ESCUELA DE POSTGRADO NEUMANN

MAESTRÍA EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

“Propuesta de mejora para la gestión de seguridad perimetral de la empresa Fasako S.A., Guayaquil – 2020”

Trabajo de Investigación
para optar el Grado a Nombre de la Nación de:

Maestro en
Gestión de Tecnologías de la Información

Autores:
Bach. Perdomo Córdova Jaime Eduardo
Bach. Núñez Noboa José Vicente

Docente Guía:
MBA. Díaz Zelada, Yvan Francisco

TACNA – PERU

2021

“El texto final, datos, expresiones, opiniones y apreciaciones contenidas en este trabajo son de exclusiva responsabilidad del (los) autor (es)”

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

DEDICATORIA

Este trabajo de investigación lo dedico a mi familia, personas de bien que me han brindado apoyo incondicional en toda etapa de mi vida, siendo el motor que me ha impulsado a seguir adelante en mis proyectos personales y académicos.

Jaime Eduardo Perdomo Córdova

DEDICATORIA

A mi Padre, mi mentor y formador que está en el cielo que desde que tengo uso de razón me inculco el estudio en lo teológico, así como en la ciencia y la tecnología como parte de integral de vida del ser humano.

Dedico también este logro a mi familia que son mi fuerza lo que me ha impulsado a continuar en los momentos más críticos de mi vida y en especial cuando creía que no tenía la capacidad y destreza para cumplir con este objetivo.

José Vicente Nuñez Noboa

AGRADECIMIENTO

Agradezco al ser supremo quien me ha forjado mi camino y dirigido siempre por el sendero correcto, por permitirme y darme la oportunidad de llegar a esta etapa profesional.

A los docentes de la Escuela de Postgrado Neumann por haber compartido sus enseñanzas, sabiduría, conocimiento experiencia profesional, otorgada con esmero, afán y comprensión con la vehemencia de ayudarnos en este gran propósito de nuestras vidas, que es obtener el Grado de Maestro en Gestión de Tecnología de Información.

Jaime Eduardo Perdomo Córdova

AGRADECIMIENTO

A Dios y mi familia como parte fundamental de mi vida espiritual y terrenal humana, son la fuente que me mantiene activo y me dan esperanza de un mañana mejor en esta vida compleja pero única y bella.

José Vicente Nuñez Noboa

RESUMEN

El presente trabajo de investigación fundamentado en una propuesta de mejora inquiere en la postura de la seguridad de la información en la empresa FASAKO S.A dedicada a brindar servicios de coworking en la ciudad de Guayaquil – Ecuador, estimando el desempeño e incremento de procesos de control de la seguridad perimetral justificado en la implementación de equipo tecnológico Firewall - Router RB3011UiAS-RM MikroTik con licenciamiento nivel 5, manteniendo las reglas y políticas de las buenas prácticas de seguridad informática.

De tal manera que acudimos a las normas internacionales de seguridad de la información como: ISO, ITIL, COBIT para mantener un lineamiento del concepto de gestión de la seguridad de la información, que garantice el continuismo del negocio basado en la integridad, confiabilidad y disponibilidad de los datos.

El capítulo I, presenta la importancia vinculada al desarrollo del presente trabajo de investigación, ya que es elemental en la evaluación del problema y sus objetivos, definiendo de manera simultánea las variables independiente y dependiente, así como la metodología de la investigación, las limitaciones y alcance del mismo.

El capítulo II contiene la conceptualización de los variables de estudios como son: Gestión de los servicios críticos de la empresa Fasako S.A. (Variables Dependiente). Gestión de la seguridad de la información de la empresa Fasako S.A. (Variable Independiente). Las mismas que fundamentan teóricamente el desarrollo del trabajo de investigación.

El capítulo III, muestra la información general de la empresa FASAKO S.A, su reseña histórica, filosofía organizacional, diseño organizacional, productos y/o servicios y diagnóstico organizacional todo lo que corresponde a los datos correspondiente como organización.

El capítulo IV, evidencia el cumplimiento de los objetivos del trabajo de investigación, mostrando el desarrollo de un plan estratégico, propuesta de mejora, proyecto de inversión, estudio del caso e investigación aplicada del tema propuesto.

ABSTRACT

This research work based on an improvement proposal inquires about the information security posture in the company FASAKO SA dedicated to providing coworking services in the city of Guayaquil - Ecuador, estimating the performance and increase of control processes of perimeter security justified in the implementation of technological equipment Firewall - RB3011UiAS-RM MikroTik router with level 5 licensing, maintaining the rules and policies of good computer security practice.

In such a way that we go to international information security standards such as: ISO, ITIL, COBIT to maintain a guideline of the information security management concept, which guarantees the continuity of the business based on integrity, reliability and availability. of the data.

Chapter I presents the importance linked to the development of this research work, since it is elementary in the evaluation of the problem and its objectives, simultaneously defining the independent and dependent variables, as well as the research methodology, limitations and scope of it.

Chapter II contains the conceptualization of the study variables such as: Management of critical services of the company Fasako S.A. (Dependent Variables). Information security management of the company Fasako S.A. (Independent variable). The same that theoretically base the development of the research work.

Chapter III shows the general information of the company FASAKO S.A, its historical review, organizational philosophy, organizational design, products and / or

services and organizational diagnosis, everything that corresponds to the corresponding data as an organization.

Chapter IV evidences the fulfillment of the objectives of the research work, showing the development of a strategic plan, improvement proposal, investment project, case study and applied research of the proposed topic.

INTRODUCCIÓN

El presente trabajo de investigación tiene como objetivo el diseño de una propuesta de mejora para la gestión de seguridad perimetral de la empresa FASAKO S.A. siendo una empresa dedicada al servicio empresarial designado como coworking (cotrabajo o trabajo en cooperación), correspondiente a oficinas y recursos compartidos.

Debido a la actividad económica de la empresa FASAKO S.A. La seguridad informática y de la información es un factor fundamental para el desarrollo de sus operaciones, por lo que la compañía FASAKO S.A., requiere una reingeniería del actual diseño de infraestructura de seguridad de red perimetral, así como de los procesos con la ayuda de herramientas tecnológicas informáticas con licencias de Comunidad en código abierto y la integración de una nueva herramienta licenciada de nivel 5 lo cual permitirá al administrador del departamento de TIC tener un nuevo sistema de gestión de seguridad de la información que permita prevenir, mitigar, monitorear alertas de posibles ataques internos y externos, así como la toma de decisiones de manera proactiva, en diferentes tipos de escenarios críticos de riesgos.

la implementación de técnicas de seguridad del Firewall Router de borde facilitará la gestión del tráfico de ingreso, y el propagado por los usuarios o equipos en la red.

Basándonos en el proceso de mejora continua en la infraestructura tecnológica de la compañía FASAKO S.A. esto permitirá tener un esquema tecnológico de escalabilidad horizontal y altamente disponible que proporcionará seguridad y fiabilidad a sus clientes potenciales, obteniendo la propiedad de incrementar el volumen de

trabajo mediante concurrencias, la implementación de nuevos servidores en entorno físico o virtual, sin que la calidad y el funcionamiento de servicio se vean afectados.

CAPITULO I

ANTECEDENTES DEL ESTUDIO

En este capítulo se ofrece una relevancia absoluta relacionada al presente trabajo de investigación, lo cual es fundamental para la determinación del problema y sus objetivos; y de manera simultánea definir las variables independiente y dependiente, así como la metodología de la investigación, las limitaciones y alcance del mismo.

1.1 TÍTULO.

PROPUESTA DE MEJORA PARA LA GESTIÓN DE SEGURIDAD PERIMETRAL DE LA EMPRESA FASAKO S.A., GUAYAQUIL – 2020

1.2 PLANTEAMIENTO DEL PROBLEMA.

La compañía FASAKO S.A. fue fundada el 5 de noviembre del 2004, por un grupo de empresarios ecuatorianos, quienes vieron la oportunidad de negocio en la creación de un servicio empresarial designado como coworking (cotrabajo o trabajo en cooperación), correspondiente a oficinas y recursos compartidos, de manera continua hasta la actualidad, acogiendo nuevas tecnologías para dar cumplimiento a la demanda de sus clientes (Vicente Nuñez Noboa, 2017).

La inmobiliaria FASAKO S.A. se encuentra ubicado en Guayaquil – Ecuador en las calles Pichincha 406 y Luque, edificio BancoPark, piso 14, oficina 1, zona comercial céntrica de la ciudad (Vicente Nuñez Noboa, 2017).

Respecto a la operatividad funcional del área tecnológica de la compañía Fasako S.A. se tiene conocimiento mediante información obtenida del departamento de

Tecnología, que la empresa fue víctima de diversos fallos de seguridad informática, en su topología de red lógica perimetral, lo cual ocasiono que su producción diaria se vea afectada de manera regular, y en ocasiones parar sus actividades por largas horas, ocasionando molestias a los usuarios que reciben el servicio de la firma.

Dado a estas circunstancias, en primera instancia se realizó un previo análisis del diseño de estructura tecnológica en el que se determinó que la compañía no poseía una infraestructura de seguridad informática y de la información, que le permitiera al departamento de TIC, prevenir, administrar y resolver ciertos escenarios de red por niveles de complejidad de forma proactiva y contigua. Por lo que se diseñó e implementó una infraestructura de seguridad perimetral bajo el manejo de herramientas open source.

En la actualidad la firma FASAKO S.A. requiere una reingeniería del actual diseño de infraestructura de seguridad de red perimetral, así como de los procesos con la ayuda de herramientas tecnológicas informáticas con licencias de Comunidad en código abierto y la integración de una nueva herramienta licenciada de nivel 5 lo cual permitirá al administrador del departamento de TIC tener un nuevo sistema de gestión de seguridad de la información que permita prevenir, mitigar, monitorear alertas de posibles ataques internos y externos, así como la toma de decisiones de manera proactiva, en diferentes tipos de escenarios críticos de riesgos.

Basándonos en el proceso de mejora continua en la infraestructura tecnológica de la compañía FASAKO S.A. esto permitirá tener un esquema tecnológico de escalabilidad horizontal y altamente disponible que proporcionará seguridad y fiabilidad a sus clientes potenciales, obteniendo la propiedad de incrementar el volumen de

trabajo mediante concurrencias, la implementación de nuevos servidores en entorno físico o virtual, sin que la calidad y el funcionamiento de servicio se vean afectados.

Debido a la actividad económica de la empresa FASAKO S.A. La seguridad informática y de la información es un factor fundamental para el desarrollo de sus operaciones, por lo que la implementación de técnicas de seguridad del Firewall Router de borde facilitará la gestión del tráfico de ingreso, y el propagado por los usuarios o equipos en la red.

1.3 OBJETIVOS DE LA INVESTIGACIÓN.

1.3.1 OBJETIVO GENERAL.

Diseñar una propuesta de mejora para la gestión de seguridad perimetral de la empresa FASAKO S.A., GUAYAQUIL – ECUADOR 2020.

1.3.2 OBJETIVOS ESPECÍFICOS

- Realizar un diagnóstico de la actual infraestructura de red perimetral de la empresa FASAKO S.A.
- Desarrollar una propuesta que atienda las necesidades identificadas en el diagnóstico previo.
- Diseñar mecanismos que permitan controlar la propuesta.
- Estimar la inversión necesaria para la implementación de la propuesta.

1.4 JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN.

1.4.1 JUSTIFICACIÓN TEÓRICA.

Según (Lostaunau, 2020) las razones del estudio de una justificación teórica son, argumentar el deseo de verificar, rechazar, confrontar o aportar aspectos de alguna

teoría, contrastar resultados o desarrollar epistemología del conocimiento, provocando el debate académico y la reflexión sobre el conocimiento. Por lo que esta investigación se realiza con el propósito de aportar con conocimiento técnicos sobre los procesos, métodos y herramientas de infraestructura tecnológicas que aportan de manera integral y dan como resultado un Sistema de Gestión de Seguridad de Información robusto, como instrumento de evaluación del logro de competencias de indagación científica, cuyos resultados podrán sistematizarse en esta propuesta, para ser incorporado como conocimiento a las Tecnologías de la información, ya que se estaría demostrando que el uso de estas metodologías mejoran el nivel de rendimiento de La empresa FASAKO S.A.

1.4.2 JUSTIFICACIÓN PRÁCTICA.

Según (Lostaunau, 2020) la justificación práctica ayuda a la solución de incógnitas, a la toma de decisiones o a la propuesta de estrategias que contribuyan a la solución del problema. Por lo que en este caso de investigación a desarrollar en la empresa FASAKO S.A. se realiza por la necesidad de mejorar el nivel de rendimiento, escalabilidad y de integración de herramientas tecnológicas tanto licenciadas como de código abierto de ciber seguridad en el actual Sistema de Gestión de Seguridad de Información que ayuden a mitigar el nivel de criticidad a los posibles riesgos que se expone el negocio por los diferentes ataques cibernéticos, y no se vea afectado en su continuidad y productividad como firma.

1.4.3 JUSTIFICACIÓN METODOLÓGICA.

Según (Fernández Bedoya, 2020) una investigación se justifica metodológicamente cuando se propone o desarrolla un nuevo método o estrategia que

permita obtener conocimiento válido o confiable. Debido a este concepto podemos decir que la elaboración y aplicación de los métodos y procesos, así como endurecimientos de seguridad, análisis forenses para cada una de las capacidades de la competencia de la empresa FASAKO S.A. mediante métodos científicos, laboratorios de escenarios de errores que pueden ser investigadas por la tecnología de procesos. Una vez que sean demostrados su validez y confiabilidad podrán ser utilizados en otros trabajos de investigación de sistemas de gestión de ciber seguridad en la información y en las diferentes instituciones educativas de postgrado.

1.5 METODOLOGÍA

1.5.1 TIPO DE INVESTIGACIÓN

De acuerdo con la naturaleza del presente trabajo esta investigación será de tipo descriptiva-explicativa debido a que busca identificar y caracterizar las variables de estudio de la problemática tratada. La presente investigación será de tipo aplicada dado que busca implementar conocimientos adquiridos para mejorar procesos de la compañía FASAKO S.A. De acuerdo al tipo de información utilizada se trata de una investigación mixta, analizando datos como la estructura de red de la empresa, vulnerabilidad del sistema y monto de inversión para el SGSI. De acuerdo a la instancia de tiempo en el que se realiza la investigación es de tipo transversal dado que observará y registrará los datos en un momento específico (Hernández Sampieri, Fernández Collado , & Baptista Lucio , 2014).

1.5.2 DISEÑO DE INVESTIGACION

El diseño de la investigación corresponde a uno no experimental debido a que no buscará manipular deliberadamente las observaciones de las variables, es decir, los

datos serán recolectados y analizados en su estado natural sin la interferencia o edición del investigador (Agudelo, Aigneren, & Ruiz, 2008).

1.5.3 TECNICAS, INSTRUMENTOS Y HERRAMIENTAS

1.5.3.1 TÉCNICAS

Se realizó un análisis de toda la infraestructura de red de la empresa usando técnicas y metodologías de Hacking Ético las cuales se dividen en 3 fases:

- Alcance
- Descubrimiento
- Análisis de vulnerabilidades

El escaneo de vulnerabilidad y la tasa de rendimiento en el consumo del ancho de banda se realizará con la herramienta Kali Linux. Los objetos o fenómenos analizados serán interpretados por el departamento de TIC, y serán presentados en reportes.

