ SANDOVAL

Para alcanzar este objetivo lo he seleccionado como experto en la materia y necesito su valiosa opinión. Para ello debe marcar con una (X) en la columna que considere para cada indicador.

Evalúe cada aspecto con las siguientes categorías:

MA : Muy adecuado.
BA : Bastante adecuado.
A : Adecuado
PA : Poco adecuado
NA : No Adecuado

N°	Aspectos que deben ser evaluados	MA	BA	A	PA	NA
I.	**Redacción**					
1.1	La redacción empleada es clara, precisa, concisa y debidamente organizada	X				
1.2	Los términos utilizados son propios de la especialidad.	X				
II.	**Estructura de la Propuesta**					
2.1	Las áreas con los que se integra la Propuesta son los adecuados.	X				
2.2	Las áreas en las que se divide la Propuesta están debidamente organizadas.	X				
2.3	Las actividades propuestas son de interés para los trabajadores y usuarios del área.	X				
2.4	Las actividades desarrolladas guardan relación con los objetivos propuestos.	X				
2.5	Las actividades desarrolladas apoyan a la solución de la problemática planteada.	X				

III	**Fundamentación teórica**					
3.1	Los temas y contenidos son producto de la revisión de bibliografía especializada.	X				
3.2	La propuesta tiene su fundamento en sólidas bases teóricas.	X				
IV	**Bibliografía**					
4.1	Presenta la bibliografía pertinente a los temas y la correspondiente a la metodología usada en la Propuesta.	X				
V	**Fundamentación y viabilidad de la Propuesta**					
5.1.	La fundamentación teórica de la propuesta guarda coherencia con el fin que persigue.	X				
5.2.	La propuesta presentada es coherente, pertinente y trascendente.	X				
5.3.	La propuesta presentada es factible de aplicarse en otras organizaciones.	X				

Mucho le agradeceré cualquier observación, sugerencia, propósito o recomendación sobre cualquiera de los propuestos. Por favor, refiéralas a continuación:

Se Sugiere su aplicación del "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PARA LA GESTIÓN DEL RIESGO DE LA INFORMACIÓN DE UNA EMPRESA COMERCIALIZADORA DE LUBRICANTES EN LA CIUDAD DE CHICLAYO" para que cuente con análisis sistemático

Validado por la: Dra. María Aurora Gonzales Vigo
Tiempo de Experiencia en Docencia Universitaria: 5 años
Cargo Actual: Docente Universitario

Fecha: 04/12/2020

VALIDACIÓN DE PROPUESTA

Estimado Mg. Ing. Oscar Enrique Salazar Carbonel

Solicito apoyo de su sapiencia y excelencia profesional para que emita juicios sobre la Propuesta que se ha elaborado en el marco de la ejecución de la tesis titulada **"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PARA LA GESTIÓN DEL RIESGO DE LA INFORMACIÓN DE UNA EMPRESA COMERCIALIZADORA DE LUBRICANTES EN LA CIUDAD DE CHICLAYO"**

Realizado por: MARIO IVAN, PÉREZ SANDOVAL

Para alcanzar este objetivo lo he seleccionado como experto en la materia y necesito su valiosa opinión. Para ello debe marcar con una (X) en la columna que considere para cada indicador.

Evalúe cada aspecto con las siguientes categorías:

MA : Muy adecuado.
BA : Bastante adecuado.
A : Adecuado
PA : Poco adecuado
NA : No Adecuado

N°	Aspectos que deben ser evaluados	MA	BA	A	PA	NA
I.	**Redacción**					
1.1	La redacción empleada es clara, precisa, concisa y debidamente organizada	X				
1.2	Los términos utilizados son propios de la especialidad.	X				
II.	**Estructura de la Propuesta**					
2.1	Las áreas con los que se integra la Propuesta son los adecuados.	X				
2.2	Las áreas en las que se divide la Propuesta están debidamente organizadas.	X				
2.3	Las actividades propuestas son de interés para los trabajadores y usuarios del área.	X				
2.4	Las actividades desarrolladas guardan relación con los objetivos propuestos.	X				
2.5	Las actividades desarrolladas apoyan a la solución de la problemática planteada.	X				
III	**Fundamentación teórica**					

3.1	Los temas y contenidos son producto de la revisión de bibliografía especializada.	X				
3.2	La propuesta tiene su fundamento en sólidas bases teóricas.	X				
IV	**Bibliografía**					
4.1	Presenta la bibliografía pertinente a los temas y la correspondiente a la metodología usada en la Propuesta.	X				
V	**Fundamentación y viabilidad de la Propuesta**					
5.1.	La fundamentación teórica de la propuesta guarda coherencia con el fin que persigue.	X				
5.2.	La propuesta presentada es coherente, pertinente y trascendente.	X				
5.3.	La propuesta presentada es factible de aplicarse en otras organizaciones.	X				

Mucho le agradeceré cualquier observación, sugerencia, propósito o recomendación sobre cualquiera de los propuestos. Por favor, refiéralas a continuación:

Propuesta realizada de manera correcta

Validado por el Magister: Oscar Enrique Salazar Carbonel

Tiempo de Experiencia en Docencia Universitaria: 07 años

Cargo Actual: Docente UNPRG

Fecha: 09/12/2020

Mg. Ing. Oscar Enrique Salazar Carbonel

DNI N° 80676706

VALIDACIÓN DE PROPUESTA

Estimado: **Mg. Ing. Carlos Rojas Ortiz**

Solicito apoyo de su sapiencia y excelencia profesional para que emita juicios sobre la Propuesta que se ha elaborado en el marco de la ejecución de la tesis titulada **"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PARA LA GESTIÓN DEL RIESGO DE LA INFORMACIÓN DE UNA EMPRESA COMERCIALIZADORA DE LUBRICANTES EN LA CIUDAD DE CHICLAYO"**

Realizado por: MARIO IVAN, PÉREZ SANDOVAL

Para alcanzar este objetivo lo he seleccionado como experto en la materia y necesito su valiosa opinión. Para ello debe marcar con una (X) en la columna que considere para cada indicador.

