UNIVERSIDAD CATÓLICA DE NUEVA ESPAÑA

Seguridad Informática Para Redes Empresariales En Las Pymes De La Ciudad De Guayaquil – Ecuador

Presentada por: Zoila Nelly Franco Castañeda

Para optar el grado de:

Doctor of Business Administration in Christian Business Administration

Tutor:

Dr. **Ernesché Rodríguez Asien**

Catholic University of New Spain

Julio 2023

AGRADECIMIENTO

A Dios, por ser mi fortaleza en este proceso de aprendizaje continuo.

A mi familia “Los Francolines” que siempre han estado brindándome su apoyo moral y emocional para culminar con éxito este nuevo logro profesional.

A mis AMIGOS mi otra familia que forma parte de mi vida y me motivan día a día a avanzar por los senderos del éxito con disciplina y responsabilidad.

A mi Tutor por su guía en el desarrollo y culminación del presente trabajo de investigación.

DEDICATORIA

A Dios, por darme bendiciones cada día y por permitirme observar las bellezas de su creación

A mis Padres, mis ángeles celestiales y guardianes que han sembrado en mí su espíritu de superación y amor.

Para ellos este nuevo trabajo de investigación que es la consolidación de este mejoramiento continuo como persona y profesional.

Tabla de Contenido

Índice de Tablas

Tabla de Figura

UNIVERSIDAD CATÓLICA DE NUEVA ESPAÑA

Repositorio – ficha de registro de tesis doctoral

Título: Seguridad Informática Para Redes Empresariales En Las Pymes De La Ciudad De Guayaquil – Ecuador.

Autor: Zoila Nelly Franco Castañeda

Tutor: Dr. Ernesché Rodriguez Asien

Institución: Catholic University of New Spain

Título obtenido: Doctor of Business Administration

Líneas de investigación y ámbitos de estudio: Administración y valoración de proyectos

Palabras claves: Seguridad informática, Redes empresariales, almacenamiento de datos, información para Pymes.

Resumen/Abstract:

En el presente trabajo de investigación se presentan las perspectivas teóricas y un análisis profundo de los modelos de aseguramiento de la información para las pequeñas y medianas empresas de la ciudad de guayaquil. Se analizan los antecedentes teóricos que comprueban la necesidad que tienen las Pymes para asegurar su activo intangible como es la información financiera administrativa o todo lo que se desarrolla dentro de la empresa. Se analizan las principales teorías sobre los modelos de aseguramiento de la información, las estructuras de redes, software y las capacidades que deben tener las personas encargadas de desarrollo, ingreso y cuidado de la información. A través de la metodología empleada se recopila la información por medio de una encuesta la cual permite determinar el nivel de seguridad que presentan actualmente las empresas determinando aspectos como tipo de equipos, softwares empleados, tipos de seguridad, capacidades del personal y controles para el aseguramiento de la información. Se muestran los resultados obtenidos y se determinan cuáles son sus principales falencias proponiendo un modelo sencillo para solucionar las mismas; se finaliza con la presentación de los aportes teóricos del trabajo además de las limitaciones conclusiones y recomendaciones.

In the present research work, the theoretical perspectives and an in-depth analysis of the information assurance models for small and medium-sized companies in the city of Guayaquil are presented. The theoretical background that proves the need for SMEs to ensure their intangible assets such as administrative financial information or everything that is developed within the company is analyzed. The main theories on information assurance models, network structures, software and the capacities that people in charge of development, entry and care of information must have are analyzed. Through the methodology used, the information is collected through a survey which allows us to determine the level of security that companies currently present, determining aspects such as type of equipment, software used, types of security, personnel capacities and controls for the information assurance. The results obtained are shown and the characteristics of their main shortcomings are determined, proposing a simple model to solve them; It ends with the presentation of the theoretical contributions of the work in addition to the limitations, conclusions and recommendations.

Adjunto PDF: Si Contacto

autor: timmygarcia@gmail.com

Contacto institución: admissions@ucne.org

INTRODUCCIÓN

La información se ha trasformado en un recurso imprescindible a nivel empresarial, es la que permite el acceso a los mercados a las grandes, medianas y pequeñas empresas, esta permite el acceso a recursos necesarios para el establecimiento o creación de compañías, a desarrollarse o crecer en los mercados y el acceso a recursos financieros necesarios para una expansión, por ello la importancia de asegurar la información es fundamental para las instituciones. (Vargas & Cristancho, 2018)

Con el proceso de globalización los países se ven en la obligación de una integración donde esté presente el intercambio constante de información en aspectos socioeconómicos, es decir en los ámbitos políticos, económicos, sociales e incluso culturales estén a disposición del mundo, que esta permita a cada ser humano una mejor toma de decisiones en los ámbitos antes mencionados. Basado en ello la información ha pasado a ser un elemento clave en todo tipo de transacciones, por ende, esta debe garantizar a sus usuarios seguridad, confiabilidad, transparencia, y un fácil acceso, basados en lenguajes universales que permita una correcta interrelación con sus usuarios. (Acuña, 2017)

Con lo antes mencionado podemos notar la importancia del manejo de la información ya no solo como registros para consultas poco frecuentes, sino para poder incursionar en el medio empresarial y ser confiable ante la sociedad y el mundo, hay que recordar que ya no hay empresa pequeña en un mundo globalizado, donde la tecnología y en especial la internet permite que desde cualquier parte del mundo se puedan desarrollar transacciones comerciales.

Según sostiene la firma de consultoría internacional Price Waterhouse Coopers (más conocida como PwC) en su informe anual, a medida que aumenta la dependencia de la sociedad y las organizaciones respecto de los datos y la interconectividad, el desarrollo de la capacidad de hacer frente a los incidentes cibernéticos se vuelve cada vez más importante (Encuesta

Mundial sobre el Estado de la Seguridad de la Información, 2017).

De aquí surge la interrogante para las empresas que tan necesario es el aseguramiento de la información, en especial de aquella que les permita la integración comercial, si deben estar prestos para una inversión en este rubro, más aún, al tomar conocimiento de cómo van evolucionando los riesgos no solo de perdida de información, sino además de los riesgos que se presentan por el mal uso que le pueden dar a estas personas ajenas a las empresas si tiene fáciles accesos a las mismas. Sin embargo, tal como señala el reporte desarrollado por la Information Systems Audit and Control Association (en adelante, ISACA3), a pesar de que el presupuesto que las empresas destinan al ámbito de la seguridad informática este indicador aumenta anualmente, su ratio de crecimiento se reduce año a año (State of Cyber Security, 2017).

Para Leal (2021) la información se la debe considerar un activo relevante para las empresas por lo cual, se debe proteger con el objetivo de aprovecharla en operaciones en las cuales puedan presentar problemas informáticos de tal forma que no se pierda el control sobre la misma; determina la importancia de emplear buenas prácticas para el aseguramiento informático en las pequeñas y medianas empresas, donde se pueda contar con un activo intangible que garantice, la protección, la reputación y supervivencia de la información de estas; Al implementar procesos de protección de la información también se da orden a otros procesos de control en las diferentes áreas quienes deben cumplir con el ingreso y verificación de la información diaria que se requiere para su protección, con ello se crearan políticas, procedimientos y los controles antes mencionados, y con ello disminuir riesgo constante por el que transitan para las empresas al momento de manejar su información.

El asecho de los ciberdelincuentes es permanente, viniendo muchas veces desde aquellos que tienen algún tipo de trato con las pymes, en Guayaquil, así como en otras ciudades del Ecuador, el robo de bases de datos para ser vendida a otras empresas o incluso ser utilizada

para crear otros delitos ha creado conciencia respecto a la necesidad de implementar la ciberseguridad.

Así mismo, las pequeñas y medianas empresas, sociedades y compañías empiezan a tener conciencia de la enorme importancia que tiene el poseer unos sistemas de seguridad de la información adecuados, así como una correcta gestión de estos. De esta forma, pese a que muchas empresas todavía asumen el riesgo de prescindir de las medidas de protección adecuadas, a nivel mundial muchas empresas aumentan sus presupuestos en ciberseguridad para prevenir los ciberataques a estas problemáticas e intentan protegerse de acuerdo con sus posibilidades y los medios con que cuentan, así mismo hay empresas sobre todo pequeñas que les cuesta hacer conciencia sobre la ciberseguridad y lo ven como un gasto más. (Zuña, Arce, & Romero, 2019)

Otro aspecto de importancia es que las empresas sean públicas o privadas desarrollen valorizaciones de riesgos en sus áreas informáticas para contrastar con el costo beneficio que significará implementarlos usando herramientas como la microsegmentación, analítica avanzada y la inteligencia artificial según las necesidades y recursos de cada organización, además se debe complementar el uso de estas herramientas de seguridad de información con el establecimiento de políticas, procesos y modelos que aborden el tema de seguridad de manera integral para mitigar el impacto que genera la perdida y fuga de información y la resiliencia para superar situaciones traumáticas que se puedan generar. (Innovación en la sociedad digital, 2021)

Es importante recalcar además, que para el aseguramiento de la información de las PYMES, se deben establecer nuevas prioridades de la gestión de la administración, que ella pueda constar con una metodología de análisis de riesgos adecuada a la empresa (Instituto Nacional de Seguridad, 2018); y con ello obtener beneficios como tales como dirigir y gestionar adecuadamente sus evaluaciones de riesgos, tomar decisiones basada en estos, proteger los

activos de información y, por último, comunicar de forma efectiva la información clave de seguridad los cuales se derivan de las siguientes características: en primera medida, se establecen equipos auto dirigidos dentro de la organización con la finalidad de dar solución a las necesidades de seguridad que esta puede tener.