El análisis será realizado mediante la aplicación de MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), en donde se estudiarán las variables en relación con sus indicadores, lo que permitirá determinar los tipos de riesgos, el valor de operación de la empresa FASAKO S.A. y el nivel de impacto y protección durante el proceso de mejora continua de seguridad perimetral, todo esto en coordinación con los objetivos de la propuesta, lo cual permitirá presentar un plan de contingencia que satisfaga los propósitos del planteamiento con el nivel de riesgo.

1.5.3.2 INSTRUMENTOS

Para la presentación de resultados, se aplicaron entrevistas a dos colaboradores del TI y a tres clientes de la empresa, de los cuales se buscó identificar aspectos relacionados con buenas prácticas empresariales y dominio en determinadas áreas asociadas a la gestión de la información. Adicional, para el desarrollo de la propuesta, se usaron gráficos de pastel y empleó la escala de Likert.

1.5.3.3 HERRAMIENTAS

Revisión documental: Se revisó la información obtenida del análisis de vulnerabilidades como marco de referencia, obtenido directamente de los registros de la empresa.

Entrevistas: se realizaron entrevistas abiertas a los empleados y socios responsables de los procesos internos de seguridad. Específicamente se entrevistó a los miembros del departamento de IT y usuarios de la empresa. Las preguntas estuvieron enfocadas a diagnosticar vulnerabilidades, necesidades y características que posee el SGSI.

1.5.4 POBLACION Y MUESTRA

1.5.4.1 POBLACIÓN

La población de estudio corresponde a los usuarios (internos y externos) de la empresa FASAKO S.A.

1.5.4.2. MUESTRA

Para llevar a cabo los objetivos planteados y aplicar los instrumentos mencionados se recurrirá a una muestra no probabilística conformada por:

- 30 usuarios externos (clientes) de la empresa FASAKO S.A
- Los 2 integrantes del departamento de IT de la empresa FASAKO S.A

Para la selección de la muestra de usuarios externos se realizó una selección a conveniencia de acuerdo a la disponibilidad de información y voluntad de participación en el estudio.

1.5.5 MODELO DE MEJORA CONTINUA.

Los procesos de mejora continua en las organizaciones según (Guerra, Monterrey, & TECSUP, 2003), significa que el indicador más fiable de la mejora de la calidad de un servicio sea el incremento continuo y cuantificable de la satisfacción del cliente. Por lo que los modelos de mejora continua son aplicados por empresas que buscan puntos débiles en sus actuales procesos, productos y servicios desarrollan en el mercado. Para esto se crean planes estratégicos que se centran en identificar las áreas por mejorar.

La metodología PDCA es el modelo por seguir para implementar nuestro diseño de mejora en este trabajo de investigación ya que permite un control eficiente de técnicas y acciones internas y externas, por medio de la estandarización de la información y mitigando al mínimo los posibles fallos de error en la toma de decisiones (Qualitas, 2016).

1.5.6 EVALUACIÓN DE RIESGOS DE LA ACTIVIDAD OPERATIVA DE LA EMPRESA FASAKO S.A.

Para este indicador se realizó un reporte de riesgos y controles donde se establecen las sugerencias y el plan de acción para contrastar y reducir los riesgos que puedan presentarse durante el proceso de propuesta de mejora de seguridad perimetral.

***Tabla 1**. Riesgos, causas y medidas preventivas para la mejora de la gestión de la red*

Riesgo	Causantes	Actividad de control
Reglas y filtros de cortafuegos	No existen controles de accesos de nivel de red.	Implementar cortafuegos como primera línea para proteger la red Comprobación periódica del funcionamiento del cortafuegos
Acceso remoto	Colaboradores acceden a la red interna sin la utilización de VPN	Implementación de un VPN
Segmentación	La red actual presenta un solo segmento	Segmentar la red
Sistema de detección de intrusiones	No se utiliza ningún software de detección de intrusiones	Invertir en software de detección de intrusiones
Inalámbrico	Identificador de red expuesto	Modificar el SSID predeterminado utilizando un cifrado WPA

Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

1.6 ALCANCES Y LIMITACIONES.

1.6.1 ALCANCES:

1. El presente estudio explorará el actual SGSI de la empresa FASAKO S.A. de la ciudad de Guayaquil, Ecuador para los profesionales del departamento en área de la tecnología de la información que trabajan en la firma.

2. La investigación abarca únicamente el rediseño y la implementación de un nuevo SGSI para la empresa FASAKO S.A. de la ciudad de Guayaquil, Ecuador dedicada al coworking, y sectores tales como comercio, servicio y público en general.

1.6.2 LIMITACIONES:

1. La falta de capacitación de partes de los directivos y empleados para implementar buenas prácticas al utilizar las herramientas y la infraestructura tecnológicas que permitan el mejor desempeño al procesar la información durante las horas de trabajo de la empresa.

2. La falta de compromiso de parte de los gerentes de no poner el ejemplo al despilfarrar el ancho de banda y permitir pasar por alto las seguridades en sus estaciones de trabajo desde y hacia el internet.

3. Asignación de un presupuesto equilibrado para mantener y mejorar el departamento de tecnología tanto en la capacitación del personal humano como en la adquisición de herramientas y el desarrollo de las mimas para el análisis forense continuo en la empresa.

CAPITULO II

MARCO TEORICO

2.1. CONCEPTUALIZACIÓN DE LAS VARIABLE DE ESTUDIO

Tabla 2 *Variables de estudio*

VARIABLE	DIMENSIONES	INDICADORES
Gestión de la Seguridad	**Gestión de los servicios críticos**	• Evaluación de riesgos de la actividad operativa • Identificación de riesgos: áreas vulnerables • Planteamiento de estrategias de recuperación de amenazas
	Gestión de la seguridad de la información	• Certificación ISO 27001 • Buenas Prácticas: ISO 27002 • Directrices de implementación: ISO 27003, ITIL • Métricas de gestión: ISO 27004, metodología PHVA • Normativa: ISO 27005

Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

Nota. Análisis Comparativo basado en las variable independiente e indicadores (Núñez Noboa & Perdomo Córdova, 2020).

2.1.1. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

En el presente trabajo de investigación se conceptualizará la variable “gestión de la seguridad de la información como intérprete de adaptar la articulación requerida en cuanto al manejo de la seguridad de la información dentro de una organización.

Dentro de las normas ISO que tratan a cerca de la seguridad de la información en todas sus dimensiones tales como el mantener un glosario estándar para todas las normas de este grupo que se encuentran en proceso, la certificación basada en requisitos para poder implementar un Sistema de Gestión de Seguridad de la Información (SGSI), el preservar un código funcional para el manejo de las buenas prácticas de un SGSI, proporcionar las directrices de quien como y cuando se deben realizar las evaluaciones de seguridad del tratamiento de los datos y las técnicas que deben aplicarse para la consideración de la gestión de los riesgos en la perdida de datos del cual son el blanco de ataques cibernéticos todas las organizaciones, sean estas grandes, pequeñas o medianas empresas, podemos mencionar las siguientes:

Tabla 3 *Normas ISO aplicadas a la seguridad de la información*

NORMA	DESCRIPCIÓN
ISO/IEC 27001	Certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.
ISO/IEC 27002	Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es un **código de buenas prácticas** para la

	gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.
ISO/IEC 27003	Directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, No está certificada actualmente.
ISO/IEC 27004	Métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.
ISO/IEC 27005	Normativa dedicada exclusivamente a la gestión de riesgos en seguridad de la información. Proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standar BS 7799 parte 3. Publicada en junio de 2008.

Nota. Recuperado de (ESPAÑA, 2019) pntic.mec.es.

2.1.1.1 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27001.

Según (NQA, 2013), la ISO 27001 es la norma internacional para los sistemas de gestión de la seguridad de la información (SGSI). Lo que brinda un cuadro enérgico para preservar la información que se puede ajustar en las empresas sean estas pequeñas, medianas o grandes empresas.

Las empresas en la actualidad por más pequeñas que sean, están expuestas a los riesgos encadenados a la seguridad de la información por lo que se decide implementar un Sistema de Seguridad de la Información (SGSI), que formalice y satisfaga con la norma ISO 27001.

La estabilidad económica y operativa de las organizaciones se ven sujetas en gran proporción a una adecuada filiación de las causas más significativas y un oportuno valor de duda relacionado a la posibilidad de comprometer de manera negativa a la información de la compañía (iso27000, 2015).

Según (ESPAÑA, 2019) la seguridad de la información conforme la ISO 27001, tiene su cimiento en la protección de su confidencialidad, integridad y disponibilidad, que comprende los pilares fundamentales de la seguridad de la información precisamente de los sistemas concentrados para su régimen.

- **Confidencialidad**: la información no debe ser expuesta a personas, entidades o procedimientos no permitidos.
- **Integridad**: conservación de la precisión y totalidad de la información y su metodología de desarrollo.

- **Disponibilidad**: acceso y uso de la información y el tratamiento de esta por parte de las personas o procesos permitidos cuando lo soliciten.

En la siguiente figura podemos apreciar los pilares fundamentales de la seguridad de la información.

***Figura 1**. Pilares fundamentales de la seguridad de la información*

Fuente: Recuperado de https://ticsalborada1.fandom.com

2.1.1.2 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27002.

Según (www.iso.org, 2013), la norma ISO / IEC 27002: 2013 proporciona pautas para los estándares de seguridad de la información de la organización y las prácticas de estas, incluida la selección, implementación y gestión de controles, teniendo en cuenta el entorno de riesgo de seguridad de la información de una institución.

Está diseñado para ser utilizado por organizaciones que tengan la intención de: seleccionar controles dentro del proceso de implementación de un Sistema de Gestión

de Seguridad de la Información basado en ISO/IEC 27001; implementar controles de seguridad de la información comúnmente aceptados; Desarrollar sus propias pautas de gestión de seguridad de la información (www.iso.org, 2013).

En un sentido más panorámico podemos decir que la seguridad de la información efectiva también promete a la gerencia y las otras partes relacionadas que los activos de la compañía están equitativamente protegidos.

En total plenitud podemos manifestar que los requisitos de la seguridad de la información son esenciales y que toda organización que busca mantener la integridad, disponibilidad y confiabilidad de los datos de su compañía, debe identificar los requisitos de seguridad, por lo que (www.iso.org, 2013), manifiesta que hay tres fuentes principales de requisitos de seguridad, los cuales son:

a) La evaluación de los riesgos para la organización, teniendo en cuenta la estrategia y los objetivos comerciales generales de la organización. A través de una evaluación de riesgos, se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de que ocurran y se estima el impacto potencial.
b) Los requisitos legales, estatutarios, reglamentarios y contractuales que una organización, sus socios comerciales, contratistas y proveedores de servicios deben satisfacer, y su entorno sociocultural.
c) El conjunto de principios, objetivos y requisitos comerciales para el manejo, procesamiento, almacenamiento, comunicación y archivo de información que una organización ha desarrollado para respaldar sus operaciones.

2.1.1.3 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27005.

Según (ISOTools Excellence, 2018) la norma ISO 27005 es uno de los estándares en la serie ISO 27000 que forman el grupo de mecanismo de riesgo cibernético, dirigido por ISO 27001.

Según manifiesta (ISO, 2018), las normas ISO 27005 proporcionan las pautas para la gestión de riesgos de la seguridad de la información, el respaldo de los conceptos generales especificados en ISO/IEC 27001, y está esquematizado para fomentar a la implementación satisfactoria de la seguridad de la información con fundamentos planteados en la gestión de riesgos.

Saber las consideraciones, prototipos, desarrollos y terminologías descritas en ISO/IEC 27001 e ISO/IEC 27002 es significativo para una interpretación completa de la gestión de riesgos de la seguridad de la información basados en la norma ISO/IEC 2005.

Esta norma se puede aplicar a todo tipo de empresas, sean estas públicas, privadas, y sin fines de lucro, que buscan gestionar los riesgos que pueden implicar la seguridad de la información de la compañía.

Mediante argumentos de (Cortes & Adolfo, 2011) podemos decir que la norma ISO/IEC 2005 es basada mediante la metodología (PHVA) Planificar-Hacer-Verificar-Actuar.

2.1.1.4 LAS ETAPAS DE LA METODOLOGÍA PHVA

- **Planificar:** Instaurar los objetivos y procedimientos indispensables para otorgar resultados de acuerdo con el régimen de seguridad de la organización.
- **Hacer:** Implementar los procesos.
- **Verificar:** Observar y evaluar procesos sobre el régimen de seguridad, objetivos, metas, y condiciones legales.
- **Actuar:** Tomar acciones para progresar incesantemente el desembargo del sistema de gestión de la seguridad.

La siguiente tabla sintetiza las tareas de gestión del riesgo en la seguridad de la información ordenadas con las cuatro etapas del PHVA.

Tabla 4 *Actividades de gestión de riesgos basadas en metodología PHVA*

PROCESO	ACTIVIDADES DE GESTIÓN DE RIESGOS
Planificar	• Establecer el contexto • Valoración del riesgo (Identificación de Activos, Amenazas, Vulnerabilidades y Controles) • Planificación del tratamiento del riesgo • Aceptación del riesgo
Hacer	Implementación del plan de tratamiento del riesgo
Verificar	Monitoreo y revisión continuos de los riesgos
Actuar	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información

Nota. Actividades gestión de riesgos PHVA recuperado de (Cortes & Adolfo, 2011)

2.1.1.5 COBIT 5 EN LA SEGURIDAD DE LA INFORMACIÓN

Según (Monfort Casañ, 2016), COBIT (Control Objectives for Information and related Technology) es una guía de mejores prácticas mostrando como ámbito de trabajo, enfocada al control y revisión de los objetivos de las tecnologías de la información (TI).

En una empresa por más pequeña que esta sea, el recurso principal que debe protegerse de manera estratégica es la información. Por lo que la tecnología de la información tiene un papel importante desde que los datos son generados, almacenados y eliminados, debido a esto directivos de empresas están esforzándose cada vez más en tener información integra, confiable y disponible, que permita tomar decisiones.

Según (Monfort Casañ, 2016), los principios de COBIT se basan en 5 factores claves para una correcta administración de las Tecnologías de la información, tal como

***Figura 2**. Principios de COBIT 5*

Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

podemos apreciar en la figura número 2.

- **Principio 1: Satisfacer las necesidades de las partes interesadas**

Las partes interesadas necesitan que la empresa cree valor. El valor para las partes interesadas y la empresa significa obtener beneficios, con un riesgo y un costo de recursos óptimos. Para cumplir con estas expectativas, es esencial que una organización tenga un objetivo de gobernanza empresarial de creación de valor (Lane, 2014).

- **Principio 2: Cubrir la empresa de un extremo a otro**

La gobernanza de la TI empresarial (GEIT) es una parte integral de la gobernanza empresarial y las necesidades para abarcar toda la empresa de un extremo a otro. El GEIT se extiende a todas las funciones de la organización, donde TI está presente, cubriendo así la Empresa de manera integral y holística (Lane, 2014).

- **Principio 3: Aplicación de un marco integrado único**

En la actualidad, las empresas utilizan una multitud de estándares y marcos: COSO; COSO ERM; ISO / IEC 9000; ISO / IEC 31000; ISO / IEC 38500; ITIL, serie ISO / IEC 27000; TOGAF; PMBOK / PRINCE2 y CMMI. COBIT 5 tiene como objetivo proporcionar un marco único integrado para el gobierno y la gestión de la TI empresarial, que abarque todas las actividades de TI en la organización y esté alineado con las mejores prácticas, estándares y marcos de la industria (Lane, 2014).

