FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

IMPLEMENTACIÓN DE UN MODELO DE PROCESOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA PYME PERUANA BASADA EN LA NORMA ISO/IEC 27005 Y METODOLOGÍA OCTAVE-S

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor(a) (es):

Bach. Martos Paredes Joel Harold

https://orcid.org/0000-0002-4409-9482

Bach. Villazon Sosa Jair Augusto

https://orcid.org/0000-0002-5950-9827

Asesor(a):

Mg. Bravo Ruiz Jaime Arturo

https://orcid.org/0000-0003-1929-3969

Línea de Investigación:

Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú

2024

Implementación de un modelo de procesos de seguridad de la información para una pyme peruana basada en la norma iso/iec 27005 y la metodología

Aprobación del jurado

DR. VASQUEZ LEYVA OLIVER

Presidente del Jurado de Tesis

MG. VIDAURRE FLORES MIGUEL ANGEL

Secretario del Jurado de Tesis

MG. ARCILA DIAZ JUAN CARLOS

Vocal del Jurado de Tesis

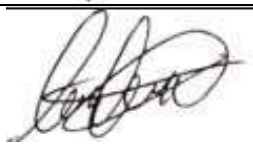
DECLARACIÓN JURADA DE ORIGINALIDAD

Quienes suscriben la DECLARACIÓN JURADA, somos **Martos Paredes Joel Harold, Villazon Sosa Jair Augusto** egresado (s) del Programa de Estudios de **Ingeniería de Sistemas** de la Universidad Señor de Sipán S.A.C, declaramos bajo juramento que somos autores del trabajo titulado:

IMPLEMENTACIÓN DE UN MODELO DE PROCESOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA PYME PERUANA BASADA EN LA NORMA ISO/IEC 27005 Y METODOLOGÍA OCTAVE-S

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán, conforme a los principios y lineamientos detallados en dicho documento, en relación con las citas y referencias bibliográficas, respetando el derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y autentico.

En virtud de lo antes mencionado, firman:

Martos Paredes Joel Harold	DNI: 77675622	
Villazón Sosa Jair Augusto	DNI: 74118632	

Pimentel, 27 de Junio 2024.

Dedicatoria

Dedicamos este proyecto de tesis en primer lugar a Dios, por guiarnos siempre por el buen camino, estando siempre con nosotros cuidándonos. A nuestros padres que son nuestros pilares para seguir continuando con nuestra carrera, ya que ellos siempre han velado por nosotros, por nuestro bienestar, educación, dándonos así las fortalezas, las motivaciones para seguir adelante siempre. A los ingenieros que nos brindaron sus conocimientos, ayudándonos siempre en esta última etapa de la vida universitaria.

Agradecimientos

En primer lugar, agradecer a Dios por permitirnos tener una buena experiencia dentro de la universidad “Señor de Sipán”, por permitirnos convertirnos en ser unos profesionales en lo que tanto nos apasiona, a nuestros padres por el constante apoyo que nos brindan en realizar nuestros objetivos y nuestros sueños, gracias a cada maestro de la Escuela Académica Profesional de Ingeniería de Sistemas, que hizo parte de este proceso de nuestras formaciones, que deja como un producto terminado, que es nuestra tesis que perdurará dentro de nuestros conocimientos y desarrollo y para la motivación de las demás generaciones que está por llegar.

Resumen

Hoy en día, toda empresa debería tener una razón de su importancia y de cómo manejar la información para su negocio. La seguridad de las informaciones en las empresas tiene como finalidad proteger los activos de información de cualquier persona de sus estados, así estén atravesando una serie de amenazas que atentan contra sus principios primordiales ya sea de confidencialidad, totalidad y disponibilidad, ya que por medio de la utilización de medidas de control de seguridad de la información permitirá gestionar y minimizar los peligros e impactos a que está expuesta y se pueda conseguir el mayor retorno de las inversiones en las oportunidades de comercio. Por eso, algunas organizaciones intentan proteger su información más importante, pero utilizan los derechos de gestión. Entre sus riesgos, tratar de evitar situaciones negativas como provocar pérdidas económicas importantes, vulneración de la confidencialidad de información, pérdida de integridad o disponibilidad de datos confidenciales. Para defender la información, las organizaciones tienen que decidir su exposición al peligro, es por esto que en PYMES se implementó el modelo de alusión para la administración de peligros de seguridad de la información integrando la metodología OCTAVE-S y la regla ISO/IEC 27005, debido a que este permitió detectar y gestionar los peligros a los que puede estar expuesta la compañía de este modo, se implementó este modelo de proceso con el fin de que la información tenga más seguridad. Por consiguiente, se espera que este modelo ayude en la administración de peligros de estabilidad de la información en las Pymes, para lograr minimizar el efecto de peligros a los que tienen la posibilidad de estar expuestas. Luego de haber implementado el modelo de alusión para la administración de peligros de seguridad, se obtuvo como consecuencia conveniente que tuvo un 80% de eficacia, lo cual permitió conseguir las metas. Esto conllevó a que la metodología OCTAVE – S se centre

solamente en las superficies que piensan más críticas, debido a que esto ayudó a enfocar el 100% de la productividad en las verdaderas amenazas para una Pequeña Y Mediana Empresa y de esta forma poder planear un control de estabilidad para la organización.

Palabras Clave: Seguridad de la Información; Gestión de Riesgos; Octave-S, norma ISO/IEC 27005; Pymes; Análisis de Riesgos; Modelo de procesos.

Abstract

Nowadays, every company should have a reason of its importance and how to manage information for its business. The purpose of information security in companies is to protect the information assets of any person of their states, even if they are going through a series of threats that attempt against their primordial principles either of confidentiality, totality and availability, since through the use of information security control measures it will allow to manage and minimize the dangers and impacts to which it is exposed and the highest return on investments in business opportunities can be achieved. Therefore, some organizations try to protect their most important information, but use management rights. Among their risks, trying to avoid negative situations such as causing significant economic losses, breach of confidentiality of information, loss of integrity or availability of confidential data. To defend the information, the organizations have to decide their exposure to danger, that is why in PYMES the allusion model for the administration of information security dangers was implemented integrating the OCTAVE-S methodology and the ISO/IEC 27005 rule, because this allowed to detect and manage the dangers to which the company can be exposed in this way, this process model was implemented in order to make the information more secure. Therefore, it is expected that this model will help in the management of information stability hazards in SMEs, in order to minimize the effect of hazards to which they are likely to be exposed. After having implemented the model of allusion for the administration of security dangers, it was obtained as a convenient consequence that it had an 80% of effectiveness, which allowed to achieve the goals. This led to the OCTAVE - S methodology to focus only on the surfaces that they think more critical, due to the fact that this helped to focus 100% of the productivity on the real

threats for a Small and Medium Company and in this way to be able to plan a stability control for the organization.

Keywords: Information Security; Risk Management; Octave-S, ISO/IEC 27005 standard; SMEs; Risk Analysis; Process Model.

Índice

Dedicatoria 4

Agradecimientos 5

Resumen 6

Abstract 8

I. INTRODUCCIÓN 13

1.1. Realidad Problemática 13

1.2. Trabajos previos 20

1.3. Teorías relacionadas al tema 32

1.3.1. Normas ISO/IEC 32

1.3.1.1. ISO/IEC 27001 32

1.3.1.2. ISO/IEC 27005 32

1.3.2. Instituto Nacional de Estándares y Tecnología (NIST) 34

1.3.3. Matriz de Evaluación de Riesgos (RAM) 34

1.3.4. Metodología OCTAVE 35

1.3.5. MEHARI 41

1.3.6. SP800-30 42

1.3.7. MAGERIT 42

1.4. Formulación del Problema 45

1.5. Justificación e importancia del estudio 45

1.6. Hipótesis 46

1.7. Objetivos 46

1.7.1. Objetivo general 46

1.7.2. Objetivos específicos 46

II. MATERIAL Y MÉTODO 46

2.1. Tipo y Diseño de Investigación 46

2.2. Población de estudio, muestra, muestreo y criterios de selección. 47

2.2.1. Población 47

2.2.2. Muestra 48

2.3. Variables, Operacionalización 50

2.3.1. Variable independiente 50

2.3.2. Variable dependiente 50

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad 52

2.4.1. Técnicas 52

2.4.2. Instrumentos 53

2.5. Procedimiento de análisis de datos 54

2.6. Criterios éticos 60

2.7. Criterios de Rigor Científico 61

III. RESULTADOS Y DISCUSIÓN 61

3.1. Resultados 61

3.2. Discusión 67

3.3. Aporte de la Investigación 69

IV. CONCLUSIONES Y RECOMENDACIONES 186

4.1. Conclusiones 186

4.2. Recomendaciones 187

REFERENCIAS 188

ANEXOS 193

I. INTRODUCCIÓN

1.1. Realidad Problemática.

La Seguridad de la información es uno de los temas más importantes en la actualidad, puesto que, con la llegada de la pandemia por el virus de SARS-CoV-2 ha obligado a las empresas a invertir más dinero en tecnología y plataformas en la nube para poder prestar o afianzar sus servicios a un público en específico, ya que de no ser así la empresa colapsaría o quebraría. Viendo que el internet es un campo muy amplio, podemos deducir que el acceso a la información es mucho más sencillo de lo que parece, por ende, las maneras de irrumpir dentro de un sistema web de una empresa es muy variado, para esto es que la seguridad de la información es vital en las empresas.

Gracias a la cobertura geográfica del Reino Unido, el Departamento Digital de Cultura, Medios y Deporte (DCMS), con la colaboración de Ipsos MORI, que se encargó de la encuesta sobre infracciones de seguridad cibernética de empresas, organizaciones benéficas e instituciones educativas del Reino Unido, esta encuesta fue realizada en 1419 empresas del Reino Unido, 741 microempresas, 265 pequeñas empresas, 210 empresas medianas y 203 grandes empresas, Pero nos centraremos en la identificación de los datos obtenidos únicamente de las empresas.

Por consiguiente, un estudio realizado por Department for Digital, Culture, Media & Sport; MP, Matt Warman, (2021), afirma que, cuatro de cada diez empresas entre micro, pequeñas, medianas y grandes, informan haber tenido ataques o violaciones de seguridad cibernética en los últimos 12 meses. Haciendo referencia a la encuesta realizada años anteriores se puede asegurar que hay un aumento

de ataques en las empresas del sector. En la siguiente figura se muestra el porcentaje obtenido de dicha investigación.

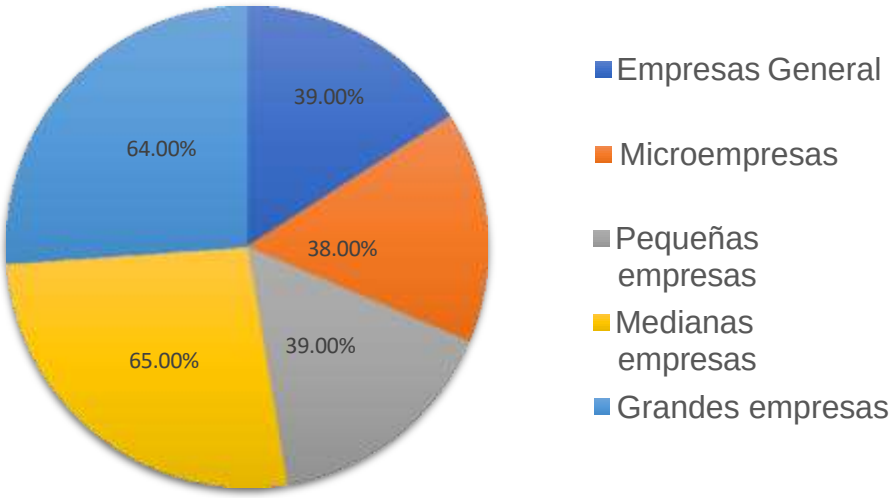


Figura 1. Porcentaje de organizaciones que han identificado brechas o ataques en los últimos 12 meses. Fuente: *(Department for Digital, Culture, Media & Sport; MP, Matt Warman, 2021)*

Existen diversos tipos de ataques o infracciones, los cuales pueden vulnerar la seguridad de las empresas y su información, Department for Digital, Culture, Media & Sport; MP, Matt Warman, (2021), también define que las empresas han podido identificar el tipo de ataque en los últimos 12 meses. En la siguiente figura

se observa el porcentaje de los ataques identificados por las empresas.

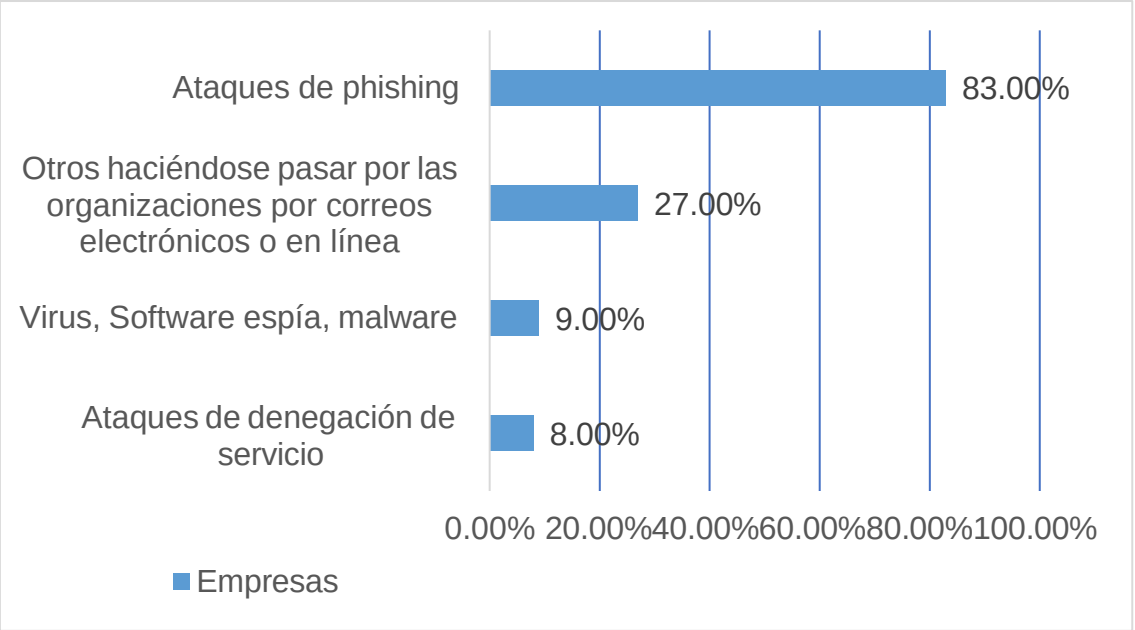


Figura 2. Porcentaje que ha identificado los siguientes tipos de brechas o ataques en los últimos 12 meses por las empresas. Fuente: (Department for Digital, Culture, Media & Sport; MP, Matt Warman, 2021)

Tabla 1.

Tabla de nivel de riesgos especificados en el caso de estudio.

Nivel	**Mínimo**	**Máximo**
Bajo	5	100
Medio	101	199
Elevado	200	540

Nota: Tomado de (García-Porras, Huamani-Pastor, & Armas-Aguirre, 2018, págs. 3-4)

Tabla 2.

Tabla de valor de riesgos especificados en el caso de estudio.

Activos	Riesgo valor	Nivel de riesgo	Residual Riesgo Valor	Reducción
Programas virtualizados	216	Elevado	109	50%
ERP	208	Elevado	101	51%
Computadoras / Laptops	139	Medio	60	57%
Sistemas operativos	85	Bajo	51	40%
Certificado electrónico	68	Bajo	23	66%
Correo electrónico	59	Bajo	28	53%

Nota: Tomado de (García-Porras, Huamani-Pastor, & Armas-Aguirre, 2018, pág. 4)

Las infracciones o ataques son muy graves si se dan en un sector muy importante, por esto Department for Digital, Culture, Media & Sport; MP, Matt Warman, (2021), afirma en su revista que el 49% de las empresas dicen que estos tipos de ataques suceden con mayor frecuencia o a más tardar una vez al mes y un 27% de éstas, experimentan ataques o violaciones una vez a la semana. Esto es un problema operativo gravísimo. En la siguiente figura, podemos detallar la frecuencia que se dan este tipo de infracciones.

Figura 3. Porcentaje de la frecuencia en que las empresas han informado que son vulneradas Fuente: (Department for Digital, Culture, Media & Sport; MP, Matt Warman, 2021)

OCTAVE y el método OCTAVE-S son 2 procedimientos desarrollados en el Software Engineering Institute (SEI) según los criterios OCTAVE, los requisitos básicos de una evaluación estratégica basada en activos del peligro de estabilidad de la información. El Procedimiento OCTAVE ha sido desarrollado primero y se aplica a memoriales empresas jerárquicas. Octave volumen uno la guía de utilización del procedimiento da una introducción de aquel procedimiento. OCTAVE-S se desarrolló para saciar las necesidades de empresas más pequeñas y menos jerárquicas.

El enfoque OCTAVE da una Resumen general del enfoque OCTAVE y las metodologías consistentes OCTAVE de SEI.

Los individuos que no se encuentren familiarizadas con el enfoque OCTAVE tiene los conceptos y principios básicos de OCTAVE.

El procedimiento OCTAVE fue creado para organizaciones que puedan sostener su propia infraestructura informática, como también, para aquellas que sean capaces de interpretar los resultados de las evaluaciones de vulnerabilidad. OCTAVE – S fue diseñado bajo la inserción, demostración y evaluación de tecnología (TIDE), gestionado para el Software Engineering Institute por John Foreman.

Cualquier organización que ya esté familiarizado con el método OCTAVE probablemente encontrará que OCTAVE – S es fácil de entender, debido que ambos procedimientos comparten una base común.

A diferencia de las evaluaciones típicas centradas en la tecnología, OCTAVE está dirigido al riesgo organizacional y se reúne en cuestiones estratégicas relacionadas con la práctica.

Usando la metodología OCTAVE, las organizaciones toman decisiones de seguridad de la información basadas en riesgos de seguridad, integridad y disponibilidad de fuentes de información críticas.

A lo largo de la revisión de OCTAVE-S, los equipamientos de estudio revisa la estabilidad a partir de diversas perspectivas para asegurar que las sugerencias se encuentren correctamente equilibradas según con las necesidades de la organización.

Todos los procesos OCTAVES producen resultados prácticos. Como resultado, las evaluaciones fragmentadas generan información que puede ayudar a mejorar el nivel de seguridad de la organización.

La diferencia entre OCTAVE – S y el método OCTAVE, se efectúa en la amplitud del conocimiento de un equipo de análisis, más que el tamaño de una organización.

Algunas personas consideran el uso de OCTAVE – S en proyectos individuales, líneas de negocio, o departamentos.

OCTAVE es un proceso voluntario. En otras palabras, todos en su organización son responsables de definir una estrategia de seguridad.

Para hacer OCTAVE – S realmente, los accesorios deberían tener un extenso entendimiento del comercio y la estabilidad de la organización, por lo cual va a poder hacer cada una de las ocupaciones por sí mismo. (Alberts, Dorofee, Steven, & Woody, 2005)

1.2. Trabajos previos.

Carnero Garay, Carbajal Ramos, Armas Aguirre, & Madrid Molina, (2020), realizaron la investigación, *Information Security risk management model of mitigating the impact on SMEs in Perú*, en la University of Wollongong de Australia. Uno de los componentes descuidados que están afectando el aumento y desarrollo de los Pymes es la estabilidad de la información, para la cual las Organizaciones muestran un presupuesto reducido, evento que afecta su tiempo de vida. Por tal sentido, se planteó un modelo de administración de peligros de estabilidad de Información. Para eso, el modelo consta de 3 etapas, entre ellas, hacer el inventario de activos de la compañía, evaluar el procedimiento que se debería ofrecer a cada peligro y diseñar indicadores que apoyen a monitorear. Los resultados obtenidos, revelaron una disminución de peligro en un 71%, después de usar 15 controles de seguimiento y entrenamiento, el efecto acumulativo se redujo en 67,6 y la gravedad se redujo a 5,5, dependiendo del valor. El modelo de gestión de riesgos puede considerarse un monitor útil para ayudar a monitorear el avance y la efectividad de los controles implementados, en este caso para minimizar los factores que dañan a las Pymes.

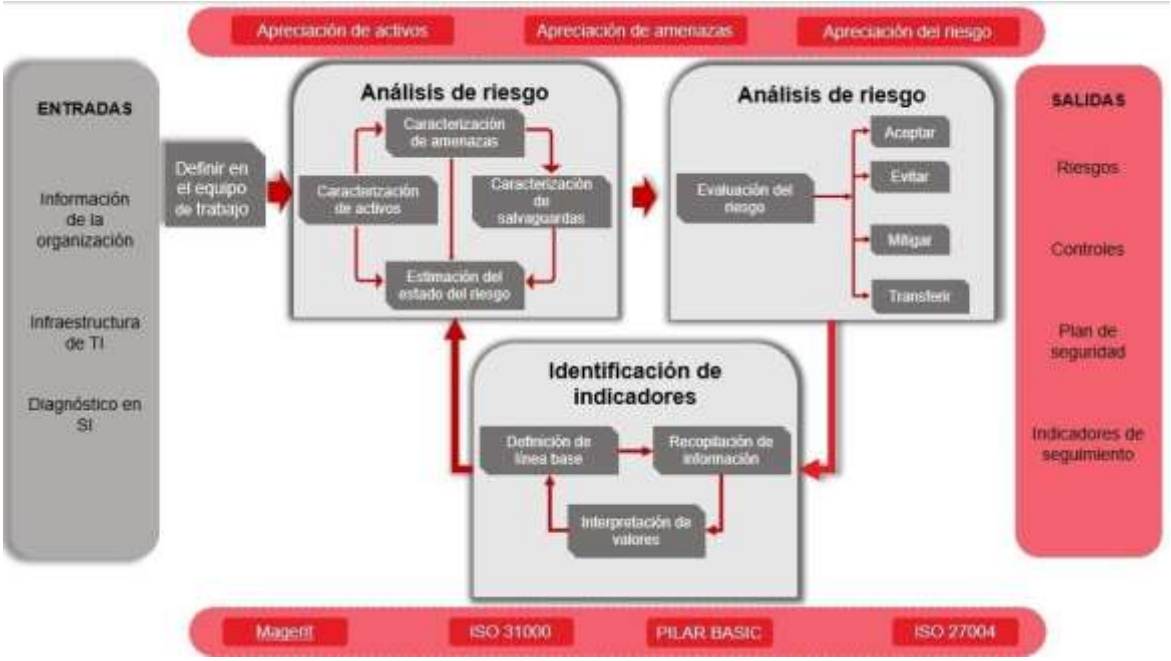


Figura 4. Modelo de gestión de riesgos de seguridad de la información. Fuente: (Carnero Garay, Carbajal Ramos, Armas Aguirre, & Madrid Molina, 2020)

Según Brodin, (2017), realizó la investigación - Security strategies for managing mobile devices in SMEs: A theoretical evaluation, en la Universidad de Skövde de Suecia. Los dispositivos móviles se consideran uno de los eslabones más débiles de la infraestructura de Tecnología de la Información (TI) de la mayoría de las empresas, de las cuales, una de cada cinco, ha experimentado una violación de dispositivo móvil y otro no sabe si ha sido ultrajada. Por esta razón, se presentó dos marcos generales, en primer lugar, el de gobernanza COBIT5, que se encargará de la identificación de los impulsores de las partes, a través de la satisfacción de necesidades, además de la optimización de recursos y de riesgos, como también, de los roles, las actividades y relaciones con respecto a la gestión y el segundo, de implementación BYOD, que se basa en la literatura y se centra en la cultura y seguridad de privacidad. El análisis brindó como resultados que todos los marcos tienen sus partes fuertes, los cuales pueden orientar sobre cómo mantener viva la estrategia después de la implementación y reflexiona sobre la

cultura organizacional. La mayor parte de los marcos, gestionan de manera correcta los desafíos que implica la seguridad, pero solo dos, tienen en cuenta los beneficios de los dispositivos móviles.

Dube & Flowerday, (2018), realizaron la investigación, *Towards a Holistic Information Security Framework for South African Small and Medium Enterprises*. Las grandes organizaciones corporativas e instituciones gubernamentales, usuarios de TIC (Tecnología de la información y la comunicación), no utilizan sus sistemas en completo aislamiento del resto del mundo, lo que introduce vulnerabilidades en las interacciones con usuarios inseguros o mal protegidos. Por tal motivo, se propone un marco de seguridad de la información más simple pero más efectivo que tiene una visión holística para asegurar los activos de información de las PYMES. Los resultados expresan que el marco propuesto reduce la complejidad de implementar el control de seguridad al centrarse en los elementos clave, los cuales, disminuirán significativamente la amenaza de un ataque. Por consiguiente, son la complejidad de las interacciones en un entorno de PYME, una limitación adicional por los recursos que están disponibles para su uso en la implementación de la seguridad, lo que no genera ingresos, es por ello, que el marco propuesto, incluye aspectos de recursos que deben incorporarse para una mejora.

Según Martinez, (2015), realizó la investigación, *Seguridad de la Información en pequeñas y medianas empresas (pymes),* en la Universidad Piloto de Colombia. Las pymes carecen de trascendencia referente a la defensa de información, en la cual, al pensar en estabilidad se comente errores, como, por ejemplo, no ver la información, no ver la infraestructura, la estabilidad solo es un hardware o programa, carecer de Antivirus, restarle trascendencia al know how y no

contemplar una estrategia de continuidad del comercio. Por esta razón, se implementará un Sistema de Administración de la Estabilidad de la Información (SGSI), la cual se basará en el periodo de Deming (PHVA) y en la regla ISO 27001;2013. Los resultados indican que, la implementación de un SGSI asegura el acceso eficiente a la información y promueve la confidencialidad, integridad y disponibilidad de la información. Por lo tanto, el lapso DEMING, puede relacionar las principales actividades que debe desarrollar una pyme que quiera realizar un sistema de gestión de seguridad de la información basado en la regla ISO 27001; 2013. Igualmente, hay muchas metodologías para realizar un SGSI, teniendo cada una de los mismos objetivos de calcular el riesgo asociado a los activos de la organización e implantar medidas para reducirlo.

Iyamuremye & Shima, (2018), realizaron la investigación, Network security testing tools for SMEs (small and medium enterprises), en el Instituto de Computación de Kobe, Japón. Actualmente, las PYMES enfrentan las mismas amenazas de seguridad de TI (Tecnología de la Información), que las organizaciones más grandes, pero sin los mismos presupuestos para manejar este problema, lo cual las hace depender cada vez más de su infraestructura de red para proporcionar servicios a sus clientes. Por tal sentido, como objetivo principal, es desarrollar una herramienta de seguridad de red económica para PYMES con una interfaz fácil y amigable para el usuario, llamada SMEsec, además, se proporcionará funciones de gestión de red, como el descubrimiento y registro de activos. Los resultados, mostraron que es posible mejorar el estado de seguridad de red de las pymes mediante una herramienta de evaluación económica, precisa y fácil de usar para las PYME. La herramienta utilizada, SMEsec, puede contribuir a resolver

problemas de seguridad de red, como la falta de expertos vinculados al tema y la limitación de presupuesto.

Giuseppi, Tortorelli, Germanà, Liberati, & Fiaschetti, (2019), realizaron la investigación, Securing Cyber-Physical Systems: An Optimization Framework based on OSSTMM and Genetic Algorithms, en la Conferencia Mediterránea sobre Control y Automatización, en Akko – Israel. El estudio de los Sistemas Ciberfísicos (CPS) se ha convertido en un tema de gran interés para los investigadores de sistemas de control, debido a que reúnen problemas derivados de la teoría clásica del control con preocupaciones relacionadas con la informática y la ciberseguridad. De tal forma, se propone un marco de optimización basado en Algoritmos Genéticos, para el control de nivel de seguridad de un Sistema Ciberfísico (CPS). Los resultados hallados, refieren que el nivel de seguridad real aumenta con las generaciones, siendo un 72,76% más seguro, además, después de realizar la optimización, el sistema aún logra resultados comparables con el mencionado anteriormente. El marco presentado, basado en algoritmos genéticos, demostró solidez como un controlador de línea en un sistema de soporte de decisiones para evaluadores de seguridad.

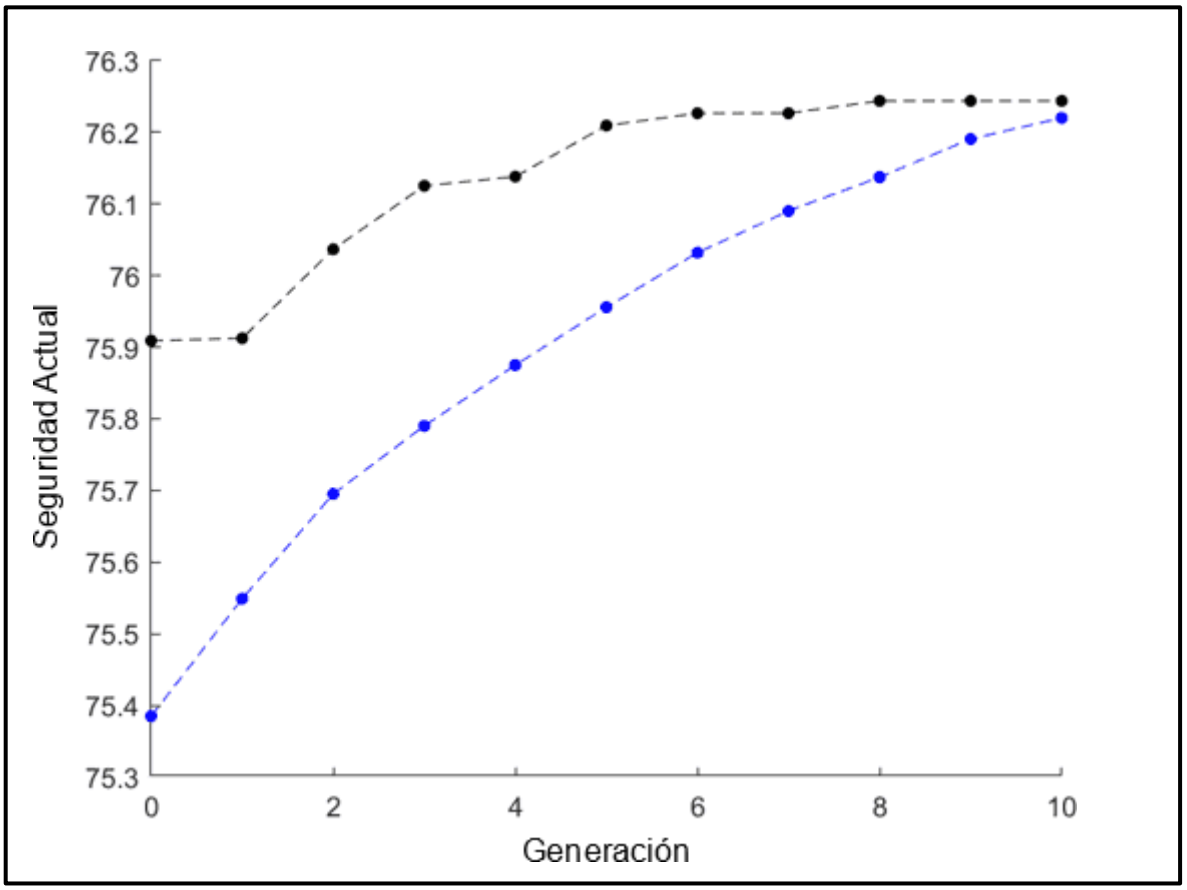


Figura 5. Simulación de la evolución de la seguridad. Fuente: (Giuseppi, Tortorelli, Germanà, Liberati, & Fiaschetti, 2019)

Rubio, Chavarria, & Mauricio, (2020), realizaron la investigación, Security architecture for the protection of digital assets in SMEs, en la Universidad Peruana de Ciencias Aplicadas, Perú. En la actualidad, se envían alrededor de 6 mil millones de correos electrónicos falsos en todo el mundo, resultando en pérdidas por fuga de datos de aproximadamente de 3 millones de dólares por empresa violada, a pesar de esto, las pymes han decidido reducir sus presupuestos de seguridad, quedando expuestas a distintas amenazas. Es por ello que se propone una arquitectura de seguridad para proteger los activos digitales de las pequeñas y medianas empresas, con el objetivo de incrementar la efectividad del mecanismo de defensa mediante el despliegue de controles efectivos. Los resultados, evidencian diversas mejoras en seguridad que puede optar dicha empresa, con lo

que puede aumentar el nivel de cumplimiento de seguridad de un 34% a un 67,86%. La propuesta de Arquitectura de seguridad, permite que las PYMES aumenten su nivel de seguridad y protejan la información que generan.

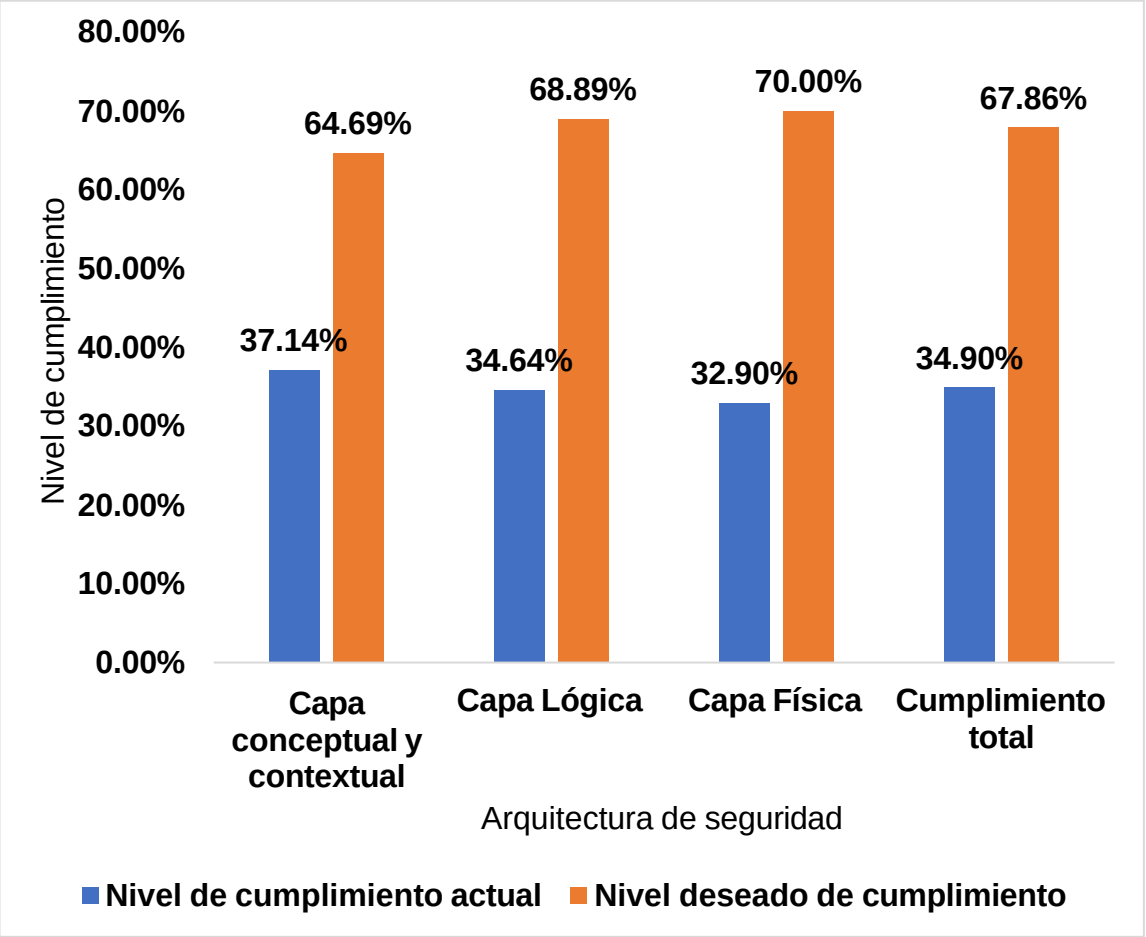


Figura 6. Diagrama de comparación del nivel de cumplimiento de la arquitectura de la seguridad. Fuente: (Rubio, Chavarria, & Mauricio, 2020)

García-Porras, Huamani-Pastor, & Armas-Aguirre, (2018), realizaron la investigación, Information Security Risk Management Model for Peruvian SMEs, en la Universidad Peruana de Ciencias Aplicadas, Perú. Mientras los sistemas de información evolucionan en la organización, el efecto del peligro se vuelve cada vez más costoso gracias a la imposibilidad de desarrollar medidas idóneas de administración de peligros y estimar el peligro de pérdidas significativas. El Banco Interamericano de Desarrollo (BD) es parte de la Organización Nacional de USA

(OEA). Por esto, se ha postulado un modelo de administración de peligros para la estabilización de la información para las pymes en Perú. Asume la metodología OCTAVES y la regla ISO / IEC 27005. 88 niveles de satisfacción para la aplicación de modelos de administración de peligros. Recomendar la administración y el cumplimiento de todos los requisitos. El modelo de administración de peligros de estabilidad de la información es simple de utilizar y le posibilita conceptualizar los controles necesarios para minimizar de manera significativa el peligro.

Montenegro & Moncayo, (2016), realizaron la investigación, Riesgo de seguridad de la información en las pymes: un modelo híbrido compatible con las NIF, Evaluación en dos pymes ecuatorianas del sector automotriz, en el Congreso Internacional de Comunicación y Gestión de la Información, Ecuador. Las PYMES, presentan dificultades de implementación, debido a distintos factores, entre ellos; el desarrollo de seguridad no forma parte de sus necesidades internas, debido a la falta de experiencia existen errores de percepción de la situación actual de la seguridad de la información y principalmente se enfocan en los negocios, siendo vulnerables a distintas amenazas cibernéticas. De tal forma, se ha propuesto desarrollar un modelo híbrido para la Evaluación y Reducción del Riesgo de Seguridad de la Información en Pymes, además de proponer mecanismos de generalización basados en ISO 27005, OCTAVE – S y MAGERIT. Los resultados encontrados, demuestran que el modelo utilizado aparte de resolver un problema específico, muestra un modelo operativo y técnicamente factible. El modelo requiere un esfuerzo razonable, e involucra a ejecutivos de negocios y personal operativo sin mayor especialización en TIC, como también, muestra la aplicabilidad técnica y operativa.

Al Friki, Aditra Putra, Suryanto, & Ramli, (2019), realizó la investigación, Evaluación de riesgos mediante la técnica de mezcla de NIST SP 800-30 Revisión 1 e ISO 27005 en empresas con objetivos de lucro: análisis de caso de la aplicación del sistema de información ZZZ en la agencia ABC en la Universidad Indonesia, Yakarta, Indonesia. El enfoque que nos da la administración es minimizar el peligro para el equilibrio de la información. Debido a que el ISO 27005 es un estándar extensamente usado por las empresas para hacer la administración de peligros de estabilidad de la información. Para eso, se busca asignar explicaciones detalladas y pasos referente a cómo usar la técnica de mezcla de ISO 27005 y NIST SP 800-30 revisión 1 para de esta forma facilitar a las piezas interesadas en el campo de la administración de peligros de estabilidad de la información la utilización de herramientas estándar alternativas al enseñar si este nuevo, se puede usar como complemento del proceso de evaluación de peligros y se puede utilizar al marco de administración de peligros ISO 27005. Los resultados obtenidos al final nos sugiere 4 escenarios de peligro elevado (prioridad), 20 moderado (segunda prioridad), 15 bajo (última prioridad) y 3 escenarios de peligro bastante bajo (sin prioridad). Este artículo se centró en la evaluación de peligros de estabilidad de la información. La búsqueda basado diferentes mapas en la que otorgó como consecuencia en la evaluación integral de peligros siguiendo el estándar ISO 27005. Se obtuvo de los detalles de la fuente de la amenaza conforme el adversario y el no contrincante en la fase de identificación de la amenaza.