Se deben considerar y analizar el impacto que tienen las tecnologías digitales en la economía y en la sociedad, se conoce que existen diversos marcos conceptuales que revisan o tratan de dimensionar los mecanismos que componen este fenómeno (Bukht & Heeks, 2017). Entre los modelos se encuentran los que están direccionados al segmento empresarial, considerando una relación directa entre la información empresarial con base en la relación que tienen las empresas con la tecnología para no solo facilitar el ingreso y procesamiento de la información, sino también el aseguramiento de la misma; haya que considerar que estas tecnologías a nivel empresarial se dividen en tres segmentos, el primero es para las empresas de servicios de telecomunicaciones y tecnología de información (núcleo TI), el segundo las empresas de aplicación de tecnologías digitales o economía digital tales como las apps, plataformas, etc., en tercer lugar las empresas de sectores tradicionales entre ellas las PYMES (CEPAL, 2021).

En Ecuador en el año 2021, se aprobó la primera Política de Ciberseguridad, la misma fue registrada en el Acuerdo Ministerial 006-2021, y se reconoció “que los interesados deben fortalecer sus capacidades para identificar, gestionar, tratar y mitigar los riesgos de ciberseguridad” (Maino, 2021); desde entonces, una serie de delitos e incidentes cibernéticos a nivel nacionales han permitido reconocer el riesgo constante por el que pasan las instituciones sin importar el giro del negocio, que resulta necesario reevaluar constantemente la seguridad en relación a los delitos que se generan con estos medios delictivos, y con este acuerdo ministerial las partes interesadas aprovechen las oportunidades actuales y futuras en los que se refiera a la cuarta revolución industrial.

Asi como Ecuador se preocupa del aseguramiento de la información en general, hay que recordar que la información contable y financiera se encuentra regulada por un marco normativo (ley 1314 de 2009), con el que se regula no solo la veracidad sino también la ejecución y calidad de los informes del aseguramiento financiero, los cuales también cuenta con una guía, principios, conceptos, técnicas, que permiten generar interpretaciones a través de dicha norma; por la importancia del aseguramiento de esta información resulta imprescindible para las pequeñas y medianas empresas la implementación de medidas que aseguren su información vulnerable, que no solo ocasiona perdida de esta, sino retraso en sus actividades, problemas al ser auditada o incremento en pagos de multas e impuestos por presentar información incompleta herrada o a destiempo. (Chávez & Loaiza, 2018)

Las pymes al igual que el resto de las organizaciones en Guayaquil, están seriamente expuestas a los nuevos delitos informáticos que vienen en incremento, que se presenta con alto nivel de riesgo y probabilidad de ocurrencia, este ciberdelito no solo puede ocasionar las pérdidas de la información, sino que además daños económicos e inclusos legales para las empresas. Por ello la importancia que deben dar las instituciones debe estar reflejada en el presupuesto asignado para el cuidado y aseguramiento de la información que evite los ataques e incidentes cibernéticos que se están generando a nivel global. Con el presente trabajo se pretende presentar estrategias de seguridad de acuerdo con las necesidades de las pequeñas y medianas empresas para luego elaborar y usar políticas, procesos, procedimiento, así como las herramientas, software en línea que ayuden a adoptar y cumplir esas estrategias, que van desde la gestión de dispositivos, monitoreo, respuesta a incidentes, bajo el marco de la ciberseguridad.

Planteamiento del Problema

Formulación del Problema

¿Como un modelo de aseguramiento de la información empresarial permitirá salvaguardar el activo intangible de las pequeñas y medianas empresas de la ciudad de

Guayaquil?

Sistematización del Problema

a. ¿Cómo los modelos de aseguramiento de la información empresarial van a permitir salvaguardas el activo intangible de las empresas?
b. ¿Cuáles son los modelos informáticos que se emplean para el aseguramiento de la información empresaria en las pequeñas y medianas empresas de la ciudad de Guayaquil?
c. ¿Como un modelo de aseguramiento de la información empresarial permite salvaguardar el activo intangible en las pequeñas y medianas empresas de la ciudad de Guayaquil?

Si bien las grandes instituciones u organizaciones se están preocupando por el desarrollo de sistemas que protegen sus activos intangibles como lo es la información general y financiera de estas, estas instituciones van aportando con software que les permiten a las empresas en menor tamaño tener una base para la implementación de las estrategias y programas que estas implantan, la pequeñas y medianas empresas de la ciudad de guayaquil no solo no cuentan con un presupuesto para el aseguramiento de la información, sino que además no tienen dichos procesos, protocolos o software que los ayude con el cuidado de está.

Estas empresas en muchas ocasiones solo cuentan con programas que les permiten el ingreso y el procesamiento de datos para generar los informes que este requiere para la toma de decisiones y para el cumplimiento con los entes de control reguladores.

Objetivos

Este proyecto de investigación busca concientizar a las empresas la importancia del aseguramiento de la información, no solo por el riesgo existente de los factores externos sino también por los factores internos como la fuga de información, exterior e incluso distorsión de

esta que ocasiona pérdidas económicas.

Objetivo General:

Determinar la importancia de un modelo de aseguramiento de la información empresarial que permita salvaguardar su activo intangible en las pequeñas y medianas empresas de la ciudad de Guayaquil.

Objetivos Específicos

Por lo antes mencionado se determinan los siguientes objetivos específicos:

a) Analizar los modelos de aseguramiento de la información empresarial que permitan salvaguardas el activo intangible**.**
b) Determinar los modelos informáticos empleados para el aseguramiento de la información empresaria en las pequeñas y medianas empresas de la ciudad de Guayaquil
c) Determinar modelo de aseguramiento de la información empresarial que permita salvaguardar su activo intangible en las pequeñas y medianas empresas de la ciudad de Guayaquil.

Hipótesis

Con la implementación de un modelo del aseguramiento de la información en las PYMEs de la ciudad de Guayaquil les permite salvaguardar sus activos intangibles.

Un modelo de aseguramiento de la información busca que, para el caso de Guayaquil, se logre estandarizar las distintas prácticas en el ejercicio de la contabilidad, auditoria, tributaria y demás información relacionada al área financiera y teniendo en cuenta que en el panorama actual las múltiples actividades económicas se realizan sobre la premisa de la globalización y el mercado mundial, basado en la información

La seguridad informática para redes empresariales en las pymes es un tema muy importante en la actualidad debido al aumento del número de amenazas informáticas y ciberataques que afectan a las empresas. A continuación, te presento algunas novedades científicas recientes en este campo.

Seguridad en la nube: la mayoría de las empresas utilizan servicios de computación en la nube para almacenar y procesar datos. La seguridad en la nube se ha convertido en una prioridad para muchas PYMEs y los proveedores de servicios en la nube están mejorando constantemente sus medidas de seguridad para proteger los datos de los clientes.

Metodología

El objetivo de esta investigación es determinar la importancia de la seguridad de la información y los modelos de gestión que contribuyen de manera efectiva a la protección de la información contable, financiera y otros aspectos críticos para las pequeñas y medianas empresas en la ciudad de Guayaquil.

Para lograr esto, se utilizará un enfoque no experimental que no interferirá con las variables analizadas ni alterará el objeto de estudio. En su lugar, se emplearán estadísticas obtenidas de bases de datos empresariales para medir la percepción de los empresarios respecto a posibles pérdidas o mal uso de la información empresarial. (Hernández, 2014)

Este aplicará un estudio de bibliográfico, los datos que se solicitaran a través de las diferentes herramientas a utilizar, se obtendrá información a través de las bases de datos empresariales e información pública que brinda el gobierno sobre diferentes aspectos empresariales, además, a través de formularios se solicitaran la información que requiere la investigación. (Cajal, 2019)

Se utilizará un enfoque mixto que combina métodos cuantitativos y cualitativos para abordar un problema de investigación simultáneo. Este enfoque permite un proceso de investigación sistemático, empírico y crítico que integra tanto la visión objetiva de la

investigación cuantitativa como la subjetiva de la investigación cualitativa para responder al problema en cuestión. Además, el análisis será transversal y correlacional, y se requerirá el uso de datos mixtos para lograr una comprensión más profunda del objeto o fenómeno de estudio. (Otero, 2018)

Para llevar a cabo este trabajo, se requiere el uso de diversas herramientas estadísticas y tecnológicas que permitan medir y analizar los datos con mayor precisión. Es por eso por lo que se aplicará un enfoque cuantitativo, el cual no solo facilita la operatividad de las variables, sino que también permite obtener resultados más precisos. (López et al, 2015).