- **Principio 4: Habilitar un enfoque holístico**

Mediante la identificación de facilitadores en toda la organización como un todo, COBIT garantiza un enfoque holístico y eficaz para el gobierno y la gestión de la TI empresarial (Lane, 2014).

- **Principio 5: Separar el gobierno de la administración**

El gobierno y la administración no son uno en la misma disciplina. El propósito, los objetivos, las actividades y la estructura organizativa de cada uno es único y distinto del otro. Como tal, COBIT separa claramente la gobernanza de la gestión en su marco (Lane, 2014).

El enfoque recomendado para la implementación de COBIT 5 es a través de un ciclo de vida de implementación de fases. Cada fase contiene componentes de gestión del programa, habilitación del cambio y mejora continua que garantizan que el programa de implementación se gestione de forma eficaz, que se abordan los aspectos conductuales y culturales y que no se trata de una iniciativa única.

2.1.1.6 ITIL EN LA SEGURIDAD DE LA INFORMACIÓN

Según (ITIL DOCS, 2020), ITIL Security Management describe el ajuste sistemático de la seguridad en una organización. Es una norma ISO 27001 que incluye todo tipo de organizaciones y especifica los requisitos para el seguimiento e

implementación de controles de seguridad según las necesidades de una organización. El objetivo principal es alinear la seguridad empresarial y de TI para que la información esté segura y se gestione de forma eficaz.

El enfoque principal de ITIL es la seguridad de la información, que radica en contrastar el acceso a la información mediante la inclusión de los siguientes componentes.

1.Controlar

- Políticas
- Organización
- Reportes

2.Planificar

- Sección SLA
- Contratos subyacentes
- Sección OLA
- Reportes

3.Implementar

- Clasificaciones
- Personal de Seguridad
- Políticas de seguridad
- Controles de acceso
- Reportes

4.Evaluar

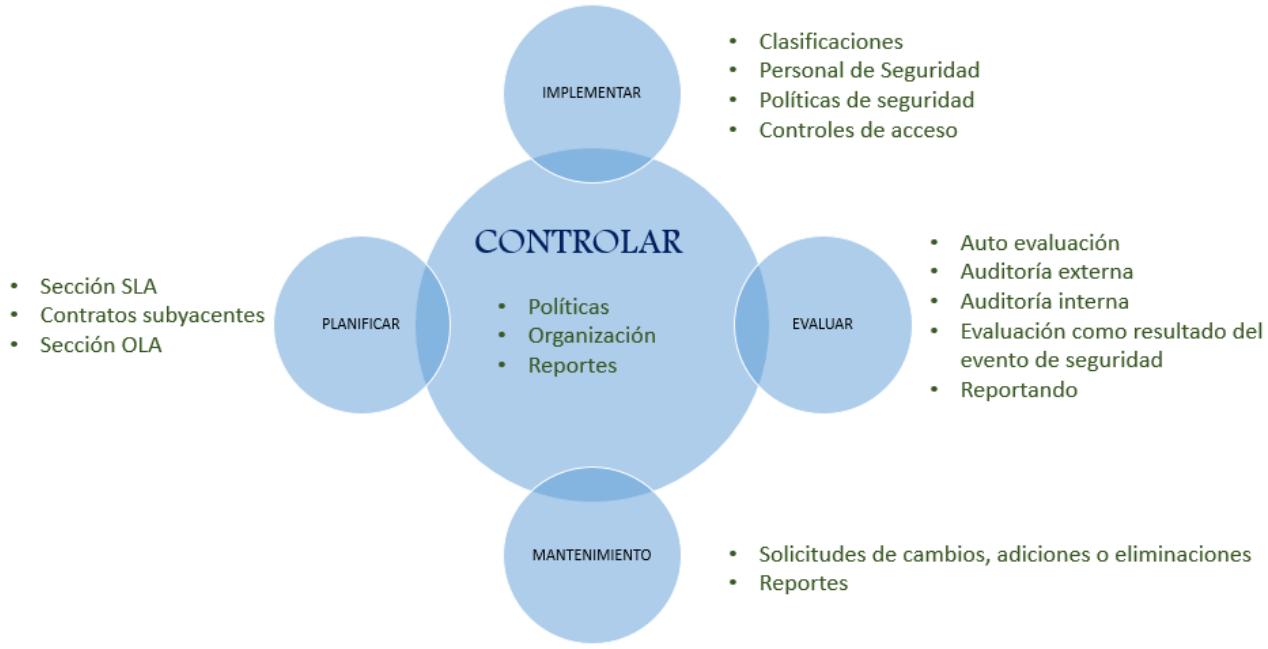
- Auto evaluación
- Auditoría externa
- Auditoría interna
- Evaluación como resultado del evento de seguridad
- Reportando

5.mantenimiento

- Solicitudes de cambios, adiciones o eliminaciones
- Reportes

En la siguiente figura podemos observar la representación gráfica de los factores que incluye una gestión de la seguridad de la información.

Figura 3. *Gestión de la seguridad de la información*



Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

Se debe tener en consideración que una norma aplicable a la seguridad de la información no será mejor que otra ya que se debe valorar la congruencia, las regiones, y sobre todo que cada compañía tiene sus características propias, de tal manera se debe acoger un patrón en mención para formar un modelo único, propio de la organización.

Tabla 5 *Comparativo COBIT, ITIL, ISO 27000*

AREA	COBIT	ITIL	ISO 27000
Funciones	Mapeo de procesos IT	Mapeo de la Gestión de Niveles de Servicios de TI	Marco de referencia de la seguridad de la información
Áreas	4 Procesos y 34 Dominios	9 Procesos	10 Dominios
Creador	ISACA	OGC	ISO International Organization for Standardization
¿Para qué se implementa	Auditoría de sistemas de información	Gestión de Niveles de Servicio	Cumplimiento del estándar de seguridad
¿Quiénes lo evalúan?	Compañías de contabilidad Compañías de consultoría en IT	Compañías de consultoría en IT	Compañías de consultoría en IT, Empresas de Seguridad, Consultores de Seguridad en redes

Nota. Comparativo COBIT, ITIL, ISO 27000 Recuperado de

(seguridadinformacioncolombia, 2010)

2.1.2. GESTION DE LOS SERVICIOS CRÍTICOS DE LA EMPRESA

Se entiende por servicios críticos a todos aquellos que son indispensables para el cumplimiento de la actividad principal de una empresa. De manera extendida se

puede decir que los servicios críticos de una empresa corresponden a su actividad principal. Siendo así los sistemas de gestión con los que se manejan estos servicios corresponden a los mecanismos que permiten la continuidad de estos y la confianza intrínseca de que estos permiten su funcionamiento óptimo y sin interrupciones. Dentro de esta gestión podemos encontrar las siguientes actividades clave

2.1.2.1 EVALUACIÓN DE RIESGOS DE LOS SERVICIOS CRÍTICOS

Las funciones de evaluación de riesgos de la operatividad de la empresa, hace factible identificar las posibles amenazas y el impacto que estas pueden ocasionar a la operación de la compañía, así como identificar los controles indispensables para evitar o aminorar los riesgos de cada suceso que pueda acaecer.

Para la emisión del reporte es indispensable resolver los siguientes puntos.

- Revisar la actividad operativa de la empresa y la relación con los servicios de Tecnología de la información.
- Establecer las áreas más vulnerables
- Considerar las posibles amenazas durante el proceso de mejora de seguridad perimetral.

En base a los resultados emitidos de este análisis, se contará con información necesaria para plantear medidas de prevención y recuperación reales al proceso de mejora continua.

2.1.2.2 IDENTIFICACIÓN DE RIESGOS DE LOS SERVICIOS CRÍTICOS

Para esto es necesario proyectar el impacto que ocasionaría cualquier evento, con lo cual llegase a impedir el funcionamiento operativo y represente perdidas latentes a la compañía.

2.1.2.3 PLANTEAMIENTO DE ESTRATEGIAS DE RECUPERACIÓN DE LOS SERVICIOS CRÍTICOS

Para establecer una estrategia de recuperación es indispensable disponer el tipo de recuperación que puede favorecer debido a la operatividad de la empresa, tomando en cuenta la relación de lo crítico y la urgencia de restauración vinculado al desempeño con la Tecnología de la Información y Comunicación (TICS).

2.2 IMPORTANCIA DE LAVARAIBLE DE ESTUDIO Y SUS DIMENSIONES

2.2.1. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La propuesta de mejora referente a infraestructura tecnológica de una organización no solo debe enfocarse en el hardware y los softwares informáticos, por lo que se debe garantizar que durante y en el término de la implementación de la propuesta de mejora para la gestión de seguridad perimetral de la empresa el estado de la información mantendrá su disponibilidad, confiabilidad e integridad, siguiendo los estándares de seguridad de la norma internacional ISO 27001.

2.2.2. GESTIÓN DE LOS SERVICIOS CRÍTICOS

La gestión de operatividad de los servicios críticos será medida y determinada con la variable independiente para valorar su relación.

Es importante realizar una gestión de riesgos de servicios críticos lo cual nos permitirá evaluar, identificar, y plantear estrategias de recuperación en caso de que se presente imprevistos durante el proceso.

2.4 DEFINICIONES CONCEPTUALES

2.4.1 GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LAS EMPRESAS.

La **seguridad de la información**, según ISO 27001, consiste en la preservación de confidencialidad, integridad y disponibilidad, así como los sistemas implicados en su tratamiento, dentro de una organización (Lisot, 2018).

2.4.2 SEGURIDAD INFORMÁTICA.

La seguridad informática se la define como el conjunto de prácticas, estrategias, métodos, herramientas y procedimientos cuya finalidad es garantizar la integridad de los equipos informáticos y de la información que contienen (OBS, 2020).

2.4.3 INFRAESTRUCTURA TECNOLÓGICA.

Se podría definir como infraestructura tecnológica al conjunto de elementos para el almacenamiento de los datos de una empresa. En la que se incluye el hardware, el software y todos los servicios necesarios para optimizar la gestión interna y seguridad de información (VEGAGESTIÓN, 2018).

2.4.4 FIREWALL/ROUTER.

Un firewall es una capa de seguridad entre su red doméstica e Internet. Dado que un enrutador es la conexión principal de una red doméstica a Internet, la función de firewall se combina en este dispositivo (NETGEAR, 2016).

2.4.5 LICENCIA NIVEL 5.

Determina las capacidades y características permitidas en el Firewall Router MikroTik:

Tabla 6 *Características licencia nivel 5 Router MikroTik*

Tiempo para actualización	**3 años**
Soporte para configuración inicial	**30 días**
Wireless AP	**Si**
Wireless Cliente and Bridge	**Si**
RIP, OSPF, BGP protocolos	**Si**
EoIP tunneles	**Ilimitado**
PPPoE tunneles	**500**
PPTP tunneles	**Ilimitado**
L2TP tunneles	**Ilimitado**
VLAN interfaces	**Ilimitado**
P2P Reglas de Firewall	**Ilimitado**
Reglas NAT	**Ilimitado**
HotSpot active users	**500**
RADIUS client	**Si**
Queues	**Ilimitado**
Web proxy	**Si**
Synchronous interfaces	**Si**

Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

2.4.6 ESTRATEGIAS DE RECUPERACIÓN

Son mecanismo utilizados para proteger, respaldar y recuperar la información de los centros de datos en caso de que esta se haya visto comprometida. Entre algunas de las estrategias de recuperación tenemos:

2.4.6.1 BACKUPS

Se refiere a copias de respaldo de la información existente en los centros de procesamiento de datos. El objetivo de contar con estas copias de seguridad es poder regresar a un punto anterior al momento de desastre, eliminación, modificación o hurto de información en donde la información aún permanecía integra y normal. Esta estrategia representa una pérdida mínima de información al ser utilizada, aunque esto dependerá del tiempo transcurrido entre la creación de la última copia de seguridad y el evento de desastre. FASAKO S.A. establece la política de crear copias de seguridad de su información de manera semanal.

2.4.6.2 MONITOREO EN TIEMPO REAL

Consiste en mantener u registro de los componentes físicos y lógicos del centro de procesamiento de datos con la capacidad de acceso permanente a esta información.

La estrategia consiste en tomar acción inmediata al detectar variaciones en los parámetros vigilados. La acción rápida minimiza el riesgo de pérdida y exposición de la información

2.4.6.3 CONTROL DE ACCESO

Puede aplicarse tanto a nivel físico como lógico y consiste en llevar un registro del acceso de los usuarios a la información para así poder identificar la fuente en caso de producirse un evento de riesgo de seguridad. Para esto es necesario contar con políticas de acceso bien definidas.

2.4.7 FILOSOFÍA ORGANIZACIONAL.

Según (Sampson Quain, 2019), la elaboración de una filosofía corporativa para una organización puede ayudar a sus clientes a comprender el propósito, los objetivos y la intención de su organización, lo que puede generar confianza y lealtad a la marca. El desafío, sin embargo, es que su filosofía corporativa debe estar en sintonía con los valores y la visión de su negocio, o comunicará un mensaje confuso. Comprender los elementos de una filosofía corporativa exitosa puede proporcionarle la inspiración necesaria para crear la suya propia.

2.4.8 DISEÑO ORGANIZACIONAL

Según (Rodrigo Bastos, 2017) la estructura organizacional generalmente tiene elementos explícitos como organigrama, roles, descripciones de puestos, cadenas de mando, junta directiva, procesos, políticas, departamentos con gerencia, etc. Pero también tiene aspectos implícitos o intangibles, como la red de relaciones y el flujo informal de información.

Según (Kimberlee Leonard, 2018), el diseño organizacional es el proceso de creación de la jerarquía dentro de una empresa. Los seis elementos del diseño organizacional ayudan a los líderes empresariales a establecer los departamentos, la cadena de mando y la estructura general de la empresa. Los aspectos de la estructura organizativa que se revisan más notablemente es el organigrama.

2.4.9 ESPECIALIZACIÓN DEL TRABAJO

Según (Kimberlee Leonard, 2018), la especialización laboral es el primero de los elementos de la estructura organizativa. Los líderes empresariales deben considerar las tareas laborales y los deberes específicos asociados con puestos determinados. Dividir

las tareas laborales entre diferentes trabajos y asignarlas a niveles definidos, es el papel de los elementos de especialización laboral.

2.4.9 DEPARTAMENTALIZACIÓN Y COMPARTIMENTOS

Según (Kimberlee Leonard, 2018), la departamentalización y los compartimentos son otros dos componentes del diseño organizacional. Los departamentos suelen ser un grupo de trabajadores con las mismas funciones generales. A menudo se desglosan en categorías amplias como funcional, producto, geográfica, de proceso y cliente. Los departamentos comunes incluyen contabilidad, fabricación, servicio al cliente y ventas.

Los compartimentos pueden tener equipos con diferentes miembros del departamento que se agrupan para lograr eficiencia. Por ejemplo, una empresa que ofrece servicios de TI a otras empresas puede tener equipos asignados a cada empresa. Cada equipo puede tener un gerente de proyecto, un diseñador gráfico, un especialista en codificación, un especialista en seguridad, un representante del cliente y un proveedor de servicios.