Evalúe cada aspecto con las siguientes categorías:

MA : Muy adecuado.
BA : Bastante adecuado.
A : Adecuado
PA : Poco adecuado
NA : No Adecuado

N°	Aspectos que deben ser evaluados	MA	BA	A	PA	NA
I.	**Redacción**					
1.1	La redacción empleada es clara, precisa, concisa y debidamente organizada	X				
1.2	Los términos utilizados son propios de la especialidad.	X				
II.	**Estructura de la Propuesta**					
2.1	Las áreas con los que se integra la Propuesta son los adecuados.	X				
2.2	Las áreas en las que se divide la Propuesta están debidamente organizadas.	X				
2.3	Las actividades propuestas son de interés para los trabajadores y usuarios del área.	X				
2.4	Las actividades desarrolladas guardan relación con los objetivos propuestos.	X				
2.5	Las actividades desarrolladas apoyan a la solución de la problemática planteada.	X				

III	**Fundamentación teórica**					
3.1	Los temas y contenidos son producto de la revisión de bibliografía especializada.	X				
3.2	La propuesta tiene su fundamento en sólidas bases teóricas.	X				
IV	**Bibliografía**					
4.1	Presenta la bibliografía pertinente a los temas y la correspondiente a la metodología usada en la Propuesta.	X				
V	**Fundamentación y viabilidad de la Propuesta**					
5.1.	La fundamentación teórica de la propuesta guarda coherencia con el fin que persigue.	X				
5.2.	La propuesta presentada es coherente, pertinente y trascendente.	X				
5.3.	La propuesta presentada es factible de aplicarse en otras organizaciones.	X				

Mucho le agradeceré cualquier observación, sugerencia, propósito o recomendación sobre cualquiera de los propuestos. Por favor, refiéralas a continuación:

Validado por el Magister:

Tiempo de Experiencia en Docencia Universitaria: 7 años

Cargo Actual: Docente USS

Fecha: 09/12/2020

Mg. Ing. Carlos Rojas Ortiz

DNI N° 16709803

CIP: 89178

VALIDACION DE PROPUESTA

Estimado

Solicito apoyo de su sapiencia y excelencia profesional para que emita juicios sobre la Propuesta que se ha elaborado en el marco de la ejecución de la tesis titulada **"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PARA LA GESTIÓN DEL RIESGO DE LA INFORMACIÓN DE UNA EMPRESA COMERCIALIZADORA DE LUBRICANTES EN LA CIUDAD DE CHICLAYO"**

Realizado por: MARIO IVAN, PÉREZ SANDOVAL

Para alcanzar este objetivo lo he seleccionado como experto en la materia y necesito su valiosa opinión. Para ello debe marcar con una (X) en la columna que considere para cada indicador.

Evalúe cada aspecto con las siguientes categorías:

MA : Muy adecuado.
BA : Bastante adecuado.
A : Adecuado
PA : Poco adecuado
NA : No Adecuado

N°	Aspectos que deben ser evaluados	MA	BA	A	PA	NA
I.	**Redacción**					
1.1	La redacción empleada es clara, precisa, concisa y debidamente organizada	X				
1.2	Los términos utilizados son propios de la especialidad.	X				
II.	**Estructura de la Propuesta**					
2.1	Las áreas con los que se integra la Propuesta son los adecuados.	X				
2.2	Las áreas en las que se divide la Propuesta están debidamente organizadas.	X				
2.3	Las actividades propuestas son de interés para los trabajadores y usuarios del área.	X				
2.4	Las actividades desarrolladas guardan relación con los objetivos propuestos.	X				
2.5	Las actividades desarrolladas apoyan a la solución de la problemática planteada.	X				
III	**Fundamentación teórica**					

3.1	Los temas y contenidos son producto de la revisión de bibliografía especializada.	X				
3.2	La propuesta tiene su fundamento en sólidas bases teóricas.	X				
IV	**Bibliografía**					
4.1	Presenta la bibliografía pertinente a los temas y la correspondiente a la metodología usada en la Propuesta.	X				
V	**Fundamentación y viabilidad de la Propuesta**					
5.1.	La fundamentación teórica de la propuesta guarda coherencia con el fin que persigue.	X				
5.2.	La propuesta presentada es coherente, pertinente y trascendente.	X				
5.3.	La propuesta presentada es factible de aplicarse en otras organizaciones.	X				

Mucho le agradeceré cualquier observación, sugerencia, propósito o recomendación sobre cualquiera de los propuestos. Por favor, refiéralas a continuación:

Sin observaciones ni sugerencias al respecto.

Validado por el Magister: Mg. Ing. Luis Alberto Ramos Martínez

Tiempo de Experiencia en Docencia Universitaria: 05 años

Cargo Actual: Jefe de la Unidad de Mantenimiento en el Hospital Regional Lambayeque

Fecha: 09/12/2020

Mg. Ing. Luis Alberto Ramos Martínez

DNI° 41218036