Es importante tener en cuenta la realización de un estudio transversal, el cual se encuadra dentro de la categoría de investigaciones observacionales. Este tipo de estudio nos permite recolectar información de una población, muestra, conjunto o subconjunto, en un período de tiempo específico (Hernández, 2014). Asimismo, se puede considerar como un estudio exploratorio debido a que no se ha abordado de manera exhaustiva un tema en particular, como lo es la importancia del aseguramiento de la información de forma específica la información empresarial (contable, financiera, de ventas, etc.), y determinar los modelos que se emplean en la actualidad.

Si se utilizan herramientas estadísticas para identificar las conexiones entre las variables independientes y dependientes, se puede clasificar la investigación como predictiva. Esto se debe a que el objetivo es no solo describir la relación entre las variables, sino también comprender las razones detrás de esa relación. Al aplicar este enfoque, se podría analizar cómo los modelos de aseguramiento de la información garantizan que las pequeñas y medianas empresas no sufran pérdidas económicas por el mal uso de estas o la perdida de estas. (Fernández, 2016).

En cuanto a la modalidad de Investigación Para llevar a cabo la investigación actual, se requiere realizar un estudio de bibliográfico-analítico con enfoque cuantitativo, tal como se

indicó previamente. Para ello, es esencial obtener información directamente de las bases de datos de entidades estatales como, INEC, Cámara de Comercio, Encuestas empresariales del gobierno nacional. El sector sobre el cual se centrará será las pequeñas y medianas empresas de la ciudad de Guayaquil, para determinar la situación actual del manejo de la información y conocer los medios o métodos informáticos que manejan para el aseguramiento de la información.

Se emplearán distintas herramientas como la observación, las bases de datos, las y las encuestas para obtener la información requerida de las empresas de la ciudad de Guayaquil. Asimismo, se llevarán a cabo análisis estadísticos descriptivos y correlacionales, incluyendo el uso del coeficiente alfa de Cronbach para evaluar la confiabilidad de la escala de preguntas de una prueba y la correlación para medir la relación entre dos variables. Estos análisis serán de gran ayuda para responder la hipótesis planteada y lograr los objetivos de la investigación mediante la recopilación de información necesaria.

Se empleará un enfoque cuantitativo en este trabajo de investigación, ya que es necesario verificar las hipótesis planteadas y lograr los objetivos establecidos. Según Hernández (2014, págs. 5-6), este enfoque permite la recolección y análisis de información para responder preguntas de investigación y comprobar hipótesis mediante la aplicación de técnicas estadísticas, especialmente inferenciales.

La estadística permite el análisis mediante el conteo, las frecuencias, correlaciones y análisis probabilístico, lo que puede generar estándares de comportamiento para una población o muestra.

Se planea utilizar dos tipos de fuentes de información para la recopilación de datos. Estas fuentes son: fuentes primarias y fuentes secundarias:

Las fuentes primarias se obtendrán a través de la encuesta o entrevista directa dirigidas al personal administrativo de las pequeñas y medianas empresas de la ciudad de

Guayaquil. Se recopilará información sobre sus equipos, software, manejo de información, personal capacitado, medios de seguridad, entre otros aspectos. (Carpio, 2018).

Por otro lado, se considerarán fuentes secundarias a los manuales de funciones y procesos existentes, que permitan a cada empleado cumplir con sus actividades asignadas de manera correcta, así como a los manuales que respalden cada actividad y permitan determinar responsabilidades y responsables. También se revisarán las políticas generales y demás documentos necesarios para el buen funcionamiento de las instituciones. (Hernández, 2014)

Se requieren dos métodos para recolectar la información. En primer lugar, se llevará a cabo el levantamiento de información de las principales bases de datos empresariales para conocer la situaciones generales y económicas de las empresas, además se realizará una encuesta dirigida a las pequeñas y medianas empresas dirigida a directores y administradores de estas. gracias al volumen de información, se puede recopilar en un corto período de tiempo. Por último, se llevará a cabo una observación documental sobre de los problemas que ha generado el no aseguramiento de la información empresarial.

Tal como se indicó previamente, esta herramienta resulta especialmente útil cuando se requiere recopilar información en grandes cantidades, ya sea en poblaciones o muestras de gran tamaño, y especialmente si los recursos disponibles para la actividad son limitados, ya sea en términos de tiempo o de presupuesto. En estos casos, se podría utilizar un cuestionario compuesto por preguntas cerradas, las cuales podrían ser validadas mediante una escala de tipo Likert y desarrolladas a través de medios digitales. Este cuestionario estaría dirigido directores y administradores de las pequeñas y medianas empresas de la ciudad de Guayaquil. (López et al, 2015).

Para ello se cuenta con las bases de datos de las principales instituciones gubernamentales como empresarial las cuales son de dominio público, y aportaron a esta investigación la información necesaria para conocer las estructuras de las empresas, número

de empleados tipos de contabilidad e importancia que estas le dan al manejo de su información y aseguramiento de esta a través de sus activos.

A continuación, se presenta el desarrollo del trabaja de investigación el cual esta divida en tres capítulos:

En el capítulo uno se mostrará un amplio marco teórico de las variables analizadas partiendo del aseguramiento de la información financiera, los antecedentes teóricos de la problemática y estudios relacionados a estas, los controles y sistemas utilizados por las pequeñas y medianas industrias, los modelos de aseguramientos y tipos procesos que garanticen el aseguramiento de la información.

En el capítulo dos se analizará el marco teórico sobre sistema de información y clasificación empresarial, además, se analizarán los Estándares y Normas Para Asegurar La Información, a través de las ISO 27000 en sus diferentes versiones. Por otro lado, se revisas las funciones, actividades y rol que tiene el departamento de información con relación al cuido de la misma, la importancia del respaldo de esta y las seguridades que se deben emplear, finalmente un marco conceptual que aclare algunos términos empleados en el teórico.

En el capítulo tres se indicará la metodología a emplear para el levantamiento de la información que nos permita analizar el comportamiento de las pequeñas y medianas empresas en cuanto a la administración y cuidado del activo intangible como es la información empresarial, se analizan los resultados de la encuesta desarrollada la cual se basa en once preguntas que ayuden a analizar lo antes mencionado. Se muestran también el aporte teórico del estudio, las limitaciones presentadas en el desarrollo, las conclusiones y lecciones aprendidas.

Capítulo 1: Aseguramiento de la Información Financiera

1.1. Antecedentes

De acuerdo con el estudio desarrollado por Armenia, Angelini, & Nonino (2021), la necesidad de evaluar los riesgos de ciberseguridad y planificar inversiones efectivas se vuelve más importante debido a la creciente cantidad de amenazas en el ciberespacio. Para la gestión de riesgos de ciberseguridad, un marco reconocido internacionalmente es el de NIST, que proporciona pautas, mejores prácticas y estándares. Sin embargo, este y otros marcos de autoevaluación producen una visión estática de la postura cibernética de una organización y no capturan la dinámica de los cambios organizacionales y los ataques cibernéticos. Esto se vuelve aún más crítico para las pequeñas y medianas empresas (PYME), ya que necesitan administrar su ciberseguridad, pero generalmente no están lo suficientemente capacitadas o equipadas para internalizar este proceso. Por lo tanto, se necesita un modelo práctico y fácil de aplicar para identificar un perfil de riesgo de ciberseguridad y su dinámica.

El estudio propone una metodología y una herramienta de dinámica de sistemas (SMECRA) para respaldar las decisiones de inversión en ciberseguridad para las PYME. SMECRA aborda la complejidad organizativa dinámica y se puede utilizar para evaluar los riesgos cibernéticos y las dinámicas relacionadas a lo largo del tiempo. Tres estudios de caso demuestran su capacidad para evaluar el estado de seguridad cibernética de una PYME y evaluar los impactos de las inversiones en el perfil de riesgo de una organización, aumentando la conciencia de seguridad cibernética. Este estudio es importante tanto para las PYME que deseen gestionar su propio riesgo de ciberseguridad como para las compañías de seguros que deseen evaluar los riesgos residuales que las PYME deseen externalizar.