2.4.10 CADENA DE MANDO

La cadena de mando, según (Kimberlee Leonard, 2018), es lo que suele ilustrar el organigrama. Muestra quién reporta a quién en la estructura de recursos humanos de la empresa. Algunas empresas tienen una jerarquía más tradicional con líderes de departamento y ejecutivos a cargo muy claros. Otras empresas utilizan una cadena de mando y una estructura más fluida en la que se considera que más personas forman parte del mismo nivel de mando en un equipo multifuncional.

Hay pros y contras de cualquier modelo. Lo importante es que los empleados sepan qué se espera de ellos y cómo consiguen que la información fluya por los canales adecuados. Si un empleado no está seguro de quién es su jefe directo debido a una cadena de mando poco clara, es posible que no transmita correctamente la información correcta a la parte correcta.

2.4.11 AMBITO DE CONTROL

El alcance del control es el elemento de diseño organizacional que considera la capacidad de cualquier gerente. Por lo que según (Kimberlee Leonard, 2018) hay límites en la cantidad de personas que una persona puede supervisar. El alcance del control se dirige a este elemento de diseño. Si un gerente tiene demasiadas personas para supervisar, podría perder su eficacia y no reconocer los problemas o los éxitos.

2.4.12 CENTRALIZACION Y DESCENTRALIZACIÓN

Podemos mencionar a la centralización y la descentralización según (Kimberlee Leonard, 2018) como los elementos de diseño organizacional que deciden el grado en que los empleados toman las decisiones en un nivel central o en varios niveles. Por ejemplo, todas las decisiones presupuestarias importantes se filtrarían al director ejecutivo y director financiero de forma centralizada. Las decisiones de servicio al cliente pueden descentralizarse dando a quienes interactúan con el cliente instrucciones sobre cómo manejar los problemas, pero la autoridad para tomar ciertas decisiones.

2.5 ANÁLISIS COMPARATIVO

Existen diversos estudios que han analizado la gestión de seguridad de entidades jurídicas. Tal es el caso de la investigación de Bermúdez y Bailón (2015)

titulada “Análisis en Seguridad Informática y Seguridad de la Información basado en la norma ISO/IEC 27001-Sistema de Gestión de Seguridad de la Información dirigido a una empresa en servicios financieros”. Dicha investigación también se centra en las normas ISO 27000 y buscó detectar las vulnerabilidades de su sistema y análisis de riesgos. El estudio concluyó que las mejoras de seguridad se basan en tres pilares: confidencialidad, integridad y disponibilidad de la información

Así mismo en el estudio titulado “Diseño de un sistema de gestión de seguridad de la información para instituciones militares” realizado por Guamán (2015). Dicho estudio también se basó en las cláusulas de la ISO 27000:2005

Otro estudio a considerar es el de Guevara (2017) titulado “Sistema de Gestión de Seguridad de la información basado en la Norma ISO/IEC 27001 para el Departamento de Tecnologías de la Información y Comunicación del Distrito 18D01 de Educación “ en el que se buscó determinar la eficacia de la gestión de los sistemas informativos de una entidad educativa. El trabajo concluyo que la ausencia de respaldos informáticos, así como procedimientos de manejo de equipos de almacenamiento hacen que la institución sea blanco fácil de ataques informáticos. Para esto se propone a la implementación de un SGSI.

El estudio de Yañez (2017) buscó evaluar la implementación de los 114 objetivos de control de la norma ISO27001 y la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) en la Subsecretaría de Economía y Empresas de Menor Tamaño. En este estudio se encontró deficiencias en el cumplimiento de 70 objetivos de control de la norma.

El trabajo de Flores (2016) consistió en la implementación de un Sistema de Gestión de Seguridad de la Información para la Unidad de Gestión Educativa Local de Chiclayo, basado en las normas internacionales ISO/IEC 27001:2013 e ISO/IEC 27002:2013, adoptando COBIT 5 como marco de trabajo

2.6 ANÁLISIS CRÍTICO

Se puede observar que la gestión de la seguridad ha sido ampliamente estudiada en el contexto ecuatoriano, sin embargo, este presente trabajo realizará el estudio pertinente para una empresa perteneciente al sector de compra venta de bienes inmuebles como lo es Fasako S.A., contribuyendo así a la literatura existente.

De acuerdo al análisis comparativo podemos realizar las siguientes observaciones en cuanto a tipo de institución objeto de estudio y método de análisis

Tabla 7 *Análisis comparativo*

Autor	Estudio	Tipo de empresa objeto de estudio	Norma
Bermúdez y Bailón (2015)	Análisis en Seguridad Informática y Seguridad de la Información	Financiera	ISO 27001
Guamán (2015)	Diseño de un sistema de gestión de seguridad de la información	Entidad militar	ISO 27000:2005
Guevara (2017)	Evaluación de mecanismos de seguridad informática	Educación	ISO/IEC 27001
Yañez (2017)	Implementación de norma de seguridad informática	Entidad gubernamental	ISO27001

Flores (2016)	Implementación de norma de seguridad informática	Educación ISO/IEC 27001:2013

Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

Como se puede apreciar los estudios en esta materia pueden abarcar una gran variedad de tipos de organización dado que en la época actual la información y sistemas informáticos son recursos clave para las operaciones de una entidad. Así mismo se observa que se tiene a las normas ISO 27000 como referente principal a la hora de evaluar sistemas de gestión ya existentes o implementar normativos

CAPITULO III

MARCO REFERENCIAL

En el presente capítulo se muestra la información general de la empresa FASAKO S.A, su reseña histórica, filosofía organizacional, diseño organizacional, productos y/o servicios y diagnóstico organizacional todo lo que corresponde a los datos correspondiente como organización.

3.1. RESEÑA HISTÓRICA

La inmobiliaria FASAKO S.A. fue constituida por el emprendimiento de un grupo socios guayaquileños, que tuvieron el desafío y la visión de crearla el 5 de noviembre del año 2004, en base a la idea de que el propietario de una pequeña empresa pueda encontrar el factor de credibilidad de trabajar en una oficina independiente para el desarrollo de sus actividades, a lo que se refiere a un espacio compartido donde coexista la posibilidad de interactuar y retransmitir con sus compañeros de trabajo.

La ideología que mantenían estos empresarios guayaquileños era de que el espacio compartido en un área de trabajo es de gran utilidad para los emprendedores, ya que el alquiler de una oficina permanente puede representar costos muy elevados para las empresas pequeñas que están iniciando sus actividades y el contrato por un local de trabajo puede estar sujeto a un arriendo por un período de inicio determinado, lo que podría aumentar la posibilidad de vulnerabilidad financiera.

Una posibilidad para cualquier empresa o negocio nuevo es lo que FASAKO S.A. empezó dando el servicio empresarial denominado coworking (cotrabajo o trabajo en cooperación) es decir oficinas y recursos compartidos, de manera ininterrumpida hasta

la actualidad, adoptando las nuevas tecnologías para satisfacer la demanda de sus clientes.

Todo esto convierte a inmobiliaria FASAKO S.A. en una empresa que ofrece soluciones de espacio para negocios y opera bajo el concepto moderno de una oficina temporal y virtual, con tecnología y equipamiento de última generación y asistencia administrativa.

Por otro lado, la empresa FASAKO S.A. se constituye como una empresa dentro de la categoría PYME (Pequeña y mediana empresa), de acuerdo a la clasificación estandarizada que maneja la Superintendencia de compañías, valores y seguros, para el tipo de empresa cuyo número de trabajadores oscila entre 10-199 empleados y cuyos ingresos están dentro del intervalo 100.001,00 – 5.000.000,00. Es decir, el caso de la empresa en cuestión. (SUPERCIAS, 2020)

3.2 FILOSOFÍA ORGANIZACIONAL.

A continuación, se mencionan la misión, visión y valores establecidos por la compañía FASAKO S.A., lo cual representa la filosofía organizacional de la empresa referente a su actividad comercial.

3.2.1 MISIÓN

Ofrecer a las pequeñas empresas, un conjunto de soluciones técnicas, aplicaciones y herramientas informáticas y de oficina, manteniendo una infraestructura corporativa accesible a recursos tecnológicos y área de trabajo, ajustado a precios asequibles.

3.2.2 VISIÓN

Ser coparticipe fundamental de nuestros clientes y expandirnos a nivel nacional como una compañía de servicios de coworking.

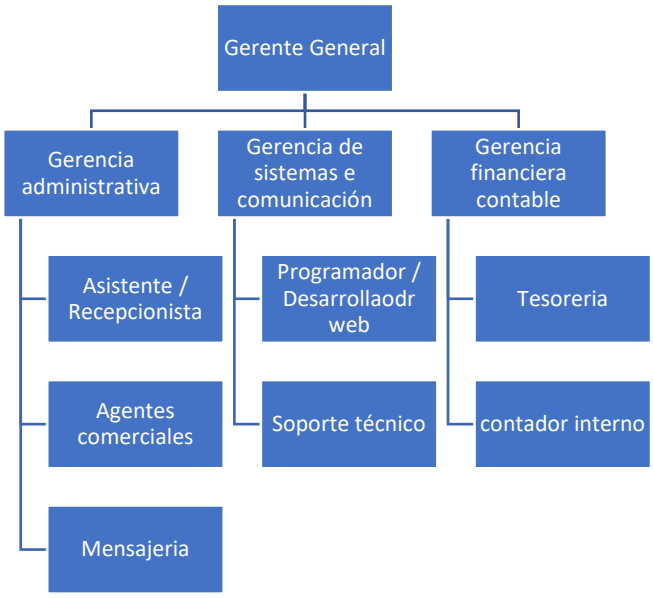
3.2.3 VALORES

- Servicio
- Integridad
- Calidad
- Responsabilidad
- Innovación
- Colaboración

3.3 DISEÑO ORGANIZACIONAL

La empresa FASAKO S.A. presenta la siguiente estructura organizacional operativa de la empresa.

Figura 4. *Diseño Organizacional Empresa Fasako S.A.*



Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

Las áreas identificadas trabajan de forma integral para permitir el desarrollo normal de la actividad económica.

Las funciones departamentales de FASAKO S.A. se indican a continuación

3.3.1 ESPECIALIZACIÓN DEL TRABAJO

3.3.1.1 GERENCIA GENERAL

El rol que desempeña el CEO de la empresa FASAKO S.A. es de gran capacidad de gestión y liderazgo, debido a la experiencia en las áreas centrales del negocio de coworking, manteniendo la atención en todos los departamentos operacionales de la compañía.

Las principales responsabilidades del CEO de FASAKO S.A. incluyen:

- Construir asociaciones importantes
- Gestión de personas
- Recaudación de fondos (inversiones, patrocinio, etc.)
- Estrategia de expansión y crecimiento de ubicaciones
- Cubrir cualquier brecha en las necesidades de personal

3.3.1.2 GERENCIA ADMINISTRATIVA

El Gerente administrativo de la empresa FASAKO S.A cumple con las tareas organizativas y de gestión que respaldan la productividad y el crecimiento de la compañía y sus departamentos o equipos individuales.

Las principales responsabilidades que cumple el administrador de la empresa FASAKO S.A. son las siguientes:

- Planificar estrategias para optimizar y mejorar las operaciones comerciales.
- Reorganizar o contratar personal para expandir las operaciones en colaboración con los equipos de recursos humanos.
- Manejar las finanzas comerciales y planificar el presupuesto con la ayuda del departamento financiero.
- Supervisar el marketing y las promociones de los productos y servicios de la empresa FASAKO S.A.
- Negociar contratos con proveedores para identificar oportunidades de ahorro de costos.

Esta gerencia se encuentra a cargo de las siguientes posiciones:

- **Asistente/Recepcionista:** este cargo es responsable de funciones como agendar citas y reuniones, recepta direccionar información dirigida a los diferentes departamentos, llevar control y registro e archivos pertinentes para la empresa, atender a los usuarios que se acerquen a la empresa y brindar apoyo y gestión en diferentes procesos internos.
- **Agentes comerciales:** Son los encargados de establecer con tanto directo con los clientes y potenciales clientes, buscando oportunidades de venta y promocionando los servicios ofertados por la compañía.
- **Mensajería**: El área de mensajería de la empresa FASAKO S.A es la responsable de distribuir documentos para instituciones, empresas, agencias gubernamentales o privadas y personas, con la finalidad de que todos los tramites sean realizados a tiempo, facilitando la operación del negocio.

3.3.1.3 GERENTE DE SISTEMAS Y COMUNICACIÓN

Uno de los principales impulsores del éxito de FASAKO S.A es la eficiencia, y la capacidad de automatizar las tareas de rutina es una excelente manera de aumentar la eficiencia general. En términos generales, el departamento de TI es el responsable de proporcionar la infraestructura para esta automatización.

En un nivel aún más básico, al implementar la gobernanza para el uso de la red mediante VLANS creadas para cada empresa que labora en los espacios alquilados de la compañía FASAKO S.A.

El departamento de TI permite a los empleados de las empresas comunicarse, colaborar y automatizar las tareas de rutina y, en general, proporcionar a los equipos la funcionalidad que necesitan para realizar sus tareas.

Es importante tener en cuenta que, aunque el departamento de TI implementa y facilita el flujo de información, no crea la política que define qué información es correcta o accesible para otros.

El departamento de TI evalúa e instala el hardware y software adecuados necesarios para mantener la red de FASAKO S.A. funcionando correctamente. Como esto implica trabajar dentro de un presupuesto asignado al departamento para dispositivos de red y software, el departamento de TI debe asegurarse de que el equipo en el que invierte satisfaga de manera óptima las necesidades de la empresa sin exceder el presupuesto.

Si un sistema de red falla, las repercusiones pueden ser costosas, no solo para la empresa FASAKO S.A y sus operaciones, sino también para todas las entidades que

realizan sus actividades en las áreas de trabajo dentro de las instalaciones de FASAKO S.A. Estas entidades podrían verse afectadas y perder la fe en la capacidad de la empresa para proporcionarles la disponibilidad del servicio sin interrupciones que afecte la operatividad del negocio.

El departamento de TI de la empresa FASAKO S.A. mantiene su plan de contingencia que pueda implementarse en caso de que el sistema falle. Debe estar diseñado para restablecer la red rápidamente o permitir que se cambie a un sistema alternativo hasta que se completen las reparaciones necesarias.

Esta gerencia se encuentra a cargo de las siguientes posiciones:

- **Programador/Diseñador web:** encargo del mantenimiento y correcto funcionamiento de la plataforma de comunicación e información de la empresa
- **Soporte técnico:** Ingeniero en sistemas encargado del mantenimiento de equipos físicos de cómputo y comunicación

3.3.1.4 GERENCIA FINANCIERTA Y CONTALBE

Las funciones del departamento de financiero de la empresa FASAKO S.A. abarca toda la gama de actividades relacionadas con el pago de proveedores, vendedores y otras partes interesadas que realizan negocios con las empresas.

Además, la función de finanzas de la compañía FASAKO S.A, también realiza un seguimiento de las cuentas por cobrar, lo que significa que hacen un seguimiento de los clientes y los clientes que deben el dinero corporativo por los servicios prestados.

Aparte de esto, la función de finanzas también maneja los pagos de seguridad social de los empleados.

Esta gerencia se encuentra a cargo de las siguientes posiciones

- **Tesorería:** encargado de la creación de políticas de cobros, manejo de caja y flujos de efectivo. Llevar el control de los recursos monetarios de la empresa.
- **Contabilidad interna:** encargado de llevar el control y registro de los movimientos contables durante las operaciones de la empresa.