Buryanina, Gogolev, Korolyuk, Lesnykh, & Suslov, (2019), realizó la investigación, Digital Differential Protection of the “Generator-Transformer” Block, en la conferencia internacional de EastConf. La principal protección por relé de los

generadores y de los bloques "generador-transformador" es la diferencial. Por esta razón, se utilizó el método alternativo de separación de los armónicos impares en las corrientes de conexión de los transformadores de potencia tras la desconexión de los cortocircuitos. Como resultado se obtuvieron que el 10% del nivel de las corrientes nominales del componente periódico, permite realizar la protección diferencial por relé de generadores, transformadores y unidades "generador-transformador". Es por ello que los transformadores de corriente tienen diferentes coeficientes nominales de transformación en relación con las corrientes secundarias del lado de la baja y de la alta tensión.

Lontsikh, Kunakov, Lontsikh, Livshitz, & Vladimirtsev, (2020), realizó la investigación, Application of information security methods based on information based on digital management approaches and the Deming cycle and the Deming cycle in the improvement of modern production modern production processes, en la Universidad ITMO de San Petersburgo de Rusia. La producción actualizada es un sistema exclusivo e incluido de producción y diseño de alta tecnología. Es por ello que se utilizó las herramientas de gestión de control integrado que proporcionan soluciones correctas mediante la creación de modelos electrónicos en el diseño de sistemas y complejos de producción. Como resultado se obtuvo que el 17,25% en comparación del método manual, se reduce la tasa media de defectos de un determinado proceso tecnológico. De tal forma que para los procesos tecnológicos identificados en la retroalimentación de la "Gestión" y la aplicación de los requisitos de seguridad de la información, es posible optimizar el proceso tecnológico de producción moderno, para reducir el porcentaje de rechazos, los materiales y el coste del tiempo.

Khalid Eisa, Shamsul Kamal, Noor Azah, Sapiee, & Kamaruddin Malik, (2019), realizó la indagación A policy-based, human-oriented information security model human-oriented, policy-based model: a case study in the UAE banking case study in the UAE banking sector,en la Facultad de Informática y Tecnología de la Información Universidad Tun Hussein Onn de Malasia. Al adoptar una política de seguridad de la información, las organizaciones establecen bases sólidas sobre las que se pueden difundir y aplicar prácticas de seguridad sólidas dentro de la organización. Se realizaron tres entrevistas semiestructuradas a expertos en seguridad de tres bancos locales de los EAU: Al Hilal Bank, Arab Bank y Sharjah Bank. Se empleó una guía de entrevista semiestructurada con cuatro preguntas principales sobre el conocimiento de la política de seguridad, la formación en materia de seguridad, la autoeficacia informática y el cumplimiento general por parte de los empleados del banco. Se obtuvo como resultado que el 40% de la eficacia del personal en el manejo de la informática y la seguridad se pueden realizar análisis y necesidades de formación a partir de la matriz. Es por eso que las empresas siguen invirtiendo en seguridad de la información, los errores humanos siguen siendo una de las causas principales de las violaciones de datos en las organizaciones.

Mashkina, Guzairov, Vasilyev, Tuliganova, & Konovalov, (2016), realizó la indagación, Information security control issues in the virtualization segment of the information system of the company, en la Universidad Técnica Estatal de Aviación de Ufa, Rusia. La investigación de los problemas de control de seguridad de la información en el clúster de virtualización debe comenzar desde la determinación de los sujetos de acceso (usuarios, procesos) y los objetos de acceso. Los sujetos de acceso en el marco de virtualización. Es por ello que se utilizó este modelo que

está construido para el caso de interacción de red en un marco virtual cuando la VM puede iniciar una conexión a una red externa (en relación con el host donde se estaba ejecutando) y está disponible desde el entorno externo como computadora independiente. Se obtuvo como resultados de resolver la tarea de construir el sistema de relaciones de acceso en el modelo de virtualización de hipervisor sobre la base del modelo de rol de delimitación de acceso para la virtualización de SI de la empresa. Es por ello que los procesos de seguridad son individuales para cada empresa y corresponden a la política de seguridad de la información desarrollada que es necesaria para la documentación clara de las tareas establecidas por el liderazgo de la empresa para establecer el conjunto de requisitos comerciales.

Zaynalov Nodir et al., (2019), realizó la investigación, Information security issues for travel companies, en la Universidad de Tecnologías de la Información de Auckland. La provisión de información turística es la implementación de la efectividad de las actividades turísticas en todos los segmentos de gestión con la base de datos de información de Turismo y su procesamiento a través de un conjunto especial de Tecnologías de la Información. La investigación en esta área se centra principalmente en los aspectos sociales de la seguridad de la información. Por ejemplo, Zimanyi y Kovary y otros analizan y analizan principalmente los factores sociales en el desarrollo del turismo y su seguridad. Al Es por ello que en cada área del turismo se obtuvo un resultado que representa el 10% de las exportaciones totales de todo el mundo y el 35% del negocio de servicios. Situado en la Enorme Ruta de la Seda, tiene un potencial real para el desarrollo de la red turística de la República de Uzbekistán, que fue popular por sus localidades viejas

con una historia y un trasfondo cultural centenarios. Por consiguiente, el desarrollo y utilización de las sugerencias y sugerencias en el campo de la estabilidad de los datos acerca de la base de la categorización de estabilidad de la información turística descrita antes mejorará todavía más la infraestructura turística, incrementará su llamativo e incrementará el flujo de turistas.

1.3. Teorías relacionadas al tema.

1.3.1. Normas ISO/IEC

1.3.1.1. ISO/IEC 27001

El proyecto SGSI incluye 5 fases. Las 5 fases son: Definición Alcance, hacer estudio de brechas, hacer evaluación de peligros, establecer controles y fines y establecer políticas y Programa SGSI.

La fase de estudio de brechas es elemental evaluar la postura de hoy de la organización en el SGSI.

La fase de estudio de brechas es elemental evaluar la postura presente de la organización en el SGSI. realizado. Este análisis propone utilizar AHP para decidir qué controles de estabilidad de la información son más importantes las necesidades y fines de la organización. Realizaremos el proceso En una organización llamada Instituto XYZ en Indonesia. (Wens, 2019)

1.3.1.2. ISO/IEC 27005

Un estándar de la serie ISO 27005 que define los principios en general de la administración de peligros de estabilidad de la información. Esta es una regla que apoya la ISO 27001 en las ocupaciones de administración de peligros y define el inicio por medio del cual se desarrollan los

procedimientos para evaluar y abordar los peligros de estabilidad de la información en la organización. Basado en el periodo de requisitos (ciclo PDCA), esta regla define ocupaciones para planear, llevar a cabo, evaluar y mejorar la administración de peligros de estabilidad de la información y promueve una cultura de optimización continua. (Agrawal, 2017)

ISO 27005 tiene un proceso paso a paso que incluye implantar el entorno, evaluar los peligros de estabilidad de la información, gestionar los peligros de estabilidad de la información, admitir los peligros de estabilidad de la información, comunicar los peligros de estabilidad de la información, monitorear y verificar los peligros y la estabilidad de la información. Entablar el entorno es un criterio necesario para implantar la administración del equilibrio de la información. Esto instituye un entorno para interpretar el alcance y las fronteras del peligro adecuados al grado de estabilidad de la información. La evaluación de peligros de estabilidad de la información es la fase de medición e interpretación de peligros cualitativos.

Los resultados de la evaluación de peligros son información sustancial para cada una de las piezas interesadas. Los directores priorizan los peligros en funcionalidad de la gravedad percibida u otros criterios establecidos. El proceso de evaluación de peligros incluye algunas ocupaciones como identificación, estudio y evaluación. Hay diversos tipos de identificadores de activos, que integran información, programa, hardware, activos de servicio, recursos humanos y activos intangibles, como la fama y la imagen de una organización. Además de la identificación de activos, la

identificación de peligros además incluye la identificación de amenazas, controles existentes y vulnerabilidades. La etapa de estudio de peligros evalúa el peligro en funcionalidad del grado y la prioridad del peligro desarrollado. La priorización de peligros se completa a lo largo de la etapa de evaluación de peligros. (blokdyk, 2019)

1.3.2. Instituto Nacional de Estándares y Tecnología (NIST)

NIST es un acrónimo del Instituto Nacional de Estándares y Tecnología. El marco de estabilidad cibernética del NIST puede contribuir a las organizaciones de todos los tamaños a entender mejor sus peligros de estabilidad cibernética, regir y reducir sus peligros y ayudarlo a establecer la era primordial. localización de las defensas de estabilidad de la red. (Al Friki, Aditra Putra, Suryanto, & Ramli, 2019)

El marco de estabilidad cibernética del NIST puede ser ejecutado en cinco aspectos dentro de una organización como identificación, protección, detección, respuesta y recuperación.

1.3.3. Matriz de Evaluación de Riesgos (RAM)

La Matriz de Evaluación de Riesgos (RAM, acrónimo de Matriz de Evaluación de Riesgos en inglés) es una herramienta útil para visualizar de manera efectiva los riesgos cuya evaluación ha sido aprobada. Cada riesgo estará representado por dos puntos en la matriz, uno en la fase de calificación y otro en la fase de evaluación. Según el valor de riesgo de cada punto, estos puntos se ubican en la intersección del eje de influencia y el eje de probabilidad.

Una Matriz de Evaluación de Peligros, además famosa como Matriz de Peligros de Posibilidad y Severidad, está diseñada para ayudarlo a reducir la posibilidad de peligro potencial para optimizar el manejo del plan. Prácticamente, una matriz de peligros es una explicación visual de los peligros que están afectando a un plan para permitir que las organizaciones desarrollen un plan de mitigación. (Markovic, 2019)

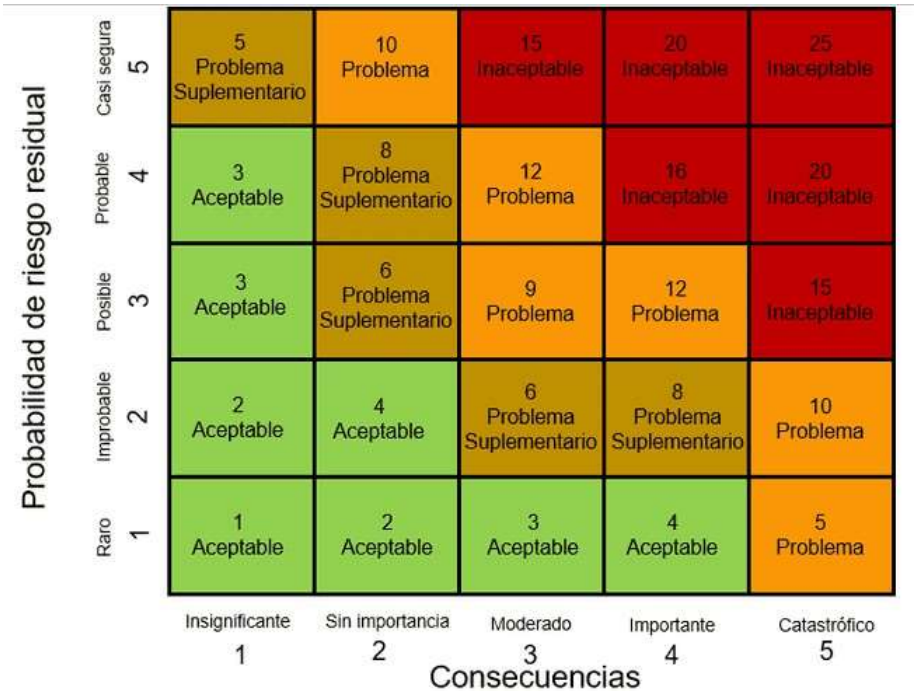


Figura 7. Matriz de evaluación de riesgo según metodología RAM. Fuente: *(Markovic, 2019)*

1.3.4. Metodología OCTAVE

Amenaza operativamente crítica, Evaluación de activos y vulnerabilidades (OCTAVE) es una metodología elaborada por CERT / CC en 2001, de los cuales la tecnología está censurada por la estabilidad y toma de elecciones sobre defensa de información, basada en peligro de confidencialidad, tienen la posibilidad de estar sujetos a totalidad y

disponibilidad de activos con información clave. (García, Fresia, & Lema Moreta, 2018)

Según OCTAVE, es una metodología autodirigida, sin embargo, requiere un equipo interdisciplinario (compuesto por personas del departamento de operaciones y TI), cuyo enfoque es diferentes necesidades de custodia y puntos de equilibrio: Peligro operacional, prácticas de estabilidad y tecnología) De igual manera, indicando que la utilización de OCTAVE. Hay 3 fases evidentemente definidas:

- La primera fase, Perspectiva operativa: Implantar qué es esencial para la organización (activos involucrados con la información) y las tácticas / medidas que se permanecen aplicando.
- La Segunda fase, Perspectiva Tecnología: investigue los factores operativos clave y encuentre sus debilidades. Esto puede dar lugar a acciones fraudulentas en activos críticos.
- La tercera fase se basa en formular tácticas y planes: En este periodo, desde la información obtenida de los pasos anteriores, se formulan tácticas y planes para afrontar a los peligros de los activos clave.

1.3.4.1. OCTAVE-S

El método de evaluación de vulnerabilidades, activos y amenazas críticas operacionales (OCTAVE) define las técnicas de planificación y evaluación estratégicas basadas en los riesgos de seguridad.

OCTAVE-S es una variante del método, adecuado para los medios limitados y las limitaciones únicas que suelen encontrarse en

organizaciones pequeñas (menos de 100 personas). OCTAVE-S consta de un pequeño equipo interdisciplinario (tres

Cinco personas) el personal de la organización, recopilan, analizan y producen información. (Alberts, Dorofee, Steven, & Woody, 2005)

Dentro de la metodología OCTAVE – S encontramos 3 fases las cuales se desglosan en 5 procesos y estos últimos son segmentados en actividades. Primero hablemos de las 3 fases de OCTAVE -S.

- Fase uno: Construir perfiles de amenaza con base en activos. Este paso es una evaluación desde una perspectiva organizacional. En este punto, el documento de investigación define los criterios de evaluación del punto final que se utilizarán más adelante para nuestra evaluación de riesgos. Además, se deben identificar los activos más relevantes para la organización y evaluar las prácticas actuales de estabilidad y control de la organización. Una vez que esta información está en su lugar, la herramienta de investigación recopila toda la información y realiza cada tarea, luego selecciona de 3 a 5 activos clave para analizar más a fondo. Finalmente, los accesorios explican tanto el perfil de amenazas como los requisitos de estabilidad de todos los activos críticos identificados.

Figura 8. La fase 01 con sus actividades y procesos de OCTAVE – S. Fuente: *(Alberts, Dorofee, Steven, & Woody, 2005)*

- Fase dos: Identificar vulnerabilidades de la infraestructura.

Este paso es una evaluación técnica, en la que el equipo realiza pruebas de alto nivel en la infraestructura de TI de la organización, correlacionándola con la estabilidad de la infraestructura bajo revisión. Con esto, puede verificar el uso de la infraestructura para comprender quién está importando activos clave y quién es responsable de configurar y mantener la infraestructura. Finalmente, la herramienta de encuesta consideró el tamaño de cada segmento de mercado, incluida la estabilidad de sus operaciones y prácticas de TI.

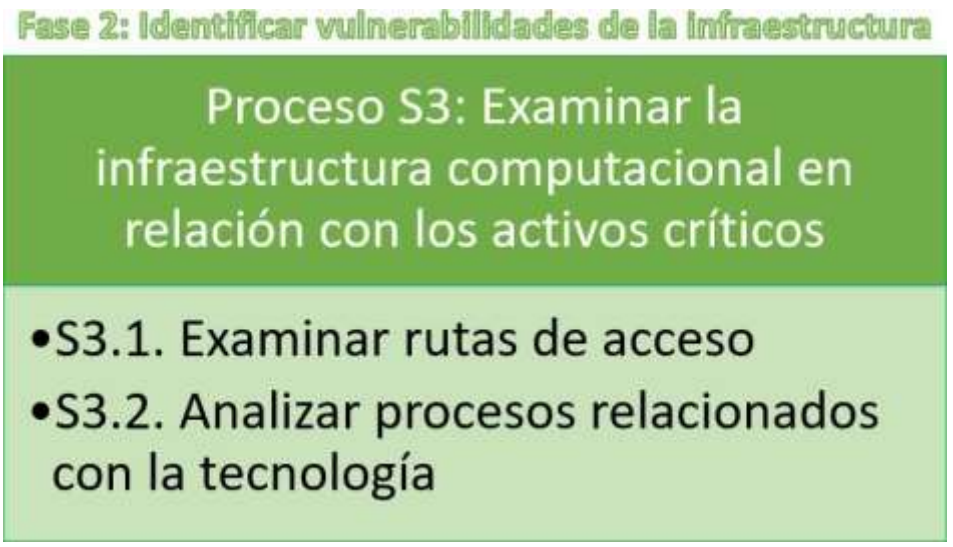


Figura 9. La fase 02 con sus actividades y procesos de OCTAVE – S. Fuente: *(Alberts, Dorofee, Steven, & Woody, 2005)*

- Fase tres: Desarrollo de Planes y Tácticas de estabilidad

  En esta etapa se identifican los peligros a los permanecen expuestos los activos críticos de la organización por los accesorios de estudio y se dictamina qué hacer con ellos.

  Los accesorios crean un plan de defensa para la organización y ejecuta planes de mitigación con la información recopilada para afrontar a los peligros que permanecen expuestos los activos críticos.

Figura 10. de La fase 03 con sus actividades y procesos de OCTAVE – S. Fuente: *(Alberts, Dorofee, Steven, & Woody, 2005)*

Finalmente, los resultados que otorga OCTAVE – S otorga los siguientes puntos:

- Un plan de defensa para toda la organización: Esto va en dirección con en relación a sus prácticas de estabilidad de la información.

  • Planes de mitigación de riesgos: Dichos aún permanecen con el propósito de minimizar los peligros asociados con los primordiales activos por medio de la mejora de los procedimientos de estabilización seleccionados.

  • Lista de actividades: tiene recursos para actividades a corto plazo correctas para combatir debilidades concretas.

  • OTROS RESULTADOS En LA OCTAVE - S: incluye los activos de información importantes que usted da a la organización, el perfil de peligro y destaca los resultados que demuestran la función de la organización para continuar buenas prácticas bien establecidas. Cabe decir que todas las etapas de la metodología

OCTAVE – S crea sus propios resultados como información eficaz para mejorar la estabilidad de la información en la organización.

1.3.4.2. OCTAVE-ALLERGO

El procedimiento OCTAVE-ALLERGO está elaborado para permitir una evaluación integral del ámbito de peligro operativo de una organización, de manera se logren obtener resultados más confiables sin la necesidad de un entendimiento profundo de la evaluación de peligros. Este procedimiento es distinto del procedimiento OCTAVE anterior en que concentra cómo se aplican los activos de información, dónde se almacenan, transmiten y procesan, cómo permanecen expuestos a amenazas y vulnerabilidades, estabilidad e interrupciones. Al igual que con el enfoque anterior, OCTAVE Allegro se puede realizar en un marco de trabajo colaborativo estilo taller y se fundamenta en las pautas, documentos de trabajo y formularios proporcionados en el apéndice de este archivo. No obstante, OCTAVE Allegro además es correcto para esos que aspiran hacer evaluaciones de peligro sin una inversión fuerte, vivencia o inversión organizacional. (Calalee, Stevens, Young y Wilson, 2007)

1.3.5. MEHARI

Busca que se establezca un instrumento sólida y base para la administración de peligros, para esto sigue un grupo de herramientas y recursos que fortalecen los principios dictados en ISO/IEC 27005:2008. Otra característica fundamental de Mehari es su simplicidad en la preparación de tácticas, puesto que se enfoca en tener en cuenta las

restricciones del comercio, como por ejemplo presupuesto y evaluación de controles existentes; además en tener en cuenta la capacidad que tiene que exponer una organización para hacer frente los escenarios de peligros que se detectan, todo con base al lenguaje común de cada una de las piezas para un exclusivo conocimiento de criterios de evaluación de peligros. Secundado de una sólida documentación, Mehari, da resoluciones de reducción y control de peligros, ya probadas en varios rubros de comercio en todo el mundo, pudiendo de esta forma más grandes adeptos para la supervisión de peligros de estabilidad de la información y permitiendo adaptar las últimas tendencias tecnológicas y procedimientos o técnicas en relación a la estabilidad de la información. (García, Fresia, & Lema Moreta, 2018)

1.3.6. SP800-30

NIST SP 800-30 se usa para dar pautas de evaluación de peligros para los sistemas de información de empresas y gobiernos y como complemento de NIST SP 800-39. Los estándares de estabilidad y otras pautas garantizan el enfoque de la evaluación de peligros NIST SP800-30 revisión para regir los peligros de estabilidad de la información. (Al Friki, Aditra Putra, Suryanto, & Ramli, 2019)

1.3.7. MAGERIT

Se caracteriza por continuar los principios dictados en la regla mundial ISO 31000, los cuales a la vez son la base para la otra regla enfocada en la administración de peligros de estabilidad de la información, ISO/IEC 27005, dicha caracterización, ha promovido para que el punto de vista de esta metodología, una vez implementada en la organización,

> se sienta como un fomento a la cultura organizacional y se manifieste como apoyo a las metas comerciales, ya que en las metas comerciales, se piensan peligros comerciales, y en dichos últimos, deberán estar presentes las metas tecnológicos de la compañía, por consiguiente, gracias a la escala analizada, una metodología de estabilidad de la información, hoy por hoy, se estima como un impulsor general para el comercio. Sin embargo, poquísimos poseen la destreza de demostrarlo con resultados hacia los directivos de la organización. (Administraciones, 2012)

Gestión de Riesgos

La gestión de riesgos es un enfoque organizado y estructurado, el cual sirve para analizar los riesgos y evaluarlos para posteriormente mitigarlo o solucionarlos, manteniendo así, la integridad de la información de una empresa. (Alwi & Zainol Ariffin, 2018)

Activos

Los activos en una empresa son aquello que tiene valor para una empresa y se puede devolver como un producto de retorno o de inversión que le puede generar ingresos.(SANTISTEBAN, 2019) define que: “un activo es un elemento de valor para la organización, el cual tiene como propósito contribuir a la consecución de sus objetivos”.

Vulnerabilidades o ataques organizacionales

(Giuseppi, Tortorelli, Germanà, Liberati, & Fiaschetti, 2019) Las vulnerabilidades o ataques organizacionales son aquellas amenazas que tiene la empresa, como consecuencia de no asegurar bien su información, dentro

de estas vulnerabilidades existen diferente tipo de ataques, identificados generalmente como:

- Virus informáticos o código malicioso
- Robo de Información
- Denegación de Servicios (DoS)
- Alteración de la Información
- Suplantación de la identidad
- Fraudes basados en el uso de computadores

Seguridad de la Información

La protección de la seguridad de la información en una empresa es muy importante proteger sus datos, ya que los accidentes o acciones malintencionada puede perder la integridad y confidencialidad de los datos almacenados. (Montenegro & Moncayo, 2016)

NIIF

Combina los métodos cuantitativos y cualitativos con la norma ISO 27005, para estimar el impacto de activos de riesgo. El modelo desarrollado formaliza las relaciones involucradas en la evaluación de riesgo, el proceso convencional cualitativo combinas métricas, técnicas y mejoras de prácticas de OCTAVE-S, MARGERIT E ISO 27005, es una norma aceptada a nivel mundial. (Montenegro & Moncayo, 2016)

PYMES

En las pequeñas o medianas empresas, los procesos buscan que las pymes pueden cuantificar el riesgo de los activos para así comprender la causa de las vulnerabilidades de una gestión de riesgos. (García-Porras, Huamani-Pastor, & Armas-Aguirre, 2018)

1.4. Formulación del Problema.

¿Cómo mejorar en forma efectiva la seguridad de la información en una PYME peruana?

1.5. Justificación e importancia del estudio.

Es fundamental detectar las deficiencias de la seguridad informática, debido a que es benéfico para prevenir la pérdida de la información y de esta forma tener una buena protección.

En esta investigación, se va a desarrollar un modelo de gestión de riesgos de la seguridad de la información para una PYME peruana, para lo cual se ha optado por elegir la metodología OCTAVE-S para la identificación de Riesgos en la que puede verse vulnerada la empresa y basándose en la norma ISO/IEC 27005 para estandarizar los riesgos y así identificar las vulnerabilidades de infraestructuras, estrategias de un perfil de amenazas de planes de seguridad.

1.6. Hipótesis.

Mediante la aplicación de un modelo de procesos de seguridad de la información basado en la norma ISO/IEC 27005 y la metodología OCTAVE-S se mejora en forma efectiva la seguridad de la información en una PYME peruana.

1.7. Objetivos.

1.7.1. Objetivo general.

Implementar un modelo de procesos de seguridad de la información para una pyme peruana basado en la norma ISO/IEC 27005 y la metodología OCTAVE - S.

1.7.2. Objetivos específicos.

a) Diagnosticar la seguridad de la información de una PYME peruana previamente seleccionada.

b) Caracterizar la metodología OCTAVE-S y la norma ISO/IEC 27005 en el contexto de la seguridad de la información.

c) Diseñar el modelo de procesos de seguridad de la información para una Pyme peruana.

d) Aplicar el modelo de procesos de seguridad de la información en el caso de estudio.

e) Evaluar el modelo mediante juicio de experto.

II. MATERIAL Y MÉTODO

2.1. Tipo y Diseño de Investigación.

El proyecto corresponde al tipo de investigación cuantitativa y tecnología aplicada, pues antecede al conocimiento científico para lograr las metas propuestas,

además, utilizará los indicadores que se han aplicado para posteriormente obtener los resultados que ayudarán a dar solución a problemas de seguridad en una PYME con el modelo implementado.

El diseño de investigación es cuasi experimental, puesto que, se va a manejar la muestra para obtener resultados reales, donde se tomarán estrategias existentes para realizarlos e identificar las posibles amenazas de los activos críticos dentro de una PYME.

2.2. Población de estudio, muestra, muestreo y criterios de selección.

2.2.1. Población

La población tomada para esta investigación son los procesos dentro de una pyme, los cuales se utilizarán para identificar de mejor manera los activos de la misma. En la siguiente tabla se plasma la población resultante:

Tabla 3.

Tabla de población de la investigación

Población	
Procesos	**Nombre**
P01	Prospección y Adquisición de Clientes
P02	Gestión de Pedidos
P03	Atención al Cliente
P04	Facturación y Cobranza
P05	Recepción de Mercancías
P06	Gestión de Inventarios
P07	Preparación de Pedidos
P08	Mantenimiento de Almacén
P09	Planificación de Rutas
P10	Transporte y Entrega
P11	Gestión de Flota

P12	Logística Inversa
P13	Tecnología y Sistemas de Información
P14	Calidad y Mejora Continua
P15	Gestión de Recursos Humanos

Nota: Los procesos de la empresa DESPENSA PERUANA S.A

2.2.2. Muestra

La muestra para el presente trabajo de investigación se consideró tomar un muestreo no probabilístico por conveniencia de la investigación, en la cual se establecerá cuatro criterios que serán medidos según:

- Valor estratégico del proceso(C1).
- Criticidad de los activos de información involucrados(C2).
- Importancia operativa y comercial de la disponibilidad, la confidencialidad y la totalidad(C3).
- Expectativas y percepciones de las partes interesadas, y consecuencias negativas para la buena voluntad y la reputación(C4).

En una escala de acuerdo con Cobit 5 desde débil (1), Normal (3), fuerte (5).

Tabla 4.

Tabla de criterios de evaluación para la muestra

Criterios de Evaluación		
C1	Valor estratégico del proceso	Es una valoración acerca del proceso que genere un impacto importante en la empresa.
C2	Criticidad de los activos	Es una valoración acerca de los activos de información involucrados.
C3	Importancia operativa y comercial	Es una valoración de la disponibilidad, confidencialidad e totalidad operativa y comercial de los procesos
C4	Expectativas y percepciones	Es una valoración sobre las expectativas y percepciones de las partes interesadas y consecuencias negativas para la buena voluntad y la reputación de la empresa

Nota: Cada criterio de evaluación se ha seleccionado, basado en la norma ISO/IEC 27005.

Tabla 5.

Tabla de clasificación y selección de la muestra

N°	Procesos	C1	C2	C3	C4	Total
P01	Prospección y Adquisición de Clientes	3	3	3	3	12
P02	Gestión de Pedidos	5	1	5	1	12
P03	Atención al Cliente	3	2	3	5	13
P04	Facturación y Cobranza	5	4	2	3	14
P05	Recepción de Mercancías	5	5	5	5	20
P06	Gestión de Inventarios	5	4	5	5	19
P07	Preparación de Pedidos	2	3	2	3	8
P08	Mantenimiento de Almacén	5	4	5	5	19
P09	Planificación de Rutas	2	3	3	3	8
P10	Transporte y Entrega	2	2	3	4	11
P11	Gestión de Flota	3	3	3	3	12
P12	Logística Inversa	2	3	3	3	11
P13	Tecnología y Sistemas de Información	5	4	5	5	19
P14	Calidad y Mejora Continua	3	2	2	4	11
P15	Gestión de Recursos Humanos	3	2	1	4	10

Fuente: Elaboración propia

Finalmente se tomará como muestra 4 procesos con nivel de criticidad mayor a 18, puesto que cumple con los criterios de evaluación de riesgos que define la norma ISO/IEC. Estos son:

Tabla 6.

Tabla de los procesos seleccionados para la muestra

MUESTRA		
PROCESOS	**NOMBRE**	**NIVEL DE CRITICIDAD**
P05	Recepción de Mercancías	20
P06	Gestión de Inventarios	19
P08	Mantenimiento de Almacén	19
P13	Tecnología y Sistemas de Información	19

Fuente: Elaboración propia.

2.3. Variables, Operacionalización.

2.3.1. Variable independiente

Modelo de procesos de seguridad de la información basado en la norma ISO/IEC 27005 y la metodología OCTAVE-S.

2.3.2. Variable dependiente

La seguridad de la información en una PYME.

Tabla 7.

Operacionalización de la variable

Variables	Dimensión	Indicador	Ítem	Técnica e instrumentos de recolección de datos
Modelo de procesos de seguridad de la información basado en la norma ISO/IEC 27005 y la metodología OCTAVE-S.	Criterios de implementación	Costo de Implementación.	$CI = \frac{\sum^{n} ct_i}{CE} x\ 100$	Revisión documental – Ficha de Resumen
		Tiempo de Implementación.	$TI = \frac{\sum_i^n tt_i}{Te}\ x\ 100$	Revisión documental – Ficha de Resumen
		Nivel de cumplimiento con estándares	$NC = [\frac{\sum_i^n PCC}{TCE}]\ x\ 100$	Revisión documental – Ficha de Resumen
La seguridad de la información en una PYME	Matriz de Ponderación	Nivel de riesgo de los activos de la seguridad de la información.	$R = PA\ x\ MD$	Revisión documental – Ficha de Resumen
		Nivel de Criticidad de los activos de la seguridad de la información.	$NC = \frac{\sum^{n} EC_i}{CAA}$	

Revisión documental – Resumen	Ficha de	Eficacia de la seguridad de la información.	$E = \frac{Ra}{\overline{Rp}} * 100$	Revisión documental – Ficha de Resumen

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad.

2.4.1. Técnicas

- **Revisión Documental**

Esta técnica fue pieza fundamental en el desarrollo de la propuesta de tesis, puesto que ayudará a identificar toda la documentación como los activos y procesos de la pyme, también los controles del modelo y sus costos y tiempos de implementación, puesto que se podrá manipular los datos y la validez de los criterios de implementación tanto del modelo como de la confiabilidad de los datos de la seguridad de la información de una pyme.

Costo de Implementación: Se revisó documentación del costo de cada control que tiene el modelo por proceso, posteriormente se recopilará información de otros modelos con el mismo fin y se calculará un costo estimado frente al costo real del modelo.

Tiempo de Implementación: Se revisó documentación del tiempo de cada control que tiene el modelo por proceso, posteriormente se recopilará información de otros modelos con el mismo fin y se calculará un tiempo estimado frente al tiempo real del modelo.

Nivel de cumplimiento con estándares: Se tomó la documentación existente del estándar ISO/IEC 27005 para definir los criterios a los que será sometido el modelo y con la documentación que arrojen los controles del modelo por cada proceso, determinar el nivel de cumplimiento con el estándar.

Nivel de riesgo de los activos de la seguridad de la información: Se revisó la documentación de los procesos de la pyme que contenga los activos críticos, estos documentos se plasman como ficha de ética y protección del empleado, ficha de registro de asistencias, visitas o de los empleados y archivos log del software que maneje la pyme para identificar sus activos.

Nivel de criticidad de los activos de la seguridad de la información: Se revisó la documentación de todos los procesos de la pyme que contenga activos de la empresa como ficha de ética y protección del empleado, ficha de registro de asistencias, visitas o de los empleados y archivos log del software que maneje la pyme para identificar sus activos.

Eficacia de la seguridad de la información: Se revisó la documentación de la pyme como ficha de seguridad y plan de contingencia frente amenazas que la pyme haya podido tener antes de aplicar el modelo y tener un punto inicial por dónde empezar.

2.4.2. Instrumentos

- **Ficha de Resumen**

Con este instrumento se podrá identificar los diferentes resultados de cada proceso basándose en los criterios señalados en el anexo 4, para lograr satisfacer las necesidades que el modelo requiera y así poder sustentar los resultados y las soluciones que este puede brindar, sin dejar de lado la validez y confiabilidad que deben tener los datos.

2.5. Procedimiento de análisis de datos.

El procedimiento de análisis se tomará con el instrumento de ficha de resumen, los cuales serán recopilados de la misma documentación del modelo y también de la misma empresa como las fichas de registros de sus activos y de los logs que arroje del software que tenga la pyme.

Criterios de implementación

Costo de Implementación: Para el costo de implementación, se calculó el costo unitario por cada proceso del modelo, luego, se identificó la cantidad de instancias en la que este proceso del modelo ha sido aplicado(instancias por cada proceso de la empresa), posteriormente, se realizó una sumatoria del costo unitario por cada proceso y se comparó con un costo estimado, previamente evaluado, para así definir el porcentaje del costo con el que se está desarrollado el modelo de seguridad de la información y la diferencia del costo real con el costo estimado.

$$CI = \frac{\sum_{i}^{n} di}{CE} \; x \; 100$$

Donde:

Descripción de las variables del indicador costo de implementación

Tabla 8.

Descripción de variables del indicador de costo de implementación.

Variable	Descripción
CI	Costo de Implementación del modelo

n	Límite total del costo unitario por control del modelo por cada proceso
i	Límite inicial del costo unitario por control del modelo por cada proceso
ct_i	Costo total de implementación del modelo por cada proceso
CE	Costo estimado de implementación del modelo que será comparado con el costo real

Fuente: Elaboración Propia.

Tiempo de Implementación: Para calcular el tiempo de implementación del modelo, primero se tomó el tiempo unitario que demoró en desarrollarse cada proceso del modelo, para posteriormente determinar la cantidad de instancias (procesos de la empresa) en donde los procesos del modelo fueron aplicados y de esto sacar un subtotal del tiempo de implementación. Finalmente, para poder aplicar la fórmula se tiene que calcular la sumatoria del subtotal del tiempo de todos los procesos para finalmente enfrentarlo a un tiempo estimado, previamente evaluado, para así definir el porcentaje del tiempo con el que se está desarrollando el modelo de seguridad de la información y también la diferencia del tiempo real con el tiempo estimado.

$$TI = \frac{\sum_{i}^{n} tti}{Te} \; x \; 100$$

Donde:

Descripción de las variables del indicador tiempo de implementación.

Tabla 9.

Descripción de las variables del indicador de tiempo de implementación.

Variable	Descripción
TI	Tiempo de implementación del modelo
Te	Tiempo estimado de implementación del modelo que será comparado con el tiempo de implementación real del modelo
n	Límite total del tiempo unitario por control del modelo por cada proceso
i	Límite inicial del tiempo unitario por control del modelo por cada proceso
tt_i	Tiempo total de implementación del modelo por cada proceso

Fuente: Elaboración Propia.

Nivel de cumplimiento con estándares: Para obtener el nivel de cumplimiento con estándares, se necesita calcular la sumatoria de los resultados de criterios cumplidos por cada proceso(en un rango de 0 a 4), para posteriormente sacar el promedio con tantos procesos de la empresa se han evaluado, finalmente se procede a dividir por el total de criterios de evaluación (según el estándar ISO/IEC 27005 son 4) y para hallar el porcentaje de cumplimiento se multiplica por 100, lo cual nos dará como resultado el nivel de cumplimiento con estándares.

$$NC = [\frac{\sum_{i}^{n} RCC}{TP} / TCE] * 100$$

Donde:

Descripción de las variables del indicador nivel de cumplimiento con estándares.

Tabla 10.

Tabla de descripción de las variables del indicador nivel de cumplimiento con estándares

Variable	Descripción
NC	Nivel de cumplimiento con estándares (Incumplido completamente, incumplido a medias, cumplido a medias, cumplido completamente)
$\sum_{i}^{n} RCC$	Sumatoria de los resultados de criterios completados por proceso
TP	Total de Procesos de la investigación
TCE	Total de criterios de comparación de estándares
n	Límite total de procesos de la empresa
i	Límite inicial de procesos de la empresa

Fuente: Elaboración Propia.

Matriz de Ponderación

Nivel de riesgo de los activos de la seguridad de la información: Este indicador ayuda a identificar el nivel de riesgo al cual están sometidos los activos críticos de la pyme para posteriormente identificar posibles soluciones y controles de mitigación posteriores.

Cabe resaltar que en base a la metodología OCTAVE - S los rangos de selección para el análisis del nivel de riesgo son los siguientes: (Alberts, Dorofee, Steven, & Woody, 2005)

Alto Riesgo (12 – 16)

Medio Riesgo (8 – 11)

Bajo Riesgo (1 - 7)

$$R = PA \times MD$$

Donde:

Descripción de las variables del indicador nivel de riesgo a los que están sometidos los activos críticos de la pyme.

Tabla 11.

Tabla de descripción de las variables del indicador nivel de riesgo a los que están sometidos los activos críticos de la pyme.

Variable	Descripción
R	Nivel de riesgo a los que están sometidos los activos críticos de la pyme.
PA	Probabilidad de amenaza existente con respecto al rubro de la pyme.
MD	Magnitud de daño con respecto a los activos críticos de la pyme.

Fuente: Elaboración Propia.

Nivel de Criticidad de los activos de la seguridad de la información: El nivel de criticidad de los activos lo necesitamos para verificar que activos dentro de los procesos previamente seleccionados son realmente importantes al momento de ejecutar el modelo. Para esto se definió una estimación de criticidad donde vemos

ítems que tienen relación con el activo seleccionado, para esto primero hacemos la sumatoria por cada grupo de activos definidos en el anexo 1 y 2. Posteriormente se realiza un promedio de los ítems totales por cada grupo de activos de la estimación de criticidad y de la cantidad de activos agrupados. El nivel de criticidad está evaluado dentro de un rango de 0 – 17:

Bajo (13 – 17)

Medio (7 – 12)

Bajo (0 - 6)

$$NC = \frac{\sum_{i}^{n} EC_i}{CAA}$$

Donde:

Descripción de las variables del indicador de nivel de criticidad de los activos de la seguridad de la información.

Tabla 12.

Tabla de descripción de las variables del indicador de nivel de criticidad de los activos de la seguridad de la información

Variable	Descripción
NC	Nivel de criticidad basado en procesos de los activos de la pyme.
EC	Estimación de Criticidad basados en la experiencia de la pyme o generales con respecto a los activos de la pyme
CAA	Cantidad de activos Agrupados

Fuente: Elaboración Propia.

Eficacia de la seguridad de la información: Este indicador nos ayuda a medir la eficacia de la seguridad que tiene la pyme en un punto inicial y al final del procedimiento y así poder sacar las conclusiones respectivas sobre la influencia del modelo.

$$E = \frac{Ra}{Rp} * 100$$

Donde:

Descripción de las variables del indicador de eficacia de la seguridad de la información.

Tabla 13.

Tabla de las variables del indicador de eficacia de la seguridad de la información

Variable	Descripción
E	Eficacia de la seguridad de la información.
Ra	Resultado alcanzado con respecto a la pyme
Rp	Resultado propuesto con respecto al modelo.

Fuente: Elaboración Propia.