En el estudio relacionando con la información y la informática desarrollados por (Romero, Figueroa, & Vera, 2018), son cruciales para el funcionamiento de las organizaciones y empresas. Hay varias amenazas que pueden afectar negativamente la

seguridad de los sistemas, como virus, malware, cibercriminales, spyware y otras. Con el aumento del uso de dispositivos móviles conectados a internet, se ha vuelto aún más importante proteger la seguridad de los sistemas. El objetivo principal de este libro es proporcionar información sobre la seguridad informática y los diferentes mecanismos de prevención que se pueden utilizar para evitar las amenazas. Este libro está dirigido a estudiantes de informática, profesionales de seguridad y docentes que están interesados en la seguridad informática. Los diferentes capítulos del libro provisto conocimientos sobre los fundamentos de la ciberseguridad, los riesgos, las amenazas y las vulnerabilidades que se pueden encontrar en una organización y cómo aumentarlas. También se discuten diferentes metodologías para el análisis de vulnerabilidades, detección, escaneos y soluciones de remediación. El capítulo final detalla un ejemplo de auditoría de seguridad para detectar vulnerabilidades en una red de datos, y también se aborda la importancia de la defensa en profundidad y la concienciación de los usuarios sobre las políticas de seguridad de la empresa.

Mientras que para los investigadores Pooja, Gupta, Chang, & Nedjah, (2021), Los avances en la nanotecnología han impulsado la tecnología IoT, que es fundamental para muchas pequeñas y medianas empresas. La evolución de los dispositivos inteligentes ha generado una gran cantidad de datos, conocidos como Big data, que se pueden analizar para obtener información valiosa y útil para la organización. Sin embargo, dado que esta información puede contener datos confidenciales, es un objetivo atractivo para los ataques de los ciberdelincuentes, como el ataque XSS, que permite a los atacantes acceder a la información personal del usuario.

Por esta razón, se ha desarrollado un enfoque para detectar ataques XSS en la red IoT con el objetivo de proteger la privacidad de los datos. Este enfoque utiliza una red neuronal de convolución (CNN) para detectar la carga útil del ataque XSS después de aplicar ciertos

métodos de preparación de datos. Con este enfoque, se espera prevenir violaciones de la privacidad y fortalecer el vínculo entre las empresas y sus usuarios. Los resultados experimentales revelaron que el enfoque logró una precisión de detección del 99% después de la ejecución exitosa de los métodos de preparación de datos.

Las pequeñas y medianas empresas son las que más contribuyen a la economía a nivel mundial, requieren la mayoría de las oportunidades de empleo y una gran parte del PIB en las economías desarrolladas. Sin embargo, son las más vulnerables a las amenazas cibernéticas y sufren graves consecuencias en caso de un ataque exitoso. Por esta razón, se ha llevado a cabo una encuesta de investigación con la participación voluntaria de ciento quince PYMES para entender los desafíos a los que se enfrentan en la implementación de controles de ciberseguridad. Los autores también propondrán una solución recomendada para las PYMES a través de un análisis de las entradas y los conceptos básicos de la ciberseguridad.

En el estudio realizado por Guy Lloyd (2020), normalmente se examina la seguridad cibernética en términos de violaciones de datos, sanciones regulatorias y perturbaciones en las operaciones empresariales, pero rara vez se destacan sus beneficios. En realidad, una seguridad cibernética efectiva permite a las empresas innovar y generar ingresos, beneficios y crecimiento. Además, la protección contra el ciberdelito puede generar beneficios reales para las pequeñas y medianas empresas (PYME) y resultar en organizaciones más valiosas. Aunque a menudo se asocia la seguridad cibernética con violaciones de datos, multas regulatorias e interrupciones de las operaciones, también hay ventajas significativas. Según una encuesta de Hiscox en 2019, el 55% de las empresas británicas sufrió un ataque cibernético ese año, en comparación con el 40% en 2018.

Guy Lloyd de CySure sostiene que la innovación empresarial, el aumento de los ingresos, las ganancias y el crecimiento depende de la seguridad cibernética efectiva. Las pequeñas y medianas empresas pueden obtener beneficios genuinos al defenderse contra el

delito cibernético. Además, a medida que las organizaciones de cualquier tamaño buscan mejorar la eficiencia a través de la digitalización, es crucial que los líderes empresariales reconsideren su mentalidad sobre la seguridad, según el experto en ciberseguridad

En el trabajo desarrollado por Ynzunza, Izar, & Bocarando (2017), El proceso de transformación digital implica cambios significativos en entidades, universidades, público y empleados, lo que conlleva la creación de nuevos modelos de negocio y prácticas comerciales. Esta transformación se logra a través del uso efectivo de la web en diferentes áreas como el diseño, la fabricación, el marketing, la venta y la promoción, lo que genera un modelo de gestión orientado a datos que mejora los procesos y aumenta las capacidades de las empresas. Las tecnologías digitales, como los teléfonos inteligentes, la computación en la nube, el big data, la inteligencia artificial, la robótica, el Internet de las cosas, la impresión 3D, la virtualización, la ciberseguridad y los sistemas de sensores, entre otros, se utilizan ampliamente en muchos entornos económicos y sociales. Las pequeñas y medianas empresas (PYMEs), que representan el 99,83% del total de empresas, el 72,7% del empleo total, el 50,6% del valor añadido total y el 55,1% de las exportaciones desempeñan un papel crucial en la economía. Para seguir siendo competitivas, es fundamental que estas empresas transformen sus estructuras organizacionales y culturas empresariales, La comprensión y adopción de tecnologías digitales es crucial para que las PYMES logren una transformación digital productiva en su proceso de fabricación. Es importante que las empresas realicen análisis de costo-beneficio para determinar qué tecnologías son adecuadas para sus necesidades. Este documento ofrece una visión integral de los factores que surgen el proceso de transformación digital y describe cómo se ha llevado a cabo en el sector manufacturero en Turquía. También se explican los programas y software que las PYMES pueden utilizar para llevar a cabo su transformación digital y profundizar de ella. Los estudios empíricos sobre las PYMES muestran que estas empresas a menudo tienen un comportamiento errático en

términos de información y de inversión en tecnologías de la comunicación (TIC).

El incremento en el uso de la tecnología en las compañías trae consigo tanto ventajas como desventajas, ya que la vulnerabilidad de la ciberseguridad se ha vuelto un problema en el proceso de digitalización. Esto es preocupante, especialmente en la actualidad, ya que los datos se consideran muy valiosos y están expuestos a riesgos cada vez mayores. Un ejemplo de la importancia de la seguridad en línea es el ataque cibernético global de mayo de 2017, que afectó a más de 230.000 ordenadores en todo el mundo. Desde entonces, los ataques a empresas han sido cada vez más comunes, no solo por parte de agentes externos sino también por parte de empleados internos. Es importante tener en cuenta que la mayoría de los ciberataques tienen como motivación la obtención de ganancias económicas, sin importar el tipo de empresa que se vea afectado (Mendivil, Borja, & Gutierrez, 2022). La obtención de beneficios económicos es el principal motivo detrás de la mayoría de los ciberataques, representando aproximadamente el 86% de ellos. Es importante destacar que los atacantes no hacen distinción entre las empresas que son víctimas de estos ataques.

De acuerdo con Leiva, Mantilla, & Córdoba (2022), Debido a la pandemia, Costa Rica ha experimentado un aumento en el estado de cibercrimen, según señala Roberto Lemaitre. En su comentario, se hace referencia a un aumento en los ataques cibernéticos en varios frentes, tales como un 9% en ataques a aplicaciones móviles, un 18% en ataques a aplicaciones web, un 7% en denegación de servicios, un 9% en fuga de información y un 29% en estafas, como la ingeniería social o phishing, que incluye las llamadas telefónicas para obtener información confidencial. Además, se menciona que los virus troyanos representan un 26% y otros tipos de ataques constituyen un 2%. Las pequeñas y medianas empresas (PYMES) también se ven afectadas por los ciberataques, como señala José Rosell, socio-director de S2 grupo, indicando que el 74% de las PYMES han sufrido problemas de seguridad en algún momento.” (Marques, 2021).

1.2. Aseguramiento de la Información

En la actualidad, debido a los estándares internacionales y a las exigencias normativas en el país, las empresas de diferentes tamaños -pequeñas, medianas y grandes- necesitan realizar un seguimiento detallado de sus procesos contables. Es fundamental asegurar la precisión de la información financiera para obtener resultados de alta calidad. Por lo tanto, para abordar este tema en profundidad en el capítulo de y marco teórico, se llevó a cabo una revisión bibliográfica exhaustiva que se centró en teorías pertinentes a la importancia del aseguramiento de unos de los activos intangibles como es la información (Chávez & Loaiza, 2018)

Para el autor Vargas, Cristancho & Méndez (2019), La globalización se enfoca en unir a todas las naciones mediante un intercambio constante de aspectos sociales, culturales, políticos y económicos. Como resultado, la información se ha vuelto un factor crucial en la interacción entre culturas, y, por lo tanto, se ha requerido la búsqueda de medidas que aseguren su confiabilidad, transparencia, seguridad y accesibilidad para establecer un lenguaje universal que fortalezca las relaciones entre los países. En la práctica, el proceso de globalización se ha consolidado principalmente en el ámbito económico, y ha tenido una gran importancia en las relaciones entre los mercados y las naciones. La información se ha vuelto un elemento relevante en la toma de decisiones tanto para los mercados como para los gobiernos a nivel mundial.