3.3.2 CENTRALIZACION

La empresa FASAKO S.A. tiene un sistema de gestión centralizado en el que las decisiones ya sean presupuestarias, administrativas, de innovación, estrategia comercial y diseño deben ser revisadas y aprobadas por la gerencia general de la empresa.

A pesar de este esquema cada departamento tiene la facultad de analizar y proponer mejoras de sus procesos.

3.4 PRODUCTOS Y/O SERVICIOS

La empresa FASAKO S.A. brinda servicios de calidad para un profesional autónomo e independiente o pequeña empresa que desea encontrar un entorno colaborativo para el desarrollo de sus funciones.

Los espacios de trabajo que FASAKO S.A. pone a disposición son de 12 a 30 m2 para el alquiler de oficinas completas para empresas o proyectos concentrados o como espacios de trabajo compartido con otros profesionales.

Todas las áreas de trabajo cuentan con lo siguiente:

- Sillas y escritorios de trabajo ergonómico
- Conectividad total en todas las áreas de trabajo
- Amplios espacios compartidos con conectividad donde pueden realizar reuniones rápidas con clientes.
- Sala de Conferencia compartida
- Internet de alta velocidad
- Acceso a impresora de red compartida
- Fotocopiadora compartida
- escáner compartido
- Sistema de seguridad
- Luz natural en todas las oficinas
- Control de acceso
- Sistema de alarma

La operatividad comercial de la compañía FASAKO S.A. radica en el servicio de coworking por lo que además de mantener espacios adecuados, y recursos compartidos para el desarrollo de funciones de las empresas que operan en las instalaciones de la organización, es la de garantizar la confidencialidad, integridad y disponibilidad de los datos de los usuarios.

Por lo que para los espacios de coworking que atienden a varias pequeñas empresas o grupos de trabajo diferentes, se crean VLAN, (Red Privada Virtual), redes virtuales separadas que sean específicas para cada empresa. De esta manera, cada grupo de trabajadores opera bajo su propia red segura dentro de la red, lo cual permite que los segmentos de trabajo colaboren bajo una capa adicional de protección.

De tal manera que a medida que los espacios de coworking de la compañía FASAKO S.A. siga creciendo, el departamento de TICS deberá seguir implementando las medidas de seguridad en las redes informáticas para prevenir cualquier ataque cibernético, y de esta manera poder garantizar la confiabilidad, disponibilidad e integridad de los datos de las empresas alojadas.

Aunque la ubicación física del espacio de coworking tendrá mucho que ver con las medidas de seguridad que se adopten, FASAKO S.A. tiene en cuenta que las amenazas pueden provenir de lugares en gran parte invisibles. Por lo que mantiene en las más altas prioridades a la seguridad de las redes.

3.5 DIAGNOSTICO ORGANIZACIONAL

El sistema de coworking que ofrece la compañía FASAKO S.A. abarca los servicios fundamentales que ayuda a los emprendedores y pequeñas empresas. Sin embargo, esto también incluye algunas contrariedades con los que se tiene que controvertir.

Según (Portugal, 2017) El diagnóstico empresarial permite a la empresa, definir el estado actual de la organización que permita tener unos resultados valorativos, que sirven para tomar decisiones en el factor tiempo para reestructurar la organización y cumplir con las metas proyectadas.

Por tal motivo se ha realizo el análisis FODA que permitirá no solo identificar las fortalezas del concepto y las oportunidades a aprovechar, sino también descubrir las debilidades y amenazas que podrían frenar su desarrollo.

3.5.1 ANALISIS FODA

3.5.1.1 FORTALEZAS

- Alta disponibilidad de recursos tecnológicos compartidos.
- Alta disponibilidad de conexión a internet.
- Flexible: es un costo variable. Las áreas de trabajo se pueden alquilar por 1 día o varios meses.
- Áreas de trabajo acorde a las necesidades de los clientes: los espacios de coworking de FASAKO S.A. ofrecen todos los servicios que un empleado puede esperar de su empresa para trabajar en óptimas condiciones. Más aún, los compañeros de trabajo no tienen que preocuparse por los suministros.
- Experiencia de socialización perfecta para evitar el trabajo solitario e improductivo en casa.
- Extensión de la red de contactos debido a las interacciones y colaboración con los demás compañeros de trabajo.
- Infraestructura tecnológica escalable.
- Compañeros de trabajo: profesionales talentosos que provienen de diferentes áreas, listos para ayudarse mutuamente, brindando consejos, apoyo e intercambio de conocimientos y experiencias.

3.5.1.2 OPORTUNIDADES

- Acuerdos con organizaciones que provean los insumos y consultoría al beneficiario.

- Generación de contratos a largo plazo que da la posibilidad de mejorar los precios.
- Generación de alianzas comerciales
- Patrocinador de recursos y apoyo para el emprendimiento de proyectos de emprendedores.
- Empresas clientes con relaciones políticas, pueden recomendar nuestro servicio a funcionarios del sector público.
- Ahorro de hasta el 50% en aprovisionamiento de oficina al colaborador.

3.5.1.3 DEBILIDADES

- Los costos de mantenimientos de infraestructura son altos.
- Necesidad de mejora de equipos tecnológicos.
- Poco espacio de parqueo en el sector

3.5.1.4 AMENAZAS

- Ataques cibernéticos
- Los emprendedores y las empresas se han visto afectadas por la crisis financiera causada por el COVID 19.
- La crisis económica a causa del COVID-19 ha frenado la creación de empresas emergentes y ha desanimado a algunos emprendedores. Esta tendencia puede reducir el número de clientes.
- Posibles incumplimientos de obligaciones estipuladas con el proveedor.

3.6 EVALUACION DE FACTORES INTERNOS Y EXTERNOS

Tabla 8 *Matriz EFI*

Factor	Ponderación	Valor	Resultado
Fortaleza			
· Alta disponibilidad de recursos tecnológicos compartidos.	0,1	4	0,4
· Alta disponibilidad de conexión a internet.	0,1	4	0,4
· Flexible: es un costo variable. Las áreas de trabajo se pueden alquilar por 1 día o varios meses.	0,15	4	0,6
· Áreas de trabajo acorde a las necesidades de los clientes: los espacios de coworking.	0,2	4	0,8
· Experiencia de socialización perfecta para evitar el trabajo solitario e improductivo en casa.	0,1	4	0,4
· Extensión de la red de contactos debido a las interacciones y colaboración con los demás compañeros de trabajo.	0,1	4	0,4
· Infraestructura tecnológica escalable.	0,1	4	0,4
· Compañeros de trabajo: profesionales talentosos	0,15	4	0,6
TOTAL	1		**4**
Debilidad			
· Los costos de mantenimientos de infraestructura son altos.	0,4	4	1,6
· Necesidad de mejora de equipos tecnológicos.	0,4	4	1,6
· Poco espacio de parqueo en el sector	0,2	2	0,4
TOTAL	1		**3,6**

Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

Tabla 9 *Matriz EFE*

Factor	Ponderación	Valor	Resultado
Oportunidad			
· Acuerdos con organizaciones que provean los insumos y consultoría al beneficiario.	0,2	4	0,8
· Generación de contratos a largo plazo que da la posibilidad de mejorar los precios.	0,15	4	0,6
· Generación de alianzas comerciales	0,15	4	0,6
· Patrocinador de recursos y apoyo para el emprendimiento de proyectos de emprendedores.	0,15	4	0,6
· Empresas clientes con relaciones políticas, pueden recomendar nuestro servicio a funcionarios del sector público.	0,2	4	0,8
· Ahorro de hasta el 50% en aprovisionamiento de oficina al colaborador.	0,15	4	0,6
TOTAL	1		**4**
Amenaza			
· Ataques cibernéticos	0,25	3	0,75
· Los emprendedores y las empresas se han visto afectadas por la crisis financiera causada por el COVID 19.	0,3	4	1,2
· La crisis económica a causa del COVID-19 ha frenado la creación de empresas emergentes y redujo el número de clientes.	0,3	4	1,2
· Posibles incumplimientos de obligaciones estipuladas con el proveedor.	0,15	3	
TOTAL	1		**3,15**

Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

Como es posible apreciar en las tablas 7 y 8, la empresa Fasako S.A. cuenta con conectividad y un sistema tecnológico avanzado, lo cual permite ofrecer comodidad respecto del acceso a la información de forma ágil en nuestros clientes, factor por demás clave en los actuales momentos, donde la eficiencia es determinante de la competitividad. Además, el alquiler de oficinas se ajusta a la necesidad de uso en cada momento del tiempo que así lo requiera un usuario, es decir, cuenta con flexibilidad en la provisión de las instalaciones, sin restricciones de tiempo. Así también es importante resaltar que las instalaciones están equipadas al menos con el 50% de los requerimientos de equipos y suministros que sean demandados por los emprendedores que ejecuten un contrato con la empresa. Cabe señalar que las instalaciones cuentan con un ambiente confortable e ideal para el desarrollo de actividades de socialización y cooperación en el trabajo.

Por lo que respecta a las oportunidades, la empresa cuenta con diversos acuerdos de cooperación conjunta con otras empresas, que están en función de la provisión de equipos, suministros y asesoría acorde a las necesidades de cada emprendimiento de los clientes.

Sin embargo, es de resaltar que la empresa presenta debilidades que deben considerarse con carácter de urgente, si lo que se quiere es mejorar las condiciones de competitividad en el mercado y en la medida de lo posible, ofrecerle mayor sostenibilidad a la actividad de Fasako S.A. Dichas debilidades se concentran principalmente en tres; la primera hace referencia a mantener una estructura de costos

ineficiente sobre el mantenimiento de su infraestructura. Esto no sólo afecta al precio final que percibe el cliente por los servicios, sino también al margen de rentabilidad de la propia empresa, por lo cual debe ser atendido cuanto antes. Así también, pese a contar con un buen nivel tecnológico en sus equipos y sistemas de información, dicha tecnología no es óptima, y si lo que se quiere es estar a la vanguardia, se debe gestionar la adquisición de tecnología de última generación. Por último, un punto débil también representa el hecho de no contar con una zona de parqueo lo suficientemente grande como para abastecer a la totalidad de clientes que puede absorber la empresa. Esto, si bien representa una debilidad, su corrección implica un nivel elevado de inversión, por lo cual, su corrección debe orientarse al mediano y largo plazo.

Finalmente, la situación actual de pandemia por covid-19, representa una amenaza en las expectativas y consecuente ejecución de emprendimientos por parte de los clientes. Por lo cual, es necesario diseñar estrategias que permitan hacer frente a la situación, como podría ser, mejorar la gestión de la bioseguridad al interior de las instalaciones, de tal suerte que se garantice la integridad en la salud de los actuales y futuros potenciales clientes, lo cual tendrá efectos positivos en sus niveles de confianza en llevar a cabo sus emprendimientos al interior de Fasako S.A.

CAPITULO IV

RESULTADOS

4.1. PROCEDIMIENTOS METODOLÓGICOS

De acuerdo con la naturaleza del presente trabajo esta investigación será de tipo descriptiva-explicativa debido a que busca identificar y caracterizar las variables de estudio de la problemática tratada. La presente investigación será de tipo aplicada dado que busca implementar conocimientos adquiridos para mejorar procesos de la compañía FASAKO S.A. De acuerdo al tipo de información utilizada se trata de una investigación mixta, analizando datos como la estructura de red de la empresa, vulnerabilidad del sistema y monto de inversión para el SGSI. De acuerdo a la instancia de tiempo en el que se realiza la investigación es de tipo transversal dado que observará y registrará los datos en un momento específico. (Hernández Sampieri, Fernández Collado , & Baptista Lucio , 2014)

Por lo que respecta al diseño de la investigación corresponde a uno no experimental debido a que no buscará manipular deliberadamente las observaciones de las variables, es decir, los datos serán recolectados y analizados en su estado natural sin la interferencia o edición del investigador (Agudelo, Aigneren, & Ruiz, 2008).

Así mismo, se realizó un análisis de toda la infraestructura de red de la empresa usando técnicas y metodologías de Hacking Ético las cuales se dividen en 3 fases:

- Alcance
- Descubrimiento
- Análisis de vulnerabilidades

El escaneo de vulnerabilidad y la tasa de rendimiento en el consumo del ancho de banda se realizará con la herramienta Kali Linux. Los objetos o fenómenos analizados serán interpretados por el departamento de TIC, y serán presentados en reportes.

El análisis será realizado mediante la aplicación de MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), en donde se estudiarán las variables en relación con sus indicadores, lo que permitirá determinar los tipos de riesgos, el valor de operación de la empresa FASAKO S.A. y el nivel de impacto y protección durante el proceso de mejora continua de seguridad perimetral, todo esto en coordinación con los objetivos de la propuesta, lo cual permitirá presentar un plan de contingencia que satisfaga los propósitos del planteamiento con el nivel de riesgo.

Para la presentación de resultados, se aplicaron entrevistas a dos colaboradores del TI y a tres clientes de la empresa, de los cuales se buscó identificar aspectos relacionados con buenas prácticas empresariales y dominio en determinadas áreas asociadas a la gestión de la información. Adicional, para el desarrollo de la propuesta, se usaron gráficos de pastel y empleó la escala de Likert.

De acuerdo con las herramientas utilizadas, se tiene lo siguiente:

Revisión documental: Se revisó la información obtenida del análisis de vulnerabilidades como marco de referencia, obtenido directamente de los registros de la empresa.,

Entrevistas: se realizaron entrevistas abiertas a los empleados y socios responsables de los procesos internos de seguridad. Específicamente se entrevistó a

los miembros del departamento de IT y usuarios de la empresa. Las preguntas estuvieron enfocadas a diagnosticar vulnerabilidades, necesidades y características que posee el SGSI.

La población de estudio corresponde a los usuarios (internos y externos) de la empresa FASAKO S.A. Para llevar a cabo los objetivos planteados y aplicar los instrumentos mencionados se recurrirá a una muestra no probabilística conformada por:

- 30 usuarios externos (clientes) de la empresa FASAKO S.A
- Los 2 integrantes del departamento de IT de la empresa FASAKO S.A

Para la selección de la muestra de usuarios externos se realizó una selección a conveniencia de acuerdo a la disponibilidad de información y voluntad de participación en el estudio.

4.2 DIAGNÓSTICO

Para el diagnóstico de la “Gestión de la seguridad” de la empresa FASAKO S.A. se analizarían las siguientes dimensiones

4.2.1 GESTIÓN DE LOS SERVICIOS CRÍTICOS DE LA EMPRESA FASAKO S.A.

La actividad principal de la empresa FASAKO S.A. es la de brindar servicio empresarial denominado coworking (cotrabajo o trabajo en cooperación) es decir oficinas y recursos compartidos, de manera ininterrumpida hasta la actualidad, adoptando las nuevas tecnologías para satisfacer la demanda de sus clientes. Por lo que las funcionalidades de los servicios no deberían ser interrumpidos en horarios

operativos de las empresas que se encuentran trabajando en las infraestructuras de la compañía FASAKO S.A.