2.6. Criterios éticos.

Confidencialidad: La estrategia de investigación consistirá en asignar un alias para asegurar la protección de la identificación personal del autor del proyecto. Además, cabe señalar que la información obtenida será recopilada de acuerdo con los estándares y valores que deben poseer los profesionales.

Derechos de Autor: Este proyecto respeta la autoría de cada documentación utilizada para respaldar la autenticidad de la información de manera citada y

referenciada a lo largo de todo el informe.

2.7. Criterios de Rigor Científico.

Confiabilidad: El proyecto obtendrá resultados estables y consistentes, porque las fórmulas establecidas se utilizan para mejorar la seguridad en una pyme con datos reales y así, asegurar la confiabilidad de la investigación y para respetar la política durante la implementación.

Coherencia: La investigación se basa en pruebas coherentes y demostrables, como los artículos científicos mencionados en los trabajos previos sobre el punto 1.2 del documento.

Validez: Para la presente investigación se utilizarán los indicadores especificados en la hoja de operacionalización. Estos indicadores ayudarán a poder medir variables y obtener datos que luego serán evaluados por expertos en la materia.

III. RESULTADOS Y DISCUSIÓN.

3.1. Resultados.

Para la obtención de resultados se precisaron los procesos del modelo desarrollado para el caso de estudio con el que se cuenta con 3 fases las cuales se subdividen en 5 procesos:

- P1: Definir la información de la organización.
- P2: Generar perfiles de amenazas.
- P3: Revisar la infraestructura tecnológica con relación a los activos críticos.
- P4: Definir y distinguir los riesgos.
- P5: Generación de un plan de control y mitigación de riesgos.

Dicho esto, los resultados se midieron en la moneda de Soles(S/). Para este indicador se elaboraron 2 instrumentos de recolección de datos, uno sirve para la recolección de datos por cada proceso esencial en la empresa Despensa Peruana

S.A. (ver anexo 3) y el otro instrumento, sirve para hallar el costo sub total de cada proceso de la empresa con cada proceso que tiene el modelo y así poder calcular el costo de implementación. Cabe resaltar que el costo de implementación estimado se obtuvo de proyectos anteriores y de la realidad de la empresa dando un total de S/ 500, puesto que, al ser una pyme, los costos elevados de implementación serían perjudiciales y nada positivos. Para mejor entendimiento se realizó la siguiente figura.

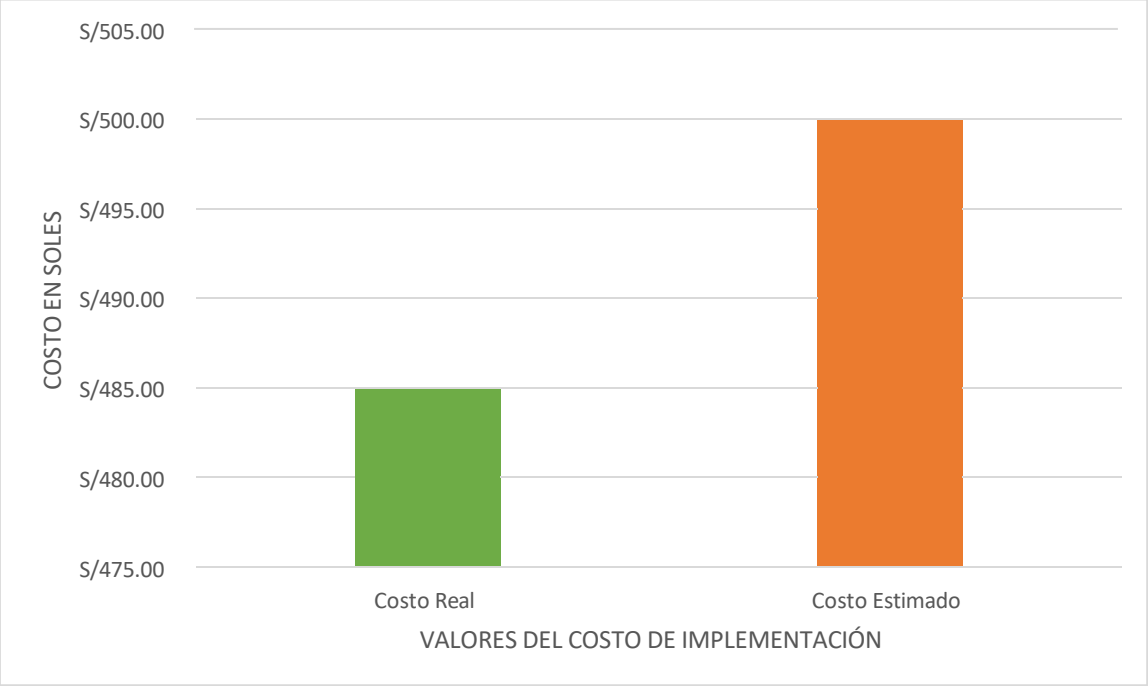


Figura 11. Diferencia entre el costo real y el costo estimado de implementación. Fuente: Elaboración propia

Según el resultado obtenido se determinó que existe una diferencia del 3% del costo estimado, el cual abarca el 100% del costo total de implementación y se llegó a la conclusión de que este último es aceptable al no superar el monto estimado para el modelo.

Tabla 14.

La diferencia del costo de implementación

Costo Implementación		
Costo total	Diferencia	Costo Estimado
S/ 485.00	S/ 15.00	S/ 500.00
97%	3%	100%

Fuente: Elaboración propia.

Cabe resaltar que el costo adquirido por cada proceso ha sido generalmente por costos de papel, tinta para impresora, pasajes, entre otros.

Para el indicador del Tiempo de implementación se realizó un cálculo parecido al del costo de implementación, sin embargo, en este indicador se utilizó el tiempo(días) como valor principal. La siguiente figura representa la diferencia entre el tiempo real con el tiempo estimado el cual fue de 60 días.

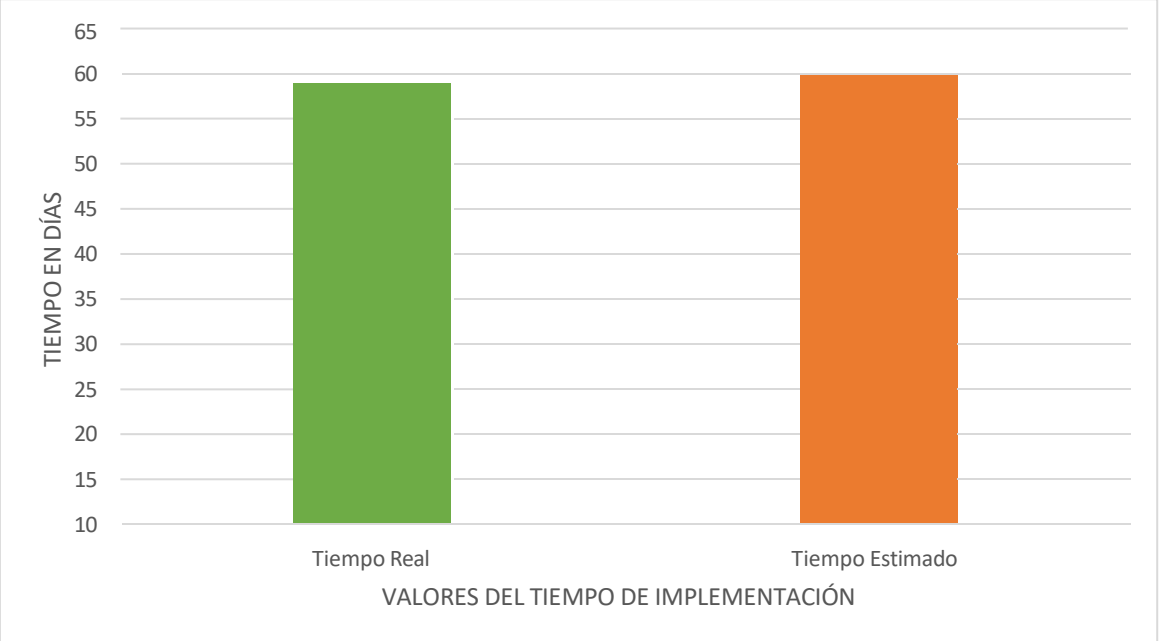


Figura 12. La diferencia entre el tiempo real y el tiempo estimado de implementación

Fuente: Elaboración propia

Según los resultados obtenidos, se puede determinar que existe una diferencia del 2% del tiempo estimado, el cual abarca el 100% del tiempo total de implementación y se llegó a la conclusión de que este último es aceptable puesto que está dentro del rango del tiempo estimado.

Tabla 15.

La diferencia del tiempo de implementación

Tiempo Implementación		
Tiempo Total	Diferencia	Tiempo Estimado
59 días	1 días	60 días
98%	2%	100%

Fuente: Elaboración propia.

Como siguiente indicador se tiene al Nivel de cumplimiento con el estándar ISO/IEC 27005, en el cual se obtuvieron altos niveles de cumplimiento por cada proceso dentro de la empresa Despensa Peruana S.A, dando un total del 92% del nivel de cumplimiento con estándares. La cual será presentada en la siguiente tabla.

Tabla 16.

El nivel de cumplimento con estándares

	NIVEL					
PROCESOS	Incumplido completamente	Incumplido	Incumplido parcialmente	Cumplido parcialmente	Cumplido completamente	Resultado
	0	1	2	3	4	
Recepción de mercancías					X	4
Gestión de inventarios				X		3

Mantenimiento de almacén		X	4
Tecnología y Sistemas de información	X		3
Total			**14**
Nivel de cumplimiento con estándares			92%

Fuente: Elaboración propia

Con el indicador de Nivel de riesgo de los activos se optó por clasificar los activos en perfiles de activos por cada proceso dentro de la empresa (ver anexo 5.1 y 5.2) el cual define algunas probabilidades de amenaza y magnitudes de daño que se tienen que tomar en cuenta para identificar dichos activos. Dentro de estos activos se realizó la ponderación respetiva para hallar el nivel de riesgo de los activos teniendo como rangos definidos por octave – s como: alto riesgo (12 – 16), medio riesgo (8 – 11), bajo riesgo (1 – 7) representada en la siguiente figura.

		riesgo			
		alta	mediana	baja	insignificante
Impacto	alta	ALTO RIESGO (12 - 16)	ALTO RIESGO (12 - 16)	MEDIO RIESGO (8 - 11)	BAJO RIESGO (1 - 7)
	mediana	ALTO RIESGO (12 - 16)	MEDIO RIESGO (8 - 11)	BAJO RIESGO (1 - 7)	BAJO RIESGO (1 - 7)
	baja	MEDIO RIESGO (8 - 11)	BAJO RIESGO (1 - 7)	BAJO RIESGO (1 - 7)	BAJO RIESGO (1 - 7)
	insignificante	BAJO RIESGO (1 - 7)	BAJO RIESGO (1 - 7)	BAJO RIESGO (1 - 7)	BAJO RIESGO (1 - 7)

Figura 13. Matriz de ponderación para el nivel de riesgo de los activos.
Fuente: Elaboración propia

Se obtuvo como resultado para los procesos más esenciales de la empresa Despensa Peruana S.A, que los tres procesos tienen un nivel de alto riesgo el cual abarca una ponderación de 12 a 16, para ver el procedimiento del cálculo de este indicador ver el anexo 5.3.

Para el indicador de nivel de criticidad de activos se apoyó de una metodología RAM visto en el punto 1.3.3, la cual sirvió para medir el nivel de criticidad de los activos a través de la estimación de criticidad, definiendo el rango de bajo (1-7), medio (8-11) y alto (12-16), la estimación de criticidad se seleccionó del anexo 5.1. Finalmente, para el cálculo del nivel de criticidad de los activos, por los procesos más relevantes de la empresa se presentan en el anexo 5.5.

Para le indicador de eficacia de la seguridad de la información fue necesario definir qué objetivos se espera completar con el modelo propuesto y así definir cuáles son los resultados propuestos y los resultados alcanzados, haciendo el cálculo por cada proceso dentro de la empresa Despensa Peruana S.A. en un rango de baja eficacia(0% - 39%), media eficacia (40% - 79%) y alta eficacia (80% - 100%), cabe resaltar que como la empresa Despensa Peruana S.A. no cuenta con una gestión de seguridad de la información, se midió en base a los objetivos adquiridos en el desarrollo del presente proyecto obteniendo como resultado el 80% de la eficacia en la empresa Despensa Peruana S.A.

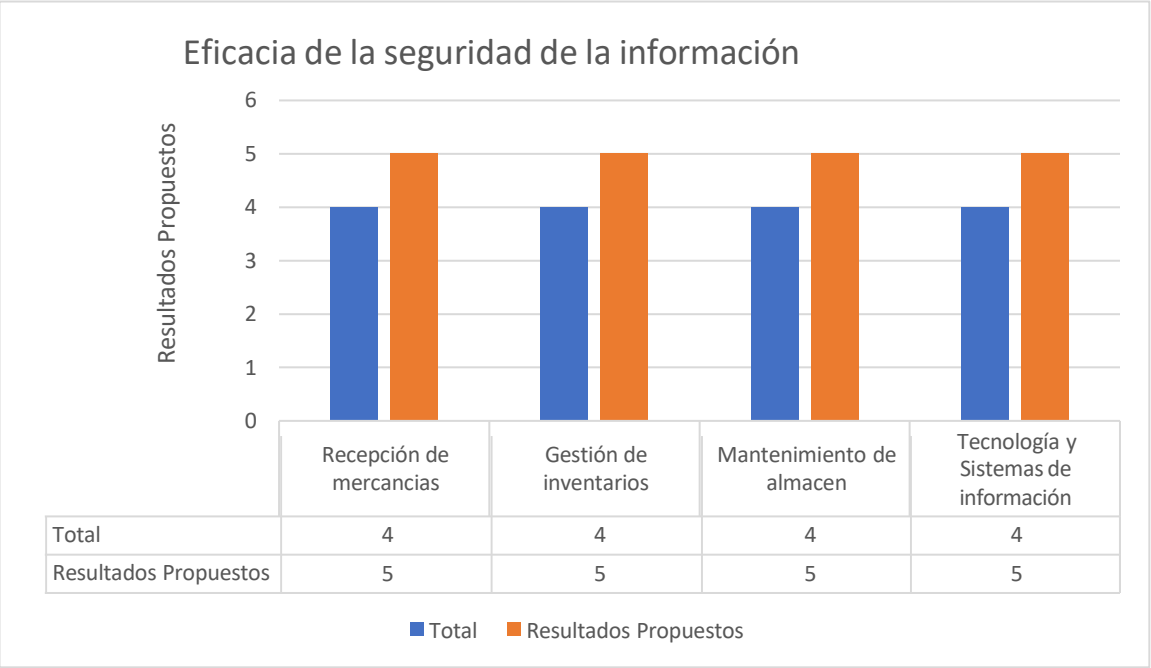


Figura 14. La eficacia de la seguridad de la información dentro la empresa Despensa Peruana S.A. Fuente: Elaboración propia

3.2. Discusión.

Según Rubio, Chavarria, & Mauricio, (2020), los resultados, evidencian diversas mejoras en seguridad que puede optar dicha empresa, con lo que puede aumentar el nivel de cumplimiento de seguridad de un 34% a un , a comparación del modelo de seguridad de la información propuesto en el presente proyecto de investigación se obtuvo un nivel de cumplimiento del 92% teniendo en cuenta que el modelo fue aplicado en 4 procesos a comparación del otro que fue, una investigación para toda la empresa.

Según Carnero Garay, Carbajal Ramos, Armas Aguirre, & Madrid Molina, (2020), los resultados obtenidos, revelaron una disminución de peligro en un 71%, después de usar 15 controles de seguimiento y entrenamiento, el efecto acumulativo se redujo en 67,6 y la gravedad se redujo a 5,5, dependiendo del

valor, en otro caso el resultado de nuestra investigación fue del 92% cumpliendo 5 controles de seguimiento y entrenamiento, pero definido para 4 procesos dentro de la empresa.

Según Martinez, (2015), hizo la averiguación, Seguridad de la Información en pequeñas y medianas organizaciones (pymes), Por consiguiente, el transcurso DEMING, puede relacionar las primordiales ocupaciones que debería desarrollar una pyme que desee hacer un sistema de administración de estabilidad de la información con base en la regla ISO 27001; 2013. En comparación a la evaluación de riesgos, la ISO 27005 (2018) explica que un acceso a la evaluación de peligros y a las elecciones sobre si los peligros requieren. Lo que nos sugiere que la exploración de peligros involucra la importancia de las razones y las fuentes de peligro, sus secuelas positivas y negativas.

3.3. Aporte de la Investigación.

Objetivo 01: Diagnosticar la seguridad de la información de una PYME peruana previamente seleccionada.

Para esta búsqueda, fue fundamental escoger una organización como caso de estudio. Esta organización debía ser una PYME comercial. El rubro de negocio del caso de estudio crea información de ventas por ello es que la compañía seleccionada tiene actividades comerciales.

Para escoger la PYME comercial, lo que se ha efectuado es tomar como referencia la cantidad de empresas a nivel nacional por región las mismas que generalmente fueron anteriormente evaluadas por el sistema financiero y han pasado a ser parte del Programa Reactiva Perú cuya cantidad a nivel nacional ascienden a la suma de 93,569 y fueron empresas que se solventaron bajo criterios de elegibilidad, condiciones del préstamo garantizado, y características de la garantía del gobierno que son las principales variables por las que el sistema financiero peruano se ha afianzado y a quienes el presente estudio estuvo dirigido, por cuanto son las que han requerido un enorme impulso para promover el incremento de sus ventas y mejores tomas de elecciones.

Tabla 17.

Listado de empresas del Perú, por regiones

N.º	REGIONES	NÚMERO DE EMPRESAS
1	Amazonas	588
2	Áncash	1813

3	Apurímac	746
4	Arequipa	4407
5	Ayacucho	708
6	Cajamarca	1885
7	Callao	1675
8	Cusco	2960
9	Huancavelica	116
10	Huánuco	889
11	Ica	1654
12	Junín	2473
13	La Libertad	3962
14	Lambayeque	24117
15	Lima	35451
16	Loreto	963
17	Madre de Dios	488
18	Moquegua	445
19	Pasco	337
20	Piura	2118
21	Puno	1542
22	San Martín	1560
23	Tacna	1365
24	Tumbes	347
25	Ucayali	960
TOTAL, EMPRESAS		**93,569**

Fuente: Reactiva Perú

Como siguiente paso, se optó por escoger a Lambayeque que lo conforman el aproximado de 24,117 empresas de los cuales en virtud al estudio se ha procedido a seleccionar el rubro de comercio que en Lambayeque lo conforman 13,128 empresas y es el rubro en que es más grande en cantidad de empresas. Tabla 18.

La identificación de las empresas en Lambayeque con respecto al rubro comercial

RUBRO	CANTIDAD
COMERCIO	13,128
TRANSPORTE, ALMACENAMIENTO Y COMUNICACIONES	2,130
INDUSTRIA MANUFACTURERA	2,024
HOTELES Y RESTAURANTES	781
ACTIVIDADES INMOBILIARIAS, EMPRESARIALES, ALQUILERES	1,502
OTROS ACTIVIDADES DE SERVICIO COMUNITARIO	1,515
AGRICULTURA, GANADERÍA, CAZA Y SILVICULTURA	1,336
ORGANIZACIONES Y ÓRGANOS EXTRATERRITORIALES	0
CONSTRUCCIÓN	1,017
PESCA	183
ELECTRICIDAD, GAS Y AGUA	23
SERVICIOS SOCIALES Y DE SALUD	223
ENSEÑANZA	206
MINERÍA	29

INTERMEDIACION FINANCIERA	20
ADMINISTRACION PUBLICA Y DEFENSA	0
HOGARES PRIVADOS CON SERVICIO DOMÉSTICO	0
TOTAL	**24,117**

Fuente: Reactiva Perú.

Como paso siguiente, se procedió a la elección de la empresa como caso de estudio teniendo en cuenta la cantidad de servicios que este tiene, el acceso a datos, procesos a los que nos es permitido por la empresa y el uso de TI que tiene la empresa.

Tabla 19.

Tabla de elección de la empresa como caso de estudio

Nombre	Cant. de Servicios	Acceso a Datos y procesos	Uso de TI
DESPENSA PERUANA S.A	15	100%	70%

Fuente: elaboración propia

Posteriormente, se identificaron los procesos de la empresa en un mapa de procesos, en donde tuvimos acceso a 10 de los 15 procesos que tiene la empresa DESPENSA PERUANA S.A, los cuales serán presentados en la siguiente figura.

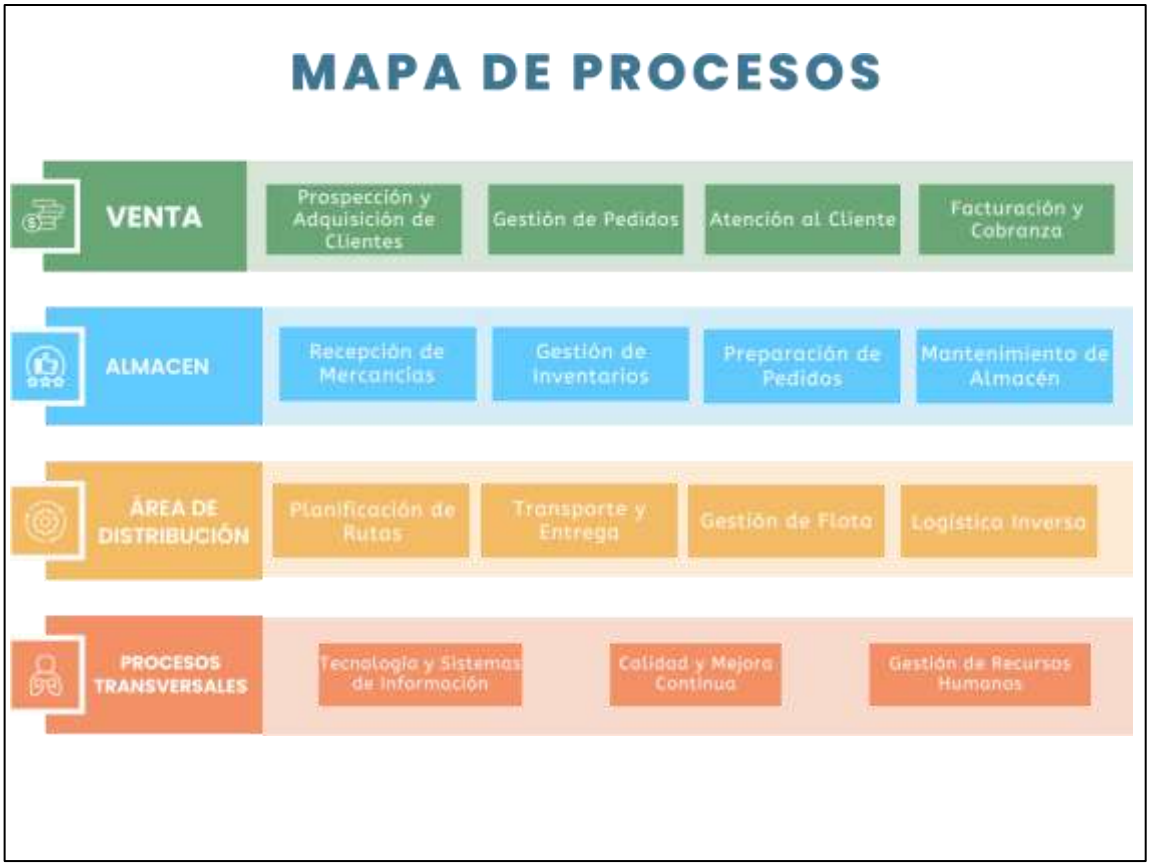


Figura 15. Mapa de proceso de la empresa del caso de estudio

Fuente: Elaboración propia

Luego, se establecieron criterios de evaluación definidos por la norma ISO/IEC 27005 para seleccionar los procesos más relevantes de la empresa para el caso de estudio.

Tabla 20.

Tabla de criterios de evaluación para evaluar los procesos.

Criterios de Evaluación		
C1	Valor estratégico del proceso	Es una valoración acerca del proceso que genere un impacto importante en la empresa.
C2	Criticidad de los activos	Es una valoración acerca de los activos de información involucrados.

C3	Importancia operativa y comercial	Es una valoración de la disponibilidad, confidencialidad e totalidad operativa y comercial de los procesos
C4	Expectativas y percepciones	Es una valoración sobre las expectativas y percepciones de las partes interesadas y consecuencias negativas para la buena voluntad y la reputación de la empresa

Fuente: Elaboración propia

Posteriormente, se evaluaron los procesos en una escala de acuerdo con Cobit 5 desde débil (1), Normal (3), fuerte (5) para poder así, seleccionar los procesos más relevantes dentro de la empresa.

Tabla 21.

Tabla de evaluación de los procesos en una escala de acuerdo con Cobit v5.

N°	Procesos	C1	C2	C3	C4	Total
P01	Prospección y Adquisición de Clientes	3	3	3	3	12
P02	Gestión de Pedidos	5	1	5	1	12
P03	Atención al Cliente	3	2	3	5	13
P04	Facturación y Cobranza	5	4	2	3	14
P05	Recepción de Mercancías	5	5	5	5	20
P06	Gestión de Inventarios	5	4	5	5	19
P07	Preparación de Pedidos	2	3	2	3	8
P08	Mantenimiento de Almacén	5	4	5	5	19
P09	Planificación de Rutas	2	3	3	3	8
P10	Transporte y Entrega	2	2	3	4	11

P11	Gestión de Flota	3	3	3	3	12
P12	Logística Inversa	2	3	3	3	11
P13	Tecnología y Sistemas de Información	5	4	5	5	19
P14	Calidad y Mejora Continua	3	2	2	4	11
P15	Gestión de Recursos Humanos	3	2	1	4	10

Fuente: Elaboración propia

Posteriormente, se seleccionaron los procesos más relevantes teniendo en cuenta los criterios previamente seleccionados y en base a la escala de Cobit v5, para así poder identificar que procesos serán óptimos para desarrollar el caso de estudio.

Tabla 22.

Tabla de selección de los procesos más relevantes.

SELECCIÓN DE PROCESOS MÁS RELEVANTES		
PROCESOS	**NOMBRE**	**NIVEL DE CRITICIDAD**
P01	Prospección y Adquisición de Clientes	12
P02	Gestión de Pedidos	12
P03	Atención al Cliente	13
P04	Facturación y Cobranza	14
P05	Recepción de Mercancías	20
P06	Gestión de Inventarios	19
P07	Preparación de Pedidos	8
P08	Mantenimiento de Almacén	19
P09	Planificación de Rutas	8
P10	Transporte y Entrega	11
P11	Gestión de Flota	12

P12	Logística Inversa	11
P13	Tecnología y Sistemas de Información	20
P14	Calidad y Mejora Continua	11
P15	Gestión de Recursos Humanos	10

Fuente: Elaboración propia

Una vez, se ha seleccionado los procesos más relevantes en la empresa, se diseñaron diagramas de procesos por cada uno, los cuales nos ayudan a identificar como es que funciona cada proceso en la empresa.

Proceso de Recepción de Mercancías

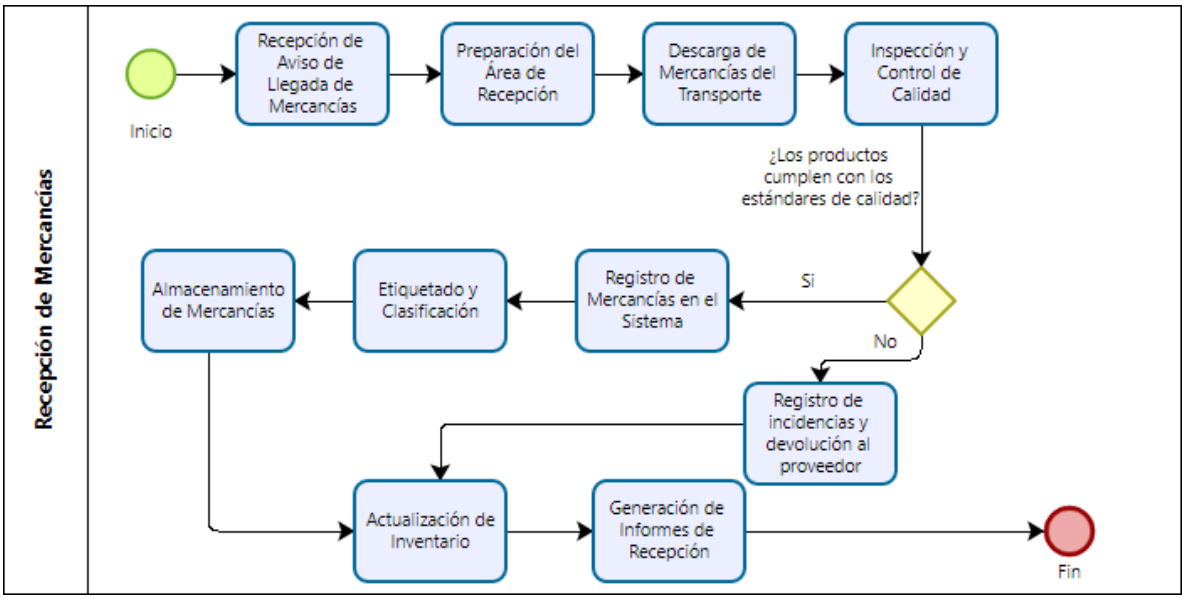


Figura 16. El proceso de recepción de mercancías

Fuente: Elaboración Propia.

Proceso de Gestión de Inventarios

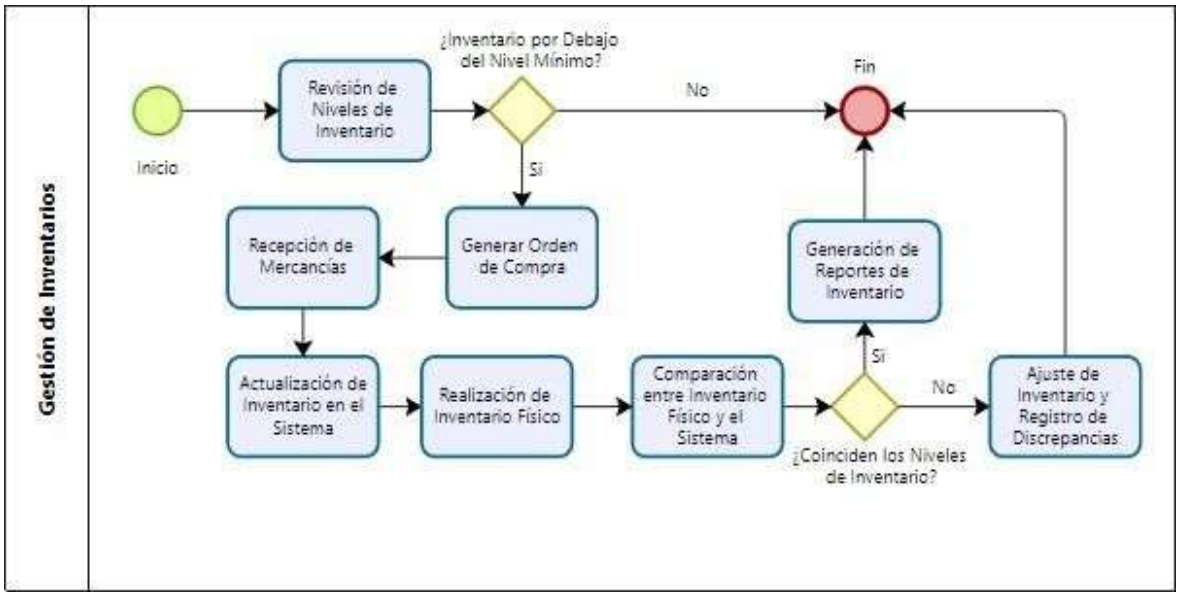


Figura 17. El proceso de gestión de inventarios

Fuente: Elaboración Propia.

Proceso de Mantenimiento de Almacén

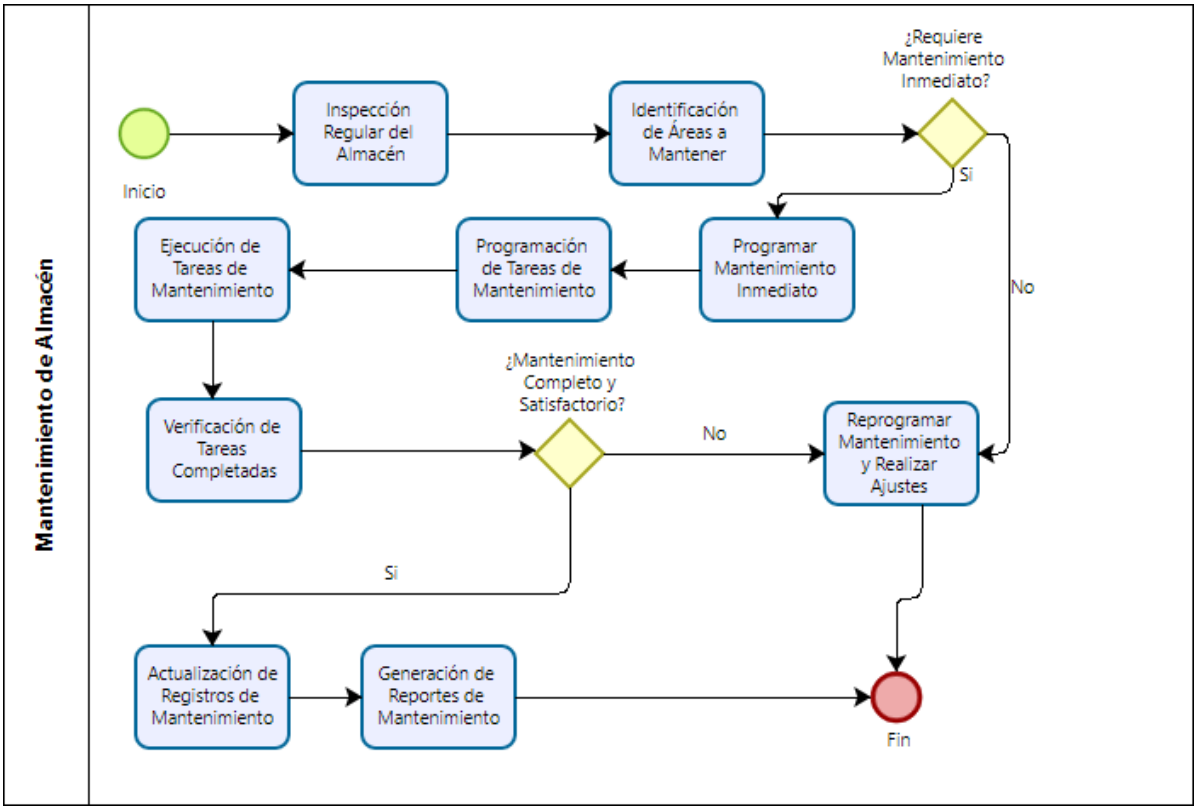


Figura 18. El proceso de mantenimiento de almacén

Fuente: Elaboración Propia.

Proceso de tecnología y sistemas de información

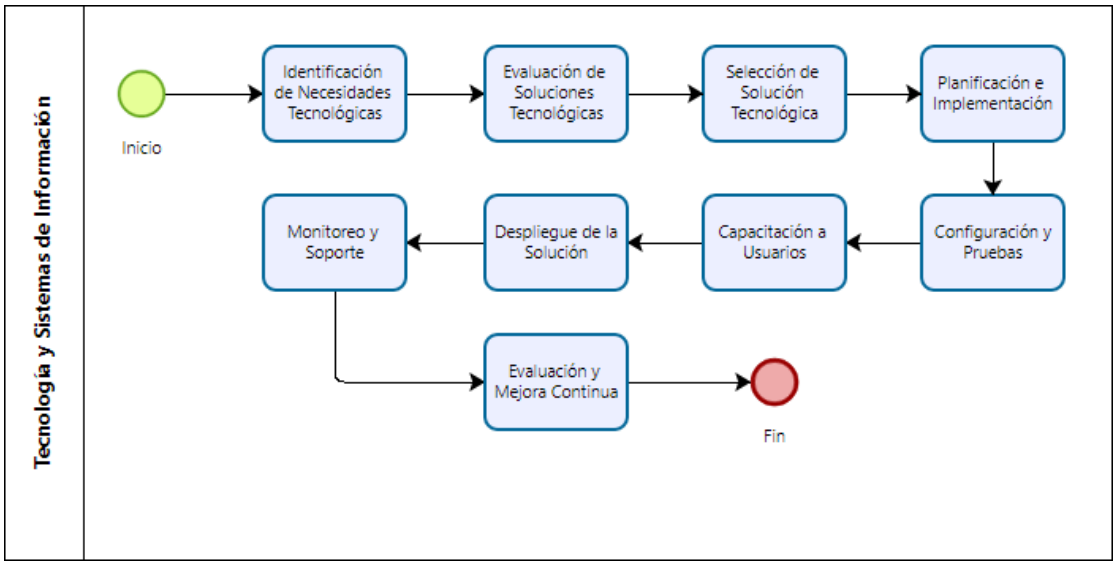


Figura 19. El proceso de tecnología y sistemas de información

Fuente: Elaboración propia.

Objetivo 02: Caracterizar la metodología OCTAVE-S y la norma ISO/IEC 27005 en el contexto de la seguridad de la información en una PYME

Se analizó el método OCTAVE-S y se concluyó que tiene tres fases de implementación.

Inicialmente, se determina la etapa preparatoria, independientemente de las etapas de implementación, ya que es en esta etapa que se designa el equipo de análisis, conformado por 3-5 personas que se comprometen con el desempeño de las funciones del proceso.

Una vez que tienes las personas responsables de implementar esta metodología, comienza la fase de desarrollo.

Fase uno: Construir perfiles de amenaza basados en activos.

En este periodo, se necesita hacer una evaluación de la perspectiva organizacional de la organización, debido a que en este periodo los equipamientos de estudio tienen la labor de conceptualizar los criterios de evaluación que después se usarán para la

evaluación de amenazas. No descuide identificar los activos de información más importantes y evaluar las medidas de seguridad y control de las que dispone actualmente la organización. Finalmente, los equipamientos de análisis definen tanto los requisitos de seguridad como los perfiles de amenazas para cada activo crítico identificado. Cabe señalar que este método nos ordena a elegir entre 3 y 5 activos de información importantes.

Fase dos: Identificar vulnerabilidades de la infraestructura.

A lo largo de esta etapa, el equipo de analistas implementa su conocimiento técnico, que hace una auditoría de elevado grado de la infraestructura de TI de la organización.

Así, se examina cómo se usa la infraestructura, para ver quién interactúa con los activos críticos y quién es el responsable de producir y conservar la infraestructura. Cabe señalar que este procedimiento nos impone a escoger entre 3 y 5 activos de información relevantes.

Fase tres: Desarrollo de Planes y Tácticas de estabilidad

A lo largo de esta fase, los accesorios de estudio establecen los peligros a los que permanecen expuestos los activos de información crítica y qué se debería realizar con ellos.

La metodología sugiere que analizamos la información recopilada para generar tácticas de custodia y planes de mitigación para afrontar los peligros que confronta la compañía.

Cabe señalar que el procedimiento OCTAVE-S tiene papeles de trabajo que tienen la posibilidad de usar en este punto, debido a que está enormemente estructurado y vinculado al portafolio de prácticas de OCTAVE y todo lo mencionado es eficaz para

que los equipamientos de estudio mejoren sus procedimientos de estabilidad en el futuro.

Finalmente, el método de determinación de ciertos resultados lo determina el equipo analítico teniendo en cuenta la confidencialidad desde diferentes puntos de vista y sin descuidar las necesidades de la empresa.

En el siguiente paso, se enumeran los principales resultados del método OCTAVE-S. Estrategia de protección para toda la organización.

- Planes de mitigación de riesgo.
- Lista de acciones.
- Listados de activos de información importantes.
- Perspectiva de buenas prácticas de seguridad.
- Un perfil de riesgo para cada activo crítico.

Cabe destacar que cada etapa del enfoque OCTAVE-S conduce a resultados útiles, ya que en el caso de una evaluación parcial se obtiene información que es útil para mejorar la seguridad en la empresa. Para una mejor comprensión, tenemos una representación gráfica del método OCTAVE -S y sus fases, con las entradas para cada una de ellas en la Figura 14.