> *"El sistema compuesto por principios, conceptos, técnicas, interpretaciones y guías, que regulan las calidades personales, el comportamiento, la ejecución del trabajo y los informes de un trabajo de aseguramiento de información. Tales normas se componen de normas éticas, normas de control de calidad de los trabajos, normas de auditoría de información financiera histórica, normas de revisión de información*

> *financiera histórica y normas de aseguramiento de información distinta de la anterior*." (Molina, 2019).

La utilización de diferentes marcos de referencia puede ayudar a las pequeñas empresas a crear protocolos de seguridad más sólidos. Uno de los marcos de referencia de seguridad más importantes a nivel mundial es el NIST Cybersecurity Framework, el cual se utiliza como guía en esta investigación. Propuesto por el Instituto Nacional de Estándares y Tecnología (NIST), este marco de referencia proporciona un lenguaje común para comprender, gestionar y expresar los riesgos de ciberseguridad para las partes interesadas. Es capaz de identificar y priorizar tareas para reducir el riesgo de ataques a la ciberseguridad de una empresa. Una característica destacada es su capacidad para ser implementada en diferentes áreas de la empresa y utilizada por distintos tipos de organizaciones, ya que se adapta a cualquier entidad. (Leiva, Mantilla, & Córdoba, 2022).

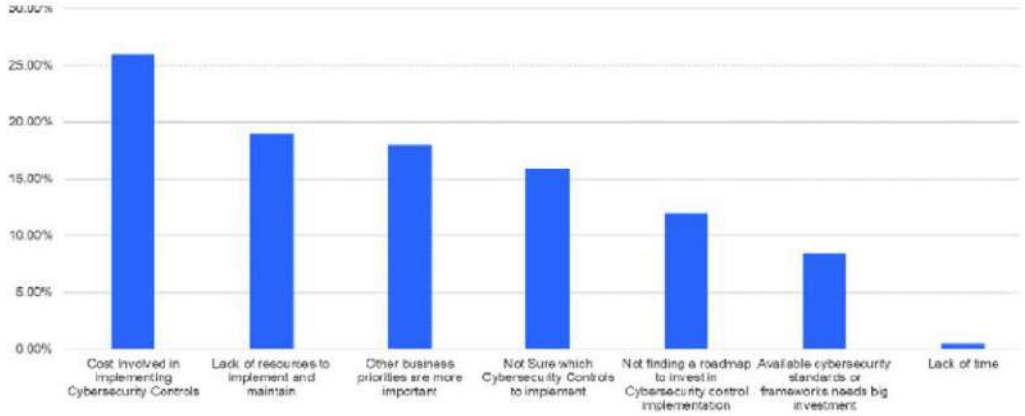
El NIST Framework divide su enfoque de ciberseguridad en 5 etapas que pueden ser utilizadas para implementar soluciones de seguridad informática. La primera etapa es la Protección, la cual implica la aplicación de controles técnicos, políticas y procesos para reducir los riesgos y proteger los activos de la organización. La segunda etapa es la Detección, que se enfoca en controlar y monitorear para identificar eventos de ciberseguridad oportunamente. La tercera etapa es la Identificación, que busca comprender el contexto y conocer los activos y amenazas existentes para administrar el riesgo de ciberseguridad. La cuarta etapa es la Recuperación, que se encarga de mantener planos de resiliencia y restaurar capacidades o servicios afectados en un incidente. Finalmente, la quinta etapa es la Responder, donde se espera se cumplan con actividades para la toma de medidas cuando se generen incidentes relacionados a la ciberseguridad que se detecten, y que permitan soportar el impacto de una amenaza potencial. (Almagro, 2019)

1.2.1. Las PYMES y los controles de ciberseguridad

El primer paso de cualquier viaje siempre es de gran importancia. El ámbito de la ciberseguridad es amplio para cualquier organización y contar con controles relacionados sólidos puede ayudarles a exigir un presupuesto adecuado, considerándolo como una inversión y destinando los recursos necesarios para cumplir con ello. En la mayoría de los estándares de ciberseguridad, se plantea una adopción completa o nula, sin un enfoque gradual que pueda brindar confianza a los inversores. Según la Figura. 1, las pequeñas y medianas empresas (pymes) sienten que tienen problemas y una falta de recursos, seguidos por otras prioridades comerciales importantes en comparación con la implementación de la seguridad cibernética. Al observar estos tres principales problemas, queda claro que las pymes no perciben que invertir en una postura de seguridad cibernética les ayudará a alcanzar los objetivos comerciales. También se evidencia una falta de conocimiento, incapacidad para encontrar una guía paso a paso para invertir en la implementación de los controles de ciberseguridad y desconocimiento de los estándares y marcos disponibles que requieren mayores inversiones, lo cual representa obstáculos adicionales que dificultan avanzar en la implementación de los controles de ciberseguridad. Cabe destacar que el tiempo necesario para implementar los controles generales de ciberseguridad se percibe como una preocupación final para las pymes.

Figura 1

Los mayores problemas que enfrentan las pymes al implementar o decidir/planear implementar controles de ciberseguridad



Los ataques cibernéticos realizados con software malicioso son conocidos comúnmente como "ataques de malware". Algunos ejemplos comunes de malware incluyen virus informáticos, gusanos, troyanos, adware, publicidad maliciosa y programas espía.

Cuando los delincuentes cibernéticos diseñan mensajes fraudulentos con la intención de engañar a personas de cualquier organización, se denomina ataque de phishing. Estos mensajes suelen enviarse a direcciones de correo electrónico e incluyen archivos adjuntos maliciosos o enlaces a sitios web peligrosos. Los hackers intentan manipular psicológicamente a las víctimas al mostrar una atención urgente hacia una acción específica mencionada en el correo electrónico. En muchos casos, incluso se envían archivos maliciosos, como currículums, a las direcciones de correo electrónico de recursos humanos de la organización, ya que se considera una posible vulnerabilidad para futuras actividades de piratería. Los ataques de phishing se llevan a cabo como campañas utilizando bases de datos filtradas de información de contacto, pero se pueden mitigar mediante la concientización sobre la seguridad cibernética y la implementación de controles de ciberseguridad. (Batra & Jain, 2021)

Además, existen otras formas de protección, como algoritmos y técnicas capaces de detectar correos electrónicos no deseados, lo que puede prevenir la mayoría de los ataques de phishing. En ocasiones, el informante puede ser un empleado, un proveedor asociado con la

organización o cualquier otra parte interesada, y a menudo tiene acceso a activos importantes dentro del entorno. Estas amenazas internas se han vuelto más evidentes en muchos ciberataques recientes. Si bien los dispositivos propiedad de la organización, como computadoras de escritorio o portátiles, pueden tener los controles necesarios implementados, los dispositivos de propiedad privada, como teléfonos inteligentes o computadoras portátiles, que son utilizados por empleados, partes interesadas, proveedores, invitados o visitantes, representan una gran amenaza. Por lo tanto, es necesaria una política de "Trae tu propio dispositivo (BYOD)" para lidiar con estos dispositivos privados. Implementar medidas de seguridad en estos dispositivos privados puede ayudar a reducir las amenazas internas. (Bang & Lee, 2012)

1.2.2. Seguridad en los Controles Físicos en las PYMES

La efectividad de los controles técnicos o físicos puede mejorarse mediante políticas, directrices y procedimientos que funcionen como controles administrativos, estableciendo así una sólida barrera de ciberseguridad para proteger los activos críticos de una organización. Estos conceptos se representan visualmente en la Figura 2, la cual resalta áreas clave responsables de los ataques cibernéticos a los que las pequeñas y medianas empresas (PYMES) son especialmente vulnerables.

Durante el resumen de la encuesta, los autores recibieron una serie de comentarios que resaltaban la necesidad de que las PYMES contaran con medidas sencillas para implementar la ciberseguridad, con el fin de satisfacer sus necesidades de seguridad, protección y prevención de robos de datos, entre otros. Fue sorprendente pero valioso conocer el estado actual de implementación del control de ciberseguridad, ya que esto reveló un alto grado de exposición al riesgo cibernético y los principales desafíos que enfrentan las PYMES al planificar e implementar controles de ciberseguridad.

Los resultados son especialmente importantes para comprender la brecha existente

entre los estándares o marcos de ciberseguridad disponibles y su adopción para lograr una sólida postura de ciberseguridad en las PYMES. Esta brecha identificada también explica por qué muchas PYMES están expuestas a diversas amenazas cibernéticas. En las secciones siguientes, los autores profundizarán en cómo cerrar estas brechas.

Figura 2

Panorama de ciber amenazas al que se enfrentan las PYMES

1.2.3. Revisión de los conceptos básicos de ciberseguridad

Durante más de cuatro décadas, la tríada de la CIA ha sido un factor clave para el éxito de los diseños de seguridad. No es sorprendente que siga siendo igualmente valiosa en el futuro a largo plazo.