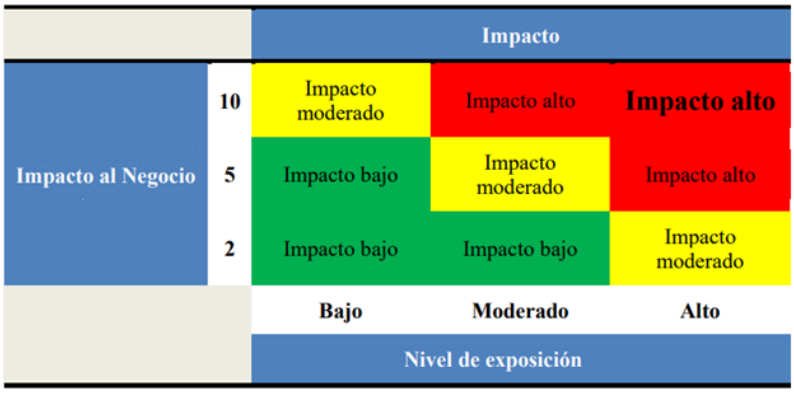
La integridad de los datos de las compañías que realizan sus actividades en las instalaciones de la empresa FASAKO S.A. depende de la buena gestión de la seguridad de la información siguiendo las normas internacionales de ISO 27000.

4.2.1.2 IDENTIFICACIÓN DE RIESGOS: AREAS VULNERABLES DE LA EMPRESA FASAKO S.A.

Mediante la identificación de los riesgos de los servicios críticos de la empresa FASAKO S.A. se considera el impacto que ocasionaría cualquier evento, con lo cual llegase a impedir el funcionamiento operativo y represente perdidas latentes a la compañía.

Se consideró la evaluación de la matriz de impacto de evaluación, la cual considera dos factores. El impacto del activo en las actividades de la empresa y el grado de vulnerabilidad

Figura 5. *Matriz de nivel de impacto*



Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

En la actualidad debido a que los sistemas informáticos se encuentran integrados en la mayoría de los procesos internos de las empresas, el riesgo de seguridad informática compromete todas las áreas de la organización. En el caso de la empresa FASAKO esta vulnerabilidad de se manifiesta en los siguientes aspectos:

Tabla 10. *Áreas que presentan información vulnerable, su grado de exposición y efectos en el negocio*

Area	Información vulnerable	Impacto en el negocio	Nivel de exposición	
Área administrativa	Información de nomina	5	Moderado	Impacto moderado
	Información de clientes (facturación, datos bancarios, información de contacto, servicios contratados)	10	Moderado	Impacto Alto
Área contable financiera	Registros contables de la empresa	5	Moderado	Impacto moderado
	Proyección presupuestaria	5	Moderado	Impacto moderado
	Información de acceso bancario	10	Bajo	Impacto Moderado
	Información de acceso a plataformas tributarias	5	Moderado	Impacto moderado
Área de sistemas y comunicación	Estructura de red de la compañía	5	Bajo	Impacto bajo
	Arquitectura de plataforma web	2	Bajo	Impacto bajo
	Información de acceso de los equipos físicos computacionales de las oficinas	10	Moderado	Impacto Alto
	Información de cuentas corporativas de colaboradores (comunicación interdepartamental)	10	Moderado	Impacto Alto

Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

4.2.1.3 ENTREVISTAS

Tabla 11. *Procedimiento de recolección de información*

Técnicas	**Procedimiento**
	¿Cuándo? Segunda semana de octubre de 2020
	¿Cómo? Se realizaron entrevistas a 2 operarios del departamento de TI, denominados; entrevistado 1 y entrevistado 2. También se entrevistó a 3 clientes; cliente 1, cliente 2 y cliente 3
Entrevista	¿Dónde? En las instalaciones de la empresa FASAKO S.A.
	¿Cuándo? Tercera semana de octubre de 2020

Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

4.2.1.3.1 ANÁLISIS DE LAS ENTREVISTAS

Por lo que respecta al estado de seguridad de la información al interior de la empresa FASAKO S.A. y sobre las expectativas de los clientes que hacen uso de los servicios de Coworking, se tiene lo siguiente:

Sobre la pregunta 1 que hace referencia a la posibilidad de haber recibido ataques cibernéticos por virus o intento de acceso a la información de la empresa por parte de terceros ajenos a la misma, los entrevistados de TI, al igual que los clientes, señalaron que dichos ataques no son frecuentes, sin embargo, no es menos cierto que

si los ha habido a nivel de todo el sistema de la empresa, lo cual es sumamente negativo, porque según manifestaron los TI, los obliga a detener sus actividades, mermando la eficiencia en la prestación de los servicios de la empresa. Por su parte, los clientes señalaron que esto también afecta a la continuidad de sus actividades cuando se presenta, generándoles pérdidas, por presencia de tiempos muertos, que son irrecuperables.

En este sentido, el entrevistado 1 del departamento de TI, señaló:

> *"En mis cuatros años de experiencia en la empresa, honestamente, no he sufrido de numerosos ataques cibernéticos, sin embargo, no es menos cierto que si los ha habido, y no sólo en el caso de mi equipo, sino a nivel de todo el sistema de la empresa, lo que ha ralentizado la realización de mis actividades, en inclusive, me ha hecho perder información útil, lo que, como imaginará, es sumamente frustrante."*

En relación con la pregunta 2, la cual se refirió a la frecuencia con la cual se han presentado dichos ataques durante el último año, los entrevistados coincidieron en que esta situación se ha presentado, al menos, entre cinco o seis veces, es decir, en promedio, una vez cada dos meses.

Sobre la pregunta 3, que pretendió verificar si la empresa actualmente consta con un sistema que permita identificar la presencia de amenazas referentes al intento de hacker su información, los clientes manifestaron desconocimiento al respecto, en tanto que, los entrevistados TI señalaron que actualmente la empresa no cuenta con un

sistema destinado al efecto, pero que está considerando implementar alguno, en este sentido el entrevistado TI 2 añadió:

> *"Conozco de intentos de parte de la gerencia de adquirir equipos que permitan mejorar la situación de seguridad de la red. Sobre todo, por las sugerencias que hemos hecho los encargados de la parte operativa, que somos los que, de alguna manera, recibimos de forma más cercana las quejas por parte de ciertos clientes. Sin embargo, aún no se han llevado a cabo dichas innovaciones."*

En relación con la pregunta 4, sobre el sistema operativo de preferencia respecto de la seguridad, los TI al igual que los clientes, manifestaron afinidad por el sistema Windows, aunque lo calificaron de necesario, pero no suficiente. En este sentido, el entrevistado 1 del departamento TI agregó:

> *"En lo personal, considero que Windows es un buen software para desempeñar mis actividades, aunque no está exento, obviamente, de ataques cibernéticos. Éste, a mi parecer, debe complementarse con un buen sistema de seguridad interna de la información."*

Por su parte, en respuesta a la pregunta 5 que buscó identificar la percepción de los entrevistados sobre la calidad de la actual tecnología de seguridad con que cuenta la empresa, hubo un consenso en que los servicios prestados son buenos, pero que la seguridad, a menudo, llega a mermar esa percepción de ventaja. Al respecto el entrevistado 2 del departamento TI indicó:

“Me parece que no es el óptimo, porque, si bien permite el bloqueo al acceso de ciertos virus, no es en todos los casos, y ha mostrado no ser lo suficientemente efectivo, particularmente, en hacer frente a amenazas relacionadas con la adquisición ilícita que hacen terceras personas a la información de la empresa. En ese sentido, yo lo considero medianamente bueno, y considero que, si está en manos de la empresa la capacidad de adquirir un sistema más seguro, sería lo ideal, no sólo para el equipo de personas que labora en la empresa, sino, sobre todo, para los clientes.”

Por lo que atañe a la pregunta 6, que hace alusión a la sugerencia de implementar un sistema de seguridad como posibilidad de aumentar la calidad de los servicios, los entrevistados manifestaron total aprobación, sobre todo, los clientes, los cuales manifestaron esto es imprescindible para desarrollar sus actividades con mayor confianza. En este sentido, el cliente 2, puntualizó:

“pienso que, si se implementa un mejor sistema de seguridad, no sufriríamos de caídas de sistema, eso sería ideal para nuestras actividades y creo que sería una relación ganar-ganar entre la empresa y nosotros que hacemos uso de las instalaciones.”

Así mismo, sobre la pregunta 7, que cuestionó de manera general si la presencia de inconvenientes en la red es común o sólo se da en casos fortuitos, los entrevistados, tanto TI como los clientes, señalaron que no es algo habitual, pero que cuando se presenta genera complicaciones tanto en trabajadores de la empresa como en los usuarios, por ende, se debe actuar lo antes posible por mejorar la calidad de la red.

En la misma línea de ideas, la pregunta 8 pretendió conocer la percepción, tanto de los entrevistados TI como de los clientes, respecto de la evaluación de la calidad de los servicios, en términos generales, que presta la empresa a sus clientes. Sobre esto, la respuesta de los entrevistados TI fue que, a excepción de los fallos de sistema, la calidad es buena. En tanto que los clientes manifestaron inconformidad. Sobre esto, el entrevistado TI 2 argumentó:

> *"Es una pregunta que, sin dudas, se relaciona con lo que dije anteriormente. No es frecuente, pero desde la perspectiva de los clientes, las consecuencias de fallos en la red perimetral, pienso que se sienten con más intensidad, ya que como cliente uno espera que no haya fallos, aún si no son muy frecuentes. En ese sentido, yo lo calificaría como bueno, pero podría ser más que sólo bueno."*

En lo referente a la pregunta 9, que pretendió conocer la percepción específicamente con relación al servicio de internet brindado por la empresa, los entrevistados manifestaron conformidad con el servicio. Particularmente, los clientes señalaron que es rápido y de calidad, pero que los problemas de seguridad de la red también suelen afectar a este servicio, aunque no es común. De esta manera, el cliente 1 agregó:

> *"Considero que el internet es bastante bueno. La empresa cuenta con internet de alta velocidad, y este sistema por lo menos, casi no falla. A excepción de situaciones atípicas, relacionadas con la seguridad, pero no es algo característico."*

Finalmente, por lo que respecta a la pregunta 10, que consideró sugerencias dirigidas a los directos de la empresa por parte de los entrevistados, sobre cómo mejorar los servicios prestados, hubo consenso en que es necesario mejorar la seguridad en el manejo de la información. En este sentido, el cliente 3 acotó:

> *"Bueno, considerando lo que he dicho previamente, mi sugerencia sería que considere la implementación de un mejor sistema de seguridad, ya que con este podría optimizar sus actividades, sin temor a sufrir paralizaciones producto de ataques cibernéticos o por intromisión de virus en la red.*

4.3 PROPUESTA DE MEJORA

Para mejorar los procesos de la empresa FASAKO S.A. se realizará un sondeo respecto a las características de la familia ISO 27000 en relación a los activos informáticos y áreas vulnerables de la empresa. Y se considerará como la implementación afectaría este impacto.

4.3.1 GESTION DE LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA FASAKO S.A.

4.3.1.1 CERTIFICACIÓN ISO 27001

La implementación de las normas ISO 27001 representarán mejoras en la gestión de seguridad de la empresa FASAKO. S.A. respecto a las ares vulnerables identificadas.

	Área administrativa		**Área contable**		**Área de sistemas**	
Característica	**Con ISO 27001**	**Sin ISO 27001**	**Con ISO 27001**	**Sin ISO 27001**	**Con ISO 27001**	**Sin ISO 27001**
Población de atacantes grande						

Capacidad de ejecución remota						
Necesidad de privilegios de administrador						
Automatización						

La presente tabla representa las áreas que fueron identificadas previamente como “áreas de riesgo”, a saber; administrativa, contable y de sistemas. Básicamente, se trata de un análisis comparativo entre las principales características del sistema de seguridad de red perimetral para cada una de las áreas, tomando en cuenta dos escenarios; el primero, que considera la aplicación de la norma ISO y el segundo que no toma en cuenta esta implementación, a modo de grupo de control.

La primera característica considerada fue “Población de atacantes grande” que se refiere al grado en que se presenta las amenazas al sistema de seguridad, si éstas son constantes o bajas, y esto se deberá evaluar con o sin la aplicación de la ISO 27001, con objeto de verificar las diferencias y la mejora con base en la innovación del sistema de seguridad. La segunda hace referencia a la “Capacidad de ejecución remota” es decir, la capacidad de respuesta del sistema ante la presencia de amenazas a la seguridad de la información interna. “La Necesidad de privilegios de administrador”, que se refiere al grado de autonomía que ofrece el sistema en cuanto a la capacidad de gestión. Y finalmente, la automatización que se refiere a la capacidad del sistema para detectar amenazas y eliminarlas de forma inmediata, por sí mismo.

4.3.1.2 BUENAS PRÁCTICAS: ISO 27002

Se dispone de las buenas prácticas y control de seguridad para cada activo informático de la empresa FASAKO S.A.

Controles Propuestos ISO/IEC 27002:2005	Área administrativa	Área contable	Área de sistemas
1. Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldos adecuada.			
2. Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.			
3. Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no divulgación que reflejan las necesidades de la organización para la protección de la información.			
4. Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de información			
5. Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.			

En cuanto a la realización de copias de respaldo para cada deportante será responsable de esta actividad el departamento de sistemas que almacenará hasta las últimas dos copias de respaldo de información. Este punto trata, básicamente, sobre una acción preventiva ante riesgos de colapso del sistema o hackeo de la información esencial de la empresa, la cual debe evitar que se pierda, para lo cual se debe prevenir

mediante la implementación de un sistema que guarde automáticamente por cada documento su respectiva copia de seguridad. Dicho sistema debe, además, someterse a pruebas con regularidad con objeto de evaluar su estado óptimo en todo momento.

Los procedimientos de operación de cada área deben ser establecidos y registrados por cada departamento, así como el correcto registro de actividades.

De forma contractual es responsabilidad del área administrativa (gestión de recursos humanos) establecer la norma de seguridad informática referente al compromiso de los colaboradores en mantener la confidencialidad de la información inherente a la empresa, así como el uso responsable de la misma y solo con el propósito de cumplir los objetivos organizacionales.

4.3.1.3 LINEAMIENTOS DE IMPLEMENTACIÓN: ISO 27003

La empresa FASAKO S.A. deberá diseñar una guía de implementación para un sistema de gestión de seguridad.

Esta guía deberá contener los siguientes pasos:

1. Definir el alcance y política del sistema de gestión de seguridad informática (SGSI).
    a. Definir procesos
    b. Definir responsables
2. Definir límites y organizacionales.
    a. Identificar estructura de la organización
    b. Describir los sistemas de gestión existentes
3. Realizar una evaluación de riesgos.

a. Identificar activos informáticos de la empresa y sus vulnerabilidades.

b. Por poner mecanismos de control

4. Obtener aprobación de la dirección para implementación

a. Generación de documentación

b. Desarrollo de sistemas

Para la empresa FASAKO S.A.

4.3.1.4 PLANTEAMIENTO DE ESTRATEGIAS DE RECUPERACIÓN DE LOS SERVICIOS CRÍTICOS DE LA EMPRESA FASAKO S.A.

El tipo de restauración que se usará para volver a tener operativos los equipos de infraestructura tecnológica en menos de 6 horas será el tipo de recuperación rápida, ya que se trabajaría en forma paralela con el actual equipo de seguridad perimetral de la infraestructura de red de la empresa FASAKO S.A. Esto como medida de plan de contingencia, de que algún evento medido en la gestión y análisis de riesgos llegase a activarse, así de esta manera se reduce el impacto de la amenaza.

Para esto se contarán con las siguientes estrategias de recuperación:

4.3.1.4.1 BACKUPS

La empresa FASAKO S.A. aplicara las siguientes políticas de realización de backups.