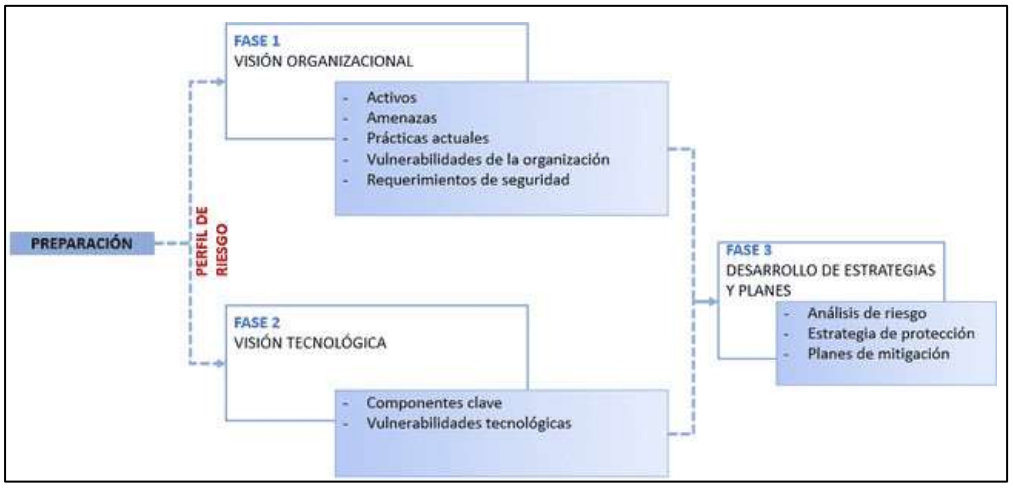


Figura 20. Las fases de OCTAVE - S

Nota: Tomado de Alberts, Dorofee, Steven, & Woody, (2005)

Cuando se tiene fijada la metodología OCTAVE – S ahora se tiene que optar por una regla o estándar que nos ayude a detectar si lo cual estamos desarrollando se puede tener en cuenta un modelo de estabilidad de la información, sin embargo, para esto es necesario detectar la razón de la administración de peligros de estabilidad de la información, pues, esto perjudica al proceso primordial y el entorno predeterminado en especial.

La norma ISO/IEC 27005 nos establece 7 procesos que debe seguir un modelo de seguridad de la información para que sea considerado como tal, basándose en lo que en un inicio se considera como gestión de riesgos de seguridad de la información.

Proceso uno: Establecimiento del contexto.

En este proceso es necesario recopilar toda la información relevante de la organización para cumplir con las expectativas de la norma, posteriormente a esto, se necesita establecer el contexto interno, ya sea definiendo el alcance, los límites y el establecimiento de la organización para que todo esto junto pueda operar la gestión de riesgos de seguridad de la información.

Punto siguiente, tenemos la guía de implementación, la cual nos sugiere que, es esencial determinar el propósito para el cual se está realizando una gestión de riesgos de seguridad de la información, puesto que esto afectará a los procesos de la empresa y el contexto en particular.

Proceso dos: Identificación de riesgos.

El propósito de este proceso es determinar el mal manejo de la organización y pueda ocasionar una pérdida de cualquier tipo, para esto se necesita identificar los activos dentro del alcance establecido, que estos tengan un nivel de detalle

específico y definan verdaderamente que campo se cubre dentro de la empresa, esto quiere decir que se necesita proporcionar al encargado del activo y la manera en que usa.

Después de identificar los activos y su entorno, necesitamos ubicar que tipos de amenazas existen, ya sea con un registro de casos incidentes o también consultar amenazas externas.

Posteriormente se identifica aquella documentación con la que cuenta la organización como documentación de controles, planes de tratamiento de riesgos y verificar que estos controles funcionen correctamente.

Cuando poseemos una lista de amenazas conocidas y una lista de activos y controles accesibles, pasamos a detectar vulnerabilidades que tienen la posibilidad de ser explotadas por amenazas para provocar perjuicios. Perjuicios a la propiedad, según ISO / IEC 27005, pudimos detectar algunas de las próximas vulnerabilidades:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión
- Otros

Luego, se debe identificar las consecuencias que las pérdidas de confidencialidad, totalidad y disponibilidad pueden tener sobre los activos y estas pueden encontrarse en diferentes escenarios de incidentes reflejadas en el tiempo de trabajo perdido, salud y seguridad, costos adicionales a lo presupuestado, reputación de la empresa, entre otros.

Proceso tres: Análisis de riesgo.

Según la norma ISO/IEC 27005, establece que para poder analizar los riesgos es necesario guiarnos de una metodología de análisis, la cual puede ser cualitativa o cuantitativa o una combinación de ambas, según sea la necesidad. También se afirma que, en la práctica, el análisis cualitativo se utiliza para obtener una indicación general del nivel de riesgo y para revelar los principales riesgos. Es esta última la que se asemeja al trabajo para el caso de estudio.

Después de identificar como será la metodología de análisis, se procede a evaluar las consecuencias ya que, esto sirve para medir el impacto comercial en la organización que puede afectar la totalidad o la pérdida de confidencialidad.

Una vez que se tiene evaluadas las consecuencias, se procede a evaluar la probabilidad con la que se pueden dar estas últimas, utilizando un análisis cualitativo, teniendo en cuenta la facilidad en que se puedan explotar estas vulnerabilidades y con qué frecuencia.

Proceso cuatro: Evaluación de riesgos.

Como punto inicial en este proceso, es necesario una lista de peligros con niveles de costo designados y criterios de evaluación de peligros para lograr medir el grado de peligro, el cual debería ser comparado con los criterios de evaluación y aprobación de peligros.

Según la norma se deben incluir algunas consideraciones:

- Características de estabilidad de la información: Si un criterio no es importante para la organización, todos los peligros involucrados que perjudiquen no tienen la posibilidad de ser tomados presente.
- La importancia de los procesos en la organización: Si se identifica que el proceso es de baja importancia para la empresa, todos los riesgos asociados a este proceso tienen una consideración menor.

Proceso cinco: Tratamiento de riesgos.

En este proceso, se seleccionan los controles para reducir, retener, evitar o compartir los riesgos y encontrar un plan de tratamiento de riesgos.

El tratamiento de riesgos tiene que darse en función a diferentes factores, como los resultados de la evaluación de riesgos, el costo específico para implementar estas opciones y los beneficios esperados. Se tiene que tener en cuenta que, por razones estrictamente económicas, se puede omitir algunos controles, dependiendo la realidad de la organización y que algunos tratamientos pueden abarcar más de un riesgo de forma eficaz. La norma nos especifica algunas opciones que se deben tomar en cuenta antes de realizar los controles de tratamiento de riesgos.

- El contexto en el que se perciben las partes afectadas por el riesgo.
- La comunicación entre sus partes tiene que ser la más adecuada.

Como consecuencia obtenemos, el proyecto de procedimiento de peligros y los peligros residuales sujetos a la elección de aseveración a causa de los elevados rangos de la organización.

Una vez tenemos identificada la descripción general de los tratamientos de riesgos, se pueden dar alguna deficiencia por parte del equipo de análisis al analizar los riesgos, se necesita establecer como es que el nivel de riesgo se introduce, elimina o modifica para que se puedan controlar y finalmente reevaluarse como aceptable. El resultado de este paso es una lista de posibles controles, con su beneficio y prioridad de implementación. Según la norma, nos especifica algunas limitaciones como limitaciones de tiempo, restricciones financieras, limitaciones técnicas, limitaciones operativas, facilidad de uso, entre otras limitaciones.

Luego, está la probabilidad de guardar peligros, esto debería tomarse dependiendo de la evaluación del peligro, esto significa a que, si el peligro cumple con los criterios de aprobación del peligro, no hay necesidad de llevar a cabo controles extras y el peligro se puede retener.

También existe la posibilidad de evitar riesgos, ya que estos puedes ser considerados muy altos y son difíciles de evitar, lo que la norma nos recomienda es realizar una determinada actividad para evitar ese riesgo, un ejemplo claro de esta actividad es en el caso de un desastre natural, en donde la alternativa más rentable sería trasladar el material físico a una zona segura.

Por otro lado, existen los riesgos compartidos, en donde implica la decisión por parte del equipo de análisis el compartir el riesgo con otra parte, que tenga la posibilidad de gestionar de manera eficaz el riesgo en particular.

Proceso seis: Aceptación de riesgos.

A lo largo de este proceso, se compilará una estrategia de procedimiento de peligros y una evaluación del peligro de acumulación, que está sujeta a la aprobación de parte de la alta dirección de la compañía. En este proceso, se identifican los peligros, está establecido la responsabilidad de la toma de elecciones y se registra formalmente.

Proceso siete: Comunicación y consulta de riesgos.

- Una vez se ha obtenido toda la información de peligro de las ocupaciones de la administración de peligros, en los procesos anteriores, se empieza a llegar a un convenio respecto a cómo se tiene que gestionar los peligros, juntando, tanto al equipo de estudio como a las demás piezas interesadas en el comercio, para lograr de esta forma debatir sobre la vida, naturaleza, forma, posibilidad,

gravedad, procedimiento y aprobación de los peligros. Conforme con la regla ISO/IEC 27005, la comunicación de peligros debería llevarse a cabo destinados a:

- Apoyar la toma de decisiones.
- Mejorar la conciencia.
- Recopilar información sobre riesgos.
- Dar seguridad sobre el resultado de la gestión de riesgos en la organización.

Finalmente, en este proceso, se define un plan de seguimiento y revisión para mejorar la gestión de riesgos, esto quiere decir que durante el tiempo que dure la gestión de riesgos en la organización, se tiene que estar en constante control de lo que se está analizando. En la siguiente figura identificamos como es el flujo en el que se da la norma ISO/IEC 27005.

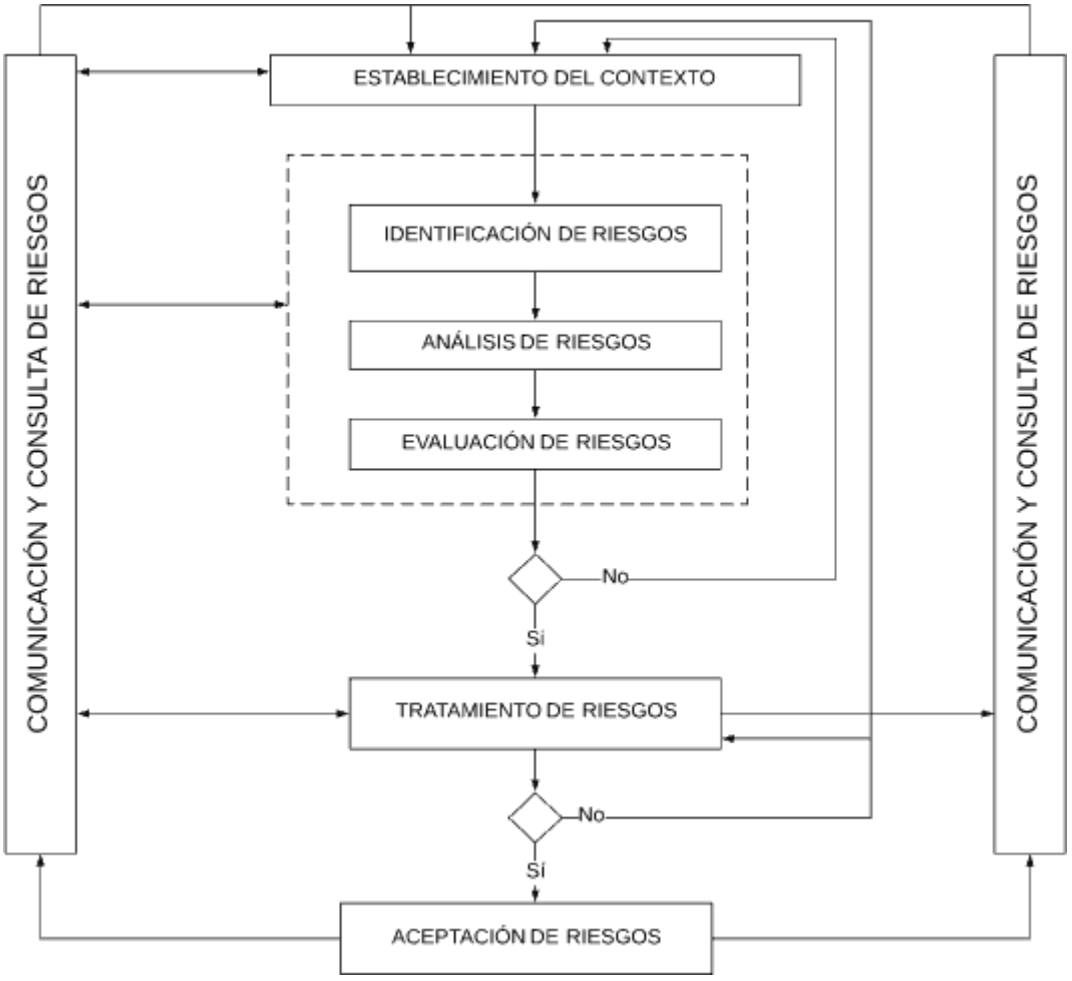


Figura 21. El proceso de gestión de riesgos según la norma ISO/IEC 27005

Fuente: (INTERNATONAL STANDAR ISO/IEC 27005, 2018)

Como siguiente paso, se consultó sobre un modelo de referencia aplicado con la metodología OCTAVE – S y la norma ISO/IEC 27005 elaborada por (García-Porras, Huamani-Pastor, & Armas-Aguirre) en (2018).

Este modelo se aplicó para una Pyme del sector cerámico, específicamente en el proceso de venta. Se tuvo la estructura del modelo el cual consiste en 3 partes: Las entradas, el modelo en sí y las salidas como resultado de la aplicación de este modelo.

En las entradas de este proceso tenemos:

- Información de la organización.

- Situación actual del sistema de información.
- Políticas de información.
- Información de la tecnología de información.
- Reconocimiento de auditoría.
- Reporte de pérdidas.

Para el modelo general, se ha seguido la estructura que brinda OCTAVE – S y ha sido plasmada en la siguiente figura.

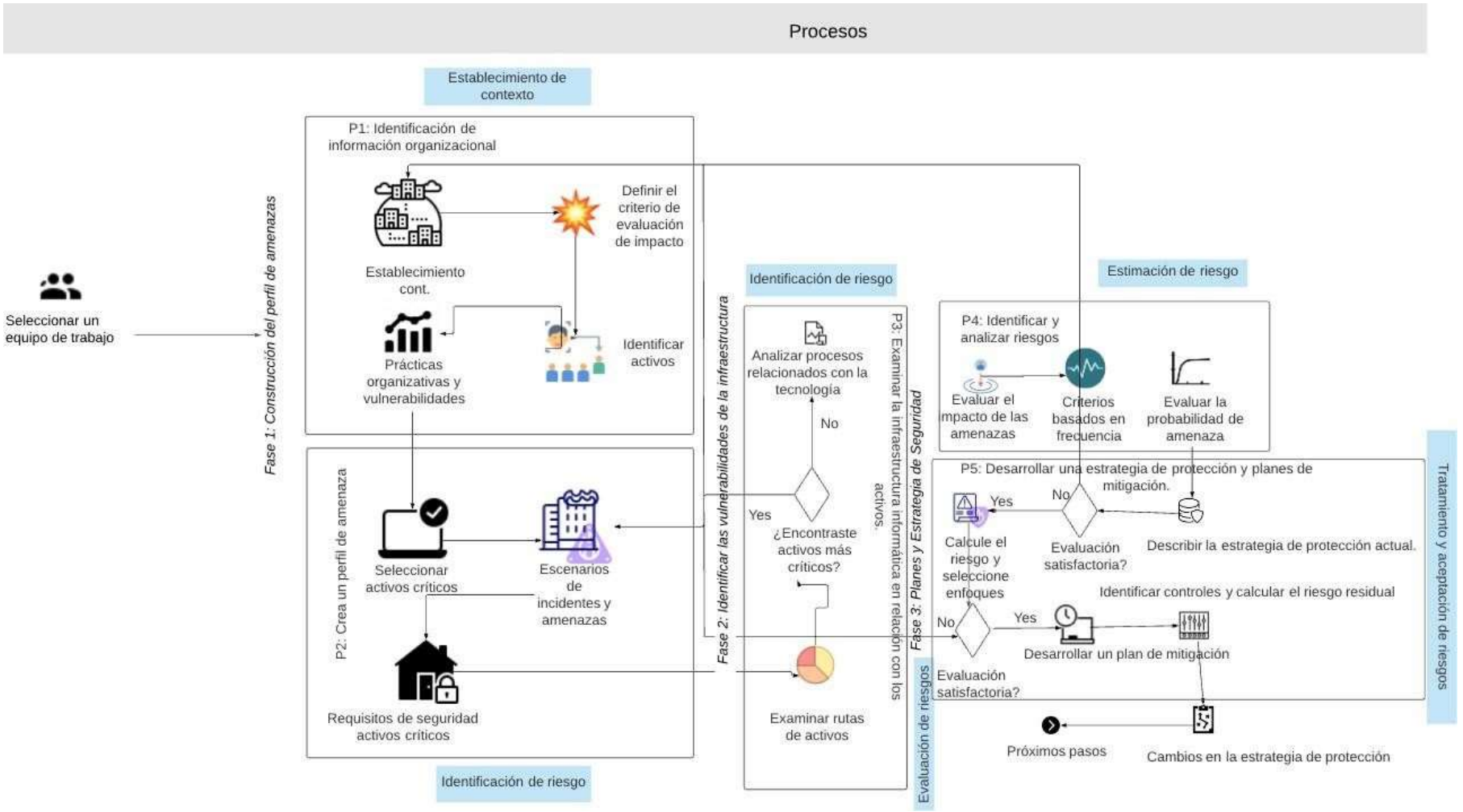


Figura 22. El modelo de referencia para la gestión de riesgos de seguridad de la información.

Nota: (García-Porras, Huamani-Pastor, & Armas-Aguirre, 2018)

Finalmente, después de haber aplicado el modelo, se obtiene la información de salida como:

- Estrategias de protección.
- Plan de mitigación.
- Listado de riesgos.
- Listado de control y mitigaciones.

Paso siguiente, se optó por analizar la realidad de la organización, ya que esto ayuda a mejorar el panorama a la hora de diseñar y aplicar el modelo propuesto para el caso de estudio.

Como punto inicial se tiene que, la empresa Despensa Peruana SA se fundó en 1995 en la ciudad de Chiclayo – Perú, es una empresa dedicada a la comercialización de productos de consumo masivo, ofreciendo productos de primera necesidad tales como: abarrotes, golosinas, gaseosas, útiles escolares, licores, entre otros. Esta empresa se inició como un negocio familiar y la cual se usó como referencia para el desarrollo del modelo.

Con esta descripción podemos señalar también la Misión u la visión de la empresa que será presentada en las siguientes descripciones.

Misión:

Despensa Peruana SA, inmersa en el rubro de comercio, brindando productos de calidad en marcas reconocidas teniendo como principales clientes a Subdistribuidores, mayoristas y minoristas. Lucha por mejorar la rentabilidad del negocio para beneficio de sus accionistas, garantizándoles rentabilidad sostenida, crecimiento y desarrollo, basados en el factor humano idóneo, productos de alta calidad.

Misión de la empresa Despensa Peruana S.A

Fuente: Despensa Peruana S.A

Visión:

Ser una empresa líder en la región norte en la comercialización de sus productos, con una clara visión de crear oportunidades e innovar junto al país, basando el éxito de la gestión en una elevada satisfacción de nuestros clientes y el bienestar de nuestros colaboradores.

Visión de la empresa Despensa Peruana S.A

Fuente: Despensa Peruana S.A

Posteriormente, se realizó un modelo Canvas para tener una visión clara de su gestión estratégica, la cual permitió analizar su modelo de negocio de forma dinámica y se muestra en la siguiente figura.

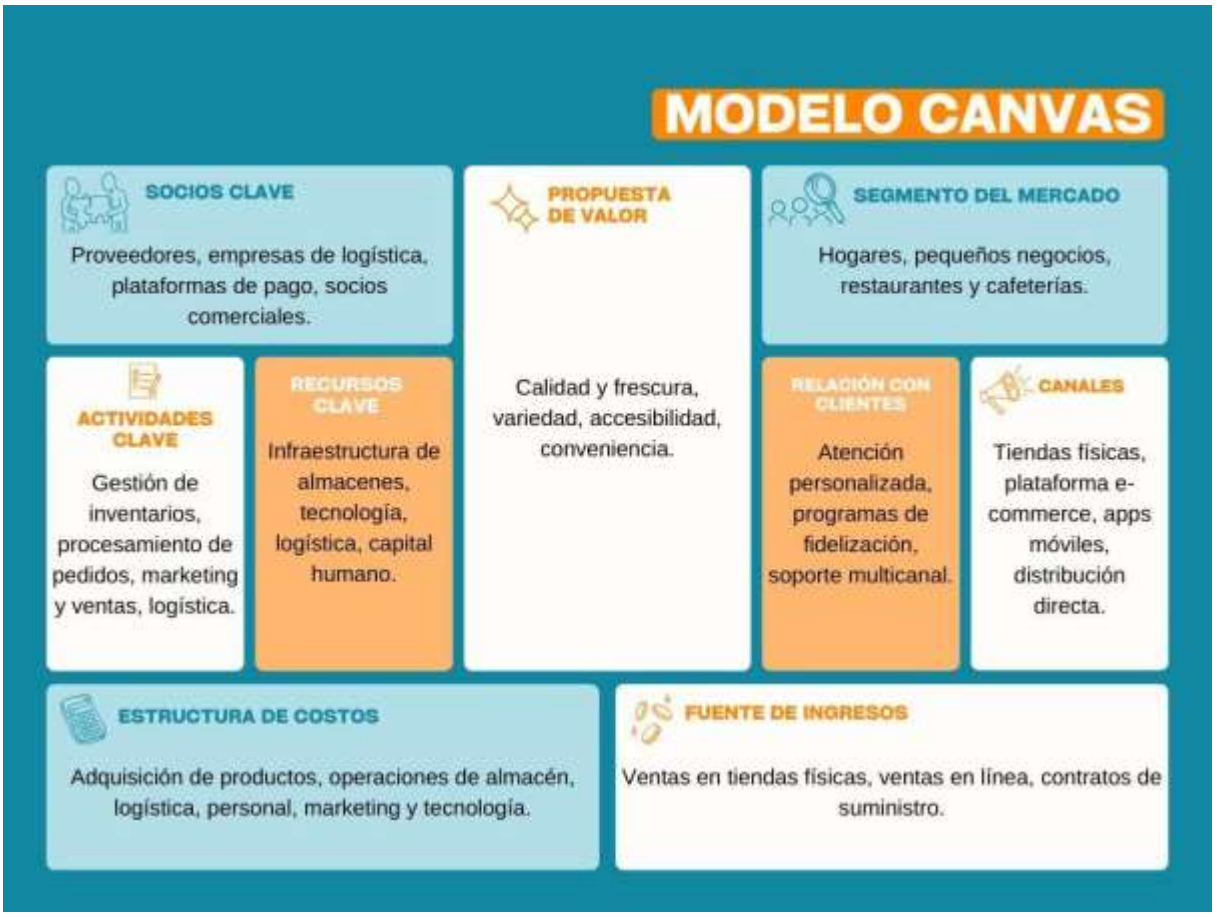


Figura 23. El modelo Canvas de *la empresa Despensa Peruana S.A*

Fuente: Elaboración Propia

Objetivo 03: Diseñar el modelo de procesos de seguridad de la información para una Pyme peruana.

Para el diseño del modelo es necesario establecer el equipo de trabajo, los cuales tienen que ser un grupo de 3 a 5 personas que tengan conocimiento del flujo que se va a trabajar y control de la infraestructura tecnológica de la organización. Para llevar a cabo todo esto, se tiene que completar la tabla del anexo 5.1.1.

Cabe resaltar que, por motivos de confidencialidad, se puede colocar alias a los expertos (E1, E2, E3, E4, E5).

Para la selección de los procesos que se van a someter al modelo de seguridad de la información se ha dispuesto de la siguiente secuencia de pasos.

Paso 1: Para este paso se necesita seleccionar todos los procesos que están involucrados con las actividades más importantes de la organización en la siguiente tabla en el siguiente anexo 5.1.2.

Paso 2: Una vez se tenga los procesos de la organización, se tienen que enfrentar con los 4 criterios que dispone la norma ISO/IEC 27005 para poder medir la relevancia de estos procesos (ver tabla 22), posteriormente se evalúan en una escala según Cobit v5 desde débil (1), Normal (3), fuerte (5). Se recomienda aplicar la tabla que se presenta a continuación en el anexo 5.1.3.

Paso 3: Posteriormente se tienen que seleccionar los procesos más relevantes dependiendo su nivel de criticidad calculado anteriormente que se muestra en el anexo 5.1.4.

Una vez se tienen los procesos más relevantes de la organización se procedió al diseño de las fases del modelo. Según la metodología OCTAVE -S y el modelo de referencia desarrollado en el objetivo 2 se ha llegado a la conclusión de separar el modelo en 3 fases que cumplirán las condiciones que nos recomiendan, tanto la metodología OCTAVE -S y la norma ISO/IEC 27005 las cuales se presentarán a continuación:

Fase 1: Creación de perfiles de amenazas: Dentro de esta fase encontramos 2 procesos, los cuales establecerán el contexto de la organización y la identificación de los riesgos. Estos procesos contienen una serie de actividades y pasos establecidos por OCTAVE -S, las cuales se plasmaron en el siguiente cuadro para un mejor entendimiento.

Tabla 23.

Los procesos de la fase 1 del modelo de seguridad

Proceso	Actividades	Pasos
P1: Definir la información de la organización	A1.1: Definir la evaluación de impacto	1
	A1.2. Definir activos de la organización	2
	A1.3. Medir las prácticas de seguridad de la organización	3,4

P2: Generar perfiles de amenazas	A2.1. Elegir los activos críticos	5,6,7,8,9
	A2.2. Definir los requisitos para la seguridad de activos críticos	10,11
	A2.3. Definir las amenazas de activos críticos	12

Nota: Tomado de Alberts, Dorofee, Steven, & Woody, (2005)

Fase 2: Identificar las vulnerabilidades en la infraestructura: Dentro de esta fase encontramos un proceso, el cual examina la infraestructura con relación a los activos críticos. Este proceso incluye una serie de actividades y pasos fijado por OCTAVE-S, las cuales se representaron en el siguiente cuadro para una mejor comprensión.

Tabla 24.

Los procesos de la fase 2 del modelo de seguridad

Proceso	Actividades	Pasos
P3: Revisar la infraestructura tecnológica con relación a los activos críticos	A3.1: Indagar las rutas de ingreso	13,14
	A3.2. Distinguir los procesos con la tecnología	15,16,17

Nota: Tomado de Alberts, Dorofee, Steven, & Woody, (2005)

Fase 3: Desarrollo de estrategias y planes de Seguridad: Dentro de esta fase encontramos dos procesos, los cuales identifican y analizan los riesgos, además del desarrollo de estrategias de protección y los planes de mitigación. Estos procesos contienen una secuencia de actividades y pasos fijados por OCTAVE-S, las cuales se plasmaron en el siguiente cuadro para un mejor entendimiento.

Tabla 25.

Los procesos de la fase 3 del modelo de seguridad

Proceso	Actividades	Pasos
P4: Definir y distinguir los riesgos	A4.3. Estimación de las probabilidades de amenaza	18,19,20
P5: Generación de un plan de control y mitigación de riesgos	A5.1: Especificar las estrategias de seguridad actuales	21,22
	A5.2. Escoger las semejanzas de mitigación	23,24

	A5.3. Generar los planes de mitigación de riesgos	25

Nota: Tomado de Alberts, Dorofee, Steven, & Woody, (2005)

Una vez se ha diseñado las fases del modelo de procesos, se procedió a la especificación de cada proceso.

- P1: Definir la información de la organización.
  - A1.1. Definir la evaluación de impacto.

    En esta actividad contamos con un solo paso, el cual se diseñó de la siguiente manera.

    Paso 1: Se definen las categorías de impacto (bajo, medio, alto) de las amenazas, hacia los procesos previamente seleccionados. Se recomienda ingresar los datos en el siguiente formato para poder establecer en el rango que se encuentren las amenazas en el anexo 5.1.5.

- A1.2. Definir activos de la organización

En esta actividad contamos con un solo paso, el cual se diseñó de la siguiente manera.

Paso 2: Se identifican los activos dentro de los procesos que se han seleccionado previamente, para eso se tiene que tomar como punto de inicio la experiencia y los conocimientos de todos los involucrados en dicho proceso para posteriormente realizar el análisis. Se recomienda utilizar la siguiente tabla para insertar los datos de los activos encontrados por cada proceso en el anexo 5.1.6.

- A1.3. Medir las prácticas de seguridad de la organización

Paso 3: Este paso se desglosa en dos sub-pasos, sin embargo, como se mencionó anteriormente, al trabajar con pymes, este paso no es tan relevante, ya que la mayoría de organizaciones no cuentan con prácticas de seguridad. De no ser así y encontrar prácticas de seguridad dentro de la organización, se consideran estos dos sub-pasos.

Paso 3a: En este sub-paso, se prevé hasta qué punto es utilizada la práctica de seguridad en la organización.

Paso 3b: En este sub-paso, se registra las prácticas que la organización está ejecutando de manera satisfactoria y los que se ejecutan de manera incorrecta u obsoleta.

La metodología OCTAVE – S nos ofrece una lista de prácticas de seguridad, las cuales son:

Práctica de Seguridad 1: Concienciación y formación en seguridad.
Práctica de Seguridad 2: Estrategia de Seguridad
Práctica de Seguridad 3: Gestión de Seguridad
Práctica de Seguridad 4: Políticas y regulaciones de seguridad
Práctica de Seguridad 5: Gestión de la Seguridad Colaborativa
Práctica de Seguridad 6: Planes de contingencia/recuperación de desastres
Práctica de Seguridad 7: Control de Acceso físico
Práctica de Seguridad 8: Monitoreo y Auditoría de seguridad Física
Práctica de Seguridad 9: Gestión de Sistemas y redes
Práctica de Seguridad 10: Monitoreo y Auditoría de Seguridad de TI
Práctica de Seguridad 11: Autenticación y Autorización
Práctica de Seguridad 12: Gestión de vulnerabilidades
Práctica de Seguridad 13: Encriptación
Práctica de Seguridad 14: Diseño y Arquitectura de Seguridad
Práctica de Seguridad 15: Gestión de Incidentes

Figura 24. La lista de prácticas de seguridad según OCTAVE – S

Fuente: Alberts, Dorofee, Steven, & Woody, (2005)

Paso 4: Una vez se completaron los pasos anteriores se determina un color del semáforo (verde, amarillo o rojo) para cada área de práctica de seguridad. Esta técnica ayuda a reflejar de mejor manera, la efectividad de las prácticas de seguridad.

	Verde	La organización está llevando a cabo las prácticas de seguridad de manera correcta.
	Amarillo	La organización está llevando a cabo las prácticas de seguridad hasta cierto punto.
	Rojo	La organización no está llevando a cabo las prácticas de seguridad.

Figura 25. La técnica de semáforo para reflejar la efectividad de las prácticas de seguridad

Fuente: Elaboración propia

Se recomienda que para identificar las prácticas de seguridad dentro de la organización se relacione con las prácticas de seguridad que recomienda OCTAVE – S, para una mejor selección de estos. Ver la tabla en el anexo 5.1.7.

- P2: Generar perfiles de amenazas
    - A2.1. Elegir los activos críticos

En este proceso se reúne en elegir los activos críticos de entre los activos ubicados antes para después, detectar qué es lo cual es necesario para lograr defender dichos activos y al final se definen las amenazas que se logren exponer en estos activos.

Paso 5: Se seleccionan de 3 a 5 activos que se tomen en cuenta críticos entre la lista de activos de información desarrollado en el paso.

Paso 6: Se identifica el activo por su nombre.

Paso 7: Se especifica el motivo por la cual ha sido seleccionado como activo crítico.

Paso 8: Se registra el responsable o el delegado de utilizar este activo crítico.

Paso 9: Se registran los probables activos involucrados con este activo crítico.

A continuación, se presenta el formato con el cual se seleccionarán los activos críticos por cada proceso en el anexo 5.1.8

- A2.2. Definir los requisitos para la seguridad de activos críticos

Paso 10: En este paso se identifican los requerimientos de estabilidad para cada activo crítico, cabe mencionar que OCTAVE – S nos ofrece un listado de requerimientos de estabilidad pre definidos, los cuales son:

- Confidencialidad: Asegura que la información se accesible, sólo para personal autorizado.
- Totalidad: Asegura que la información logre ser modificada sólo por personal autorizado.
- Disponibilidad: Esta medida sugiere, la época que está funcionando un sistema o equipo, respecto al tiempo total que realmente debe funcionar.
- Entre otros.

Después, se muestra el siguiente formato para ordenar los activos críticos, ante los requerimientos de estabilidad pre definidos por OCTAVE – S.

Paso 11: En este paso, se definen aquellos requisitos más transcendentes de seguridad para cada activo crítico dentro de los procesos seleccionados previamente. Se presenta el siguiente formato

para identificar los requisitos más esenciales para cada activo crítico dentro de los procesos seleccionados en el anexo 5.1.9

- A2.3. Definir las amenazas de activos críticos

En esta actividad se identifica un paso, sin embargo, la metodología nos menciona un análisis más específico, como identificar los actores internos y externos que pueden ocasionar una amenaza ya sea accidentalmente, como deliberadamente, para los activos que se están identificando, pero como estamos hablando de una pyme, omitimos estos pasos, ya que el personal es reducido y no hay muchas especificaciones en ese aspecto.

Paso 12: En este paso se completa apropiadamente la identificación de amenazas para cada activo, tomando en cuenta las siguientes categorías de amenazas propuestas por OCTAVE – S.

- C1: Personal teniendo ingreso a la red
- C2: Personal usando ingreso físico
- C3: Dificultades del sistema
- C4: Otros problemas

Para el desarrollo de este paso se presenta el siguiente formato en el anexo 5.1.10.

- P3: Revisar la infraestructura tecnológica con relación a los activos críticos

Este proceso se centra en analizar las rutas hacia los activos críticos a través de la infraestructura tecnológica, así como las operaciones preseleccionadas.

  - A3.1. Indagar las rutas de ingreso

    Paso 13: En este paso se detecta cuáles son los componentes (router, switch, pcs, usuarios) con los que cuenta la infraestructura tecnológica de la organización y los usuarios encargados de la manipulación de dicho componente. Para representarlo mejor, se sugiere utilizar el siguiente formato en el anexo 5.1.11.

Paso 14: En este paso, las posibles rutas de acceso se modelan en la infraestructura tecnológica de la organización, y este esquema debe implementarse en Cisco Packet Tracer. Se ha introducido el siguiente diagrama de infraestructura tecnológica.

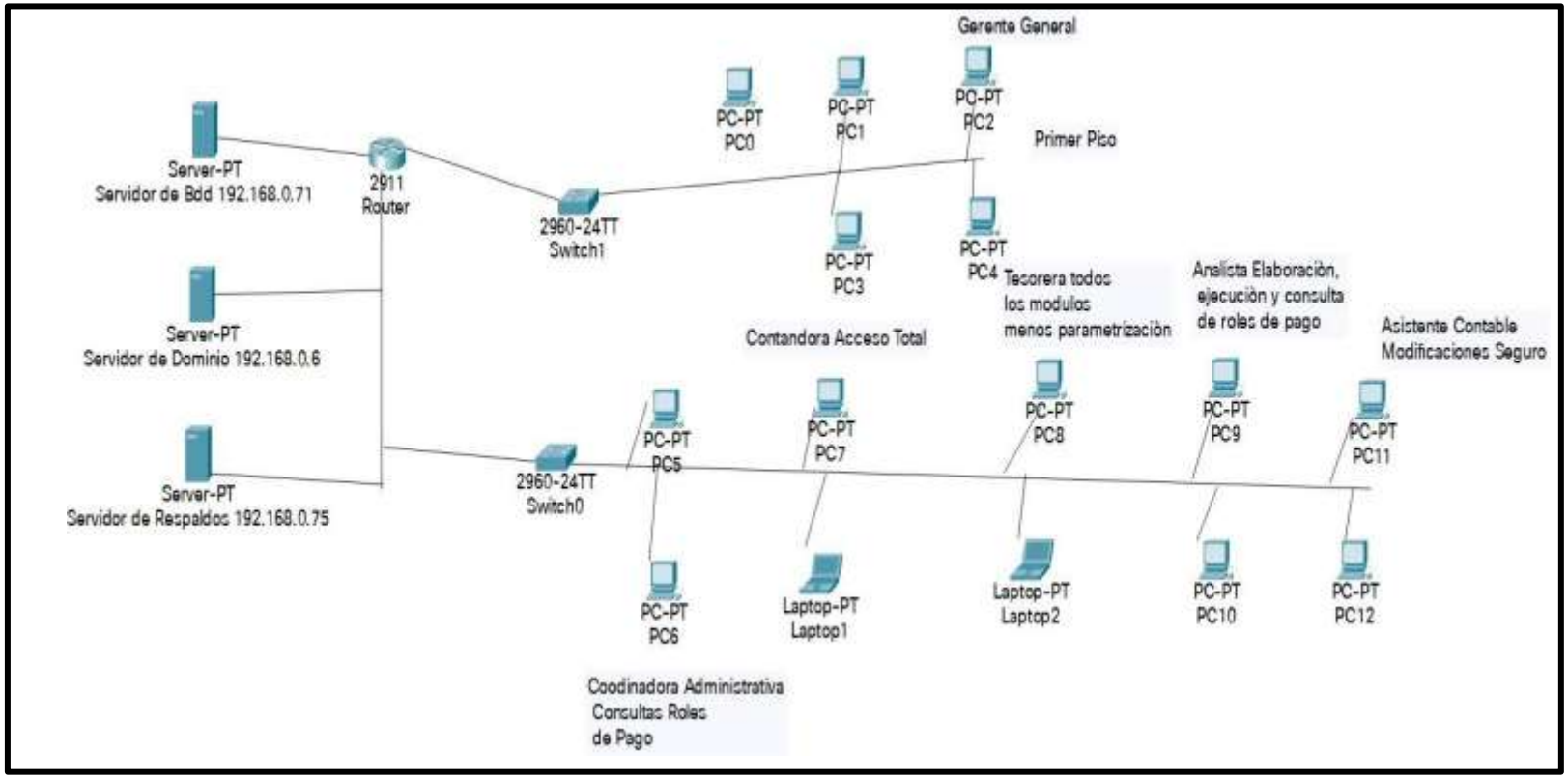


Figura 26. La infraestructura tecnológica de la organización

Fuente: Elaboración propia

- A3.2. Distinguir los procesos con la tecnología

En esta actividad se desarrollan 3 pasos, que se describirán a continuación.

Paso 15: Este paso contiene dos sub pasos, presentados a continuación.

Paso 15a: Se establece qué clase de elementos permanecen involucrados con uno o más activos críticos.

Paso 15b: En este paso, los contenidos principales se asocian con cada clase de artículo.

Paso 16: En este paso, la responsabilidad del supervisor y el mantenedor se asigna a cada categoría de artículo en la red.

Paso 17: En este paso, la estimación de estabilidad se tiene en cuenta en los procesos predefinidos en el anexo 5.1.12.

- P4: Identificación y análisis de riesgos
  - A4.3. Estimación de las probabilidades de amenaza

Paso 19: Se analiza el impacto de cada activo crítico y sus amenazas en los diferentes procesos de la empresa. Las amenazas seleccionadas son las que fueron determinadas en el paso 12. En la siguiente tabla se encuentra en el anexo 5.1.13.