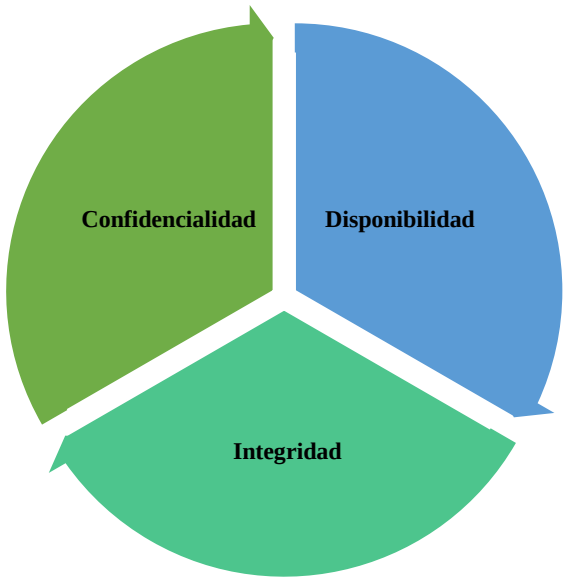
Los principios adicionales de la literatura sociotécnica de seguridad pueden seguir siendo satisfechos mediante la tríada de la CIA. Por ejemplo, la autenticidad, el no repudio, la responsabilidad y la ética pueden ser alcanzados a través de la integridad en la tríada CIA. La corrección en la especificación se logra mediante la integridad y la disponibilidad. La confianza se alcanza a través de la confidencialidad y la integridad. Además, la gestión de identidad puede ser lograda por los tres elementos de la tríada CIA. Durante los últimos 50 años, se han utilizado modelos de seguridad clásicos como Bell-LaPadula, Biba y Clarke

Wilson para representar la seguridad. (Samonas & Coss, 2014)

El modelo de seguridad de Bell-LaPadula se enfoca en mantener la confidencialidad y contribuir a la seguridad, el modelo Biba se centra en aumentar la integridad, y el modelo de seguridad de Clarke Wilson es un enfoque avanzado que ayuda a mantener la integridad en una transacción bien formada. Todos estos modelos se desarrollan con la tríada CIA como base. No se puede cumplir ninguno de los modelos de seguridad sin la tríada de la CIA. Además, si una organización intenta cumplir con uno de los aspectos de la tríada de la CIA, automáticamente estará contribuyendo al menos en una pequeña parte a los otros dos, ya que se superponen, como se muestra en la Figura 3.

Figura 3

Panorama de ciber amenazas al que se enfrentan las PYMES



Nota; International Journal of Information Management Data Insights (2022)

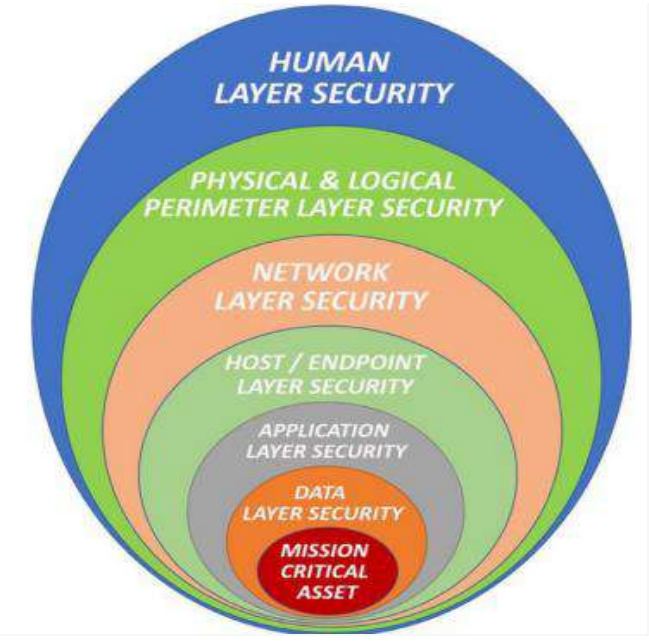
Más tarde, varias industrias adoptaron este modelo conceptual, incluso enfoques de ciberseguridad en capas. En la era digital, la Defensa en Profundidad (DiD) se refiere a una

estrategia integral de implementación de ciberseguridad en múltiples capas, como se muestra en la figura 4. Estas capas representan diferentes estados en los que los datos o la información pueden encontrarse, como datos en reposo, en tránsito o en uso.

El objetivo de cada capa es fortalecer la seguridad de una organización al reducir las vulnerabilidades que pueden dar lugar a amenazas cibernéticas. Esto ayuda a disminuir el riesgo de ataques cibernéticos exitosos. Si un ciberdelincuente logra vulnerar la seguridad de una capa, encontrará mayores dificultades para llevar a cabo prácticas poco éticas, ya que superar la siguiente capa se convertirá en otro desafío y así sucesivamente.

Figura 4

Diferentes capas consideradas en el concepto de defensa en profundidad



Nota; International Journal of Information Management Data Insights (2022)

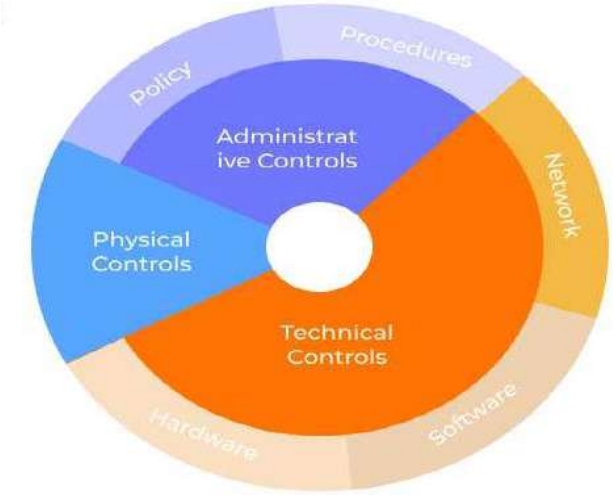
Como se muestra en la Figura 5, MCA ocupa una posición central en todas las capas de seguridad. Para mejorar la seguridad en cada capa, se puede emplear el cifrado de información importante en la base de datos y realizar copias de seguridad periódicas de la

misma. Además, tanto los dispositivos finales, como computadoras portátiles, de escritorio, servidores o teléfonos móviles, deben contar con protección mediante dispositivos a nivel de red y software de protección de punto final. Para aumentar la seguridad en la capa de aplicación, es fundamental diseñarla desde el principio siguiendo las mejores prácticas de codificación de seguridad. Asimismo, se deben evitar accesos no autorizados a la red de la organización para salvaguardar su seguridad. Tanto la seguridad física como la digital en los puntos perimetrales deben protegerse utilizando los controles adecuados para mitigar los riesgos al máximo. Es importante destacar que los seres humanos suelen ser el eslabón más débil y pueden contribuir a ataques cibernéticos exitosos, ya sea a través de amenazas internas o falta de conocimiento. Por lo tanto, resulta crucial implementar una capa de seguridad que motive a los humanos a reducir los riesgos. Para cualquier pequeña o mediana empresa, es esencial contar con controles de ciberseguridad que refuercen las áreas de Personas, Procesos y Tecnología. Cualquier marco de seguridad o estándar que no aborde adecuadamente los problemas en estas tres áreas estará incompleto. Los controles mínimos de ciberseguridad para las PYMES deben brindar un nivel de protección en cada capa que se muestra en la Figura 5.

Esto contribuirá a una defensa en profundidad, aunque los autores sugieren que, en lugar de tener todas las capas prioritarias desde el principio, las PYMES deberían comenzar con las capas prioritarias en el primer nivel y luego ampliar la cobertura de las capas con el tiempo. En muchos casos, los activos de misión crítica están relacionados con la información, por lo que es fundamental mejorar la gestión efectiva de los "Activos de información" en diferentes entornos y sistemas, lo cual se puede lograr principalmente a través de la conciencia entre los seres humanos involucrados. (Evans & Price, 2020)

Figura 5

Arquitectura De Seguridad De Defensa En Profundidad



1.2.4. Identificar tipos de control que cumplan con la tríada CIA

Existen tres categorías principales de controles de seguridad física en ciberseguridad: controles técnicos/lógicos y administrativos. Cada categoría tiene múltiples controles con propósitos específicos que buscan prevenir, detectar, disuadir, recuperar y corregir riesgos.

Para implementar una estrategia de defensa en profundidad, las pequeñas y medianas empresas (PYMES) deben mapear los controles mínimos de ciberseguridad relevantes para reducir el riesgo de manera satisfactoria. Para cumplir con la prioridad del triángulo de la CIA (Confidencialidad, Integridad y Disponibilidad), las PYMES deben mapear la máxima cantidad de controles y sus funciones correspondientes. Incluso pueden encontrar una superposición de controles en ciertas funciones, lo que les permite alcanzar múltiples objetivos con una sola implementación de control. Por ejemplo, el software de protección de punto final actual incluye características como antivirus, antispyware, antiransomware, prevención de pérdida de datos, control de dispositivos y cifrado de disco completo.