- Los backups serán de tipo snapshot de cada una de las máquinas virtuales
- Los respaldos se almacenarán en un sistema tipo cloud perteneciente a una cuenta propia del centro de procesamiento de datos

- Los backups se realizarán con una periodicidad de una semana los días viernes después de las 20:00,
- Se almacenarán siempre las últimas dos versiones anteriores de backups.

4.3.1.4.2 MONITOREO EN TIEMPO REAL

El monitoreo se ejecutará desde el lunes hasta sábado en un horario de 07:00 a 20:00. Se implementará un sistema de monitoreo que elaboré y envié un reporte del estado actual del centro de datos a los correos institucionales del equipo de IT. Para la acción inmediata ante incidentes se utilizará una herramienta de acceso remoto utilizando un VPN

4.3.1.4.3 CONTROL DE ACCESO

Se propone la implementación de un sistema de acceso biométrico ZKTeco que tenga registrado a todos los colaboradores y permita el registro del nombre, cargo, horario de acceso, información a la que se accedió para así mantener un control.

Se propone contar a su vez con un sistema de tarjetas magnéticas para el uso de usuarios invitados a quienes se registrarán los mismos datos al momento del acceso a la información.

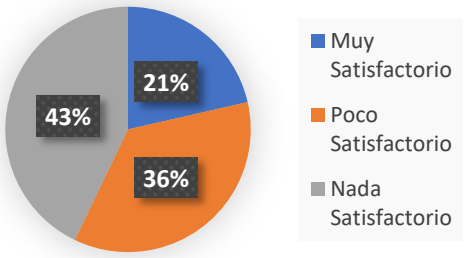
4.3.1.5 MATRIZ DE PROCESOS DE TI

En la matriz se muestra el resultado obtenido y su respectivo porcentaje, el cual fue calculado teniendo como base que 14 ítems representan el 100%.

Resumen Matriz De Procesos de TI

Calificación de riesgos	Item	Porcentajes
Muy Satisfactorio	3	21,00%
Poco Satisfactorio	5	36,00%
Nada Satisfactorio	6	43,00%

Figura 6. *Resumen Estadístico Matriz Procesos de TI*



Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

4.3.1.6 DIAGNÓSTICO DEL ESTADO DE LOS DOMINIOS

Luego del análisis del estado actual de cada dominio de la empresa FASAKO S.A. se presenta un resumen de los controles realizado para el diagnóstico de mejora según alcance el cual lo podemos observar en el anexo n°1.

4.4 MECANISMOS DE CONTROL

4.4.1 MÉTRICAS DE GESTIÓN: ISO 27004

La empresa FASAKO S.A. presenta el actual estatus de métricas de gestión de seguridad informática. A continuación, se exponen las métricas esperadas y las observaciones a modificar

Tabla 12 *Métricas FASAKO S.A.*

Control de la ISO 27004	**Medida esperada**	**Medida encontrada**	**Observaciones**
Inventario de activos informáticos	2 actualizaciones en el año	1	El software necesita mantenerse actualizado, se requiere una frecuencia bianual.
Políticas de control de acceso	1 política de cortafuegos	0	Carencia de política de cortafuegos.
Uso de información confidencial	4 cambios de contraseña en el año	1	Debido a la naturaleza de la empresa (coworking) se maneja información de agentes externos en los equipos por lo que se debe realizar un mayor seguimiento los medios de acceso
Procedimiento de acceso seguro	Existencia de perfiles de	Si	Se maneja correctamente

	usuario de la empresa		
Herramientas administradoras del sistema	Programas de antivirus (1) Presencia de programas institucionales de gestión (1) Conexión a tierra del edificio principal (1)	Si	La cantidad de programas de seguridad presentes en los equipos es adecuada, sin embargo existen falencias de actualización
Protección de equipos	Mantenimiento de equipos mensualmente	Mantenimiento trimestral.	Se debe realizar mantenimiento mensual para garantizar el estado óptimo de equipos y prever exposición de información
Copias de seguridad	1 copia semanalmente	1 copia cada 2 meses aprox.	Las copias de seguridad deben realizarse con mayor frecuencia. Almacenando las últimas dos versiones por departamento.

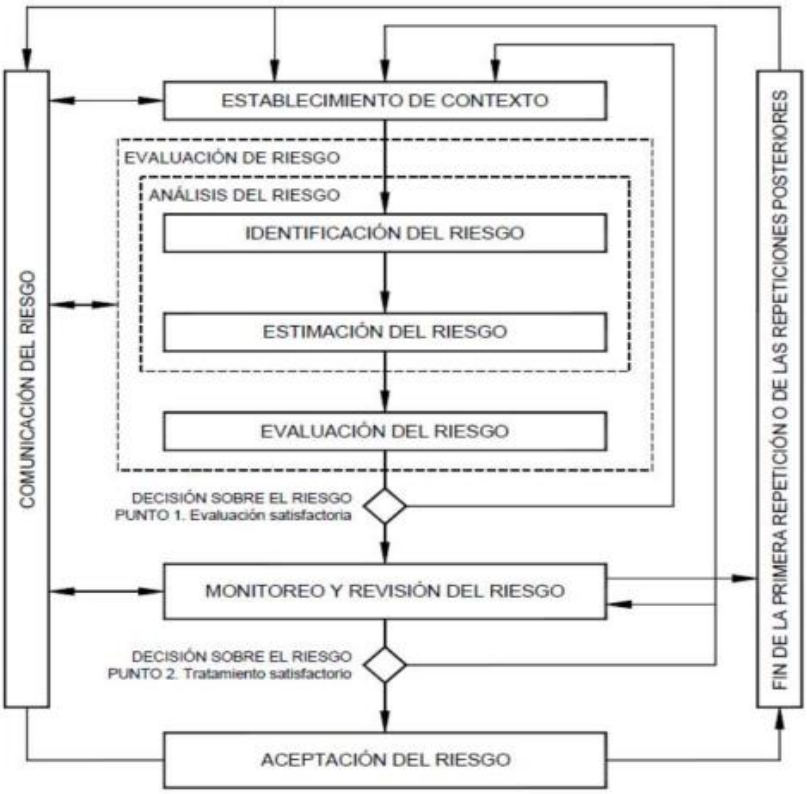
Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

4.4.2 Normativa: ISO 27005

Finalmente, la gestión administrativa de la seguridad informática de la empresa FASAKO S.A. debe responder al siguiente esquema propuesto:

Figura 7. Procesos de gestión de riesgo informático



Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

El esquema anterior representa el proceso que se deberá seguir por parte del equipo encargado de gestionar la seguridad del nuevo sistema a implementarse. Dicho esto, como se puede visualizar, consta de una serie de pasos interrelacionados. En primera instancia, ante una posible situación de riesgo informático, se deberá

contextualizar el problema. Es decir, identificar específicamente a qué área corresponde. Posteriormente, se deberá evaluar la magnitud del riesgo, es decir, cuáles son los posibles efectos o consecuencias que podría generar la amenaza; en esta etapa, será importante mensurar el daño con base en estimaciones, al tiempo que se realizan las evaluaciones sobre el mismo. Es decir, se trata de una etapa analítica, donde se busca evaluar minuciosamente la problemática a palear, ubicándolo en su contexto.

Posteriormente, se deberán aplicar las medidas correctivas con base en las normas de seguridad, en el marco de las Normas ISO que se planteó en la propuesta del presente trabajo. Luego de la aplicación de las medidas correctivas, se deberá realizar el respectivo monitoreo en torno a la medida adoptada y su efecto en la disminución del riesgo presentado. Finalmente, se deberá reportar la amenaza, a través de la comunicación efectiva, a todos los integrantes del sistema de seguridad, estableciendo un precedente y una manera de palear la amenaza ante una posterior aparición.

4.5. ESTIMACIÓN DE LA INVERSIÓN PARA LA IMPLEMENTACIÓN DE LA PROPUESTA

En el presente su apartado, se presenta la estimación de los costos de inversión, particularmente, referentes a la programación de las actividades que, en términos generales se destinarán a la implementación arquitectónica del nuevo sistema de seguridad perimetral que tendrá la empresa FASAKO S.A. Este presupuesto a su vez, tendrá que ser nuevamente revisado en la medida que el proyecto se vaya delimitando en la práctica, definiendo su alcance, el período que tomará la reparación con exactitud,

y los costos de las distintas actividades de ingeniería, con mayor profundidad. Así como la forma en que se vayan asignando los recursos que se destinarán al proyecto, en cada momento del tiempo. Adicionalmente, se requerirá revisar constantemente los precios de los equipos de hardware y software, ya que podrían existir posteriormente ofertas más asequibles y eficientes que las planteadas en el presupuesto estimado. En todo caso, el presupuesto estimado que se presenta a continuación, ha sido elaborado con base en criterios de eficiencia, considerando precios de mercado.

4.5.1. PRESUPUESTO ESTIMADO DE IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD PERIMETRAL

ACTIVIDAD	Total de H/H requeridas para la instauración del Sistema (por fase)	Costo por H/H	Costo por fase y total de la implementación del sistema
Diagnóstico de la situación actual	280	$20,00	$5.600,00
Planificación y control de la fase de implementación	400	$25,00	$10.000,00
Plan de tratamiento de riesgos	120	$30,00	$3.600,00
Formulación de indicadores de gestión de riesgos	200	$35,00	$7.000,00
Plan de implementación de migración de IPv4 a IPv6.	280	$18,00	$5.040,00
Plan de seguridad física	320	$25,00	$8.000,00
Plan de seguridad lógica	320	$28,00	$8.960,00
Instalación y puesta en marcha	560	$20,00	$11.200,00
Estimado del costo global de los elementos tecnológicos de seguridad perimetral [Hardware y software]	No aplica	No aplica	$60.350,00
COSTO GLOBAL ESTIMADO			**$119.750,00**

Elaborado por: (Núñez Noboa , José Vicente; Perdomo Córdova, 2020)

Fuente: Elaboración propia

En la presente tabla, se ha presupuestado la inversión que requerirá la implementación del sistema de seguridad perimetral, para lo cual se ha considerado, por una parte, la mano de obra cualificada para la actividad, cuya unidad se ha determinado en horas hombre, con las respectivas horas necesarias para cada una de las actividades (ordenadas por fase de implementación) y sus costos respectivos, determinado según los costos por hora de trabajo.

En ese sentido, para la fase de diagnóstico, se estimaron alrededor de siete técnicos especialistas en sistemas de seguridad de red, los cuales realizaron sus actividades en el lapso de una semana; considerando 40 horas de trabajo por semana, se requirieron un total de 280 horas, por el precio de $20,00 por hora, se estimaron costos por $5.600,00.

Posteriormente, para la ejecución de la fase de planificación y control de la fase de implementación, se requirió de, al menos, dos semanas de trabajo, para un total de cinco trabajadores en esta actividad, se estimaron costos por $10.000,00. Así mismo, para el plan de tratamiento de riesgos, se requirió de tres técnicos por un lapso de una semana de trabajo, es decir, 120 horas hombre, que representó $3.600. Por lo que corresponde a la formulación de indicadores de gestión de riesgos, se precisará de 5 cinco especialistas, en un lapso estimado de una semana, es decir, 200 horas de trabajo, lo que implica $7.000,00.

Así mismo, para las fases de implementación de los planes de seguridad, tanto físico como lógico, se requirió de siete y cuatro técnicos, respectivamente, los cuales realizaron sus actividades a lo largo de dos semanas, con un total de 600 horas de trabajo, lo que significó costos de inversión por cerca de $17.000. También, se requirió

de siete técnicos para la fase de instalación y puesta en marcha del sistema, con un total de las 560 horas de trabajo y costos de 11.200,00. Adicionalmente, el costo de inversión inicial bordeó los $120.000,00 considerando elementos tecnológicos de seguridad perimetral (Hardware y software) que se estimaron en algo más de $60.000,00, los cuales se requerirán para la implementación inicial del sistema de seguridad perimetral.

Por último, cabe señalar que en todas las actividades se considera la participación de los recursos necesarios tanto internos como de consultoría externa, expertos en seguridad informática, en normas de gestión de seguridad informática ISO 27000, en ITIL y en ingeniería de redes de informática.

CAPITULO V

CONCLUSIONES

La actual infraestructura de la empresa Fasako S.A. presenta factores de riesgo que deben ser controlados para una mejor gestión relativa a las actividades operativas de seguridad informática, entre los cuales destacan: reglas y filtros cortafuegos, por inexistencia de controles de acceso de nivel de red; acceso remoto, por la no utilización de VPN por parte de los colaboradores al acceder a la red interna; segmentación, debido a que la actual red está concentrada en un solo segmento y ausencia de un sistema de detección de intrusiones. Así también, se detectó riesgo operativo debido a la integración de los sistemas informáticos internos de la empresa, siendo los más representativos; área administrativa, área contable financiera y el área de sistemas de comunicación.

Para mejorar los procesos operativos de seguridad informática se planteó la ejecución de un sondeo respecto a las características de la familia ISO 27000 con relación a los activos informáticos y áreas vulnerables de la empresa. En tal sentido, se consideró en términos generales, la implementación de buenas prácticas y control de seguridad para cada activo informático de la empresa FASAKO S.A.

Con el propósito de controlar la buena gestión en el cumplimiento de la propuesta sugerida se diseñaron los siguientes mecanismos relacionados con el control de la ISO 27004: realización de al menos 2 actualizaciones en el año del inventario de activos informáticos; implementación de políticas de cortafuegos, mejorando el control del acceso a la red; realizar al menos 4 cambios de contraseña a nivel de todo el

sistema durante el año; crear perfiles de usuario de la empresa; implementar programas de antivirus y de gestión institucional; dar mantenimiento a los equipos mensualmente y generar al menos una copia de seguridad semanalmente. Finalmente, implementar la norma administrativa de gestión informativa ISO 27005.

Por último, se estimó el costo de la inversión inicial requerida para implementar el sistema de seguridad perimetral, mismo que fue de $119.750,00. Del cual, $59.400,00 se presupuestó para llevar a cabo seis fases sucesivas de implementación y $60.350,00 para la adquisición de hardware y software

ANEXOS

DIAGNOSTICO DEL ESTADO DE LOS DOMINIOS

Competencias								
Dominios	**Controles**	**Muy Satisfactorio**	**Poco**	**Nada**	**No Aplica**	**En Ejecución**	**Minima Ejecución**	**Ejecución Ideal**
Dominio 1 - Políticas de procesos de la información	2	0	2	0	0	50%	75%	100%
Dominio 2 - Seguridad de las comunicaciones	7	0	5	2	0	36%	75%	100%
Dominio 3 - Seguridad física y del entorno	6	3	2	1	0	67%	75%	100%
Dominio 4 - de gestión de continuidad del negocio	10	1	5	4	0	35%	75%	100%

Matriz De Diagnóstico

Estado	Descripción
Muy Satisfactorio	Se Aplica El Proceso Según Delineamientos Norma ISO 27001 SGSI. En Un 100%.
Poco Satisfactorio	Se Aplica El Proceso Según Delineamientos Norma ISO 27001 SGSI. En Un 50%.
Nada Satisfactorio	No Se Aplica Proceso Según Delineamientos Norma ISO 27001 SGSI. En Un 0%.