Paso 20: A lo largo de este proceso, se identifican medidas que calculan la posibilidad de una amenaza. Es dependiente de cuántas veces ocurrió en el pasado. La posibilidad de una amenaza a el equilibrio de la información se considera usando una mezcla de datos brutos y vivencia personal, que se recibe primordialmente del personal de TI de la organización. Cabe señalar que este paso es opcional, debido a que la Pyme podría ser la primera ocasión que se implemente la administración del equilibrio de la información, además, este paso se puede tener en cuenta salteado, debido a que no existe un registro histórico del material de averiguación.

Paso 21: En este paso, los criterios de probabilidad definidos en el paso anterior sirven como referencia para asignar un valor de probabilidad (alto, medio, bajo) a cada activo significativo, así como la amenaza del activo. Debe utilizar el siguiente formato en el anexo 5.1.14.

- P5. Generación de un plan de control y mitigación de riesgos
  - A5.1. Especificar las estrategias de seguridad actuales

Paso 22: En este paso, se transmite el estado de la señal de cada proceso, que se definió en el paso 4. Para cada proceso, se determina el enfoque actual de la organización para hacer frente a las amenazas. Es probable que las prácticas de estabilidad ocurran en dos grupos, algunos de los cuales son estratégicos y operativos, y se considera que estos últimos reducen los riesgos específicos de activos específicos, porque son prácticas que mantienen operaciones continuas. Tenga en cuenta que las propiedades de la superficie estratégica son diferentes de las propiedades de la superficie activa. Para ello se ha elaborado una tabla con prácticas estables.

Práctica de seguridad estratégicas	Práctica de seguridad operativa
1. Concienciación y formación en seguridad 2. Estrategia de seguridad 3. Gestión de seguridad 4. Políticas y regulaciones de seguridad 5. Gestión de la seguridad colaborativa 6. Planes de contingencia/Recuperación de desastres	7. Control de acceso físico 8. Monitoreo y auditoría de seguridad física 9. Gestión de sistemas y redes 10. Monitoreo y auditoría de seguridad de TI 11. Autenticación y autorización 12. Gestión de vulnerabilidades 13. Encriptación 14. Diseño y arquitectura de seguridad 15. Gestión de incidentes

Figura 27. Las prácticas de estabilidad según OCTAVE – S

Fuente: Alberts, Dorofee, Steven, & Woody, (2005)

Para la definición de este paso, OCTAVE – S afirma la siguiente información por cada práctica de seguridad, ya sea estratégica u operativa.

- El estado del semáforo.
- Medir cada práctica de seguridad para un área específica tal como se refleja en la organización.
- Hace bien la organización en un área.
- Qué organización no está funcionando bien actualmente en un área.

- A5.2. Escoger las semejanzas de mitigación

Paso 23: En este paso, el estado de la bandera se pasa a cada método de seguridad. Como resultado, tenemos una visión global de la interacción de las amenazas con las prácticas de seguridad típicas.

Paso 24: Empieza con la selección de maneras estables en las que se llevarán a cabo las mitigaciones. Las zonas concretas se llaman zonas de regresión. OCTAVE - S ofrece escoger 3 superficies para eludir un plan de estabilización a extenso plazo y enfocarse en mitigar los peligros más importantes. No existe un proceso de selección predeterminado que nos ayude a elegir zonas de práctica estable como superficies de mitigación.

- A5.3. Generar los planes de mitigación de riesgos

Paso 25: Se definen planes de mitigación de peligros para las superficies identificadas en el paso anterior.

La estrategia de cobertura tiene como objetivo reducir el riesgo de activos importantes y es principalmente para realizar operaciones o tomar medidas contra las amenazas al activo.

OCTAVE - S nos brinda orientación sobre ocupaciones degradadas para todas las superficies de práctica de estabilización, considerando las ocupaciones agotadas proporcionadas por la herramienta, y las adaptamos para desarrollar un proyecto de estabilización.

Objetivo 04: Aplicar el modelo de procesos de seguridad de la información en el caso de estudio

La jefa de Recursos Humanos Lizbeth Anghelly Linares Seclén, mostró interés en el presente proyecto, puesto que, este modelo fue un aporte muy valioso para su organización. La participación de la jefa de recursos humanos ha sido muy importante, ya que ella era la encargada de compartirnos la información de los procesos y sus activos de la empresa Despensa Peruana S.A ya que sin dicha información no se ha podido desarrollar el proyecto de investigación.

Tabla 26.

El equipo de análisis

MIEMBROS	FUNCIÓN EN EVALUACIÓN
LIZBETH ANGHELLY LINARES SECLÉN	Jefa de Recursos Humanos
MARTOS PAREDES JOEL HAROLD VILLAZÓN SOSA JAIR AUGUSTO	Tesista de la escuela profesional de Ingeniería de Sistemas

Fuente: Elaboración propia

- P1: Definir la información de la organización.
    - A1.1. Definir la evaluación de impacto.

Tabla 27.

Descripción del impacto del proceso de recepción de mercancías

PROCESO: Recepción de Mercancías	
DESCRIPCIÓN DEL IMPACTO	Rango (alto, medio, bajo)
La vulneración del proceso de Recepción de Mercancías tiene un impacto significativo y negativo en la empresa Despensa Peruana S.A, afectando la calidad del inventario, la eficiencia operativa, la satisfacción del cliente y la competitividad en el mercado.	ALTO

Fuente: Elaboración propia

Tabla 28.

Descripción del impacto del proceso de gestión de inventarios

PROCESO: Gestión de Inventarios	
DESCRIPCIÓN DEL IMPACTO	Rango (alto, medio, bajo)
La vulneración del proceso de Gestión de Inventarios tiene un impacto significativo y negativo en la operación del almacén, la calidad del inventario, las finanzas, la satisfacción del cliente, la competitividad, los empleados y la planificación y toma de decisiones dentro de la empresa Despensa Peruana S.A.	ALTO

Fuente: Elaboración propia

Tabla 29.

Descripción del impacto del proceso de mantenimiento de almacén

PROCESO: Mantenimiento de Almacén	
DESCRIPCIÓN DEL IMPACTO	Rango (alto, medio, bajo)
La vulneración del proceso de Mantenimiento de Almacén tiene un impacto significativo y negativo en la eficiencia operativa, la calidad del inventario, las finanzas, la satisfacción del cliente, la competitividad y la seguridad de los empleados dentro de la empresa Despensa Peruana S.A.	ALTO

Fuente: Elaboración propia

Tabla 30.

Descripción del impacto del proceso de tecnología y sistemas de información.

PROCESO: Tecnología y Sistemas de Información	
DESCRIPCIÓN DEL IMPACTO	Rango (alto, medio, bajo)
La vulneración del proceso de Tecnología y Sistemas de Información tiene un impacto significativo y negativo en la operación, productividad, finanzas, satisfacción del cliente, competitividad, toma de decisiones y los empleados dentro de la empresa Despensa Peruana S.A.	ALTO

Fuente: Elaboración propia

- A1.2. Definir activos de la organización

Se encontraron los siguientes activos dentro de la empresa Despensa Peruana S.A.

Infraestructura del Almacén: Instalaciones físicas donde se recibe la mercancía.

Muelles de Carga y Descarga: Áreas específicas donde los camiones son cargados y descargados.

Equipos de Manipulación: Carretillas elevadoras, transpaletas y otros equipos utilizados para mover mercancías.

Sistemas de Gestión de Almacén (WMS): Software que gestiona la recepción y el flujo de mercancías dentro del almacén.

Escáneres y Dispositivos de Lectura: Equipos para la lectura de códigos de barras y RFID para registrar la entrada de mercancías.

Documentación de Recepción: Formularios y registros que verifican y documentan la recepción de mercancías.

Sistemas de Gestión de Inventario (IMS): Software que rastrea y administra el inventario en tiempo real.

Bases de Datos de Inventario: Archivos y registros electrónicos que contienen información detallada sobre los niveles y ubicaciones de inventario.

Procedimientos y Políticas de Inventario: Documentos que describen las reglas y métodos para la gestión del inventario.

Informes de Inventario: Reportes que proporcionan análisis y estados actuales del inventario.

Personal de Inventario: Empleados encargados de la gestión, control y auditoría del inventario.

Tecnología de Identificación (RFID, códigos de barras): Tecnologías utilizadas para rastrear y gestionar los productos en el inventario.

Plan de Mantenimiento: Documentación que detalla las rutinas y procedimientos de mantenimiento programado.

Equipos de Mantenimiento: Herramientas y máquinas necesarias para realizar trabajos de mantenimiento en el almacén.

Sistemas de Control de Clima: Equipos como aires acondicionados y calefactores que aseguran las condiciones adecuadas para el almacenamiento.

Personal de Mantenimiento: Empleados responsables de llevar a cabo las tareas de mantenimiento.

Registros de Mantenimiento: Documentación que registra todas las actividades de mantenimiento realizadas.

Proveedores de Servicios de Mantenimiento: Empresas externas que proporcionan servicios especializados de mantenimiento.

Servidores y Centros de Datos: Infraestructura que aloja las aplicaciones y datos empresariales.

Redes de Comunicación: Infraestructura de red que permite la comunicación interna y externa.

Sistemas de Gestión Empresarial (ERP): Software integral que integra diversos procesos de negocio.

Bases de Datos: Sistemas que almacenan y gestionan datos empresariales críticos.

Equipos Informáticos: Computadoras, terminales y otros dispositivos utilizados por los empleados.

Software de Seguridad y Protección de Datos: Programas que protegen la infraestructura tecnológica de amenazas y garantizan la integridad de los datos.

Personal de TI: Empleados especializados en la gestión, mantenimiento y desarrollo de sistemas de información.

Documentación Técnica: Manuales, guías y registros que documentan la configuración y mantenimiento de los sistemas tecnológicos.

Tabla 31.

Identificación de los activos para el proceso de Recepción de mercancías

PROCESO: Recepción de Mercancías	
ACTIVOS	DESCRIPCIÓN
Infraestructura del Almacén	Instalaciones físicas donde se recibe la mercancía la empresa Despensa Peruana S.A.
Muelles de Carga y Descarga	Áreas específicas donde los camiones son cargados y descargados dentro de la empresa Despensa Peruana S.A.
Equipos de Manipulación	Carretillas elevadoras, transpaletas y otros equipos utilizados para mover mercancías dentro de la empresa Despensa Peruana S.A.
Sistemas de Gestión de Almacén (WMS)	Software que gestiona la recepción y el flujo de mercancías dentro del almacén de la empresa Despensa Peruana S.A.
Escáneres y Dispositivos de Lectura	Equipos para la lectura de códigos de barras y RFID para registrar la entrada de mercancías de la empresa Despensa Peruana S.A.
Documentación de Recepción	Formularios y registros que verifican y documentan la recepción de mercancías dentro de la empresa Despensa Peruana S.A.

Fuente: Elaboración propia

Tabla 32.

Identificación de los activos para el proceso Gestión de inventarios

PROCESO: Gestión de Inventarios	
ACTIVOS	DESCRIPCIÓN
Sistemas de Gestión de Inventario (IMS)	Software que rastrea y administra el inventario en tiempo real dentro de la empresa Despensa Peruana S.A.
Bases de Datos de Inventario	Archivos y registros electrónicos que contienen información detallada sobre los niveles y ubicaciones de inventario de la empresa Despensa Peruana S.A.
Procedimientos y Políticas de Inventario	Documentos que describen las reglas y métodos para la gestión del inventario dentro de la empresa Despensa Peruana S.A.
Informes de Inventario	Reportes que proporcionan análisis y estados actuales del inventario de la empresa Despensa Peruana S.A.
Personal de Inventario	Empleados encargados de la gestión, control y auditoría del inventario dentro de la empresa Despensa Peruana S.A.
Tecnología de Identificación (RFID, códigos de barras)	Tecnologías utilizadas para rastrear y gestionar los productos en el inventario de la empresa Despensa Peruana S.A.

Fuente: Elaboración propia

Tabla 33.

Identificación de los activos para el proceso Mantenimiento de almacén

PROCESO: Mantenimiento de Almacén	
ACTIVOS	DESCRIPCIÓN
Plan de Mantenimiento	Documentación que detalla las rutinas y procedimientos de mantenimiento programado de la empresa Despensa Peruana S.A.
Equipos de Mantenimiento	Herramientas y máquinas necesarias para realizar trabajos de mantenimiento en el almacén de la empresa Despensa Peruana S.A.
Sistemas de Control de Clima	Equipos como aires acondicionados y calefactores que aseguran las condiciones adecuadas para el almacenamiento dentro de la empresa Despensa Peruana S.A.
Personal de Mantenimiento	Empleados responsables de llevar a cabo las tareas de mantenimiento dentro de la empresa Despensa Peruana S.A.
Registros de Mantenimiento	Documentación que registra todas las actividades de mantenimiento realizadas dentro de la empresa Despensa Peruana S.A.
Proveedores de Servicios de Mantenimiento	Empresas externas que proporcionan servicios especializados de mantenimiento dentro de la empresa Despensa Peruana S.A.

Fuente: Elaboración propia

Tabla 34.

Identificación de los activos para el proceso Tecnología y sistemas de información.

PROCESO: Tecnología y Sistemas de Información	
ACTIVOS	DESCRIPCIÓN
Servidores y Centros de Datos	Infraestructura que aloja las aplicaciones y datos empresariales dentro de la empresa Despensa Peruana S.A.
Redes de Comunicación	Infraestructura de red que permite la comunicación interna y externa para la empresa Despensa Peruana S.A.
Sistemas de Gestión Empresarial (ERP)	Software integral que integra diversos procesos de negocio para la empresa Despensa Peruana S.A.
Bases de Datos	Sistemas que almacenan y gestionan datos empresariales críticos de la empresa Despensa Peruana S.A.
Equipos Informáticos	Computadoras, terminales y otros dispositivos utilizados por los empleados de la empresa Despensa Peruana S.A.
Software de Seguridad y Protección de Datos	Programas que protegen la infraestructura tecnológica de amenazas y garantizan la integridad de los datos de la empresa Despensa Peruana S.A.
Personal de TI	Empleados especializados en la gestión, mantenimiento y desarrollo de sistemas de información de la empresa Despensa Peruana S.A.
Documentación Técnica	Manuales, guías y registros que documentan la configuración y mantenimiento de los sistemas tecnológicos de la empresa Despensa Peruana S.A.

Fuente: Elaboración propia

- A1.3. Medir las prácticas de seguridad de la organización

Para esta actividad se procedió a utilizar las prácticas de seguridad que ofrece la metodología OCTAVE – S, posteriormente a esto, se optó por brindarle un identificador a cada práctica de seguridad para poder trabajar fácilmente en los procesos de más adelante.

Cabe resaltar que como se trabajó con 4 procesos y estos procesos tienen la misma relación entre sí, solo se ha completado una tabla por qué las prácticas de seguridad se aplican en general.

Tabla 35.

Selección de las prácticas de seguridad dentro de la organización

Todos los procesos			
ID	Práctica de seguridad	Descripción	Estado
1	Concienciación y formación en seguridad.	La empresa Despensa Peruana S.A. realiza capacitaciones ocasionales, pero no tiene un programa estructurado y continuo.	
2	Estrategia de Seguridad	La empresa Despensa Peruana S.A. tiene una estrategia básica, pero no está completamente alineada con las metas comerciales y carece de detalles específicos.	
3	Gestión de Seguridad	La gestión de seguridad es ad-hoc y reactiva, sin una supervisión consistente.	
4	Políticas y regulaciones de seguridad	Existen políticas básicas, pero no están completamente documentadas ni actualizadas regularmente.	

5	Gestión de la Seguridad Colaborativa	La colaboración es mínima y no está formalizada en procedimientos claros.	
6	Planes de contingencia/recuperación de desastres	La empresa tiene un plan básico, pero carece de detalles y pruebas regulares.	
7	Control de Acceso físico	Hay controles básicos, como cerraduras y personal de seguridad, pero no hay medidas avanzadas.	
8	Monitoreo y Auditoría de seguridad Física	No se realizan auditorías regulares ni monitoreo continuo.	
9	Gestión de Sistemas y redes	La gestión de sistemas y redes se realiza de manera básica, sin herramientas avanzadas.	
10	Monitoreo y Auditoría de Seguridad de TI	No se implementan herramientas de monitoreo continuo ni se realizan auditorías regulares.	
11	Autenticación y Autorización	Se utilizan contraseñas básicas, sin mecanismos avanzados de autenticación.	
12	Gestión de vulnerabilidades	La gestión de vulnerabilidades se realiza de manera reactiva y sin un proceso estructurado.	

13	Encriptación	La encriptación se usa de manera limitada y no se aplica de manera uniforme en toda la empresa.	
14	Diseño y Arquitectura de Seguridad	La seguridad no se considera de manera integral en el diseño y desarrollo de sistemas.	
15	Gestión de Incidentes	La empresa no tiene un plan formal de gestión de incidentes, las respuestas son improvisadas.	

Nota: Los estados de semáforo sirven para ubicar con mayor exactitud las prácticas de seguridad en cada ítem.
Fuente: Elaboración propia

- P2: Generar perfiles de amenazas
    - A2.1. Elegir los activos críticos

Tabla 36.

Selección de los activos críticos para el proceso de Recepción de mercancías

PROCESO: Recepción de Mercancías				
ID ACTIVO CRÍTICO	NOMBRE ACTIVO CRÍTICO	RESPONSABLE	ACTIVOS RELACIONADOS	MOTIVO DE ACTIVO CRÍTICO
AC1	Sistemas de Gestión de Almacén (WMS)	Personal de almacén, Gerente de Logística, Equipo de TI	Computadoras y terminales de acceso. Red de comunicación interna. Escáneres de códigos de barras y RFID.	Este software es esencial para gestionar y registrar la entrada de mercancías de manera precisa y eficiente, asegurando la integridad de los datos de inventario desde el momento de la recepción.
AC2	Muelles de Carga y Descarga	Personal de almacén, Gerente de Logística, Personal de mantenimiento.	Equipos de carga y descarga (carretillas elevadoras, transpaletas). Sistema de seguridad (cámaras de vigilancia, sensores). Documentación de recepción y envío.	Estos son puntos cruciales para la entrada y salida de mercancías. Un problema en esta infraestructura puede causar retrasos significativos en la recepción y envío de productos.

Fuente: Elaboración propia

Tabla 37.

Selección de los activos críticos para el proceso de Gestión de inventarios

PROCESO: Gestión de Inventarios				
ID ACTIVO CRÍTICO	NOMBRE ACTIVO CRÍTICO	RESPONSABLE	ACTIVOS RELACIONADOS	MOTIVO DE ACTIVO CRÍTICO
AC3	Sistemas de Gestión de Inventario (IMS)	Personal de inventarios, Gerente de Inventarios, Equipo de TI.	Bases de datos de inventario. Software de gestión empresarial (ERP). Equipos de identificación (escáneres, RFID).	Este sistema es vital para rastrear y gestionar el inventario en tiempo real, asegurando la disponibilidad y exactitud de los datos de inventario, lo cual es crucial para todas las operaciones de la empresa.
AC4	Bases de Datos de Inventario	Administradores de bases de datos, Equipo de TI.	Servidores de bases de datos. Sistemas de respaldo y recuperación de datos. Software de seguridad y encriptación.	Contienen toda la información detallada sobre los niveles y ubicaciones de inventario. La pérdida o corrupción de estos datos puede paralizar la gestión de inventarios.

Fuente: Elaboración propia

Tabla 38.

Selección de los activos críticos para el proceso de Mantenimiento de almacén

PROCESO: Mantenimiento de Almacén				
ID ACTIVO CRÍTICO	NOMBRE ACTIVO CRÍTICO	RESPONSABLE	ACTIVOS RELACIONADOS	MOTIVO DE ACTIVO CRÍTICO
AC5	Plan de Mantenimiento	Gerente de Mantenimiento, Personal de Mantenimiento.	Software de gestión de mantenimiento. Herramientas y equipos de mantenimiento. Registros y documentación de mantenimiento.	Una planificación adecuada asegura que las tareas de mantenimiento se realicen de manera oportuna y eficiente, previniendo fallos en el almacén que podrían afectar la operación diaria.
AC6	Equipos de Mantenimiento	Personal de Mantenimiento, Gerente de Mantenimiento.	Herramientas manuales y eléctricas. Equipos de diagnóstico y reparación. Inventario de repuestos y materiales de mantenimiento.	Herramientas y máquinas son necesarias para realizar las tareas de mantenimiento. Su disponibilidad y funcionalidad son críticas para mantener el almacén en buenas condiciones.

Fuente: Elaboración propia

Tabla 39.

Selección de los activos críticos para el proceso de Tecnología y sistemas de información

PROCESO: Tecnología y Sistemas de Información				
ID ACTIVO CRÍTICO	NOMBRE ACTIVO CRÍTICO	RESPONSABLE	ACTIVOS RELACIONADOS	MOTIVO DE ACTIVO CRÍTICO
AC7	Servidores y Centros de Datos	Equipo de TI, Administradores de Sistemas.	Infraestructura de red. Sistemas de enfriamiento y alimentación ininterrumpida (UPS). Sistemas de respaldo y recuperación de datos.	Alojan las aplicaciones y datos empresariales. Son fundamentales para el funcionamiento de los sistemas de gestión, almacenamiento y comunicación de la empresa. Un fallo en estos sistemas puede causar una interrupción significativa de las operaciones
AC8	Sistemas de Gestión Empresarial (ERP)	Equipo de TI, Gerentes de Departamento	Servidores de aplicaciones. Bases de datos empresariales. Interfaces de usuario y estaciones de trabajo.	Integran diversos procesos de negocio, proporcionando una visión unificada y coordinada de las operaciones empresariales. Su funcionamiento es esencial para la eficiencia y efectividad de la empresa.

AC9	Software de Seguridad y Protección de Datos	Equipo de TI, Especialistas en Seguridad Informática.	Firewalls y sistemas de detección de intrusos. Software antivirus y antimalware. Herramientas de encriptación y gestión de claves.	Protegen la infraestructura tecnológica de amenazas y garantizan la integridad y confidencialidad de los datos. La seguridad de los sistemas de información es crítica para prevenir ciberataques y pérdida de datos.

Fuente: Elaboración propia

- A2.2. Definir los requisitos para la seguridad de activos críticos

Se tomaron en cuenta los siguientes requerimientos de seguridad:

  - Confidencialidad: Asegura que la información sea accesible, sólo para personal autorizado.
  - Totalidad: Asegura que la información logre ser modificada sólo por personal autorizado.
  - Disponibilidad: Esta medida sugiere, la época que está funcionando un sistema o equipo, respecto al tiempo total que realmente debe funcionar.
  - Entre otros.

A continuación, se presenta el siguiente formato para organizar los activos críticos, frente a los requerimientos de seguridad pre definidos por OCTAVE – S.

Tabla 40.

Identificar los requerimientos más importantes para cada activo crítico del proceso de Recepción de mercancías

PROCESO: Recepción de Mercancías		
ID ACTIVO CRÍTICO	REQUERIMIENTO DE SEGURIDAD	DESCRIPCIÓN
AC1	Totalidad, confidencialidad, disponibilidad	Este software es esencial para gestionar y registrar la entrada de mercancías de manera precisa y eficiente. Asegura la integridad de los datos de inventario desde el momento de la

		recepción, garantizando que sólo el personal autorizado pueda acceder y modificar esta información.
AC2	Totalidad, confidencialidad, disponibilidad	Los muelles son puntos cruciales para la entrada y salida de mercancías. Un problema en esta infraestructura puede causar retrasos significativos, impactando negativamente en la operación.

Fuente: Elaboración propia

Tabla 41.

Identificar los requerimientos más importantes para cada activo crítico del proceso de Gestión de inventarios

PROCESO: Gestión de Inventarios		
ID ACTIVO CRÍTICO	REQUERIMIENTO DE SEGURIDAD	DESCRIPCIÓN
AC3	Totalidad, confidencialidad, disponibilidad	Este sistema es vital para rastrear y gestionar el inventario en tiempo real. Asegura la disponibilidad y exactitud de los datos de inventario, lo cual es crucial para todas las operaciones de la empresa.

AC4	Totalidad, confidencialidad, disponibilidad	Contienen toda la información detallada sobre los niveles y ubicaciones de inventario. La pérdida o corrupción de estos datos puede paralizar la gestión de inventarios.

Fuente: Elaboración propia

Tabla 42.

Identificar los requerimientos más importantes para cada activo crítico del servicio Mantenimiento de almacén

PROCESO: Mantenimiento de Almacén		
ID ACTIVO CRÍTICO	REQUERIMIENTO DE SEGURIDAD	DESCRIPCIÓN
AC5	Totalidad, confidencialidad, disponibilidad	Una planificación adecuada asegura que las tareas de mantenimiento se realicen de manera oportuna y eficiente, previniendo fallos en el almacén que podrían afectar la operación diaria.
AC6	Totalidad, confidencialidad, disponibilidad	Herramientas y máquinas son necesarias para realizar las tareas de mantenimiento. Su disponibilidad y funcionalidad son críticas para mantener el almacén en buenas condiciones.

Fuente: Elaboración propia

Tabla 43.

Identificar los requerimientos más importantes para cada activo crítico del servicio Tecnología y Sistemas de información

PROCESO: Tecnología y Sistemas de Información		
ID ACTIVO CRÍTICO	REQUERIMIENTO DE SEGURIDAD	DESCRIPCIÓN
AC7	Totalidad, confidencialidad, disponibilidad	Alojan las aplicaciones y datos empresariales. Son fundamentales para el funcionamiento de los sistemas de gestión, almacenamiento y comunicación de la empresa. Un fallo en estos sistemas puede causar una interrupción significativa de las operaciones.
AC8	Totalidad, confidencialidad, disponibilidad	Integran diversos procesos de negocio, proporcionando una visión unificada y coordinada de las operaciones empresariales. Su funcionamiento es esencial para la eficiencia y efectividad de la empresa.
AC9	Totalidad, confidencialidad, disponibilidad	Protegen la infraestructura tecnológica de amenazas y garantizan la integridad y confidencialidad de los datos. La seguridad de los sistemas de información es crítica para prevenir ciberataques y pérdida de datos.

Fuente: Elaboración propia

- A2.3. Definir las amenazas de activos críticos

Se completó apropiadamente la identificación de amenazas para cada activo, considerando las próximas categorías de amenazas definidas por OCTAVE – S.

- C1: Personal teniendo ingreso a la red
- C2: Personal usando ingreso físico
- C3: Dificultades del sistema
- C4: Otros problemas

Tabla 44.

Identificación de las categorías por cada activo crítico del proceso de Recepción de mercancías

PROCESO: Recepción de Mercancías		
ID ACTIVO CRÍTICO	CATEGORÍA DE AMENAZA	DESCRIPCIÓN
AC1	C1	Un empleado malintencionado o descuidado podría acceder indebidamente al sistema WMS, comprometiendo la confidencialidad y la integridad de los datos de inventario. Podría resultar en modificaciones no autorizadas de inventario o acceso a información sensible de productos almacenados.
	C2	Un empleado con acceso físico al centro de datos o a las terminales del sistema WMS podría manipular o dañar equipos críticos para la operación del sistema. Interrupción en la recepción y gestión de mercancías debido a la falta de disponibilidad del sistema.
	C3	Problemas técnicos como fallas de hardware, errores de software o interrupciones en la red podrían afectar la disponibilidad y la funcionalidad del sistema WMS. Retrasos en la gestión de inventarios y en la operación de los muelles de carga y descarga, afectando la eficiencia operativa.
	C4	Incluye amenazas no específicas como desastres naturales, fallos de energía, errores humanos no intencionales, entre otros, que podrían afectar la seguridad

		y disponibilidad del sistema WMS. Pérdida de datos críticos de inventario, interrupción prolongada de las operaciones debido a eventos imprevistos.
	C1	Un empleado podría acceder a sistemas de control de seguridad de los muelles para permitir acceso no autorizado a mercancías. Robo o manipulación de mercancías durante el proceso de carga o descarga.
	C2	Un empleado con acceso físico podría comprometer la seguridad de los muelles, permitiendo el ingreso de personal no autorizado o de mercancías ilícitas. Pérdidas económicas por mercancías faltantes o dañadas, problemas legales por incumplimiento de normativas de seguridad.
AC2	C3	Fallos en equipos como puertas automáticas, sistemas de control de acceso o sistemas de iluminación podrían afectar la operación eficiente de los muelles. Retrasos en la recepción y envío de mercancías, afectando la cadena de suministro y la satisfacción del cliente.
	C4	Incluye amenazas como condiciones climáticas adversas, accidentes en el área de carga o descarga, o incidentes de seguridad no previstos. Daños físicos a las instalaciones, interrupción de las operaciones, posibles riesgos para la seguridad del personal.

Fuente: Elaboración propia

Tabla 45.

Identificación de las categorías por cada activo crítico del proceso de Gestión de inventarios

PROCESO: Gestión de Inventarios		
ID ACTIVO CRÍTICO	CATEGORÍA DE AMENAZA	DESCRIPCIÓN
AC3	C1	Acceso no autorizado de empleados a la red del sistema IMS, comprometiendo la seguridad y la confidencialidad de los datos de inventario. Manipulación de datos de inventario, pérdida de integridad en los registros de stock.
	C2	Acceso físico no autorizado a servidores o terminales que manejan el sistema IMS, posiblemente resultando en alteraciones de inventario. Interrupción de la gestión de inventarios, errores en el control de stock debido a cambios no autorizados.
	C3	Problemas técnicos como fallos de hardware, errores de software o interrupciones de red que impiden el acceso oportuno a los datos de inventario. Retrasos en la gestión de pedidos, falta de disponibilidad de datos críticos para la toma de decisiones empresariales.
	C4	Incluye eventos imprevistos como desastres naturales, cortes de energía prolongados, o errores humanos involuntarios que pueden afectar la disponibilidad y la seguridad del sistema IMS. Pérdida de datos de inventario, disminución de la eficiencia operativa, costos adicionales para la recuperación y reparación de sistemas.
AC4	C1	Acceso no autorizado a la red que alberga las bases de datos de inventario, comprometiendo la seguridad y la confidencialidad de la información almacenada. Pérdida de datos sensibles, violación de la privacidad de clientes y proveedores.

C2	Acceso físico no autorizado a los servidores o centros de datos que alojan las bases de datos de inventario. Modificación o eliminación de registros de inventario, errores en la gestión de stock.
C3	Problemas técnicos como fallos de hardware, errores de software o interrupciones en la red que impiden el acceso y la gestión de datos de inventario. Retrasos en la gestión de inventarios, falta de disponibilidad de datos críticos para la toma de decisiones operativas.
C4	Incluye factores como desastres naturales, fallos de energía, o errores humanos no intencionales que pueden comprometer la integridad y la disponibilidad de las bases de datos de inventario. Interrupción de las operaciones, pérdida de datos críticos, costos elevados para la recuperación y restauración de información.

Fuente: Elaboración Propia

Tabla 46.

Identificación de las categorías por cada activo crítico del proceso de Mantenimiento de almacén

PROCESO: Mantenimiento de Almacén		
ID ACTIVO CRÍTICO	CATEGORÍA DE AMENAZA	DESCRIPCIÓN
AC5	C1	Acceso no autorizado de empleados a sistemas que gestionan el plan de mantenimiento, comprometiendo la confidencialidad y la integridad de las tareas programadas. Modificación no autorizada de horarios y tareas de mantenimiento, afectando la eficiencia operativa del almacén.
	C2	Acceso físico no autorizado a archivos impresos o sistemas físicos que contienen el plan de mantenimiento, lo que podría resultar en cambios no autorizados o pérdida de documentación crítica. Interrupción en las operaciones de mantenimiento planificadas, posibles daños a la infraestructura del almacén debido a mantenimiento inadecuado.
	C3	Problemas técnicos como fallas de software o hardware que impidan el acceso oportuno al plan de mantenimiento programado. Retrasos en las tareas de mantenimiento preventivo, posibles fallos de equipos y sistemas debido a la falta de mantenimiento adecuado.
	C4	Incluye amenazas como condiciones climáticas extremas, cambios inesperados en la disponibilidad de recursos, o errores humanos que puedan interferir con la ejecución adecuada del plan de mantenimiento. Aumento de costos operativos debido a reparaciones no planificadas, posible daño a la reputación debido a la incapacidad para cumplir con estándares de seguridad y mantenimiento.

AC6	C1	Acceso no autorizado de empleados a sistemas que controlan la operación y mantenimiento de equipos críticos. Manipulación de ajustes y configuraciones de equipos que pueden llevar a fallos operativos o daños a la infraestructura del almacén.
	C2	Acceso físico no autorizado a herramientas y máquinas utilizadas para el mantenimiento, lo que podría resultar en daños físicos a equipos o interferencias con operaciones programadas. Interrupción en las operaciones de mantenimiento preventivo y correctivo, posibles riesgos para la seguridad del personal debido a manipulación no autorizada de equipos.
	C3	Fallos técnicos en herramientas y equipos de mantenimiento que impidan su funcionamiento adecuado. Retrasos en la ejecución de tareas de mantenimiento, posibles fallos operativos debido a la falta de mantenimiento oportuno.
	C4	Incluye amenazas como accidentes de trabajo, falta de capacitación adecuada para el uso seguro de equipos, o falta de recursos necesarios para la reparación y mantenimiento. Aumento de riesgos para la seguridad del personal, posibles daños a equipos críticos, impacto negativo en la productividad debido a paros no programados.

Fuente: Elaboración propia

Tabla 47.

Identificación de las categorías por cada activo crítico del proceso de Tecnología y sistemas de Información

PROCESO: Tecnología y Sistemas de Información		
ID ACTIVO CRÍTICO	CATEGORÍA DE AMENAZA	DESCRIPCIÓN
AC7	C1	Acceso no autorizado de empleados a sistemas que gestionan servidores y centros de datos. Posible manipulación de datos críticos, comprometiendo la integridad y confidencialidad de la información empresarial.
	C2	Acceso físico no autorizado a salas de servidores o equipos que alojan infraestructura crítica. Daño físico a equipos, posible pérdida de datos debido a manipulación no autorizada o robo de hardware.
	C3	Problemas técnicos como fallos de hardware, errores de software o interrupciones en la red que afecten la disponibilidad y el rendimiento de servidores y centros de datos. Interrupción de servicios críticos, pérdida de datos, potencial impacto negativo en la reputación de la empresa.
	C4	Incluye amenazas como desastres naturales, cortes de energía prolongados, o fallos humanos que puedan afectar la disponibilidad y la seguridad de servidores y centros de datos. Pérdida de datos críticos, interrupción prolongada de servicios empresariales, costos elevados para la recuperación y reparación de sistemas.
AC8	C1	Acceso no autorizado de empleados a sistemas que gestionan el ERP, comprometiendo la seguridad y confidencialidad de los datos empresariales. Manipulación de registros financieros, pérdida de confianza de los clientes y proveedores.

	C2	Acceso físico no autorizado a terminales o equipos que manejan el ERP, lo que podría resultar en cambios no autorizados o errores en la gestión de procesos empresariales. Interrupción en la ejecución de pedidos, posible incumplimiento de acuerdos contractuales debido a errores en la facturación o gestión de inventarios.
	C3	Problemas técnicos como fallos de software, errores de programación o interrupciones en la red que afecten la disponibilidad y el rendimiento del ERP. Retrasos en la toma de decisiones, errores en la planificación de recursos empresariales, posibles fallos en la gestión financiera y de inventario.
	C4	Incluye amenazas como cambios en las regulaciones gubernamentales, cambios en las condiciones de mercado, o errores humanos que puedan afectar la eficiencia y efectividad del ERP. Costos adicionales por errores en la gestión empresarial, pérdida de oportunidades de negocio, dificultades para adaptarse a cambios regulatorios.
	C1	Acceso no autorizado de empleados a sistemas que gestionan software de seguridad, comprometiendo la eficacia de las medidas de protección contra amenazas cibernéticas. Vulnerabilidades de seguridad, riesgo de ciberataques o intrusiones maliciosas.
AC9	C2	Acceso físico no autorizado a dispositivos o equipos que ejecutan software de seguridad, posiblemente resultando en manipulación no autorizada de configuraciones de seguridad. Brechas de seguridad, compromiso de la integridad de los datos empresariales, potencial robo de información sensible.
	C3	Problemas técnicos como fallos de software, actualizaciones no aplicadas o configuraciones erróneas que debiliten las defensas de seguridad. Exposición a amenazas cibernéticas, riesgo de pérdida de datos o interrupción de servicios críticos debido a vulnerabilidades no mitigadas.

C4	Incluye situaciones como cambios en las normativas de seguridad, errores humanos en la administración de configuraciones de seguridad, o incidentes de seguridad inesperados. Costos adicionales para mitigar vulnerabilidades, penalizaciones regulatorias, y pérdida de confianza por parte de clientes y socios comerciales.

Fuente: Elaboración propia

- P3: Revisar la infraestructura tecnológica con relación a los activos críticos
  - A3.1. Indagar las rutas de ingreso

Tabla 48.

Formato de identificación de componentes

COMPONENTES DEL SISTEMA		
ID COMPONENTE	NOMBRE DEL COMPONENTE	USUARIO ENCARGADO DEL COMPONENTE
COMP1	Servidor de aplicaciones	Administrador de Sistemas
COMP2	Servidor de bases de datos	Administrador de Bases de Datos
COMP3	Switch de red	Administrador de Redes
COMP4	Router	Administrador de Redes
COMP5	Estaciones de trabajo (PC)	Usuarios de Oficina
COMP6	Laptop de ejecutivos	Ejecutivos y Gerentes
COMP7	Sistema de seguridad física (CCTV)	Seguridad o Administrador de Instalaciones
COMP8	Sistema de Control de Acceso Físico	Seguridad o Administrador de Instalaciones
COMP9	Terminal del sistema ERP	Personal de Administración y Finanzas
COMP10	Dispositivos móviles (smartphones, tablets)	Personal de Almacén y Logística

Fuente: Elaboración propia

Se diseñó un modelo de las rutas de acceso con todos sus componentes con el programa de packet tracer v8.2.2 para poder examinar las rutas de acceso.

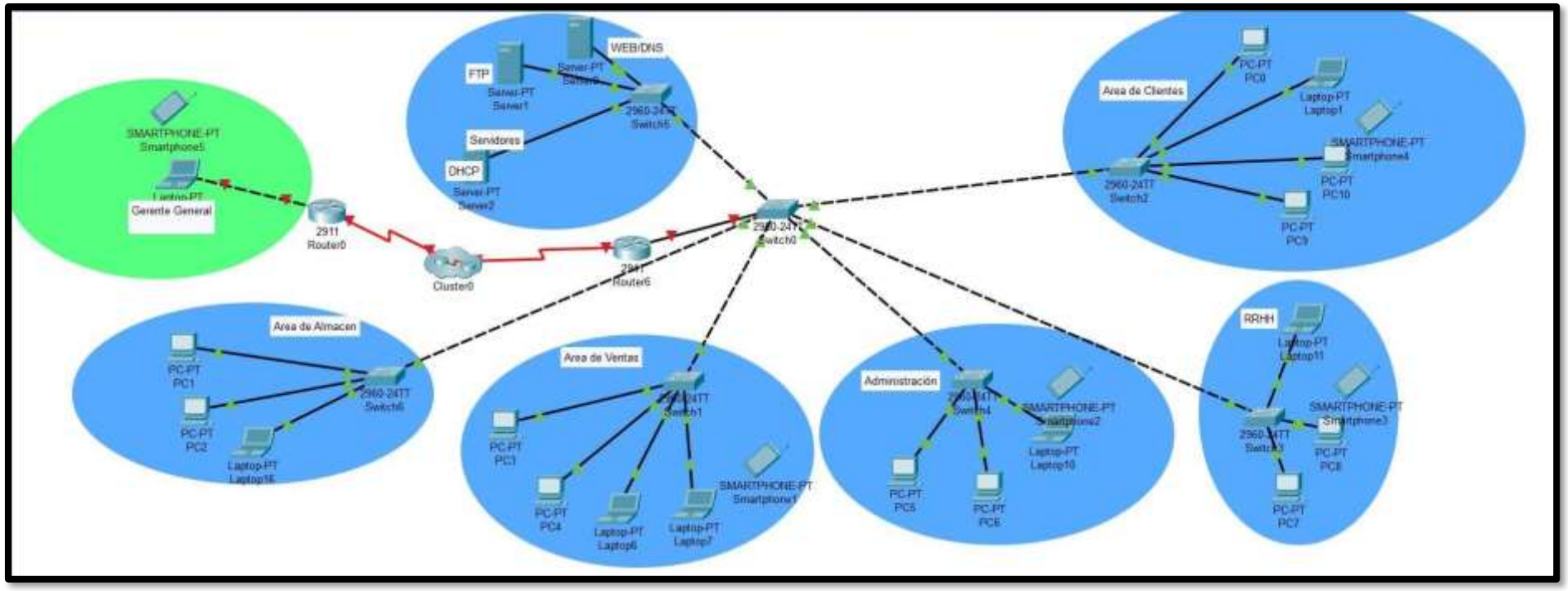


Figura 28. La infraestructura tecnológica de la empresa Despensa Peruana

Fuente: Elaboración propia

- A3.2. Distinguir los procesos con la tecnología

Tabla 49.