Esto cumple con los requisitos de múltiples controles técnicos necesarios para prevenir una amplia gama de riesgos. Si una PYME realiza una evaluación de vulnerabilidad y pruebas de penetración (VAPT) como control de detección para identificar problemas en sus activos, seguido de la corrección de esos problemas, esto ayudará en las funciones de

detección, prevención y corrección. Es importante que las PYMES inviertan en controles físicos, lógicos/técnicos y administrativos mínimos para salvaguardar el triángulo de la CIA y obtener la máxima cobertura de riesgo. La Tabla 2 proporciona ejemplos de tipos clave de controles de seguridad. Los controles preventivos ayudan a evitar problemas de ciberseguridad, los controles de detección ayudan a encontrar problemas o actividades maliciosas, y los controles correctivos ayudan a solucionar y corregir irregularidades o problemas detectados (Cannon et al., 2016). Los controles disuasivos actúan como una medida de disuasión para los atacantes al hacerse visibles en el sistema, mientras que los controles de recuperación ayudan a restaurar la normalidad después de un incidente. (Harris & Maymi, 2016)

1.2.5. Medidas de seguridad

La seguridad de la información implica resguardar la información de ser accedida, modificada o eliminada sin autorización. Se refiere a la protección de las tecnologías de software y hardware, y se enfoca en la protección de los sistemas informáticos que se conectan a través de redes de computadoras. Es crucial entender la diferencia entre estos términos, aunque no existe un consenso general sobre sus significados y hasta qué punto se solapan o son intercambiables. Se puede entender que la seguridad de la información en el ámbito informático, también conocida como seguridad cibernética o informática, se enfoca en proteger los sistemas informáticos de posibles daños o robos de su hardware, software o información almacenada, así como evitar interrupciones o desvíos en los servicios que brindan. Esto involucra el control del acceso al hardware y la protección contra posibles amenazas en la red, como la inserción de datos y código malicioso, y cualquier daño causado por la negligencia física de los operadores, ya sea intencional, accidental o debido a engaños que los hagan desviarse de los procedimientos de seguridad establecidos. (Barzanallana, 2019)

Las medidas de seguridad informática son un conjunto de técnicas y estrategias que se implementan para proteger la información y los sistemas informáticos de posibles amenazas. Estas medidas se dividen en tres categorías principales: físicas, lógicas y administrativas: (Muñoz, Zapata, & Vida, 2019)

1. **Medidas físicas**: Estas medidas están diseñadas para proteger los recursos físicos del sistema informático, como los servidores, los dispositivos de almacenamiento, los cables y los equipos de red. Algunas de las medidas físicas más comunes incluyen:
    a. ***Control de acceso físico***: Este control se encarga de asegurar que sólo el personal autorizado pueda acceder a las áreas de almacenamiento del sistema informático. Esto se puede lograr a través de la implementación de sistemas de identificación y autenticación, como tarjetas de acceso, huellas dactilares o contraseñas.
    b. ***Protección contra incendios***: Se implementan medidas de prevención y protección contra incendios en las instalaciones físicas para evitar la pérdida de información y equipos informáticos.
    c. ***Protección contra inundaciones***: Las medidas de protección contra inundaciones incluyen la implementación de sistemas de drenaje y la elevación de los equipos informáticos a lugares más altos para evitar daños por inundaciones.
    d. ***Protección contra cortes eléctricos***: Los sistemas informáticos deben contar con medidas de protección contra cortes eléctricos, como baterías de respaldo, generadores eléctricos y sistemas UPS (uninterruptible power supply).
2. **Medidas lógicas:** Estas medidas estarán para proteger los sistemas informáticos de posibles amenazas en línea, como virus, malware y ataques de hackers. Algunas de

las medidas lógicas más comunes incluyen:

   a. ***Protección contra virus y malware:*** Se instalan software de seguridad para detectar y eliminar virus y malware.
   b. ***Firewalls***: Los firewalls se utilizan para proteger los sistemas informáticos de posibles ataques de hackers y malware.
   c. ***Actualizaciones de seguridad***: Los sistemas informáticos deben contar con actualizaciones de seguridad para protegerse contra las últimas amenazas.

3. **Medidas administrativas**: Estas medidas están implementadas para asegurarse de que los usuarios del sistema informático sigan las políticas y procedimientos establecidos para proteger la información y los sistemas. Algunas de las medidas administrativas más comunes incluyen:

   a. ***Políticas y procedimientos de seguridad***: Se fundamentan políticas y procedimientos para proteger los sistemas informáticos y la información.
   b. ***Entrenamiento del personal***: Se realiza capacitación al personal para asegurarse de que entiendan las políticas y procedimientos de seguridad.
   c. ***Auditoría y monitoreo***: Se realiza monitoreo continuo y auditoría para detectar y prevenir posibles violaciones de seguridad.

Para el autor Stallings (2017), la seguridad informática es un campo crucial en la sociedad actual, debido a la creciente información que se maneja en el entorno digital. Es fundamental proteger los sistemas informáticos de posibles amenazas que puedan dañar la integridad, la confidencialidad y la disponibilidad de los datos. Las medidas de seguridad informática se refieren a las acciones que se deben tomar para garantizar la protección de los sistemas y datos en línea.

1. **Identificación de amenazas**: Se refiere al proceso de identificación de las amenazas

que pueden afectar los sistemas informáticos. Esto incluye la identificación de virus, malware, ataques de phishing, entre otros. La identificación de amenazas permite tomar medidas preventivas y reducir los riesgos.

2. **Evaluación de riesgos**: La evaluación de riesgos se refiere al proceso de identificar los riesgos asociados a la seguridad informática, y determinar la probabilidad y el impacto de cada uno de ellos. Esto permite establecer un plan de acción para minimizar los riesgos.
3. **Política de seguridad**: La política de seguridad informática es un conjunto de reglas y procedimientos que fundaron la manera en que una organización protege sus sistemas y datos. Esta política debe ser implementada en todos los niveles de la organización para garantizar la seguridad de la información.
4. **Control de acceso**: El control de acceso se refiere a la limitación del acceso a los sistemas y datos de una organización. Esto se logra mediante la implementación de medidas de autenticación y autorización que aseguren que solo las personas autorizadas pueden acceder a la información.
5. **Seguridad física:** La seguridad física se refiere a las medidas de seguridad necesarias para proteger los sistemas y datos de una organización de daños físicos, como incendios, inundaciones, entre otros. (Espinosa, 2014)

1.2.6. Preocupaciones de la seguridad informática

Para Paul & Colm (2019), la definición de seguridad informática consiste en la implementación de medidas de control para garantizar la confidencialidad, integridad y disponibilidad de todos los elementos que conforman los sistemas informáticos. En otras palabras, se trata de garantizar que la información y los componentes de los equipos informáticos sean utilizables, al mismo tiempo que se mantienen protegidos contra el acceso o modificación no autorizados por parte de personas o programas maliciosos.

La seguridad informática se ocupa de cuatro áreas principales:

1. ***Confidencialidad***: - Solo las personas de la empresa o autorizados deben tener el acceso a los recursos de datos o dispositivos que contiene la información.
2. ***Integridad***: - Solo los usuarios autorizados a cada área deben tener la capacidad y los permisos para modificar la información cuando sea requerido.
3. ***Disponibilidad***: - La información de las diferentes áreas deben estar disponibles para cuando la requieran los usuarios sean estos internos o externos.
4. ***Autenticación***: - cuando se requiera de información de deben asegurara de que ¿se está brindando la información realmente con quién cree que se está comunicando?

La seguridad informática es un tema muy relevante en la actualidad, ya que los sistemas informáticos y las redes se han convertido en herramientas fundamentales para el desarrollo de actividades empresariales, académicas y personales. La seguridad informática se refiere a las medidas que se toman para proteger los sistemas y datos informáticos de posibles amenazas externas e internas.

La seguridad informática se puede dividir en diferentes categorías, como la seguridad de la red, la seguridad de la información, la seguridad física y la seguridad de los dispositivos. Cada una de estas categorías tiene sus propios desafíos y amenazas, por lo que es importante tener un enfoque integral para garantizar la seguridad de los sistemas informáticos (Chávez & Loaiza, 2018).

Para Stallings (2017), en su libro donde habla sobre la seguridad informática: principios y prácticas determina y permite comprender los principios básicos de la de esta, el autor cubre los temas clave como la criptografía, la seguridad de la red y la seguridad de la información. Por otro lado, los autores Whitman, Mattord, & Green, (2014). en su libro principios de seguridad informática es una guía completa para comprender sus principios fundamentales, se expone la importancia de la seguridad de la información, la seguridad de la

red, la seguridad física y la gestión de la seguridad informática. Finalmente, el autor Orozco (2018), El objetivo es desarrollar una solución tecnológica a nivel de drive que facilite o agiliten la entrega de la información y que esta sea confiable a través de un sistema de gestión de operaciones para freelancers, por ello, la importante determinar los elementos fundamentales requeridos para construir una infraestructura en la nube que cumpla con los más altos estándares de seguridad.