Matriz De Procesos de TI

Pregunta	Valoración	Recomendación
¿La empresa ejecuta procesos de análisis de vulnerabilidades, mantenimiento, Harding, mejora continua del actual sistema de gestión de riesgo de la información?	**Nada Satisfactorio**	Gestionar Análisis De Vulnerabilidades continuos.
¿La empresa desarrollo plan de proyecto, donde se Identifica prioridades dentro de los objetivos para la mejora continua en el actual sistema de gestión de riesgo de la información?	**Muy Satisfactorio**	
¿La empresa contó con la gerencia general para iniciar el proyecto de mejora del SGSI?	**Muy Satisfactorio**	
¿La empresa ha detallado las amenazas internos y externos que pueden perturbar el desarrollo de implementación del SGSI?	**Muy Satisfactorio**	
¿La empresa ha descrito a los interesados, estableciendo necesidades y expectativas según alcance del SGSI?	**Poco Satisfactorio**	Se debe detallar e identificar cuáles son las prioridades según necesidad por departamento en la implantación del Sistema de Gestión de riesgo de Información.
¿La empresa ha identificado objetivos a implementar en el SGSI?	**Poco Satisfactorio**	Se debe priorizar objetivos para la mejora en productividad con respecto al SGSI.
¿Los directivos de la empresa tienen claro el alcance y los límites del Sistema de Gestión de gestión de riesgo de la información?	**Poco Satisfactorio**	Documentar el alcance del SGSI.

¿La empresa ha documentado las políticas del SGSI, aprobado por la Gerencia de TIC's o la Gerencia general?	**Nada Satisfactorio**	Realizar la documentación pertinente que permita ejecutar políticas SGSI. según el marco legal debidamente socializado.
¿La empresa ha definido un manual de funciones según responsabilidad para cada miembro del departamento de TIC's?	**Poco Satisfactorio**	Se debe limitar roles y funciones para cada etapa de la Implementación SGSI.
¿La empresa ha definido indicadores de desempeño para mitigar los riesgos de la seguridad de la información?	**Poco Satisfactorio**	Se debe definir la metodología a seguir para la gestión de riesgos y describir en una matriz los resultados que apunten al SGSI.
¿La empresa ha documentado la aplicación de controles requeridos por la entidad?	**Nada Satisfactorio**	Se debe Crear documento de declaración de aplicabilidad de controles de la norma ISO 27001.
¿La empresa ha evaluado las aptitudes del personal que afecta el funcionamiento de la seguridad de la Información?	**Nada Satisfactorio**	Se debe conservar evidencia de las capacidades del personal del departamento de TIC's. para definir plan de capacitación que les permitan adquirir competencias respectivas.
¿La empresa ha establecido un proceso de comunicaciones en lo que se refiere al sistema de gestión de riesgo de la información?	**Nada Satisfactorio**	Se debe desarrollar informes que indique comunicación; fechas, involucrados, etc.
¿La empresa tiene documentación e informes referente al Sistema de Gestión de riesgo de la información?	**Nada Satisfactorio**	Todos los logs generada del SGSI debe estar debidamente documentada.

Seguridad De Las Comunicaciones

Anexo			**Estado**
A13	**Seguridad de las comunicaciones**		
A13.1	Gestión de la seguridad de las redes		
	Objetivo: Prevenir y Mitigar los posibles ataques externos e internos en el flujo de la información que concurre en la red de datos.		
A13.1.1	Controles de redes	Control: Gestión y filtrado de páginas, aplicaciones y servicios.	No cumple
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los servicios que deben estar disponibles según necesidad por usuarios y dependencias.	No cumple
A13.1.3	Separación en las redes	Control: Direccionamiento VLSM, segmentación de redes tipos multicast.	No cumple

Seguridad física y del entorno

Anexo			**Estado**
A11.2	**Equipos**		
	Objetivo: Prevenir, mitigar, daño, robo, y la interrupción de las operaciones de la empresa.		
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar asegurados en su ubicación.	Cumple satisfactoriamente
A11.2.2	Servicios de suministro	Control: Las tomas deben estar polarizadas y conectados al sistema de redundancia de energía.	Cumple parcialmente
A11.2.3	Seguridad en el cableado.	Control: debe existir cableado estructurado de voz y dato así como el tendido eléctrico debe cumplir las normas técnicas para evitar ruido e interferencias	Cumple parcialmente

		electromagnéticas.	
A11.2.4	Mantenimiento preventivo correctivo.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Cumple satisfactoriamente
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	No cumple
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	No cumple
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	Cumple satisfactoriamente
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Cumple parcialmente
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	Cumple parcialmente
A12.3	Copias de respaldo		
	Objetivo: Proteger contra la perdida de datos		
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Cumple satisfactoriamente

Aspectos de gestión de continuidad del negocio

Anexo			Estado
A17	**Aspectos de gestión de continuidad del negocio**		
A17.1	Continuidad de Seguridad de la información		
	Objetivo: Para la continuidad del negocio deben aplicarse procesos y metodologías de seguridad de la información y comunicación organización.		
A17.1.1	Planificación para la continuidad del core del negocio	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	No cumple
A17.1.2	Implementación para la continuidad del core del negocio	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	No cumple
A17.1.3	Monitoreo y verificación para la continuidad del negocio	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	No cumple
A17.2	Redundancias		
	Objetivo: Asegurar la disponibilidad del internet hacia los clientes, así como las demás herramientas de tecnología en la comunicación.		

A17.2.1	Disponibilidad de equipos	Control: Las implementaciones tecnológicas deben permitir redundancia y escalabilidad y puesta en marcha en tiempos cortos.	Cumple parcialmente

FORMATO DE ENTREVISTA

GUÍA DE ENTREVISTA
OBJETIVO: Determinar el estado de seguridad de la información al interior de la empresa FASAKO S.A.
SUJETO DE ESTUDIO: EMPRESA FASAKO S.A.
GIRO DE NEGOCIO: Prestación de Servicios de coworking en la ciudad de Guayaquil-Ecuador.
ENTREVISTADO:
CARGO QUE OCUPA:
ENTREVISTADOR: Jaime Eduardo Perdomo Córdova y José Vicente Núñez Noboa
FECHA Y HORA DE ENTREVISTA:
1. En relación a sus labores diarias, ¿Ha sido víctima de alguna forma de ataque informático, ya sea por la presencia de virus o por usuarios ajenos a la actividad de la empresa?
2. ¿Con qué frecuencia durante el último año de labores ha detectado la presencia de virus en el equipo informático a su disposición?

3. **¿Dispone actualmente la empresa de un sistema que permita identificar la presencia de amenazas referentes al intento de acceso a la información confidencial de la institución?**
4. **¿Qué sistema operativo considera usted que brinda mayor seguridad en la ejecución de sus tareas diarias?**
5. **¿Cómo considera usted al sistema actual de seguridad con que cuenta la empresa FASAKO S.A.?**
6. **¿Considera que a través de aplicación de un sistema que optimice la seguridad informática en la red sea posible incrementar la calidad de los servicios ofrecidos por FASAKO S.A.?**
7. **¿Es habitual que se presenten inconvenientes en la red o sólo se da en casos fortuitos?**
8. **¿Cómo calificaría usted a la calidad de los servicios que presta la institución a sus clientes?**
9. **¿Qué opinión le merece la calidad del servicio de internet brindado por FASAKO S.A.?**
10. **¿Qué sugerencia haría usted a la empresa para mejorar la calidad de los servicios que brinda?**

VALIDEZ DE CONTENIDO

Para la evaluación de la validez de contenido del instrumento utilizado (entrevista) se utilizó la metodología de Hernández Nieto denominada “Coeficiente de validez de contenido”.

ESCALA DE VALORES																
1= Aceptable 2= Deficiente 3=Regular 4=Bueno 5= Excelente																
CONTENIDO		EVALUACIÓN														
		JUEZ 1					**JUEZ 2**					**JUEZ 3**				
ÍTEM	**INDICADORES GENERALES**	**1**	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
1	COHERENCIA					x					x				x	
	CLARIDAD					x					x					x
	ESCALA				x						x					x
	RELEVANCIA					x					x				x	
2	COHERENCIA					x					x					x
	CLARIDAD					x					x					x
	ESCALA					x					x				x	
	RELEVANCIA					x					x					x
3	COHERENCIA					x					x					x
	CLARIDAD				x						x				x	
	ESCALA				x					x					x	
	RELEVANCIA					x					x					x
4	COHERENCIA					x					x					x
	CLARIDAD					x					x					x
	ESCALA				x					x						x
	RELEVANCIA					x					x					x
5	COHERENCIA					x					x				x	
	CLARIDAD					x					x					x
	ESCALA					x					x					x
	RELEVANCIA					x					x					x
6	COHERENCIA					x					x					x

	CLARIDAD					x					x				x	
	ESCALA				x						x				x	
	RELEVANCIA					x					x					x
7	COHERENCIA					x					x					x
	CLARIDAD					x					x					x
	ESCALA					x					x				x	
	RELEVANCIA					x					x					x
8	COHERENCIA					x					x					x
	CLARIDAD				x					x						x
	ESCALA					x				x						x
	RELEVANCIA					x					x					x
9	COHERENCIA					x					x					x
	CLARIDAD					x					x					x
	ESCALA				x						x					x
	RELEVANCIA					x					x				x	
10	COHERENCIA					x					x					x
	CLARIDAD					x					x					x
	ESCALA					x					x					x
	RELEVANCIA					x					x					x

Fuente: *Elaboración propia, a partir de la metodología del Coeficiente de validez de contenido de Hernández Nieto (2002).* (Pedrosa , Suárez Álvarez, & García Cueto, 2014)

Ítem	**Juez 1**	**Juez 2**	**Juez 3**	**Sxi**	**Mx**	**CVCi**	**Pei**	**CVCti**
ítem 01	19	20	18	57	2,85	0,95	0,04	0,91
Ítem 02	20	20	19	59	2,95	0,98	0,04	0,95
ítem 03	18	19	18	55	2,89	0,96	0,04	0,93
Ítem 04	19	19	20	58	2,90	0,97	0,04	0,93
ítem 05	20	20	19	59	2,95	0,98	0,04	0,95
Ítem 06	19	20	18	57	2,85	0,95	0,04	0,91
ítem 07	20	20	19	59	2,95	0,98	0,04	0,95
Ítem 08	19	18	20	57	2,85	0,95	0,04	0,91
ítem 09	19	20	19	58	2,90	0,97	0,04	0,93
ítem 10	20	20	20	60	3,00	1,00	0,04	0,96
							Ind. Validez	**0,93**

Donde;

Sxi =Sumatoria de los puntajes asignados por cada juez J a cada uno de los ítems “i”

Mx=Cociente entre el valor de Sxi y el valor máximo de la escala utilizada por los jueces

Pei = probabilidad del error por cada ítem (probabilidad de concordancia aleatoria entre los jueces

J = Número de jueces asignando puntajes a cada ítem.

CVCti= Coeficiente de validez de contenido total de cada ítem

Análisis:

Como se puede visualizar en la tabla el CVC total promedio para los 10 ítems considerados en el estudio fue de 0,93 mayor que 0,90 valor que indica validez y concordancia excelentes.

BIBLIOGRAFÍA

Di Iorio, A., & Castellote, M. (2017). *El rastro digital del delit.* Mar del Plata: Universidad FASTA Ediciones.

Bermùdez, K., & Bailón, E. (2015). . Analisis en Seguridad Informática y Seguridad de la Información basado en la norma ISO/IEC 27001-Sistema de Gestion de Seguridad de la Información dirigo a una empresa en servicios financieros.

Bustamante, F. (2013). Sistema de gestión en seguridad basado en la norma OHSAS 18001 para la empresa Constructora Eléctrica IELCO (Master's thesis).

Catoira, F. (24 de Julio de 2012). *WeliveSecurity*. Obtenido de https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

Cervantinos, C. E. (2018). *Centro Estudios Cervantinos*. Obtenido de https://www.centroestudioscervantinos.es/tipos-de-investigacion-y-caracteristicas/#5_Explicativa

Díaz, A. (19 de 01 de 2017). *Data business Intelligence*. Obtenido de https://dbibyhavas.io/es/blog/que-son-los-logs/

Flores, V. (2016). Diseño de un sistema de gestión de la seguridad de la información para la unidad de gestión educativa local-Chiclayo. *INGENIERÍA: Ciencia, Tecnología e Innovación,*, 3(1), 42-57.

Guaman, J. (2015). Diseño de un sistema de gestión de seguridad de la informacion para instituciones militares.

Guevara, R. (2017). Sistema de Gestión de Seguridad de la información basado en la Norma ISO/IEC 27001 para el Departamento de Tecnologías de la Información y Comunicación del Distrito 18D01 de Educación.

Hernández Sampieri, R., Fernández Collado , C., & Baptista Lucio , M. (2014). *Metodología de la Investigación.* México D.F.: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V. Obtenido de https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

https://cybersecurity.att.com/. (18 de 03 de 2020). *https://cybersecurity.att.com/*. Obtenido de https://cybersecurity.att.com/: https://cybersecurity.att.com/

Lisot. (14 de 05 de 2018). *Tu empresa de mantenimiento informático*. Obtenido de https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/

mikrotik. (18 de 03 de 2020). *https://mikrotik.com/product/RB3011UiAS-RM.* Obtenido de https://mikrotik.com/product/RB3011UiAS-RM: https://mikrotik.com/product/RB3011UiAS-RM

nelly. (2020). *Solo Ejemplos*. Obtenido de https://www.soloejemplos.com/ejemplos-de-justificacion-teorica-practica-y-metodologica/

NETGEAR. (28 de 11 de 2016). *NETGEAR*. Obtenido de https://kb.netgear.com/224/What-is-a-firewall

Núñez Noboa , J. V., & Perdomo Córdova, J. E. (2020). Proyecto de Investigación. Guayaquil, Guayas, Ecuador.

OBS. (2020). *OBS Business School*. Obtenido de https://obsbusiness.school/es/blog-investigacion/propiedad-intelectual-y-seguridad-de-la-informacion/seguridad-informatica-definicion

Ovhcloud. (2020). *Ovhcloud*. Obtenido de https://www.ovh.com/world/es/anti-ddos/principio-anti-ddos.xml

Pedrosa , I., Suárez Álvarez, J., & García Cueto, E. (2014). Evidencias Sobre la Validez de Contenido: Avances Teóricos y Métodos para su Estimación. *Acción Psicológica, 10*(2), 3-20. Obtenido de http://scielo.isciii.es/pdf/acp/v10n2/02monografico2.pdf

Significados. (10 de 12 de 2019). *Tipos de investigación*. Obtenido de https://www.significados.com/tipos-de-investigacion/

SUPERCIAS. (25 de 12 de 2020). *Superintendencia de Compañías, Valores y Seguros*. Obtenido de Ranking Empresarial: https://appscvs.supercias.gob.ec/rankingCias/

TORI, C. (2008). *Hacking Etico.* Buenos Aires: Mastroianni.

VEGAGESTIÓN. (06 de 02 de 2018). *La infraestructura tecnológica: definición, tipos e importancia*. Obtenido de https://vegagestion.es/la-infraestructura-tecnologica-definicion-tipos-e-importancia/

Xperts, Academy. (2015). *Introducción a MikroTik RouterOS & RouterBOARD .* Guayaqyuil: Network Xperts S.A. .

Yáñez Cáceres, N. (2017). Sistema de gestión de seguridad de la información para la Subsecretaría de Economía y empresas de menor tamaño.