Estimación del grado de seguridad

PROCESO: Todos los procesos			
ID ACTIVO CRÍTICO	COMPONENTE	RESPONSABLE	ESTIMACIÓN
AC1	Servidores de aplicaciones, Estaciones de trabajo (PC).	Administrador de Sistemas, Usuarios de oficina.	ALTA
AC2	Equipos de mantenimiento, CCTV.	Personal de mantenimiento, Seguridad o Administrador de Instalaciones	MEDIA
AC3	Servidores de aplicaciones, Estaciones de trabajo (PC).	Administrador de Sistemas, Usuarios de oficina.	ALTA
AC4	Servidores de bases de datos, Estaciones de trabajo (PC).	Administrador de Bases de Datos, Usuarios de oficina.	ALTA
AC5	Servidores de aplicaciones, Estaciones de trabajo (PC).	Administrador de Sistemas, Usuarios de oficina.	ALTA
AC6	Estaciones de trabajo (PC), Laptop de ejecutivos.	Usuarios de oficina, Ejecutivos y Gerentes.	MEDIA

AC7	Servidores de aplicaciones, Servidores de bases de datos, Switch de red, Router.	Administrador de Sistemas, Administrador de Bases de Datos, Administrador de Redes.	ALTA
AC8	Terminal del ERP, Estaciones de trabajo (PC), Laptop de ejecutivos.	Personal de Administración y Finanzas, Usuarios de oficina, Ejecutivos y Gerentes.	ALTA
AC9	Estaciones de trabajo (PC), Servidores de aplicaciones.	Usuarios de oficina, Administrador de Sistemas.	ALTA

Fuente: Elaboración propia

- P4: Identificación y análisis de riesgos
  - A4.3. Estimación de las probabilidades de amenaza

Tabla 50.

Evaluación de las probabilidades de amenaza

PROCESO: Todos los procesos		
ID ACTIVO CRÍTICO	AMENAZA	DESCRIPCIÓN DEL IMPACTO
AC1	C1, C2, C3	Acceso no autorizado de personal a los sistemas de gestión de almacén (WMS), interferencia física en los muelles de carga y descarga, problemas operativos del sistema que afectan la gestión de inventario.
AC2	C2	Acceso físico no autorizado al área de muelles de carga y descarga, posibilidad de alteración o interferencia en las operaciones logísticas.

AC3	C1, C2, C3	Acceso no autorizado a los sistemas de gestión de inventarios (IMS), interferencia física en equipos de gestión de inventarios, problemas operativos que afectan la precisión del inventario.
AC4	C1, C2, C3	Acceso no autorizado a las bases de datos de inventario, interferencia física en equipos de gestión de inventarios, problemas operativos que afectan la integridad de los datos de inventario.
AC5	C1, C3	Acceso no autorizado a los planes de mantenimiento, problemas operativos relacionados con el mantenimiento preventivo y correctivo.
AC6	C2	Acceso físico no autorizado a equipos de mantenimiento, posibilidad de daños intencionados o interferencia en las operaciones de mantenimiento.
AC7	C1, C2, C3	Acceso no autorizado a servidores y centros de datos, acceso físico no autorizado a equipos críticos de infraestructura, problemas operativos que afectan la disponibilidad y seguridad de datos críticos.
AC8	C1, C2, C3	Acceso no autorizado a sistemas de gestión empresarial (ERP), interferencia física en terminales y estaciones de trabajo críticas, problemas operativos que afectan la integridad y disponibilidad de datos empresariales.
AC9	C1, C3	Acceso no autorizado a software de seguridad y

	protección de datos, problemas operativos relacionados con la seguridad informática y la protección de datos sensibles.

Fuente: Elaboración propia

- Para desarrollar esta actividad, debido a que es la primera vez que se aplica OCTAVE - S en Despensa Peruana S.A. y debido a la falta de datos maestros, archivos históricos y documentación sobre amenazas y personal humano de Tecnología de información sin experiencia y conocimiento de estabilidad de la información, se decidió no calcular la probabilidad de amenazas y, por lo tanto, continuar con los siguientes pasos.

- P5. Generación de un plan de control y mitigación de riesgos
  - A5.1. Especificar las estrategias de seguridad actuales

Práctica de seguridad estratégicas	Práctica de seguridad operativa
1. Gestión de seguridad	2. Control de accesos físicos 3. Monitoreos y auditorías de seguridad física 4. Monitoreo y auditoría de seguridad de TI 5. Diseño y arquitectura de seguridad

Figura 29. La distribución entre prácticas de seguridad estratégicas y operativas

Fuente: Elaboración propia

Para el desarrollo de este paso tomó en cuenta la siguiente información por cada práctica de seguridad, ya sea estratégica u operativa.

- Estado de los semáforos
- La medida en que cada práctica de seguridad refleja un área de la organización.
- Las actividades de una empresa de forma deficiente en el área.

A5.2. Escoger las semejanzas de mitigación

Se seleccionaron las medidas de seguridad mediante las cuales se implementaron las actividades de mitigación. No existen procesos de selección establecidos que nos ayuden a identificar el área de práctica de seguridad como área de mitigación así que consideramos los factores de valor del impacto de la amenaza, las condiciones del

semáforo, las operaciones que probablemente mejorarán y las áreas donde el riesgo pudo mitigarse significativamente para muchos activos.

Área de Mitigación 1: Gestión de la Seguridad

- AC1 - Sistemas de Gestión de Almacén (WMS): Este activo crítico comprende los sistemas de gestión de almacén, esenciales para administrar y registrar la entrada de mercancías de manera precisa y eficiente. Incluye software y sistemas utilizados para mantener la integridad y precisión del inventario desde la recepción hasta el almacenamiento.
    - Medidas de Mitigación: Implementar controles de acceso físico y lógico, documentar y comunicar políticas de seguridad de acceso, y capacitar al personal en el manejo seguro de estos sistemas.
    - Responsables: Administrador de Sistemas, Gerente de Almacén.

Área de Mitigación 2: Control de Ingreso Físico

- AC2 - Muelles de Carga y Descarga: Este activo crítico incluye los puntos de entrada y salida de mercancías en los muelles de carga y descarga. Son cruciales para asegurar la eficiencia y seguridad de las operaciones logísticas.
    - Medidas de Mitigación: Implementar sistemas de control de acceso físico, establecer políticas claras para el control de ingreso, y capacitar al personal en seguridad y protocolos de ingreso.
    - Responsables: Gerente de Operaciones, Seguridad.

Área de Mitigación 3: Control y Auditoría de Seguridad Física

- AC3 - Bases de Datos de Inventario: Contiene información detallada sobre los niveles y ubicaciones de inventario. Es crucial para la gestión precisa y efectiva del inventario de la empresa.
    - Medidas de Mitigación: Implementar controles de acceso a bases de datos, encriptación de datos sensibles, y auditorías regulares para garantizar la integridad y confidencialidad de la información.
    - Responsables: Administrador de Base de Datos, Gerente de Almacén.
- AC5 - Plan de Mantenimiento: Incluye el plan de mantenimiento preventivo y correctivo de equipos críticos en el almacén. Es fundamental para asegurar la disponibilidad y funcionalidad de los equipos.
    - Medidas de Mitigación: Implementar un plan de mantenimiento riguroso, capacitar al personal en procedimientos de mantenimiento seguro, y documentar adecuadamente todas las actividades de mantenimiento.
    - Responsables: Gerente de Mantenimiento, Ingeniero de Mantenimiento.

Área de Mitigación 4: Gestión de Vulnerabilidades

- AC4 - Plan de Mantenimiento: Este activo crítico incluye el plan de mantenimiento preventivo y correctivo para equipos y sistemas en el almacén. Asegura la disponibilidad y operatividad continua de los activos físicos.

    - Medidas de Mitigación: Implementar un programa de mantenimiento proactivo, capacitar al personal en técnicas de mantenimiento seguro, y documentar todas las actividades relacionadas con el mantenimiento.
    - Responsables: Gerente de Mantenimiento, Ingeniero de Mantenimiento.
- AC7 - Servidores y Centros de Datos: Incluye servidores y centros de datos que almacenan y procesan datos críticos de la empresa. Son esenciales para la continuidad y seguridad de las operaciones empresariales.
    - Medidas de Mitigación: Implementar sistemas de monitoreo y auditoría continua, mejorar las políticas de seguridad física, y reforzar los controles de acceso y gestión de equipos críticos.
    - Responsables: Administrador de Sistemas, Administrador de Seguridad de la Información.

Área de Mitigación 5: Diseño de Ingeniería y Estabilidad

- AC6 - Equipos de Mantenimiento: Incluye herramientas y máquinas utilizadas para realizar tareas de mantenimiento en el almacén. Esencial para garantizar la eficiencia y efectividad de las operaciones de mantenimiento.
    - Medidas de Mitigación: Implementar controles de acceso a equipos críticos, proporcionar entrenamiento en seguridad y uso adecuado de herramientas, y mantener un inventario actualizado de equipos.

- Responsables: Gerente de Mantenimiento, Equipo de Mantenimiento.

- AC8 - Sistemas de Gestión Empresarial (ERP): Incluye herramientas y máquinas utilizadas para realizar tareas de mantenimiento en el almacén. Esencial para garantizar la eficiencia y efectividad de las operaciones de mantenimiento.
  - Medidas de Mitigación: Implementar controles de acceso a equipos críticos, proporcionar entrenamiento en seguridad y uso adecuado de herramientas, y mantener un inventario actualizado de equipos.
  - Responsables: Gerente de Mantenimiento, Equipo de Mantenimiento.

Área de Mitigación 6: Tecnología y Sistemas de Información

- AC9 - Software de Seguridad y Protección de Datos: Comprende el software utilizado para proteger la infraestructura tecnológica y los datos sensibles de la empresa contra amenazas cibernéticas.
  - Medidas de Mitigación: Implementar software antivirus y antimalware, configurar firewalls y sistemas de detección de intrusiones, y capacitar al personal en prácticas seguras de seguridad informática.
  - Responsables: Administrador de Seguridad de la Información, Equipo de TI.

- A5.3. Generar los planes de mitigación de riesgos

5.3.1. Plan absoluto de seguridad:

Alcance: Actividades de Mitigación de la Gestión de la Seguridad.

- Documentación de Funcionalidades y Responsabilidades de Seguridad: Todas las funciones y responsabilidades relacionadas con la seguridad deben ser claramente documentadas y puestas a disposición de todos los empleados que interactúan con estos procesos.
    - Medidas de mitigación:
        - Crear un manual de seguridad que detalle las responsabilidades de cada puesto relacionado con la seguridad.
        - Realizar sesiones informativas periódicas para asegurar que todos los empleados comprendan sus roles y responsabilidades.
    - Roles y responsabilidades:
        - Gerente General: Supervisar la creación y distribución del manual de seguridad.
        - Administrador de Seguridad de la Información: Actualizar el manual de seguridad según sea necesario y conducir las sesiones informativas.

- Actualización de Políticas y Métodos de Seguridad: Mantener las políticas y métodos de seguridad actualizados es esencial para asegurar que la empresa esté protegida contra amenazas emergentes.
    - Medidas de mitigación:
        - Establecer un calendario para revisar y actualizar las políticas de seguridad regularmente.
        - Incluir actualizaciones de políticas en el proceso de incorporación de nuevos empleados.
    - Roles y responsabilidades:
        - Gerente General: Aprobar las actualizaciones de políticas de seguridad.
        - Equipo de TI: Implementar cambios tecnológicos necesarios para las nuevas políticas.
        - Recursos Humanos: Incorporar las políticas actualizadas en el proceso de inducción de nuevos empleados.
- Recuperación de Activos de la Organización: Asegurar que todos los activos de la organización, como portátiles, dispositivos electrónicos y documentos confidenciales, sean recuperados al finalizar la relación laboral de un empleado.
    - Medidas de mitigación:
        - Implementar un proceso formal para la devolución de activos al finalizar el empleo.

        - Realizar auditorías periódicas para asegurar que todos los activos están contabilizados.
    - Roles y responsabilidades:
        - Gerente de Recursos Humanos: Coordinar el proceso de devolución de activos.
        - Administrador de Sistemas: Verificar que todos los dispositivos electrónicos sean devueltos y restablecidos.

Áreas de Mitigación Específicas

1. Gestión de la Seguridad
    - Impacto: Falta de procesos formales y capacitación en seguridad de la información.
    - Medidas:
        - Documentar y comunicar procedimientos de gestión de seguridad.
        - Establecer programas de capacitación continua en seguridad.
    - Estado: Amarillo.
2. Control de ingreso Físico
    - Impacto: Falta de políticas de control de acceso físico.
    - Medidas:
        - Implementar un sistema de control de acceso físico.
        - Definir y documentar roles y responsabilidades para el control de ingreso.

- Estado: Amarillo.

3. Control y Auditoría de seguridad física
    - Impacto: Falta de políticas de monitoreo de entrada física.
    - Medidas:
        - Implementar sistemas de monitoreo y auditoría física.
        - Establecer procedimientos para auditar el ingreso físico regularmente.
    - Estado: Amarillo.
4. Gestión de Vulnerabilidades
    - Impacto: Falta de procesos para identificar y gestionar vulnerabilidades.
    - Medidas:
        - Implementar herramientas para la identificación y gestión de vulnerabilidades.
        - Realizar evaluaciones de vulnerabilidades regularmente.
    - Estado: Rojo.
5. Diseño de ingeniería y seguridad
    - Impacto: Falta de un esquema documentado de topología de red y seguridad.
    - Medidas:
        - Documentar y mantener actualizados los esquemas de red y seguridad.
        - Alinear el diseño de seguridad con las mejores prácticas de la industria.

- Estado: Rojo

Este plan absoluto de seguridad para Despensa Peruana S.A. proporciona una guía clara y estructurada para mitigar riesgos en sus procesos críticos, asegurando la protección de sus activos y la continuidad de sus operaciones.

Objetivo 05: Evaluar el modelo mediante juicio de experto

Para la validación del instrumento se usó la metodología Delphi para lo cual se considerando tres expertos; así como también para aplicar la razón de validez se aplicó a 5 expertos haciendo uso de la siguiente formula por cada ítem:

$$CVR = \frac{n_e - \frac{N}{2}}{N}$$

Tabla 51.

Las variables descritas para el juicio de expertos

Variable	Descripción
CVR	Razón de validez de contenido
N	Número de expertos
n_e	Numero de expertos indican esencial

Fuente: Elaboración propia

Nota: Resultados obtenidos por los expertos en la validez del instrumento.

Fuente: Elaboración propia.

Para el instrumento de validación se desarrolló en el formato que se puede visualizar en el anexo 5.4.

Posteriormente, se distribuyó la encuesta a los expertos para poder validar si el instrumente es esencial, útil o no necesaria, con la opción para colocar una observación en cada pregunta si el experto lo requiere.

Tabla 52. El cálculo del CVR con las respuestas de los expertos

Ne	N	ITEM	E1	E2	E3	E4	E5	CVR
5	5	1	0	1	1	1	0	1.000
5	5	2	0	1	1	1	1	1.000
5	5	3	1	1	1	1	1	1.000
5	5	4	1	1	1	1	1	1.000
5	5	5	1	1	1	1	1	1.000
5	5	6	1	1	0	1	1	1.000
5	5	7	1	1	0	1	0	1.000
5	5	8	1	1	1	1	1	1.000
5	5	9	1	1	1	1	1	1.000
5	5	10	1	1	1	1	1	1.000
5	5	11	1	1	1	1	1	1.000
5	5	12	1	1	1	1	1	1.000
5	5	13	1	1	1	1	1	1.000
5	5	14	1	1	1	1	1	1.000
5	5	15	1	1	1	1	1	1.000
5	5	16	1	1	1	1	1	1.000
5	5	17	1	1	1	1	1	1.000
5	5	18	1	1	1	1	1	1.000

Fuente: Elaboración propia.

Una vez que se han analizado y corregido las observaciones brindadas por los expertos, se procedió a evaluar el juicio de expertos. Las respuestas se pueden visualizar a continuación.

EXPERTO 01

UNIVERSIDAD SEÑOR DE SIPÁN

VALIDEZ DE INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN

IMPLEMENTACIÓN DE UN MODELO DE PROCESOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA PYME PERUANA BASADA EN LA NORMA ISO/IEC 27005 Y LA METODOLOGÍA OCTAVE-S

LAMBAYEQUE 2021

Autores: Martos Paredes Joel Harold
Villazón Sosa Jair Augusto

Es de gran relevancia, realizar la evaluación de los instrumentos de recolección de información con la finalidad de confirmar que estos sean válidos y que los resultados obtenidos a partir de éstos sean utilizados eficientemente; brindando aportes tanto al área investigativa de la carrera profesional de Ingeniería de Sistemas como a sus aplicaciones. Agradecemos su valiosa colaboración.

N°	DIMENSIONES/ITEMS	Claridad[1]		Pertinencia[2]		Relevancia[3]		Observaciones
		SI	NO	SI	NO	SI	NO	
Variable: La seguridad de la información en una PYME								
Indicador Nivel de riesgo de los activos de la seguridad de la información.								
1	¿Considera usted que se debería desarrollar un modelo de seguridad para que sus informaciones no estén en riesgo?	X		X		X		
2	¿Recomendaría usted a PYMES para gestionar la seguridad de sus informaciones?	X		X		X		

[1] ***Claridad***: *Los enunciados se entienden fácilmente*

[2] ***Pertinencia***: *La pregunta está relacionada con la dimensión, variable, etc.*

[3] ***Relevancia:*** *La pregunta planteada permite solucionar alguna parte del problema planteado*

Indicador: Nivel de Criticidad de los activos de la seguridad de la información.								
3	¿Recomendaría usted a PYMES, contratar a un personal especializado y que se dedique exclusivamente a la seguridad de información?	X		X		X		
Indicador: Eficacia de la seguridad de la información.								
4	¿Recomendaría usted a PYMES, implementar mecanismos formales para verificar si se está cumpliendo todos los procesos que el cliente solicita?	X		X		X		
5	¿Antes de solicitar los servicios de PYMES, usted revisaría todo su perfil empresarial?	X		X		X		
6	¿Contrataría usted los servicios de PYMES, para una mejor seguridad de información en sus equipos?	X		X		X		
7	¿Considera usted que si se implementa la norma ISO 27005 en su PYME la seguridad de su información mejoraría?	X		X		X		
8	¿Considera usted que la norma ISO 27005 ayudaría a controlar la pérdida de información en las empresas?	X		X		X		
9	¿Considera usted que desarrollando un modelo de procesos de la seguridad de la información podrá mejorar los riesgos para las empresas?	X		X		X		

En su opinión, el instrumento resulta:

(X) Aplicable ( ) Aplicable con correcciones ( ) No Aplicable

APELLIDOS Y NOMBRE	Ing. Milagros del Carmen Castañeda Barbarán.
GRADO ACADÉMICO	Maestría en Ingeniería de sistemas con mención en tecnología de información y gestión de software.

Chiclayo 20 de noviembre de 2021

MILAGROS DEL CARMEN CASTAÑEDA BARBARAN
INGENIERA DE SISTEMAS
REG. CIP. 182291

FIRMA DE EXPERTO
DNI: 17452557

UNIVERSIDAD SEÑOR DE SIPÁN

VALIDEZ DE INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN

IMPLEMENTACIÓN DE UN MODELO DE PROCESOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA PYME PERUANA BASADA EN LA NORMA ISO/IEC 27005 Y LA METODOLOGÍA OCTAVE-S LAMBAYEQUE 2021

Autores: Martos Paredes Joel Harold
Villazón Sosa Jair Augusto

Es de gran relevancia, realizar la evaluación de los instrumentos de recolección de información con la finalidad de confirmar que estos sean válidos y que los resultados obtenidos a partir de éstos sean utilizados eficientemente; brindando aportes tanto al área investigativa de la carrera profesional de Ingeniería de Sistemas como a sus aplicaciones. Agradecemos su valiosa colaboración.

Nº	DIMENSIONES/ITEMS	Claridad[1]		Pertinencia[2]		Relevancia[3]		Observaciones
		SI	NO	SI	NO	SI	NO	
Variable: Modelo de procesos de seguridad de la información basado en la norma ISO/IEC 27005 y la metodología OCTAVE-S.								
Indicador: Costo de Implementación.								
1	¿Considera usted que el gasto llevado a cabo favorece a las PYMES?	X		X		X		
2	¿Estima usted que el precio de implementación está bastante sobrevalorado del presupuesto?	X		X		X		

[1] ***Claridad***: *Los enunciados se entienden fácilmente*
[2] ***Pertinencia***: *La pregunta está relacionada con la dimensión, variable, etc.*
[3] ***Relevancia***: *La pregunta planteada permite solucionar alguna parte del problema planteado*

Indicador: Tiempo de Implementación.								
3	¿Considera usted que si se implementa un modelo basado en la norma ISO 27005 y la metodología OCTAVE- S para PYMES, este reducirá los riesgos de seguridad de dicha información?	X		X		X		
Indicador: Nivel de cumplimiento con estándares								
4	¿Considera usted que al implementar la norma ISO 27005, esta permitirá identificar los riesgos de seguridad de la información de su empresa?	X		X		X		
5	¿Considera usted que, si se usa diferentes metodologías, estás ayudarían a disminuir los riesgos de seguridad de la información de su PYME y la integridad de la misma?	X		X		X		
6	¿En qué intervalo de tiempo se encuentra el procesamiento de actividades relacionadas con la seguridad de la información de su empresa?	X		X		X		
7	¿Considera usted que con el uso de nuestro modelo de seguridad basado en la norma ISO 27005 y la metodología OCTAVE-S generará satisfacción a la empresa respecto a la reducción de riesgos a la que está expuesta su información?	X		X		X		
8	La norma ISO 27005 establece que primero se debe analizar los riesgos con el fin de evitar que la información esté en peligro ¿Usted considera que esta etapa es importante?	X		X		X		

9	¿Conoce usted acerca de la implementación de procesos para la seguridad de la información?	X		X		X		

En su opinión, el instrumento resulta:

(X) Aplicable ( ) Aplicable con correcciones ( ) No Aplicable

Chiclayo 20 de noviembre de 2021

APELLIDOS Y NOMBRE	Ing. Milagros del Carmen Castañeda Barbarán.
GRADO ACADÉMICO	Maestría en Ingeniería de sistemas con mención en tecnología de información y gestión de software.

FIRMA DE EXPERTO
DNI: 17452557

EXPERTO 02

UNIVERSIDAD SEÑOR DE SIPÁN

Ficha de Validación de Metodología

Título: Implementación de un Modelo de Procesos de Seguridad de la Información para una Pyme Peruana basada en la norma ISO/IEC 27005 Y la Metodología OCTAVE-S

Indicaciones: Señor especialista se le pide la pronta colaboración, que luego de una rigurosa evaluación de los instrumentos del cuestionario, marque con un aspa (X) en el casillero que crea conveniente de acuerdo a su criterio y experiencia profesional.

Nº	DIMENSIONES/ITEMS	Esencial	Útil	No Necesaria	Observaciones
1	¿Considera usted que el gasto llevado a cabo favorece a las PYMES?		X		
2	¿Estima usted que el precio de implementación está bastante sobrevalorado del presupuesto?		X		
3	¿Considera usted que si se implementa un modelo basado en la norma ISO 27005 y la metodología OCTAVE- S para PYMES, este reducirá los riesgos de seguridad de dicha información?	X			
4	¿Considera usted que al implementar la norma ISO 27005, esta permitirá identificar los riesgos de seguridad de la información de su empresa?	X			
5	¿Considera usted que, si se usa diferentes metodologías, estás	X			

	ayudarían a disminuir los riesgos de seguridad de la información de su PYME y la integridad de la misma?				
6	¿En qué intervalo de tiempo se encuentra el procesamiento de actividades relacionadas con la seguridad de la información de su empresa?	X			
7	¿Considera usted que con el uso de nuestro modelo de seguridad basado en la norma ISO 27005 y la metodología OCTAVE-S generará satisfacción a la empresa respecto a la reducción de riesgos a la que está expuesta su información?		X		
8	La norma ISO 27005 establece que primero se debe analizar los riesgos con el fin de evitar que la información esté en peligro ¿Usted considera que esta etapa es importante?	X			
9	¿Conoce usted acerca de la implementación de procesos para la seguridad de la información?		X		
10	¿Considera usted que se debería desarrollar un modelo de seguridad para que sus informaciones no estén en riesgo?	X			
11	¿Recomendaría usted a PYMES para gestionar la seguridad de sus informaciones?	X			
12	¿Recomendaría usted a PYMES, contratar a un personal especializado y que se dedique exclusivamente a la		X		

	seguridad de información?				
13	¿Recomendaría usted a PYMES, implementar mecanismos formales para verificar si se está cumpliendo todos los procesos que el cliente solicita?	X			
14	¿Antes de solicitar los servicios de PYMES, usted revisaría todo su perfil empresarial?	X			
15	¿Contrataría usted los servicios de PYMES, para una mejor seguridad de información en sus equipos?	X			
16	¿Considera usted que si se implementa la norma ISO 27005 en su PYME la seguridad de su información mejoraría?	X			
17	¿Considera usted que la norma ISO 27005 ayudaría a controlar la pérdida de información en las empresas?	X			
18	¿Considera usted que desarrollando un modelo de procesos de la seguridad de la información podrá mejorar los riesgos para las empresas?	X			

APELLIDOS Y NOMBRE	Villazón Sosa Sofía
GRADO ACADÉMICO	INGENIERO DE SISTEMAS

FIRMA DE EXPERTO
DNI: 47654981

UNIVERSIDAD SEÑOR DE SIPÁN

Ficha de Validación de Instrumento

Nombre Instrumento a validar: Cuestionario

Titulo: Implementación de un Modelo de Procesos de Seguridad de la Información para una Pyme Peruana basada en la norma ISO/IEC 27005 Y la Metodología OCTAVE-S

Indicadores	Criterios	Calificación			
		Deficiente	Regular	Bueno	Muy bueno
		De 0 a 5	De 6 a 10	De 11 a 15	De 16 a 20
Claridad	Los enunciados se entienden fácilmente			15	
Pertinencia	La pregunta está relacionada con la dimensión, variable, etc.				18
Relevancia	La pregunta planteada permite solucionar alguna parte del problema planteado				16

Valoración (0-20): 16 Colocar el logo institucional

En su opinión, el instrumento resulta:

(X) Aplicable ( ) Aplicable con correcciones ( ) No Aplicable

APELLIDOS Y NOMBRE	Villacorta Sosa Sofía
GRADO ACADÉMICO	INGENIERO DE SISTEMAS

FIRMA DE EXPERTO
DNI: 47053485

EXPERTO 03

UNIVERSIDAD SEÑOR DE SIPÁN

Ficha de Validación de Metodología

Titulo: Implementación de un Modelo de Procesos de Seguridad de la Información para una Pyme Peruana basada en la norma ISO/IEC 27005 Y la Metodología OCTAVE-S

Indicaciones: Señor especialista se le pide la pronta colaboración, que luego de una rigurosa evaluación de los instrumentos del cuestionario, marque con un aspa (X) en el casillero que crea conveniente de acuerdo a su criterio y experiencia profesional.

Nº	DIMENSIONES/ITEMS	Esencial	Útil	No Necesaria	Observaciones
1	¿Considera usted que el gasto llevado a cabo favorece a las PYMES?	X			
2	¿Estima usted que el precio de implementación está bastante sobrevalorado del presupuesto?	X			
3	¿Considera usted que si se implementa un modelo basado en la norma ISO 27005 y la metodología OCTAVE- S para PYMES, este reducirá los riesgos de seguridad de dicha información?	X			
4	¿Considera usted que al implementar la norma ISO 27005, esta permitirá identificar los riesgos de seguridad de la información de su empresa?	X			
5	¿Considera usted que, si se usa diferentes metodologías, estás	X			

	ayudarían a disminuir los riesgos de seguridad de la información de su PYME y la integridad de la misma?	
6	¿En qué intervalo de tiempo se encuentra el procesamiento de actividades relacionadas con la seguridad de la información de su empresa?	X
7	¿Considera usted que con el uso de nuestro modelo de seguridad basado en la norma ISO 27005 y la metodología OCTAVE-S generará satisfacción a la empresa respecto a la reducción de riesgos a la que está expuesta su información?	X
8	La norma ISO 27005 establece que primero se debe analizar los riesgos con el fin de evitar que la información esté en peligro ¿Usted considera que esta etapa es importante?	X
9	¿Conoce usted acerca de la implementación de procesos para la seguridad de la información?	X
10	¿Considera usted que se debería desarrollar un modelo de seguridad para que sus informaciones no estén en riesgo?	X
11	¿Recomendaría usted a PYMES para gestionar la seguridad de sus informaciones?	X
12	¿Recomendaría usted a PYMES, contratar a un personal especializado y que se dedique exclusivamente a la	X

	seguridad de información?	
13	¿Recomendaría usted a PYMES, implementar mecanismos formales para verificar si se está cumpliendo todos los procesos que el cliente solicita?	X
14	¿Antes de solicitar los servicios de PYMES, usted revisaría todo su perfil empresarial?	X
15	¿Contrataría usted los servicios de PYMES, para una mejor seguridad de información en sus equipos?	X
16	¿Considera usted que si se implementa la norma ISO 27005 en su PYME la seguridad de su información mejoraría?	X
17	¿Considera usted que la norma ISO 27005 ayudaría a controlar la pérdida de información en las empresas?	X
18	¿Considera usted que desarrollando un modelo de procesos de la seguridad de la información podrá mejorar los riesgos para las empresas?	X

APELLIDOS Y NOMBRE	Gonzales Jerez, Miguel Angel
GRADO ACADÉMICO	INGENIERO DE SISTEMAS

FIRMA DE EXPERTO
DNI:

USS | UNIVERSIDAD SEÑOR DE SIPÁN

Ficha de Validación de Instrumento

Nombre Instrumento a validar: Cuestionario

Titulo: Implementación de un Modelo de Procesos de Seguridad de la Información para una Pyme Peruana basada en la norma ISO/IEC 27005 Y la Metodología OCTAVE-S

Indicadores	Criterios	Calificación			
		Deficiente	Regular	Bueno	Muy bueno
		De 0 a 5	De 6 a 10	De 11 a 15	De 16 a 20
Claridad	Los enunciados se entienden fácilmente				20
Pertinencia	La pregunta está relacionada con la dimensión, variable, etc.				20
Relevancia	La pregunta planteada permite solucionar alguna parte del problema planteado				20

Valoración (0-20): 20

En su opinión, el instrumento resulta:

(X) Aplicable ( ) Aplicable con correcciones ( ) No Aplicable

APELLIDOS Y NOMBRE	Gonzales Jiménez Miguel Angel
GRADO ACADÉMICO	INGENIERO DE SISTEMAS

FIRMA DE EXPERTO
DNI:

EXPERTO 04

USS | UNIVERSIDAD SEÑOR DE SIPÁN

Ficha de Validación de Metodología

Título: Implementación de un Modelo de Procesos de Seguridad de la Información para una Pyme Peruana basada en la norma ISO/IEC 27005 Y la Metodología OCTAVE-S

Indicaciones: Señor especialista se le pide la pronta colaboración, que luego de una rigurosa evaluación de los instrumentos del cuestionario, marque con un aspa (X) en el casillero que crea conveniente de acuerdo a su criterio y experiencia profesional.

Nº	DIMENSIONES/ITEMS	Esencial	Útil	No Necesaria	Observaciones
1	¿Considera usted que el gasto llevado a cabo favorece a las PYMES?	X			
2	¿Estima usted que el precio de implementación está bastante sobrevalorado del presupuesto?		X		
3	¿Considera usted que si se implementa un modelo basado en la norma ISO 27005 y la metodología OCTAVE- S para PYMES, este reducirá los riesgos de seguridad de dicha información?		X		
4	¿Considera usted que al implementar la norma ISO 27005, esta permitirá identificar los riesgos de seguridad de la información de su empresa?	X			
5	¿Considera usted que, si se usa diferentes metodologías, estás		X		

	ayudarían a disminuir los riesgos de seguridad de la información de su PYME y la integridad de la misma?				
6	¿En qué intervalo de tiempo se encuentra el procesamiento de actividades relacionadas con la seguridad de la información de su empresa?	X			
7	¿Considera usted que con el uso de nuestro modelo de seguridad basado en la norma ISO 27005 y la metodología OCTAVE-S generará satisfacción a la empresa respecto a la reducción de riesgos a la que está expuesta su información?	X			
8	La norma ISO 27005 establece que primero se debe analizar los riesgos con el fin de evitar que la información esté en peligro ¿Usted considera que esta etapa es importante?	X			
9	¿Conoce usted acerca de la implementación de procesos para la seguridad de la información?	X			
10	¿Considera usted que se debería desarrollar un modelo de seguridad para que sus informaciones no estén en riesgo?	X			
11	¿Recomendaría usted a PYMES para gestionar la seguridad de sus informaciones?		X		
12	¿Recomendaría usted a PYMES, contratar a un personal especializado y que se dedique exclusivamente a la		X		

	seguridad de información?		
13	¿Recomendaría usted a PYMES, implementar mecanismos formales para verificar si se está cumpliendo todos los procesos que el cliente solicita?		X
14	¿Antes de solicitar los servicios de PYMES, usted revisaría todo su perfil empresarial?		X
15	¿Contrataría usted los servicios de PYMES, para una mejor seguridad de información en sus equipos?	X	
16	¿Considera usted que si se implementa la norma ISO 27005 en su PYME la seguridad de su información mejoraría?	X	
17	¿Considera usted que la norma ISO 27005 ayudaría a controlar la pérdida de información en las empresas?	X	
18	¿Considera usted que desarrollando un modelo de procesos de la seguridad de la información podrá mejorar los riesgos para las empresas?	X	

APELLIDOS Y NOMBRE	Maguen Niño Gissela Luisa Elena
GRADO ACADÉMICO	INGENIERO DE SISTEMAS

FIRMA DE EXPERTO
DNI:

UNIVERSIDAD SEÑOR DE SIPÁN

Ficha de Validación de Instrumento

Nombre Instrumento a validar: Cuestionario

Título: Implementación de un Modelo de Procesos de Seguridad de la Información para una Pyme Peruana basada en la norma ISO/IEC 27005 Y la Metodología OCTAVE-S

Indicadores	Criterios	Calificación			
		Deficiente	Regular	Bueno	Muy bueno
		De 0 a 5	De 6 a 10	De 11 a 15	De 16 a 20
Claridad	Los enunciados se entienden fácilmente				20
Pertinencia	La pregunta está relacionada con la dimensión, variable, etc.				18
Relevancia	La pregunta planteada permite solucionar alguna parte del problema planteado				19

Valoración (0-20): 19

En su opinión, el instrumento resulta:

(X) Aplicable ( ) Aplicable con correcciones ( ) No Aplicable

Ingresar el logo institucional

APELLIDOS Y NOMBRE	Maguiña Niño Gissella Luisa Elena
GRADO ACADÉMICO	INGENIERO DE SISTEMAS

FIRMA DE EXPERTO
DNI:

EXPERTO 05

USS | UNIVERSIDAD SEÑOR DE SIPÁN

Ficha de Validación de Metodología

Titulo: Implementación de un Modelo de Procesos de Seguridad de la Información para una Pyme Peruana basada en la norma ISO/IEC 27005 Y la Metodología OCTAVE-S

Indicaciones: Señor especialista se le pide la pronta colaboración, que luego de una rigurosa evaluación de los instrumentos del cuestionario, marque con un aspa (X) en el casillero que crea conveniente de acuerdo a su criterio y experiencia profesional.

N°	DIMENSIONES/ITEMS	Esencial	Útil	No Necesaria	Observaciones
1	¿Considera usted que el gasto llevado a cabo favorece a las PYMES?		X		
2	¿Estima usted que el precio de implementación está bastante sobrevalorado del presupuesto?		X		
3	¿Considera usted que si se implementa un modelo basado en la norma ISO 27005 y la metodología OCTAVE- S para PYMES, este reducirá los riesgos de seguridad de dicha información?	X	X		
4	¿Considera usted que al implementar la norma ISO 27005, esta permitirá identificar los riesgos de seguridad de la información de su empresa?	X			
5	¿Considera usted que, si se usa diferentes metodologías, estás	X			

166

	ayudarían a disminuir los riesgos de seguridad de la información de su PYME y la integridad de la misma?				
6	¿En qué intervalo de tiempo se encuentra el procesamiento de actividades relacionadas con la seguridad de la información de su empresa?	X			
7	¿Considera usted que con el uso de nuestro modelo de seguridad basado en la norma ISO 27005 y la metodología OCTAVE-S generará satisfacción a la empresa respecto a la reducción de riesgos a la que está expuesta su información?	X			
8	La norma ISO 27005 establece que primero se debe analizar los riesgos con el fin de evitar que la información esté en peligro ¿Usted considera que esta etapa es importante?	X			
9	¿Conoce usted acerca de la implementación de procesos para la seguridad de la información?	X			
10	¿Considera usted que se debería desarrollar un modelo de seguridad para que sus informaciones no estén en riesgo?	X			
11	¿Recomendaría usted a PYMES para gestionar la seguridad de sus informaciones?	X			
12	¿Recomendaría usted a PYMES, contratar a un personal especializado y que se dedique exclusivamente a la	X			

	seguridad de información?	
13	¿Recomendaría usted a PYMES, implementar mecanismos formales para verificar si se está cumpliendo todos los procesos que el cliente solicita?	X
14	¿Antes de solicitar los servicios de PYMES, usted revisaría todo su perfil empresarial?	X
15	¿Contrataría usted los servicios de PYMES, para una mejor seguridad de información en sus equipos?	X
16	¿Considera usted que si se implementa la norma ISO 27005 en su PYME la seguridad de su información mejoraría?	X
17	¿Considera usted que la norma ISO 27005 ayudaría a controlar la pérdida de información en las empresas?	X
18	¿Considera usted que desarrollando un modelo de procesos de la seguridad de la información podrá mejorar los riesgos para las empresas?	X

APELLIDOS Y NOMBRE	Maquen Alvino Jose Carlos E.
GRADO ACADÉMICO	INGENIERO DE SISTEMAS

FIRMA DE EXPERTO
DNI:

UNIVERSIDAD SEÑOR DE SIPÁN

Ficha de Validación de Instrumento

Nombre Instrumento a validar: Cuestionario

Título: Implementación de un Modelo de Procesos de Seguridad de la Información para una Pyme Peruana basada en la norma ISO/IEC 27005 Y la Metodología OCTAVE-S

Indicadores	Criterios	Calificación			
		Deficiente	Regular	Bueno	Muy bueno
		De 0 a 5	De 6 a 10	De 11 a 15	De 16 a 20
Claridad	Los enunciados se entienden fácilmente				18
Pertinencia	La pregunta está relacionada con la dimensión, variable, etc.				19
Relevancia	La pregunta planteada permite solucionar alguna parte del problema planteado				19

Valoración (0-20): 19

En su opinión, el instrumento resulta:

(X) Aplicable ( ) Aplicable con correcciones ( ) No Aplicable

APELLIDOS Y NOMBRE	Naquen Niño José Carlos E.
GRADO ACADÉMICO	INGENIERO DE SISTEMAS

FIRMA DE EXPERTO
DNI:

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones.

- Para seleccionar la empresa se tuvo en consideración todas aquellas en la región de Lambayeque, las cuales según reactiva Perú llegan a la cantidad de 24,117 en general y dado el caso de estudio son 13,128 empresas del rubro del comercio, siendo Despensa Peruana S.A. la empresa esencial para el desarrollo del caso de estudio por su fácil acceso a la información de sus activos digitales.

- Generar perfiles de amenaza, posibilita tener una iniciativa casi perfecta de probables situaciones en donde los activos críticos pueden verse involucrados.

- El modelo desarrollado se centra solamente en los procesos que son considerados críticos para la organización, esto sirve para poder enfocar el 100% de la productividad en las verdaderas amenazas para una pyme y así poder planificar un control de seguridad para la organización.

- El modelo, apoyándose con la metodología OCTAVE - S, sirve esencialmente para obtener una base y poder evitar los riesgos que se presenten a futuro. Esto sirve para documentar la experiencia de los analistas para una posterior mejora y actualizar nuevas medidas de defensa para la organización.

- El apoyo financiero, el entendimiento entre los altos rangos de la organización más los analistas, se complementan perfectamente para poder gestionar la seguridad de la información de forma correcta y ordenada.

4.2. Recomendaciones.

Se recomienda seguir al pie de la letra las actividades propuestas en el modelo de seguridad, con la misión de mitigar aquellas amenazas que dañen los activos críticos de la organización y reducir la posibilidad de que sucedan riesgos futuros.

Para evitar problemas hacia las actividades normales de la empresa, es recomendable comprobar periódicamente las políticas y actividades, puesto que, la tecnología avanza constantemente y cada día se descubren nuevos riesgos que tienen que ser controlados para evitar peligros futuros.

Se recomienda, definir procedimientos correctos, para que los integrantes de la organización conozcan a detalle las ocupaciones que les pertenecen a cada uno, frente a distintas emergencias.

REFERENCIAS.

Administraciones, M. d. (2012). MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. *Madrid: Ministerio de Hacienda y Administraciones Públicas*.

Agrawal, V. (2017). A Framework for the Information Classification in ISO 27005 Standard.

Al Friki, M., Aditra Putra, F., Suryanto, Y., & Ramli, K. (2019). Evaluación de riesgos mediante la técnica de combinación de NIST SP 800-30. *La Quinta Conferencia Internacional de Sistemas de Información 2019*, 1206-1215.

Alberts, C., Dorofee, A., Steven, J., & Woody, C. (2005). OCTAVE®-S Implementation. *Carnegie Mellon University*.

Alwi, A., & Zainol Ariffin, K. A. (2018). Information Security Risk Assessment for the Malaysian Aeronautical Information Management System. *Cyber Resilience Conference*, 1-4.

blokdyk, g. (2019). ISO 27005 A Complete Guide - 2020 Edition. *5STARCooks*.

Brodin, M. (2017). Security strategies for managing mobile devices in SMEs: A theoretical evaluation. 1-6.

Buryanina, N. S., Gogolev, R. O., Korolyuk, Y. F., Lesnykh, E. V., & Suslov, K. V. (2019). Digital Differential Protection of the «Generator-Transformer» Block. *IEEE*, 1-4.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Improving the Information Security Risk. *CarnegieMellon*.

Carnero Garay, D. F., Carbajal Ramos, M. A., Armas Aguirre, J., & Madrid Molina, J. M. (2020). Information security risk management model for mitigating the

impact on SMEs in Peru. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 1-7.

Department for Digital, Culture, Media & Sport; MP, Matt Warman. (24 de Marzo de 2021). *gov.uk.* Obtenido de Cyber Security Breaches Survey 2021: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Dube, E., & Flowerday, S. (2018). Towards a Holistic Information Security Framework for South African Small and Medium Enterprises. 1-4.

García, H., Fresia, Y., & Lema Moreta, L. M. (2018). Modelo de Madurez para el Análisis de Riesgos de los Activos de Información basado en las Metodologías MAGERIT, OCTAVE y MEHARI; con enfoque a Empresas Navieras. *Repositorio digital de la Universidad de Especialidades Espíritu Santo UEES*, 1-11.

García-Porras, C., Huamani-Pastor, S., & Armas-Aguirre, d. J. (2018). Information Security Risk Management Model for Peruvian SMEs. *2018 IEEE Sciences and Humanities International Research Conference (SHIRCON)*, 1-5.

Giuseppi, A., Tortorelli, A., Germanà, R., Liberati, F., & Fiaschetti, A. (1 de Julio de 2019). *Securing Cyber-Physical Systems: An Optimization Framework based on OSSTMM and Genetic Algorithms.*

Goman, M. (2019). Current State of IT Risk Analysis in Management Frameworks: Is It Enough? *60th International Scientific Conference on Information Technology and Management Science of Riga Technical University*, 1-5.

Holguín García, F. Y., & Lema Moreta, L. M. (2018). Maturity Model for the Risk Analysis of Information. 1-11.

Huamani Pastor, S. C., Loparte Alvarado, R. F., & García Porras, J. C. (2018). Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas. *Revista peruana de computación y sistemas*, 10.

ISO/IEC. (2018). INTERNATONAL STANDAR ISO/IEC 27005.

Iyamuremye, B., & Shima, H. (2018). Network security testing tools for SMEs (small and medium enterprises. *2018 IEEE International Conference on Applied System Invention (ICASI)*, 414-417.

Khalid Eisa, H. A., Shamsul Kamal, A. K., Noor Azah, S., Sapiee, J., & Kamaruddin Malik, b. (2019). A policy driven, human oriented information security model: a case study in UAE banking sector. *IEEE*, 12-17.

Kim, D., & Solomon, M. G. (2016). Fundamentals of Information Systems Security. *Jones & Bartlett Learning*.

Lefebure, P., Jacques, D., & Jacques, L. (2016). Analysis of the risks and potential interest associated with nanotechnologies in the field of defense and security: French Ministry of Defense. *Chlorodia LLC*.

Lontsikh, P. A., Kunakov, E. P., Lontsikh, N. P., Livshitz, I., & Vladimirtsev, A. V. (2020). Information Security Methods' Application Based on the Digital Management Approaches and the Deming Cycle in Improving the Modern Production's Processes. *IEEE*, 123-126.

Markovic, I. (2019). How to use the risk assessment matrix to organize your project better. *TMS-Outsource*.

Martinez Cortes, J. F. (2015). *Universidad Piloto de Colombia.* Obtenido de http://polux.unipiloto.edu.co/: http://polux.unipiloto.edu.co:8080/00002332.pdf

Mashkina, I. V., Guzairov, M. B., Vasilyev, V. I., Tuliganova, L. R., & Konovalov, A. S. (2016). Issues of information security control in virtualization segment of company information system. *IEEE*, 161-163.

Meriah, I., & Latifa Ben, A. (2018). A Survey of Quantitative Security Risk Analysis Models for Computer Systems. *Proceedings of the 2nd International Conference on Advances in Artificial Intelligence*, 36-40.

Montenegro, C., & Moncayo, D. (2016). Information security risk in SMEs: A hybrid model compatible with IFRS: Evaluation in two Ecuadorian SMEs of automotive sector. *2016 6th International Conference on Information Communication and Management (ICICM)*, 115-120.

normalización, O. I. (2013). ISO/IEC 27001:2013. *Ginebra: Organización Internacional de la normalización*.

Reactiva Perú. (2020). Estadísticas del programa REACTIVA PERÚ. *Ministerio de Economía y Finanzas*, 0-2.

Rubio, N., Chavarria, L., & Mauricio, D. (2020). Security architecture for the protection of digital assets in SMEs. *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE*, 1-6.

SANTISTEBAN, J. C. (2019). *MODELO BASADO EN METODOLOGÍAS DE GESTIÓN DE RIESGOS DE TI PARA CONTRIBUIR EN LA MEJORA DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN EN EMPRESAS DEL SECTOR AGROINDUSTRIAL DE LA REGIÓN DE LAMBAYEQYE.* Obtenido de http://tesis.usat.edu.pe/: http://tesis.usat.edu.pe/bitstream/20.500.12423/2159/1/TM_BandaSantistebanJose.pdf

Setiawan, H., Aditya Putra, F., & Rifa Pradana, A. (2017). Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 revision 1: A case study at communication data applications of XYZ institute. *International Conference on Information Technology Systems and Innovation*.

Wens, C. v. (2019). ISO 27001 Handbook: Implementing and auditing an Information Security Management System in small and medium-sized businesses. *New York: Independently published*.

Zaynalov Nodir, R., Mukhamadiev Abdinabi, N., Bekmurodov Ulugbek, B. u., Mavlonov Obid, N., Kiyamov Jasur, U., & Qilichev, D. (2019). Information Security Issues For Travel Companies. *IEEE*, 1-4.

ANEXOS.

Anexo 1. Resolución de aprobación del proyecto de investigación

USS | UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°0445-2021/FIAU-USS

Pimentel, 27 de mayo de 2021

VISTO:
El Acta de reunión N°1305-2021 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida mediante oficio N°0227-2021/FIAU-IS-USS de fecha 19 de mayo de 2021, y;

CONSIDERANDO:
Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48° que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y tesis son aprobados por el Comité de Investigación y derivados a la Facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El periodo de vigencia de los mismos será de dos años, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24° señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; es individual o en pares para obtener un título profesional. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C.".

Que, según documentos de Vistos el Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS acuerdan aprobar los temas de las Tesis a cargo de los estudiantes del curso de Investigación I que se detallan en el anexo de la presente Resolución.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:

ARTÍCULO 1°: APROBAR, el tema de la Tesis perteneciente a la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de los estudiantes del Programa de estudios de INGENIERÍA DE SISTEMAS según se detalla en el anexo de la presente Resolución.

ARTÍCULO 2°: ESTABLECER, que la inscripción del Tema de la Tesis se realice a partir de emitida la presente resolución y tendrá una vigencia de dos (02) años.

ARTÍCULO 3°: DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Cc: Interesado, Archivo

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°0445-2021/FIAU-USS

Pimentel, 27 de mayo de 2021

ANEXO

N°	AUTOR (ES)	TEMA DE TESIS
1	RIMARACHIN ESCRIBANO NERI RUT NIÑO MORENO NAJHELY YAMILETT	EVALUACIÓN DE TÉCNICAS DE CIFRADO PARA EL INTERCAMBIO DE DATOS DE INTERNET DE LAS COSAS EN EL ÁMBITO DE LA SALUD
2	GUEVARA CHAMBERGO JHON DENNIS BOBADILLA CAMPOS ROLANDO MARTIN	DESARROLLO DE UNA METODOLOGÍA DE GESTIÓN DE RIESGOS AD HOC BASADA EN MARCOS INTERNACIONALES Y BUENAS PRÁCTICAS PARA UNA EMPRESA MANUFACTURERA PERUANA
3	CIEZA CELIS JESUS ABELARDO OJEDA ROMERO ANTHONNY JHONATAN	EVALUACIÓN DEL DESEMPEÑO DE LOS ESQUEMAS DE SEGURIDAD DE RED PARA COMBATIR VULNERABILIDADES EN REDES INALÁMBRICAS BASADAS EN EL PROTOCOLO WPA2
4	MENDOZA FERRÉ ESPERANZA NATALY CABRERA SANCHEZ KEVIN ALONSO	COMPARACIÓN DEL RENDIMIENTO DE TECNOLOGÍAS DE VIRTUALIZACIÓN PARA EL DESPLIEGUE DE APLICACIONES CON ARQUITECTURA DE MICROSERVICIOS
5	TEMOCHE GOMEZ LENNIN BILLEY	DESARROLLO DE UN MÉTODO PARA DETECTAR CON EFICIENCIA LAS VULNERABILIDADES INFORMÁTICAS DE ATAQUE CROSS-SITE SCRIPTING UTILIZANDO TÉCNICAS DE APRENDIZAJE AUTOMÁTICO
6	CASTRO MEDINA MIGUEL ANGEL	IMPLEMENTACIÓN DE UNA METODOLOGÍA AD HOC DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA EDITORA DE DIARIO REGIONAL PERUANO
7	MURO ESPINOZA JUAN JOSE	DESARROLLO DE UNA METODOLOGÍA AD HOC DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA UN INSTITUTO SUPERIOR PEDAGÓGICO PERUANO
8	DIAZ ZAVALA ROXANA KARINA FRIAS VASQUEZ LADY	DESARROLLO DE UNA METODOLOGÍA AD HOC DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA UNA UNIDAD DE GESTIÓN EDUCATIVA PERUANA
9	CARRASCO BORDA APARICIO	DESARROLLO DE UN MODELO DE PROCESOS AD HOC PARA EL DESARROLLO DE SOFTWARE POR LICENCIA PARA UNA MYPE DE SERVICIOS DE TI BASADO EN ISO/IEC 29110
10	OTERO MORALES JAVIER LIZARDO AQUINO SOSA NOELIA STEPHANY	DESARROLLO DE UN MODELO DE PROCESOS BASADO EN NORMAS DE PEQUEÑAS ORGANIZACIONES PARA MEJORAR LA CONSTRUCCIÓN DE SOFTWARE EN UN ÁREA DE DESARROLLO DE GOBIERNO MUNICIPAL
11	CALDERON YNOÑAN PAMELA DEL CARMEN PRIETO NEIRA FRANCK ALBERSON	DESARROLLO DE UN MÉTODO BAJO EL ENFOQUE ÁGIL EN ENTORNOS DE EXPERIENCIA DE USUARIO UI/UX PARA ASEGURAR LA USABILIDAD WEB
12	FLORES TINEO HUGO GALVANI DOLORIER POMA RONY RAUL	EVALUACIÓN DE LA USABILIDAD EN ENTORNOS VIRTUALES DE APRENDIZAJE PARA USUARIOS DE LAS ZONAS RURALES DEL PERÚ UTILIZANDO LA NORMA ISO/IEC 25010
13	CHANCAFE CASTRO JULIO JOEL	DESARROLLO DE UN MODELO DE PROCESOS AD HOC PARA EL DESARROLLO DE SOFTWARE PARA UNA MUNICIPALIDAD BASADO EN ISO/IEC 29110
14	SALAZAR DAVILA GIANFRANCO STEVEN	COMPARACIÓN DE TÉCNICAS DE VALIDACIÓN DE REQUISITOS DE SOFTWARE PARA MEDIR LA INFLUENCIA EN EL ÉXITO DE LOS PROYECTOS DE DESARROLLO EN PEQUEÑAS EMPRESAS PERUANAS
15	RIOJA MESIA CHARLES SEGUNDO FERNANDEZ RIOJA JUAN NICANOR	IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE INCIDENCIAS BASADO EN ITIL PARA MEJORAR EL SERVICIO DE TI EN UNA MUNICIPALIDAD DISTRITAL DE LA REGIÓN LAMBAYEQUE
16	ALFARO PAJARES JUAN PEDRO	EVALUACIÓN DEL DESEMPEÑO DE PROCESOS DE NEGOCIO GESTIONADOS POR BPM EN UNA EMPRESA CONSTRUCTORA PERUANA
17	MONSALVE FERNANDEZ LENIN ESTALIN	IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE SERVICIOS DE TI BASADO EN ITIL PARA MEJORAR LA GESTIÓN DE LOS SERVICIOS DE LA DIRECCIÓN DE TECNOLOGÍA DE UN GOBIERNO REGIONAL PERUANO
18	PEREZ CAMPOS DE QUIROZ BETTY MAGALY	EVALUACIÓN DEL DESEMPEÑO DE PROCESOS DE NEGOCIO GESTIONADOS POR BPM EN UNA MICRO EMPRESA PERUANA DESARROLLADORA DE SOFTWARE
19	MONTJOY PITA BRUNO	DESARROLLO DE UN SISTEMA DE RECOMENDACIÓN AUTOMÁTICA PARA EL TRATAMIENTO DE LAS PLAGAS EN CULTIVOS DE ARROZ DE LAS VARIEDADES QUE SE PRODUCEN EN LA REGIÓN LAMBAYEQUE
20	CRUZ FLORES JOSE ANTONIO CHAVEZ ANGULO GERMAN NEPTALI	IMPLEMENTACIÓN DE ARQUITECTURA EMPRESARIAL BASADO EN METODOLOGÍA ÁGIL PARA ALINEAR LAS TECNOLOGÍAS DE INFORMACIÓN CON LOS OBJETIVOS DE NEGOCIO DE UN ESTABLECIMIENTO PERUANO DE SALUD BUCAL

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°0445-2021/FIAU-USS

Pimentel, 27 de mayo de 2021

N°	AUTOR (ES)	TEMA DE TESIS
21	PISFIL CORONADO JOSE LUIS FELIPE	IMPLEMENTACIÓN DE ARQUITECTURA EMPRESARIAL BASADA EN METODOLOGÍA ÁGIL PARA ALINEAR TI CON LOS PROCESOS DE NEGOCIO EN UNA EMPRESA CONSTRUCTORA PERUANA DE OBRAS CIVILES
22	ABAD HERRERA JOHNNY BENSO TEPE ESPINOZA LUIS RAMON	IMPLEMENTACIÓN DE ITIL V4 PARA MEJORAR LOS SERVICIOS DE TI EN EL CENTRO DE SISTEMAS DE INFORMACIÓN DE UNA UNIDAD DE GESTIÓN EDUCATIVA LOCAL PERUANO
23	URRUTIA VASQUEZ MIGUEL JULCA ROJAS ALEX ROGELIO	DESARROLLO DE UN MÉTODO DE IDENTIFICACIÓN AUTOMÁTICA DE ATAQUES SPOOFING DE ENVENENAMIENTO ARP EN LA SUPLANTACIÓN DE IDENTIDAD EN REDES LAN
24	SANCHEZ CELADA EELIN FERNANDEZ ROMAN ISMAEL	COMPARACIÓN DE ARQUITECTURAS DE IDS HÍBRIDO PARA LA IDENTIFICACIÓN DE ATAQUES DE DOS EN LOS SERVIDORES WEB DE UNA MUNICIPALIDAD PROVINCIAL PERUANA
25	PERALES CHAVEZ JEFFERSON ADRIAN	IMPLEMENTACIÓN DE UN MODELO DE ARQUITECTURA DE INDUSTRIA 4.0 PARA MEJORAR LA INTEROPERABILIDAD ENTRE SISTEMAS DE UNA EMPRESA PERUANA
26	MAGALLANES CARBAJAL KENSER	EVALUACIÓN DE LA EFICIENCIA DE LOS ALGORITMOS DE CRIPTOGRAFÍA PARA CUMPLIR CON LOS NIVELES DE SEGURIDAD DE DATOS DE UNA EMPRESA FINANCIERA PERUANA
27	RACCHUMI LECCA JESUS MANUEL	DESARROLLO DE UN MIDDLEWARE PARA MEJORAR LA COMUNICACIÓN ENTRE DOS INTERFACES DE LMS Y CRM EN EL PROCESO DE REGISTRO Y EMISIÓN DE CREDENCIALES DE USUARIOS
28	CASTRO QUISQUEN JAIME ELTON	COMPARACIÓN DE ALGORITMOS DE CIFRADO DE DATOS EN EL ASEGURAMIENTO DE VIDEO LLAMADA SOBRE REDES IP
29	PEREZ DIAZ NEILER WILTER CHINCHAY MALDONADO JORGE OBED	IMPLEMENTACIÓN DE TECNOLOGÍA SANDBOX PARA PROTEGER DE ATAQUES RANSOMWARE EN UNA RED INFORMÁTICA LOCAL DE UNA ENTIDAD FINANCIERA
30	MOSCOSO PAREDES ANIBAL	DISEÑO DE UN MODELO DE ARQUITECTURA DE SEGURIDAD DE BAJO COSTO PARA REFORZAR LA SEGURIDAD DE LA RED DEL HOGAR ANTE ATAQUES INFORMÁTICOS
31	MARTINEZ CUMPA JORGE JOSE	EVALUACIÓN DE FACTIBILIDAD DE USO DE TECNOLOGÍA WIRELESS 5GHZ PARA PROPORCIONAR SERVICIOS DE COMUNICACIÓN INALÁMBRICA EN LOS CENTROS POBLADOS RURALES DE LA REGIÓN LAMBAYEQUE
32	CAMPOS BARRERA SANDRO PAUL PASTOR OLIVA CESAR AUGUSTO	IMPLEMENTACIÓN DE UN MÉTODO DE CLASIFICACIÓN PARA DETECTAR LA DESERCIÓN DE ESTUDIANTES DE LA CARRERA DE INGENIERÍA DE INDUSTRIAS ALIMENTARIAS DE UNA UNIVERSIDAD NACIONAL PERUANA BASADO EN APRENDIZAJE DE MAQUINA
33	PICON VASQUEZ ANGEL GABRIEL CESPEDES SALAZAR JUAN CARLOS	DESARROLLO DE UN MÉTODO DE CLASIFICACIÓN AUTOMÁTICA BASADA EN TÉCNICAS ESTADÍSTICAS Y DE MACHINE LEARNING PARA CLASIFICAR A LOS POSTULANTES DE ACUERDO AL PERFIL DE TRABAJO DE UN CALL CENTER
34	MIÑANO SANCHEZ CARLOS JOHNY	COMPARACIÓN DE TÉCNICAS DE MINERÍA DE DATOS PARA DESCUBRIR INFORMACIÓN RELEVANTE DE VENTAS DE UNA MYPE COMERCIAL
35	MARTOS PAREDES JOEL HAROLD VILLAZON SOSA JAIR AUGUSTO	IMPLEMENTACIÓN DE UN MODELO DE PROCESOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA PYME PERUANA BASADO EN LA NORMA ISO/IEC 27005 Y LA METODOLOGÍA OCTAVE-S
36	QUISPE PUEMAPE LUIS ALONSO	IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO/IEC 27001:2014 EN UNA EMPRESA PERUANA DE TELECOMUNICACIONES
37	CHUCO AGUILAR GERSON RAUL	IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADA EN ISO/IEC 27001 PARA MEJORAR EL NIVEL DE SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN EN UNA EMPRESA CONSTRUCTORA DE OBRAS CIVILES
38	CAJUSOL ROJAS JOSE DEL CARMEN	IMPLEMENTACIÓN DE UNA PLATAFORMA WEB PARA LA PLANIFICACIÓN Y MONITOREO DE RUTAS DE RECOJO DE RESIDUOS SÓLIDOS DE UN MUNICIPIO DE LA REGIÓN LAMBAYEQUE
39	VALLEJOS RAMOS FERNANDO RAFAEL	DESARROLLO DE UN MÉTODO DE OPTIMIZACIÓN DE USO DE TELA EN EL PROCESO DE ELABORACIÓN DE PRENDAS TEXTILES DE MICROEMPRESAS PERUANAS
40	REQUEJO NAVARRO JERSONS EXPRANSHER	EVALUACIÓN DE ALGORITMOS CRIPTOGRÁFICOS PARA MEJORAR SEGURIDAD EN UNA RED PRIVADA VIRTUAL

Anexo 2. Carta de aceptación de la empresa Despensa Peruana SA

CARTA DE ACEPTACIÓN DE LA EMPRESA

Chiclayo. 18 de junio de 2024.

Mg. Ing. Víctor Tuesta Monteza

Director de Escuela de Ingeniería de Sistemas.

Universidad Señor de Sipán

Presente

REF: **Carta de la Facultad de Ingeniería, Arquitectura y Urbanismo de la Universidad Señor de Sipán de fecha 18 de junio de 2024.**

Tengo el agrado de dirigirme a Usted, con la finalidad de hacer de su conocimiento que el **Sr. MARTOS PAREDES JOEL HAROLD y el Sr. VILLAZÓN SOSA AUGUSTO JAIR,** alumnos de la Escuela de Ingeniería de Sistemas de la Institución Universitaria que Usted representa, han sido admitidos para realizar su investigación en el desarrollo de su Tesis denominada " Implementación de un Modelo de Procesos de la Seguridad de la Información para una Pyme Peruana Basada en la Norma ISO/IEC 27005 y la Metodología Octave-S" en nuestra empresa, teniendo como fecha 18 de junio del 2024.

Aprovecho la oportunidad para expresarle mi consideración y estima personal.

Atentamente,

Lizbeth Anghelly Linares Seclén
Jefe de Recursos Humanos

Anexo 3. Instrumentos de recolección de datos, con su respectiva validación de los instrumentos.

Ficha de Resumen

Criterios de implementación

FICHA DE RESUMEN N°____

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correctos, puesto que será verificada posteriormente.

FECHA: _____

Proceso de la empresa	Procesos del modelo	Costo Unitario
	P1 Identificación de la información de la organización.	
	P2 Creación de perfiles de amenaza	
	P3 Revisar la infraestructura tecnológica con relación a los activos críticos	
	P4 Definir y distinguir los riesgos	
	P5 Generación de un plan de control y mitigación de riesgos	

Conclusión:

_____

_____

_____

Ficha de recopilación de datos por cada proceso para el indicador de costo de implementación.

Costo De implementación

FICHA DE RESUMEN N° ___

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correctos, puesto que será verificada posteriormente.

FECHA: _____

Procesos del modelo	Costo Subtotal	Costo Total	Formula	Resultado
P1			$CI = \frac{\sum_i^n ct_i}{CE} \ x\ 100$	
P2				
P3				
P4				
P5				

Detalle:

_____

_____

_____

Ficha de recopilación de datos por cada proceso para el indicador de costo de implementación.

FICHA DE RESUMEN N°___

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correctos, puesto que será verificada posteriormente.

FECHA: _____

Proceso de la empresa	Procesos del modelo	Tiempo Unitario
	P1 Identificación de la información de la organización.	
	P2 Creación de perfiles de amenaza	
	P3 Revisar la infraestructura tecnológica con relación a los activos críticos	
	P4 Definir y distinguir los riesgos	
	P5 Generación de un plan de control y mitigación de riesgos	

Conclusión:

_____

_____

_____

Tiempo de implementación

FICHA DE RESUMEN N° ___

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correctos, puesto que será verificada posteriormente.

FECHA: _____

Procesos del modelo	Tiempo Subtotal	Tiempo Total	Formula	Resultado
P1			$CI = \frac{\sum_i^n ct_i}{CE}\ x\ 100$	
P2				
P3				
P4				
P5				

Detalle:

_____

_____

_____

_____

_____

Nivel de cumplimiento con estándares

FICHA DE RESUMEN N°____

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: _____

Marque con un aspa (x) cuántos criterios

PROCESOS	NIVEL					Resultado
	Incumplido completamente	Incumplido	Incumplido parcialmente	Cumplido parcialmente	Cumplido completamente	
	0	1	2	3	4	
P1						
P2						
P3						
P4						
Total de los resultados						

Total de los resultados	Total de procesos	Total de criterios de evaluación	Formula	Resultado (%)
			$NC = \left[\frac{\frac{\sum_i^n RCC}{TP}}{TCE}\right] * 100$	

		ESTANDAR 27005
CRITERIO	ITEM	Los cuatro pasos de la implantación
CRI1	1	Establece un plan de comunicación interno y externo
CRI2	2	Define el contexto organizacional
CRI3	3	Realiza tratamientos de riesgos
CRI4	4	Realiza control y planificación de mitigación de riesgos

Nivel de Riesgo de los activos de la seguridad de la información

FICHA DE RESUMEN N°___

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: _____

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
				$R = PA \times MD$	

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

Conclusión:

_____

_____

_____

Nivel de criticidad de los activos de la seguridad de la información

FICHA DE RESUMEN N°___

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: _____

PROCESO	ACTIVOS	ESTIMACION DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
						$NC = \frac{\sum_i^n EC_i}{CAA}$	

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

Conclusión:

_____

_____

_____

_____

Eficacia de la seguridad de la información

FICHA DE RESUMEN N°____

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: _____

Procesos de la empresa	Procesos del modelo	RESULTADOS ALCANZADOS (SI O NO)	TOTAL	RESULTADOS PROPUESTO	Fórmula	Resultado
	P1				$E = \frac{Ra}{Rp} * 100$	
	P2					
	P3					
	P4					
	P5					

Considerar los siguientes rangos de evaluación:

No Eficaz	0% – 39%
Medio Eficaz	40% – 79%
Eficaz	80% - 100%

Conclusión:

_____

_____

_____

_____

Cálculo del promedio de los resultados obtenidos en la eficacia de la seguridad de la

FICHA DE RESUMEN N°___

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: _____

Proceso de la empresa	% alcanzado en el proceso	Promedio

Considerar los siguientes rangos de evaluación:

No Eficaz	0% – 39%
Medio Eficaz	40% – 79%
Eficaz	80% - 100%

Conclusión:

_____

_____

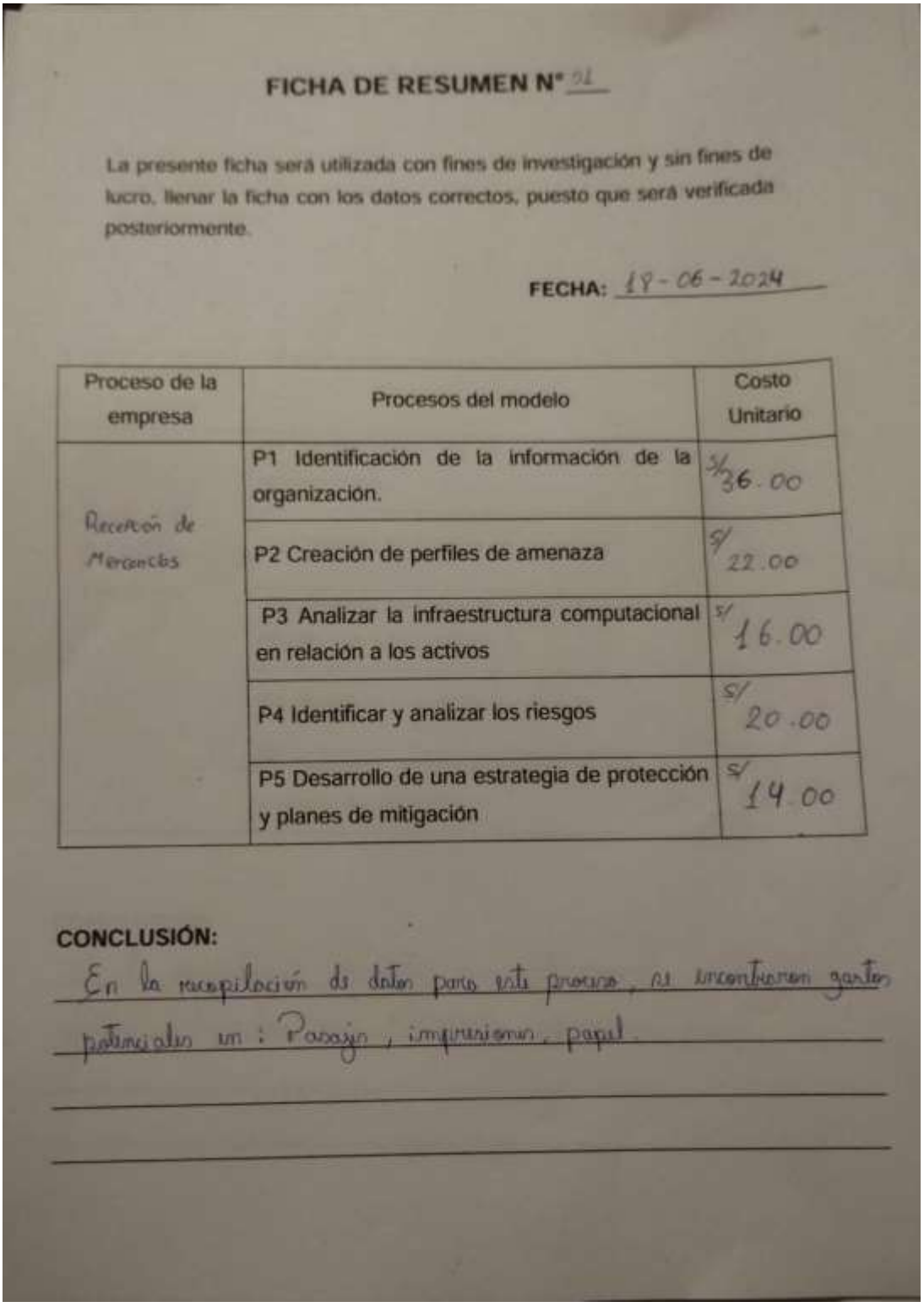
_____

_____

información.

INSTRUMENTOS DE RECOPILACIÓN DE DATOS LLENADOS

COSTO DE IMPLEMENTACIÓN



FICHA DE RESUMEN N° 01

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correctos, puesto que será verificada posteriormente.

FECHA: 19-06-2024

Proceso de la empresa	Procesos del modelo	Costo Unitario
Recepción de Mercancías	P1 Identificación de la información de la organización.	S/ 36.00
	P2 Creación de perfiles de amenaza	S/ 22.00
	P3 Analizar la infraestructura computacional en relación a los activos	S/ 16.00
	P4 Identificar y analizar los riesgos	S/ 20.00
	P5 Desarrollo de una estrategia de protección y planes de mitigación	S/ 14.00

CONCLUSIÓN:

En la recopilación de datos para este proceso, se encontraron gastos potenciales en: Pasajes, impresiones, papel.

FICHA DE RESUMEN N°02

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correctos, puesto que será verificada posteriormente.

FECHA: 18-06-2024

Proceso de la empresa	Procesos del modelo	Costo Unitario
Gestión de Inventarios	P1 Identificación de la información de la organización.	S/ 28.00
	P2 Creación de perfiles de amenaza	S/ 30.00
	P3 Analizar la infraestructura computacional en relación a los activos	S/ 26.00
	P4 Identificar y analizar los riesgos	S/ 18.00
	P5 Desarrollo de una estrategia de protección y planes de mitigación	S/ 26.00

CONCLUSIÓN:

En la recopilación de datos para este proceso, se encontraron gastos potenciales en: Pasajes, impresiones, papel.

FICHA DE RESUMEN N° 03

La presente ficha será utilizada con fines de investigación y sin fines de lucro. llenar la ficha con los datos correctos, puesto que será verificada posteriormente.

FECHA: 18-06-2024

Proceso de la empresa	Procesos del modelo	Costo Unitario
Monitoreo de Alarmas	P1 Identificación de la información de la organización.	S/ 26.00
	P2 Creación de perfiles de amenaza	S/ 24.00
	P3 Analizar la infraestructura computacional en relación a los activos	S/ 35.00
	P4 Identificar y analizar los riesgos	S/ 24.00
	P5 Desarrollo de una estrategia de protección y planes de mitigación	S/ 32.00

CONCLUSIÓN:

En la recopilación de datos para este proceso, se encontraron gastos patrimoniales en: Papaya, impresiones, papel.

FICHA DE RESUMEN N° 04

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correctos, puesto que será verificada posteriormente.

FECHA: 18-06-2024

Proceso de la empresa	Procesos del modelo	Costo Unitario
Tecnologia y Sistemas de Información	P1 Identificación de la información de la organización.	S/ 28.00
	P2 Creación de perfiles de amenaza	S/ 18.00
	P3 Analizar la infraestructura computacional en relación a los activos	S/ 22.00
	P4 Identificar y analizar los riesgos	S/ 16.00
	P5 Desarrollo de una estrategia de protección y planes de mitigación	S/ 24.00

CONCLUSIÓN:

En la recopilación de datos para esta proxima, se encontraron gastos potenciales en: Certificación, pasajes, impresiones, papel.

FICHA DE RESUMEN N° 05

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correctos, puesto que será verificada posteriormente.

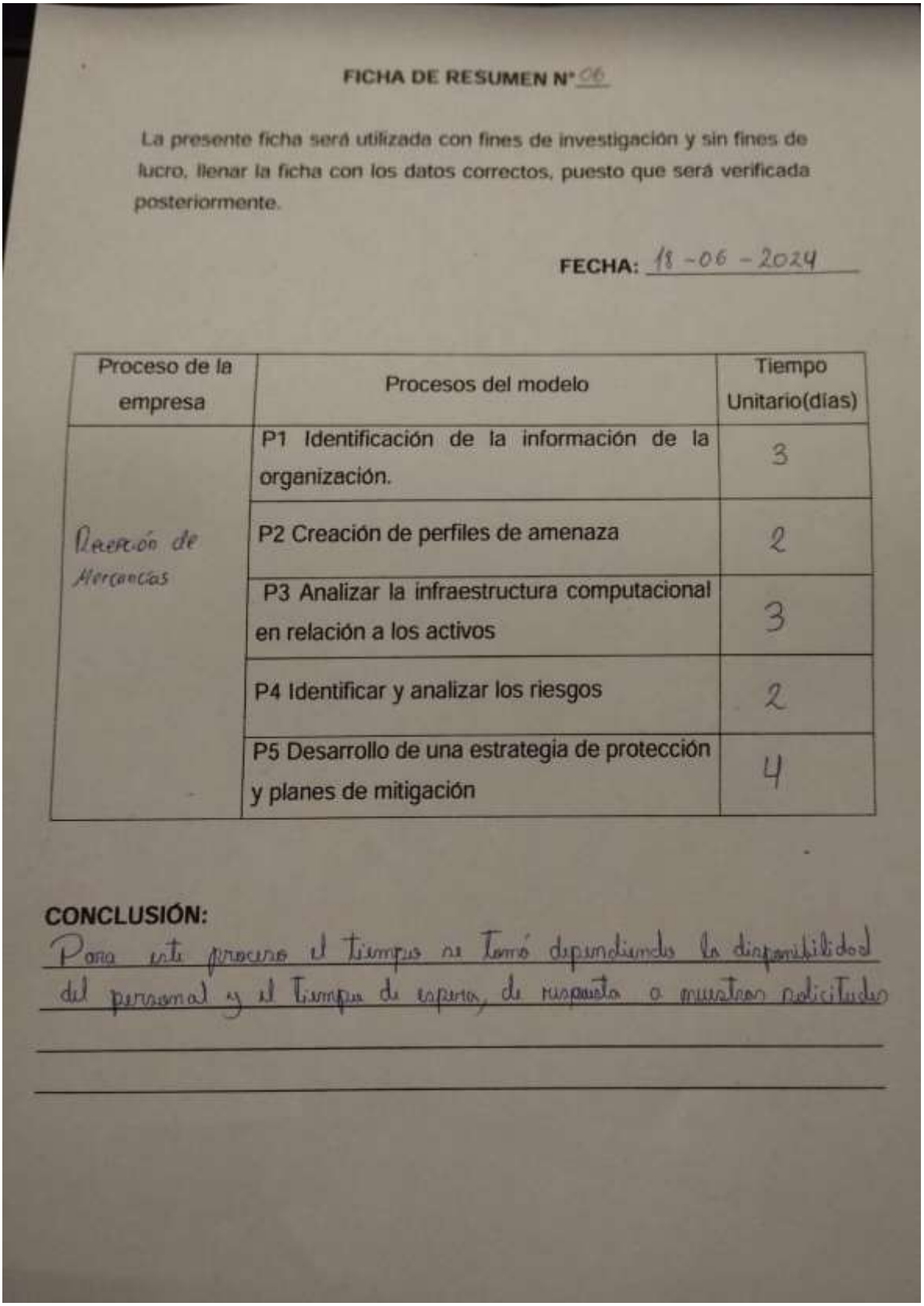
FECHA: 18-06-2024

Procesos del modelo	Costo Subtotal	Costo Total	Formula	Resultado
P1	S/ 118.00	S/ 485.00	$CI = \frac{\sum_i^n ct_i}{CE} \times 100$ $CE = S/ 500.00$	97 %
P2	S/ 94.00			
P3	S/ 99.00			
P4	S/ 78.00			
P5	S/ 96.00			

DETALLE:

El aporte generado en cada una de los procesos, ha sido completamente documentado, con respecto a todos los gastos requeridos por el equipo de trabajo

Tiempo de Implementación



FICHA DE RESUMEN N° 06

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correctos, puesto que será verificada posteriormente.

FECHA: 18-06-2024

Proceso de la empresa	Procesos del modelo	Tiempo Unitario(días)
Recepción de Mercancías	P1 Identificación de la información de la organización.	3
	P2 Creación de perfiles de amenaza	2
	P3 Analizar la infraestructura computacional en relación a los activos	3
	P4 Identificar y analizar los riesgos	2
	P5 Desarrollo de una estrategia de protección y planes de mitigación	4

CONCLUSIÓN:

Para este proceso el tiempo se tomó dependiendo la disponibilidad del personal y el tiempo de espera, de respuesta a nuestras peticiones

FICHA DE RESUMEN N° 07

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correctos, puesto que será verificada posteriormente.

FECHA: 18-06-2024

Proceso de la empresa	Procesos del modelo	Tiempo Unitario(días)
Gestión de Inventarios	P1 Identificación de la información de la organización.	3
	P2 Creación de perfiles de amenaza	2
	P3 Analizar la infraestructura computacional en relación a los activos	4
	P4 Identificar y analizar los riesgos	2
	P5 Desarrollo de una estrategia de protección y planes de mitigación	4

CONCLUSIÓN:

Para este proceso el tiempo se tomó dependiendo la disponibilidad del personal y el tiempo de espera de respuesta a nuestras solicitudes

FICHA DE RESUMEN N° 08

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correctos, puesto que será verificada posteriormente.

FECHA: 18-06-2024

Proceso de la empresa	Procesos del modelo	Tiempo Unitario(días)
Mantenimiento de Almacen	P1 Identificación de la información de la organización.	4
	P2 Creación de perfiles de amenaza	2
	P3 Analizar la infraestructura computacional en relación a los activos	3
	P4 Identificar y analizar los riesgos	3
	P5 Desarrollo de una estrategia de protección y planes de mitigación	4

CONCLUSIÓN:

Para este proceso el tiempo fue más prolongado, puesto que la demora de las respuestas a nuestras solicitudes ha sido mayor a comparación de los otros procesos.

FICHA DE RESUMEN N° 09

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correctos, puesto que será verificada posteriormente.

FECHA: 18-06-2024

Proceso de la empresa	Procesos del modelo	Tiempo Unitario(días)
Tecnología y Sistemas de Información	P1 Identificación de la información de la organización.	3
	P2 Creación de perfiles de amenaza	3
	P3 Analizar la infraestructura computacional en relación a los activos	2
	P4 Identificar y analizar los riesgos	2
	P5 Desarrollo de una estrategia de protección y planes de mitigación	4

CONCLUSIÓN:

Para este proceso el tiempo se tomó dependiendo la disponibilidad del personal y el tiempo de espera de respuesta a nuestras solicitudes.

FICHA DE RESUMEN N° 10

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correctos, puesto que será verificada posteriormente.

FECHA: 11 - 06 - 2024

Procesos del modelo	Tiempo Subtotal	Tiempo Total	Formula	Resultado
P1	13 días	59 días	$CI = \frac{\sum_i^n ct_i}{CE} \times 100$ TE = 60 días	98%
P2	9 días			
P3	12 días			
P4	9 días			
P5	16 días			

DETALLE:

El desarrollo de Todos los procesos ha otorgado un tiempo determinado el cual esta cerca al tiempo estimado, cumpliendo lo acordado con la empresa.

Nivel de cumplimiento con estándares

FICHA DE RESUMEN N° 11

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18-06-2024

Marque con un aspa (x) cuántos criterios

PROCESOS	NIVEL					Resultado
	Incumplido completamente	Incumplido	Incumplido parcialmente	Cumplido parcialmente	Cumplido completamente	
	0	1	2	3	4	
P1					X	4
P2				X		3
P3					X	4
P4				X		3
Total de los resultados						14

Total de los resultados	Total de procesos	Total de criterios de evaluación	Formula	Resultado (%)
14	4	4	$NC = \left[\frac{\frac{\sum_{i=1}^{n} RCC}{TP}}{TCE}\right] * 100$	92%

		ESTANDAR 27005
CRITERIO	ITEM	Los cuatro pasos de la implantación
CRI1	1	Establece un plan de comunicación interno y externo
CRI2	2	Define el contexto organizacional
CRI3	3	Realiza tratamientos de riesgos
CRI4	4	Realiza control y planificación de mitigación de riesgos

Nivel de riesgo

FICHA DE RESUMEN N° 12

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18-06-2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Recepción de Mercancías	Sistema de Gestión de Almacén (SGA)	4	4	$R = PA \times MD$	16
	Muelles de Carga y descarga	4	4		
	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

Este proceso es crítico, Puesto que, Cualquier interrupción puede Paralizar la cadena de Suministro, causando retrasos en la operación. La alta Probabilidad de amenaza se debe a la Frecuencia de operaciones y la alta magnitud de daño debido a la dependencia en la exactitud y la velocidad del proceso.

FICHA DE RESUMEN N° 13

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18-06-2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Prospección y adquisición de clientes	Base de datos de clientes	2	3	$R = PA \times MD$	5
	Sistema de gestión de relaciones con clientes (CRM)	2	3		
	Información de contacto de clientes	2	2		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

La base de datos contiene información valiosa sobre clientes potenciales. Su vulneración pueden resultar en pérdida de oportunidades de negocio.

FICHA DE RESUMEN N° 14

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18-06-2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Gestión de pedidos	Sistema de gestion de Pedidos (OMS)	3	3	$R = PA \times MD$	9
	Base de datos de Pedidos	3	3		
	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

En este proceso el nivel de riesgo ha sido 9 lo cual determina un riesgo medio para la empresa.

FICHA DE RESUMEN N° 15

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18-06-2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Atención al cliente	Sistema de Ticketing	2	2	$R = PA \times MD$	7
	Base de datos de clientes	3	3		
	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

En este proceso el nivel de riesgo ha sido 7 lo cual determina un riesgo bajo para la empresa.

FICHA DE RESUMEN N° 16

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18-06-2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Facturación y Cobranza	Sistema de Facturación	3	3	$R = PA \times MD$	11
	Base de datos de transacciones	3	4		
	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

En este proceso el nivel de riesgo ha sido 11 la cual determina un riesgo medio para la empresa.

FICHA DE RESUMEN N° 17

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18 – 06 – 2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Gestión de Inventarios	Sistema de gestión de inventario	4	4	$R = PA \times MD$	16
	Base de datos de inventario	4	4		
	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

Este proceso es fundamental para la operación de la empresa. Un fallo aquí puede llevar a la falta de productos disponibles para la venta, lo cual impacta directamente en los ingresos y la satisfacción del cliente.

FICHA DE RESUMEN N° 18

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18 - 06 - 2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Preparación de Pedidos	Sistema de gestión de pedidos	3	3	$R = PA \times MD$	8
	Equipos de picking	2	3		
	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

En este proceso el nivel de riesgo ha sido 8 lo cual determina un riesgo medio para la empresa.

FICHA DE RESUMEN N° 19

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18-06-2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Mantenimiento de almacen	Plan de mantenimiento	4	4	$R = PA \times MD$	14
	Equipos de mantenimiento	4	3		
	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

El mantenimiento adecuado del almacen asegura que todas las operaciones se realicen sin interrupciones. La alta probabilidad de amenaza y magnitud de daño se deben a la importancia de mantener la infraestructura en buen estado para evitar fallos operativos.

FICHA DE RESUMEN N° 20

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18 - 06 - 2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Planificación de rutas	Software de planificación de rutas	3	3	$R = PA \times MD$	9
	Base de datos de rutas y entregas	3	3		
	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

En este proceso el nivel de riesgo ha sido 9 lo cual determina un riesgo medio para la empresa

FICHA DE RESUMEN N° 21

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18 - 06 - 2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Transporte y entrega	Vehículos de entrega	3	3	$R = PA \times MD$	9
	Sistema de seguimiento de entregas	3	3		
	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

En este proceso el nivel de riesgo ha sido 9 lo cual determina un riesgo medio para la empresa.

FICHA DE RESUMEN N° 22

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18 - 06 - 2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Gestión de Flota	S.G de flota	3	3	$R = PA \times MD$	9
	Vehículos de empresa	3	3		
	-	-	-		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

En este proceso el nivel de riesgo ha sido 9 lo cual determina un riesgo medio para la empresa.

FICHA DE RESUMEN N°23

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18-06-2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Logistica Inversa	Sistema de devoluciones	3	3	$R = PA \times MD$	9
	Base de datos de devoluciones	3	3		
	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

En este proceso el nivel de riesgo ha sido 9 lo cual determina un riesgo medio para la empresa.

FICHA DE RESUMEN N° 24

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18-06-2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Tecnología y sistemas de Información	Servidores y centro de datos	4	4	$R = PA \times MD$	16
	Sistema de gestión empresarial ERP	4	4		
	Software de seguridad y Protección de datos	4	4		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

La infraestructura Tecnológica es la columna vertebral de todas las operaciones de la empresa. Un fallo en estos sistemas puede causar una interrupción significativa en todas las áreas de la empresa, justificando una alta probabilidad de amenaza y una alta magnitud de daño.

FICHA DE RESUMEN N° 25

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 18-06-2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Calidad y mejora continua	S.G de calidad	3	3	$R = PA \times MD$	7
	Documentación de procesos	2	2		
	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

En este proceso el nivel de riesgo ha sido 7 lo cual determina un riesgo bajo para la empresa.

FICHA DE RESUMEN N° 26

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 11-06-2024

PROCESO	ACTIVOS	Probabilidad de Amenaza (1: insignificante; 2: baja; 3: mediana; 4: alta)	Magnitud de daño (1: insignificante; 2: baja; 3: mediana; 4: alta)	Formula	Resultado
Gestión de Recursos humanos	S.G. Recursos Humanos	3	3	$R = PA \times MD$	9
	Base de datos de empleados	3	3		
	-	-	-		

Considerar los siguientes rangos de evaluación:

Alto Riesgo	12 – 16
Medio Riesgo	8 – 11
Bajo Riesgo	1 – 7

CONCLUSIÓN:

En este proceso el nivel de riesgo ha sido 9 lo cual determina un riesgo medio para la empresa.

Criticidad de activos de la información

FICHA DE RESUMEN N° 29

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19-06-2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
Prospección y Adquisición de Clientes	B.D clientes	2	3	3	8	$NC = \frac{\sum_i^n EC_i}{CAA}$	8.5
	CRM	3	3	3	9		
	—	—	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Este proceso tiene una estimación de criticidad de 8.5 por lo que se considera que es una estimación de criticidad media.

FICHA DE RESUMEN N° 08

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19-06-2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
Gestión de Pedidos	S.G. de Pedidos	1	2	3	6	$NC = \frac{\sum_i^n EC_i}{CAA}$	6.5
	B.D. Pedidos	2	2	3	7		
	—	—	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Este proceso tiene una estimación de criticidad de 6.5 por lo que se considera que es una estimación de criticidad baja.

FICHA DE RESUMEN N° 29

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19-06-2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
Atención al cliente	Sistema de Ticketing	1	2	3	6	$NC = \frac{\sum_1^n EC_i}{CAA}$	6.5
	B.D. clientes	2	2	3	7		
	—	—	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Este proceso tiene una estimación de criticidad de 6.5 por lo que se considera que es una estimación de criticidad baja.

FICHA DE RESUMEN N° 30

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19-06-2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
Facturación y Cobranza	Sistema de Facturación	2	2	3	7	$NC = \frac{\sum_i^n EC_i}{CAA}$	7.5
	B.D. Transacciones	1	3	4	8		
	—	—	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Este proceso tiene una estimación de criticidad de 7.5 por lo que se considera que es una estimación de criticidad media, ya que redondeando 7.5 es 8.

FICHA DE RESUMEN N° 31

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19-06-2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
Recepción de Mercancías	S.G. Almacen	6	5	5	16	$NC = \frac{\sum_{i}^{n} EC_i}{CAA}$	15
	Muelles de Carga y descarga	5	5	4	14		
	—	—	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Este proceso es considerado uno de los más críticos Puestos que sus activos están Comprometidos en toda la empresa, ya que afecta la calidad del inventario, la eficiencia operativa, la satisfacción del cliente y la competitividad en el mercado.

FICHA DE RESUMEN N° 32

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19-06-2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD			Total	Formula	Resultado
		Aspectos estratégicos	Costos directos	Costos indirectos			
Gestión de Inventarios	S.G. Inventario	6	5	5	16	$NC = \frac{\sum_1^n EC_i}{CAA}$	15
	B.D. Inventario	5	5	4	14		
	—	—	—	—			

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Este Proceso tiene una estimación alta porque afectaría la calidad de inventario, las finanzas, la satisfacción del cliente, los empleados y la toma de decisiones, si este se ve afectado.

FICHA DE RESUMEN N° 33

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 14-06-2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
Preparación de Pedidos	S.G. Pedidos	3	4	4	11	$NC = \frac{\sum_i^n EC_i}{CAA}$	9.5
	Equipos de Picking	2	3	3	8		
	—	—	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Este proceso tiene una estimación de criticidad de 9.5 por lo que se considera, que es una estimación de criticidad media.

FICHA DE RESUMEN N° 34

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19-06-2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
Mantenimiento de Almacen	Plan de mantenimiento	6	5	5	16	$NC = \frac{\sum_i^n EC_i}{CAA}$	16
	Equipos de mantenimiento	6	5	5	16		
	—	—	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Este proceso es uno de los más criticos, ya que si este se Volnera, afectaría la eficacia operativa, la calidad de inventario, las finanzas, etc.

FICHA DE RESUMEN N° 35

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19-06-2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
Planificación de rutas	Software de planificación de rutas	2	3	3	8	$NC = \frac{\sum_i^n EC_i}{CAA}$	8.5
	B.D. rutas y entregas	3	3	3	9		
	—	—	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Este proceso tiene una estimación de criticidad de 8.5 por lo que se considera, que es una estimación de criticidad media.

FICHA DE RESUMEN N° 36

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19 - 06 - 2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
Transporte y Entrega	Vehículos de entrega	1	1	3	5	$NC = \frac{\sum EC_i}{CAA}$	4.5
	Sistema de Seguimiento de entregas	2	1	1	4		
	—	—	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Este proceso tiene una estimación de criticidad de 4.5 por lo que se considera, que es una estimación de criticidad baja.

FICHA DE RESUMEN N° 33

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 14-06-2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
Gestión de flota	S.G. flota	2	4	5	11	$NC = \frac{\sum_i^n EC_i}{CAA}$	10
	Vehículos de empresa	1	5	3	9		
	—	—	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Esta posee tiene una estimación de criticidad de 10 por lo que se considera, que es una estimación de criticidad media.

FICHA DE RESUMEN N° 38

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 14-06-2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
Logística Inversa	Sistema de devoluciones	4	2	1	7	$NC = \frac{\sum_i^n EC_i}{CAA}$	6.5
	BD devoluciones	2	3	1	6		
	—	—	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Este proceso tiene una estimación de criticidad de 6.5 por lo que se considera, que es una estimación de criticidad baja.

FICHA DE RESUMEN N° 39

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19-06-2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
Tecnología y Sistemas de Información	Servidores y centro de datos	6	5	5	16	$NC = \frac{\sum_{i}^{n} EC_i}{CAA}$	16
	ERP	6	5	5	16		
	Software de seguridad y protección de datos	6	5	5	16		

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Este es el proceso más importante dentro de la infraestructura técnológica de la empresa y si esta se vulnera, toda la información de la empresa sería expuesta.

FICHA DE RESUMEN N° 40

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19-06-2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
Calidad y mejora continua	S.G calidad	5	2	1	8	$NC = \frac{\sum_i^n EC_i}{CAA}$	7
	Documentación de procesos	3	2	1	6		
	—	—	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Este proceso tiene una estimación de criticidad de 7 por lo que se considera, que es una estimación de criticidad bajo.

FICHA DE RESUMEN N°41

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19-06-2024

PROCESO	ACTIVOS	ESTIMACIÓN DE CRITICIDAD					
		Aspectos estratégicos	Costos directos	Costos indirectos	Total	Formula	Resultado
Gestión de Recursos humanos	S.G. Recursos humanos	6	2	1	9	$NC = \frac{\sum_i^n EC_i}{CAA}$	7.5
	B.D. Postulantes	2	3	1	6		
	—	—	—	—	—		

Considerar los siguientes rangos de evaluación:

Alto	12 – 16
Medio	8 – 11
Bajo	1 – 7

CONCLUSIÓN:

Este proceso tiene una estimación de criticidad de 7.5 por lo que se considera, que es una estimación de criticidad medio, ya que si redondiamos 7.5 sería 8.

Eficacia de la seguridad de la Información

FICHA DE RESUMEN N° 42

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19 - 06 - 2024

Procesos de la empresa	Procesos del modelo	RESULTADOS ALCANZADOS (SI O NO)	TOTAL	RESULTADOS PROPUESTO	Fórmula	Resultado
Recepción de Mercancías	P1	Si	4	5	$E = \frac{Ra}{Rp} * 100$	80%
	P2	Si				
	P3	Si				
	P4	Si				
	P5	NO				

Considerar los siguientes rangos de evaluación:

No Eficaz	0% – 39%
Medio Eficaz	40% – 79%
Eficaz	80% - 100%

CONCLUSIÓN:

Este proceso tiene un 80% de resultados alcanzados, puesto que se cumple la mayoría de procesos del modelo.

FICHA DE RESUMEN N° 43

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19-06-2024

Procesos de la empresa	Procesos del modelo	RESULTADOS ALCANZADOS (SI O NO)	TOTAL	RESULTADOS PROPUESTO	Fórmula	Resultado
Gestión de Inventarios	P1	Si	4	5	$E = \frac{Ra}{Rp} * 100$	80%
	P2	Si				
	P3	Si				
	P4	Si				
	P5	NO				

Considerar los siguientes rangos de evaluación:

No Eficaz	0% – 39%
Medio Eficaz	40% – 79%
Eficaz	80% - 100%

CONCLUSIÓN:

Este proceso tiene un 80% de resultados alcanzados, puesto que se cumplió la mayoría de procesos del modelo.

FICHA DE RESUMEN N°44

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19 - 06 - 2024

Procesos de la empresa	Procesos del modelo	RESULTADOS ALCANZADOS (SI O NO)	TOTAL	RESULTADOS PROPUESTO	Fórmula	Resultado
Mantenimiento de Almacén	P1	Si	4	5	$E = \frac{Ra}{Rp} * 100$	80%
	P2	Si				
	P3	Si				
	P4	Si				
	P5	No				

Considerar los siguientes rangos de evaluación:

No Eficaz	0% – 39%
Medio Eficaz	40% – 79%
Eficaz	80% - 100%

CONCLUSIÓN:

Este proceso tiene un 80% de resultados alcanzados, puesto que se cumplio la mayoria de procesos del modelo

FICHA DE RESUMEN N° 45

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 14-06-2024

Procesos de la empresa	Procesos del modelo	RESULTADOS ALCANZADOS (SI O NO)	TOTAL	RESULTADOS PROPUESTO	Fórmula	Resultado
Tecnología y Sistemas de Información	P1	Si	4	5	$E = \frac{Ra}{Rp} * 100$	80%
	P2	Si				
	P3	Si				
	P4	Si				
	P5	NO				

Considerar los siguientes rangos de evaluación:

No Eficaz	0% – 39%
Medio Eficaz	40% – 79%
Eficaz	80% - 100%

CONCLUSIÓN:

Este proceso tiene un 80% de resultados alcanzados, puesto que se cumplio la mayoria de procesos del modelo.

FICHA DE RESUMEN N° 46

La presente ficha será utilizada con fines de investigación y sin fines de lucro, llenar la ficha con los datos correcto, puesto que será verificada posteriormente.

FECHA: 19-06-2024

Proceso de la empresa	% alcanzado en el proceso	Promedio
Proceso de Recepción de Mercancías	80%	80%
Proceso de Gestión de Inventarios	80%	
Proceso de Mantenimiento de Almacén	80%	
Proceso de tecnología y sistemas de información	80%	

Considerar los siguientes rangos de evaluación:

No Eficaz	0% – 39%
Medio Eficaz	40% – 79%
Eficaz	80% - 100%

CONCLUSIÓN:

En todos los procesos se obtuvo un 80% de resultados alcanzados, ya que en el último proceso del modelo quedaron pendientes la implementación del plan de seguridad y control de riesgos de los procesos más críticos de la empresa Despensa Peruana S.A.

Anexo 5. Otros anexos

5.1. Tablas del modelo de implementación para la seguridad de la información.

5.1.1.

Tabla 53.

El equipo de análisis para el modelo de proceso

MIEMBROS	FUNCIÓN EN EVALUACIÓN

Fuente: Elaboración Propia.

5.1.2.

Tabla 54.

La selección de procesos

N°	Procesos

Fuente: Elaboración propia

5.1.3.

Tabla 55.

Evaluación para la relevancia de procesos

N°	Procesos	C1	C2	C3	C4	Total

Fuente: Elaboración propia

5.1.4.

Tabla 56.

Los procesos más relevantes de la organización

PROCESOS MÁS RELEVANTES		
PROCESOS	**NOMBRE**	**NIVEL DE CRITICIDAD**

Fuente: Elaboración Propia

5.1.5.

Tabla 57.

Formato para describir el impacto hacia los activos por cada proceso

PROCESO:	
DESCRIPCIÓN DEL IMPACTO	Rango (alto, medio, bajo)

Fuente: Elaboración propia

5.1.6.

Tabla 58.

Formato para describir los activos dentro de los procesos

PROCESO:	
ACTIVOS	DESCRIPCIÓN

Fuente: Elaboración propia

5.1.7.

Tabla 59.

Formato para seleccionar las prácticas de seguridad dentro de la organización y asignarle un estado

PROCESO:		
Práctica de seguridad	Descripción	Estado

Fuente: Elaboración propia

5.1.8.

Tabla 60.

Formato de selección de activos críticos

NOMBRE DEL PROCESO				
ID ACTIVO CRÍTICO	NOMBRE ACTIVO CRÍTICO	RESPONSABLE	ACTIVOS RELACIONADOS	MOTIVO DE ACTIVO CRÍTICO

Fuente: Elaboración propia

5.1.9.

Tabla 61.

Formato para identificar los requerimientos más importantes para cada activo crítico

PROCESO:		
ID ACTIVO CRÍTICO	REQUERIMIENTO DE SEGURIDAD	DESCRIPCIÓN

Fuente: Elaboración propia

5.1.10.

Tabla 62.

Formato de identificación de las categorías por cada activo crítico

PROCESO:		
ID ACTIVO CRÍTICO	CATEGORÍA DE AMENAZA	DESCRIPCIÓN

Fuente: Elaboración propia

5.1.11.

Tabla 63.

Formato de identificación de componentes

COMPONENTES DEL SISTEMA		
ID COMPONENTE	NOMBRE DEL COMPONENTE	USUARIO ENCARGADO DEL COMPONENTE

Fuente: Elaboración propia

5.1.12.

Tabla 64.

Formato de la estimación del grado de seguridad

PROCESO:			
ID ACTIVO CRÍTICO	COMPONENTE	RESPONSABLE	ESTIMACIÓN

Fuente: Elaboración propia

5.1.13.

Tabla 65.

Formato para evaluar las probabilidades de amenaza

PROCESO:		
ID ACTIVO CRÍTICO	AMENAZA	DESCRIPCIÓN DEL IMPACTO

Fuente: Elaboración propia

5.1.14.

Tabla 66.

Formato para evaluar la probabilidad de amenaza del activo crítico

PROCESO:			
ID ACTIVO CRÍTICO	AMENAZA	CRITERIO DE EVALUACIÓN	PROBABILIDAD DE AMENAZA (ALTO, MEDIO, BAJO)

Fuente: Elaboración propia

5.2. Gráfico de estimación de criticidad para los activos críticos de la empresa.

Aspectos estratégicos para definir la criticidad	Costos directos	Costos Indirectos
• Muertes o lesiones asociadas a la destrucción del activo • Costos de reposición • Pérdidas de facturación • Disponibilidad de respaldos/redundancia • Acuerdos de soporte técnico • Información crítica • Imagen de la empresa	• Pérdidas financieras por costo de reposición de activos • Primas de seguro más altas debido a incremento de la siniestralidad • Aumento en franquicias de seguro • Respuesta de medios de comunicación • Costos no cubiertos por seguro	• Cobertura mediatica negativa • Opinión pública • Costos Adicionales marketing y control de daños(RRPP) • Demandas de accionistas • Problemas de clima organizacional, rotación de personal

5.3. Cuadro de procesos y sus activos clasificados

PROCESO	ACTIVOS
Prospección y Adquisición de Clientes	Base de Datos de Clientes
	CRM (Customer Relationship Management)
Gestión de Pedidos	Sistema de Gestión de Pedidos (OMS)
	Base de Datos de Pedidos
Atención al Cliente	Sistema de Ticketing
	Base de Datos de Clientes
Facturación y Cobranza	Sistema de Facturación
	Base de Datos de Transacciones
Recepción de Mercancías	Sistemas de Gestión de Almacén (WMS)
	Muelles de Carga y Descarga
Gestión de Inventarios	Sistemas de Gestión de Inventario (IMS)
	Bases de Datos de Inventario
Preparación de Pedidos	Sistemas de Gestión de Pedidos (OMS)
	Equipos de Picking
Mantenimiento de Almacén	Plan de Mantenimiento
	Equipos de Mantenimiento
Planificación de Rutas	Software de Planificación de Rutas
	Base de Datos de Rutas y Entregas
Transporte y Entrega	Vehículos de Entrega
	Sistema de Seguimiento de Entregas
Gestión de Flota	Sistema de Gestión de Flota
	Vehículos de Empresa
Logística Inversa	Sistema de Devoluciones

	Base de Datos de Devoluciones
Tecnología y Sistemas de Información	Servidores y Centros de Datos
	Sistemas de Gestión Empresarial (ERP)
	Software de Seguridad y Protección de Datos
Calidad y Mejora Continua	Sistema de Gestión de Calidad
	Documentación de Procesos
Gestión de Recursos Humanos	Sistema de Gestión de Recursos Humanos (HRMS)
	Base de Datos de Empleados

5.4. Cuadro de ponderación del nivel de riesgo de los activos

PROCESO	ACTIVOS	PROBABILIDAD DE AMENAZA (1: insignificante,2: baja,3:mediana,4:alta)	MAGNITUD DE DAÑO (1: insignificante,2: baja,3: mediana,4: alta)
Prospección y Adquisición de Clientes	Base de Datos de Clientes	2	3
	CRM (Customer Relationship Management)	2	3
	Información de contacto de clientes	2	2
Gestión de Pedidos	Sistema de Gestión de Pedidos (OMS)	3	3
	Base de Datos de Pedidos	3	3
Atención al Cliente	Sistema de Ticketing	2	2
	Base de Datos de Clientes	3	3
Facturación y Cobranza	Sistema de Facturación	3	3
	Base de Datos de Transacciones	3	4
Recepción de Mercancías	Sistemas de Gestión de Almacén (WMS)	4	4
	Muelles de Carga y Descarga	4	4
Gestión de Inventarios	Sistemas de Gestión de Inventario (IMS)	4	4
	Bases de Datos de Inventario	4	4
Preparación de Pedidos	Sistemas de Gestión de Pedidos (OMS)	3	3
	Equipos de Picking	2	3
Mantenimiento de Almacén	Plan de Mantenimiento	4	4
	Equipos de Mantenimiento	4	3
Planificación de Rutas	Software de Planificación de Rutas	3	3
	Base de Datos de Rutas y Entregas	3	3
Transporte y Entrega	Vehículos de Entrega	3	3
	Sistema de Seguimiento de Entregas	3	3
Gestión de Flota	Sistema de Gestión de Flota	3	3
	Vehículos de Empresa	3	3
	Sistema de Devoluciones	3	3

Logística Inversa	Base de Datos de Devoluciones	3	3	
Tecnología y Sistemas de Información	Servidores y Centros de Datos	4	4	
	Sistemas de Gestión Empresarial (ERP)	4	4	
	Software de Seguridad y Protección de Datos	4	4	
Calidad y Mejora Continua	Sistema de Gestión de Calidad	3	3	
	Documentación de Procesos	2	2	
Gestión de Recursos Humanos	Sistema de Gestión de Recursos Humanos (HRMS)	3	3	
	Base de Datos de Empleados	3	3	

5.5. Cuadro de la estimación de criticidad de los procesos de la empresa Despensa Peruana S.A.

PROCESO	ACTIVOS	ESTIMACIÓN CRITIC				
		Aspectos estratégicos para definir la criticidad	Costos directos	Costos indirectos	Probabilidad de amenaza	PROM
Prospección y Adquisición de Clientes	Base de Datos de Clientes	2	3	3	8	8.5
	CRM (Customer Relationship Management)	3	3	3	9	
Gestión de Pedidos	Sistema de Gestión de Pedidos (OMS)	1	2	3	6	6.5
	Base de Datos de Pedidos	2	2	3	7	
Atención al Cliente	Sistema de Ticketing	1	2	3	6	6.5
	Base de Datos de Clientes	2	2	3	7	
Facturación y Cobranza	Sistema de Facturación	2	2	3	7	7.5
	Base de Datos de Transacciones	1	3	4	8	
Recepción de Mercancías	Sistemas de Gestión de Almacén (WMS)	6	5	5	16	15
	Muelles de Carga y Descarga	5	5	4	14	
Gestión de Inventarios	Sistemas de Gestión de Inventario (IMS)	6	5	5	16	15
	Bases de Datos de Inventario	5	5	4	14	
Preparación de Pedidos	Sistemas de Gestión de Pedidos (OMS)	3	4	4	11	9.5

	Equipos de Picking	2	3	3	8	
Mantenimiento de Almacén	Plan de Mantenimiento	6	5	5	16	16
	Equipos de Mantenimiento	6	5	5	16	
Planificación de Rutas	Software de Planificación de Rutas	2	3	3	8	8.5
	Base de Datos de Rutas y Entregas	3	3	3	9	
Transporte y Entrega	Vehículos de Entrega	1	1	3	5	4.5
	Sistema de Seguimiento de Entregas	2	1	1	4	
Gestión de Flota	Sistema de Gestión de Flota	2	4	5	11	10
	Vehículos de Empresa	1	5	3	9	
Logística Inversa	Sistema de Devoluciones	4	2	1	7	6.5
	Base de Datos de Devoluciones	2	3	1	6	
Tecnología y Sistemas de Información	Servidores y Centros de Datos	6	5	5	16	16
	Sistemas de Gestión Empresarial (ERP)	6	5	5	16	
	Software de Seguridad y Protección de Datos	6	5	5	16	
Calidad y Mejora Continua	Sistema de Gestión de Calidad	5	2	1	8	7
	Documentación de Procesos	3	2	1	6	
Gestión de Recursos Humanos	Sistema de Gestión de Recursos Humanos (HRMS)	6	2	1	9	7.5

Base de Datos de Empleados	2	3	1	6	

5.6. Formato para la ficha de validación de expertos (sin observaciones)

VALIDEZ DE INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN

IMPLEMENTACIÓN DE UN MODELO DE PROCESOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA PYME PERUANA BASADA EN LA NORMA ISO/IEC 27005 Y LA METODOLOGÍA OCTAVE-S

LAMBAYEQUE 2021

Autores: Martos Paredes Joel Harold
Villazón Sosa Jair Augusto

Es de gran relevancia, realizar la evaluación de los instrumentos de recolección de información con la finalidad de confirmar que estos sean válidos y que los resultados obtenidos a partir de éstos sean utilizados eficientemente; brindando aportes tanto al área investigativa de la carrera profesional de Ingeniería de Sistemas como a sus aplicaciones. Agradecemos su valiosa colaboración.

Nº	DIMENSIONES/ITEMS	Esencial	Útil	No necesaria	Observaciones
Variable: La seguridad de la información en una PYME					
Indicador Nivel de riesgo de los activos de la seguridad de la información.					
1	¿Considera usted que se debería desarrollar un modelo de seguridad para que sus informaciones no estén en riesgo?				

2	¿Recomendaría usted a PYMES para gestionar la seguridad de sus informaciones?				
Indicador: Nivel de Criticidad de los activos de la seguridad de la información.					
3	¿Recomendaría usted a PYMES, contratar a un personal especializado y que se dedique exclusivamente a la seguridad de información?				
Indicador: Eficacia de la seguridad de la información.					
4	¿Recomendaría usted a PYMES, implementar mecanismos formales para verificar si se está cumpliendo todos los procesos que el cliente solicita?				
5	¿Antes de solicitar los servicios de PYMES, usted revisaría todo su perfil empresarial?				
6	¿Contrataría usted los servicios de PYMES, para una mejor seguridad de información en sus equipos?				
7	¿Considera usted que si se implementa la norma ISO 27005 en su PYME la seguridad de su información mejoraría?				

8	¿Considera usted que la norma ISO 27005 ayudaría a controlar la pérdida de información en las empresas?				
9	¿Considera usted que desarrollando un modelo de procesos de la seguridad de la información podrá mejorar los riesgos para las empresas?				

En su opinión, el instrumento resulta:

( ) Aplicable ( ) Aplicable con correcciones ( ) No Aplicable

APELLIDOS Y NOMBRE	
GRADO ACADÉMICO	INGENIERO DE SISTEMAS

SELLO Y FIRME DEL EXPERTO
DNI:

VALIDEZ DE INSTRUMENTO DE RECOLECCIÓN DE INFORMACIÓN

IMPLEMENTACIÓN DE UN MODELO DE PROCESOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA PYME PERUANA BASADA EN LA NORMA ISO/IEC 27005 Y LA METODOLOGÍA OCTAVE-S

LAMBAYEQUE 2021

Autores: Martos Paredes Joel Harold
Villazón Sosa Jair Augusto

Es de gran relevancia, realizar la evaluación de los instrumentos de recolección de información con la finalidad de confirmar que estos sean válidos y que los resultados obtenidos a partir de éstos sean utilizados eficientemente; brindando

aportes tanto al área investigativa de la carrera profesional de Ingeniería de Sistemas como a sus aplicaciones. Agradecemos su valiosa colaboración.

Nº	DIMENSIONES/ITEMS	Esencial	Útil	No necesaria	Observaciones
Variable: Modelo de procesos de seguridad de la información basado en la norma ISO/IEC 27005 y la metodología OCTAVE-S.					
Indicador: Costo de Implementación.					
1	¿Considera usted que el gasto llevado a cabo favorece a las PYMES?				
2	¿Estima usted que el precio de implementación está bastante sobrevalorado del presupuesto?				
Indicador: Tiempo de Implementación.					
3	¿Considera usted que si se implementa un modelo basado en la norma ISO 27005 y la metodología OCTAVE- S para PYMES, este reducirá los riesgos de seguridad de dicha información?				
Indicador: Nivel de cumplimiento con estándares					
4	¿Considera usted que al implementar la norma ISO 27005, esta permitirá identificar los riesgos de seguridad de la información de su empresa?				

5	¿Considera usted que, si se usa diferentes metodologías, estás ayudarían a disminuir los riesgos de seguridad de la información de su PYME y la integridad de la misma?				
6	¿En qué intervalo de tiempo se encuentra el procesamiento de actividades relacionadas con la seguridad de la información de su empresa?				
7	¿Considera usted que con el uso de nuestro modelo de seguridad basado en la norma ISO 27005 y la metodología OCTAVE-S generará satisfacción a la empresa respecto a la reducción de riesgos a la que está expuesta su información?				
8	¿Considera usted que la norma ISO 27005 ayudaría a controlar la pérdida de información en las empresas?				
9	¿Considera usted que desarrollando un modelo de procesos de la seguridad de la información podrá mejorar los riesgos para las empresas?				

En su opinión, el instrumento resulta:

() Aplicable ( ) Aplicable con correcciones ( ) No Aplicable

APELLIDOS Y NOMBRE	
GRADO ACADÉMICO	INGENIERO DE SISTEMAS

SELLO Y FIRME DEL EXPERTO

DNI:

5.4. Formato para la ficha de validación de expertos (con observaciones)

Ficha de Validación de Instrumento

Nombre Instrumento a validar: Cuestionario

Título: Implementación de un Modelo de Procesos de Seguridad de la Información para una Pyme Peruana basada en la norma ISO/IEC 27005 Y la Metodología OCTAVE-S

Indicadores	**Criterios**	**Calificación**			
		Deficiente	**Regular**	**Bueno**	**Muy bueno**
		De 0 a 5	**De 6 a 10**	**De 11 a 15**	**De 16 a 20**
Claridad	Los enunciados se entienden fácilmente				
Pertinencia	La pregunta está relacionada con la dimensión, variable, etc.				
Relevancia	La pregunta planteada permite solucionar alguna parte del problema planteado				

Valoración (0-20): _____

En su opinión, el instrumento resulta:

( ) Aplicable ( ) Aplicable con correcciones ( ) No Aplicable

APELLIDOS Y NOMBRE	
GRADO ACADÉMICO	INGENIERO DE SISTEMAS

_____

FIRMA DE EXPERTO
DNI:

Ficha de Validación de Metodología

Título: Implementación de un Modelo de Procesos de Seguridad de la Información para una Pyme Peruana basada en la norma ISO/IEC 27005 Y la Metodología OCTAVE-S

Indicaciones: Señor especialista se le pide la pronta colaboración, que luego de una rigurosa evaluación de los instrumentos del cuestionario, marque con un aspa (X) en el casillero que crea conveniente de acuerdo a su criterio y experiencia profesional.

	DIMENSIONES/ITEMS	Esencial	Útil	No Necesaria	Observaciones
1	¿Considera usted que el gasto llevado a cabo favorece a las PYMES?				
2	¿Estima usted que el precio de implementación está bastante sobrevalorado del presupuesto?				
3	¿Considera usted que si se implementa un modelo basado en la norma ISO 27005 y la metodología OCTAVE- S para PYMES, este reducirá los riesgos de seguridad de dicha información?				
4	¿Considera usted que al implementar la norma ISO 27005, esta permitirá identificar los riesgos de seguridad de la información de su empresa?				
5	¿Considera usted que, si se usa diferentes metodologías, estás ayudarían a disminuir los riesgos de seguridad de la información de su PYME y la integridad de la misma?				

6	¿En qué intervalo de tiempo se encuentra el procesamiento de actividades relacionadas con la seguridad de la información de su empresa?				
7	¿Considera usted que con el uso de nuestro modelo de seguridad basado en la norma ISO 27005 y la metodología OCTAVE-S generará satisfacción a la empresa respecto a la reducción de riesgos a la que está expuesta su información?				
8	La norma ISO 27005 establece que primero se debe analizar los riesgos con el fin de evitar que la información esté en peligro ¿Usted considera que esta etapa es importante?				
9	¿Conoce usted acerca de la implementación de procesos para la seguridad de la información?				
	¿Considera usted que se debería desarrollar un modelo de seguridad para que sus informaciones no estén en riesgo?				
11	¿Recomendaría usted a PYMES para gestionar la seguridad de sus informaciones?				
12	¿Recomendaría usted a PYMES, contratar a un personal especializado y que se dedique exclusivamente a la seguridad de información?				
13	¿Recomendaría usted a PYMES, implementar mecanismos formales para verificar si se está cumpliendo todos los procesos que el cliente solicita?				
14	¿Antes de solicitar los servicios de PYMES, usted revisaría todo su perfil empresarial?				
15	¿Contrataría usted los servicios de PYMES, para una mejor seguridad de información en sus equipos?				
16	¿Considera usted que si se implementa la norma ISO 27005 en su PYME la seguridad de su información mejoraría?				
17	¿Considera usted que la norma ISO 27005 ayudaría a controlar la pérdida de información en las empresas?				
18	¿Considera usted que desarrollando un modelo de procesos de la seguridad de la información podrá mejorar los riesgos para las empresas?				

APELLIDOS Y NOMBRE	
GRADO ACADÉMICO	INGENIERO DE SISTEMAS

_____

FIRMA DE EXPERTO
DNI:

Reporte de similitud

NOMBRE DEL TRABAJO

IMPLEMENTACIÓN DE UN MODELO DE PROCESOS DE SEGURIDAD DE LA INFORMACIÒN PARA UNA PYME PERUANA BASADA

AUTOR

Joel Harold / Jair Augusto Martos Paredes / Villazón Sosa

RECUENTO DE PALABRAS

23203 Words

RECUENTO DE CARACTERES

125401 Characters

RECUENTO DE PÁGINAS

189 Pages

TAMAÑO DEL ARCHIVO

2.8MB

FECHA DE ENTREGA

Apr 29, 2024 3:31 PM GMT-5

FECHA DEL INFORME

Apr 29, 2024 3:33 PM GMT-5

17% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 15% Base de datos de Internet
- 2% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 9% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 8 palabras)