Capítulo 2: Sistema De Información Y Clasificación Empresarial

2.1. Sistemas de Información

En los últimos años, el estudio de los sistemas de información se ha convertido en uno de los principales temas de investigación en el ámbito de la gestión empresarial. La complejidad del entorno en el que las empresas operan se ha ido incrementando con la globalización, la internacionalización de las compañías, la mayor competencia en los mercados de bienes y servicios, la velocidad de desarrollo de las tecnologías de la información, la incertidumbre del entorno y la disminución del ciclo de vida de los productos. Todo esto ha convertido la información en un elemento esencial para la gestión, supervivencia y crecimiento de las organizaciones empresariales. Si antes los recursos fundamentales eran la tierra, el trabajo y el capital, hoy en día la información se ha convertido en otro insumo de gran importancia en las empresas. (Gurmendi, 2018)

Hay diversas definiciones para un sistema de información, pero una de las más precisas fue propuesta, según los autores (Huerta, Gaete, & Pedraja, 2020), un sistema de información es un conjunto formal de procesos que trabajan sobre una colección de datos estructurada según las necesidades de la empresa. Este sistema recopila, procesa y distribuye selectivamente la información necesaria para la operación y actividades de dirección y control de la empresa. Además, este sistema apoya parcialmente los procesos de toma de decisiones necesarios para desempeñar funciones de negocio de acuerdo con la estrategia de la empresa.

Cada sistema de información se basa en la recopilación, procesamiento y conversión de datos en información, que luego se proporciona a los usuarios del sistema. La figura 1 muestra un proceso de retroalimentación, donde se evalúa si la información obtenida cumple con las expectativas previas. Además de la información, existen otros dos elementos

fundamentales que conforman un sistema de información: los usuarios (entre los que se incluyen el personal directivo, los empleados y cualquier otro individuo de la organización que haga uso de la información en su labor) y los equipos (que engloban tanto la tecnología informática como el software, el hardware y las tecnologías de almacenamiento y comunicación de datos).

Existen diversos criterios para clasificar los sistemas de información. En la siguiente tabla se presentan algunas de las principales tipologías de estos sistemas que pueden encontrarse.

Tabla 1

Clasificación de los sistemas de Información

Tipo de Sistema de Información	Tipos
Grado de formalidad	Formales Informales
Automatización	Manuales Informáticos
Relación con la toma de decisiones	Estratégicos (alta dirección) Gerencial (nivel intermedio) Operativos (control operativo)
Funcionalidad	Gestión comercial · Gestión contable Gestión financiera · Gestión de Recursos Humanos · Gestión de la Producción
Grado Especialización	Específicos Generales

Nota: Tipología de Sistemas de Información (Basado en García Bravo, 2000 y Edwars, Ward y Bythesway, 1998)

No obstante, la clasificación más beneficiosa es aquella propuesta por K y J Laudon en 1996, la cual categoriza los sistemas de información según su utilidad en los distintos niveles jerárquicos de la empresa. Estos niveles constan de cuatro niveles fundamentales: un nivel operativo que se enfoca en las actividades cotidianas de la empresa, un nivel de conocimiento que involucra a los empleados responsables de gestionar la información (usualmente el departamento de informática), un nivel administrativo que engloba a los gerentes intermedios de la organización y un nivel estratégico que comprende a la alta dirección de la empresa.

Según los niveles antes mencionados se determina la siguiente clasificación a los sistemas de información:

a. **Los Sistemas de Procesamiento de Operaciones (SPO)** son sistemas informáticos que gestionan las tareas diarias y rutinarias de una empresa, como el seguimiento de pedidos, el registro de empleados, las aplicaciones de nómina y la auditoría. Estos sistemas generan información que será utilizada por otros sistemas de información de la empresa y son empleados por el personal de los niveles más bajos de la organización (nivel operativo).
b. **Los Sistemas de Trabajo del Conocimiento (STC)** son sistemas de información que apoyan a los agentes que manejan información en la creación e integración de nuevos conocimientos para la empresa. Estos sistemas forman parte del nivel de conocimiento y se utilizan en estaciones de trabajo para la administración.
c. **Los Sistemas de Automatización en la Oficina (SAO)** son sistemas informáticos que aumentan la productividad de los empleados que manejan información en los niveles más bajos de la organización. Ejemplos de estos sistemas incluyen procesadores de texto, agendas electrónicas, hojas de cálculo y correo electrónico. Los SAO se encuentran en el nivel de conocimiento, al igual que los STC.

d. **Los Sistemas de Información para la Administración (SIA)** son sistemas de información utilizados en el proceso de planificación, control y toma de decisiones a nivel administrativo. Proporcionan informes sobre las actividades diarias de la empresa, como el control de inventarios, el presupuesto anual y el análisis de decisiones de inversión y financiación. Los SIA son empleados por la gerencia y los directivos de los niveles intermedios de la organización.

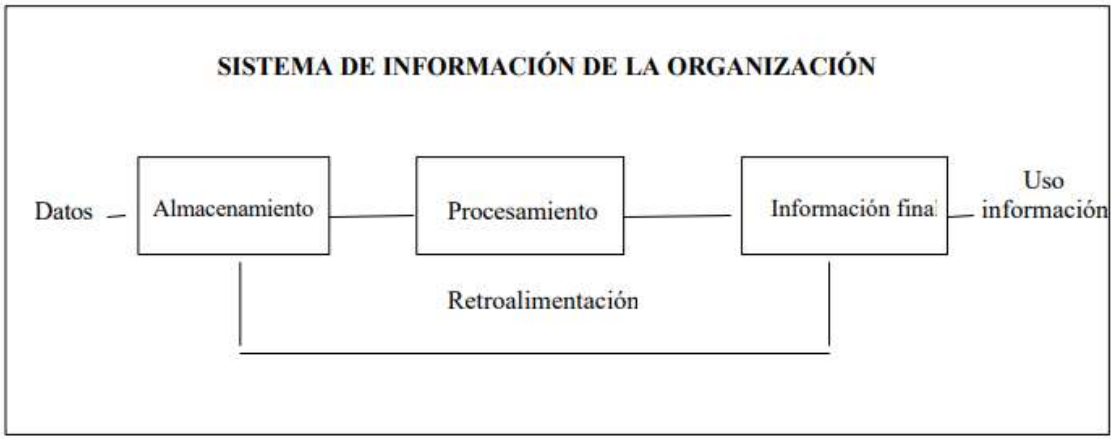
e. **Los Sistemas para el Soporte de Decisiones (SSD)** son sistemas informáticos interactivos que ayudan a los usuarios en el proceso de toma de decisiones. Se utilizan para resolver problemas no estructurados utilizando diferentes datos y modelos, como el análisis de costos, el análisis de precios y beneficios y el análisis de ventas por zona geográfica. Los SSD son empleados por la gerencia intermedia de la organización.

f. **Los Sistemas de Soporte Gerencial (SSG)** son herramientas informáticas que se utilizan en el nivel estratégico de las organizaciones para tomar decisiones importantes mediante el uso de tecnologías avanzadas y gráficos. Estos sistemas son utilizados por la alta dirección de la empresa con el objetivo de diseñar la estrategia general de la compañía, lo que incluye la planificación de ventas a largo plazo, la planificación operativa y la gestión de recursos humanos.

Los sistemas de información pueden ser analizados en función de las distintas áreas de una empresa, como ventas y marketing, producción y fabricación, finanzas, contabilidad y recursos humanos. Cada una de estas áreas requiere de aplicaciones informáticas y equipos específicos que deben estar coordinados entre sí. Si no se realiza una coordinación adecuada, la empresa puede experimentar problemas en el intercambio de datos entre las distintas áreas, redundancia de datos, ineficiencias y costos de comunicación más altos. Por lo tanto, es fundamental planificar y desarrollar los sistemas de información de manera adecuada, como se detallará en secciones posteriores. (Laudon & Laudon, 2016)

Figura 6

Modelo de Sistema de Información organizacional



Nota: Sistema de Información de la Organización empresarial: funciones

De acuerdo con Castañeda, Ortega, & García, (2016), consideran que el objetivo principal de los sistemas de información:

> *Es procesar la información que entra a una organización, permitir su análisis, almacenamiento y presentación, proveyendo a las directivas de una organización la información necesaria facilitando la gestión de la organización. Un sistema de información debe estar diseñado para poder cumplir con los objetivos estratégicos de la organización (pp. 3).*

2.1.1. Evolución De Los Sistemas De información

En los últimos años, ha habido una evolución en los sistemas de información, y ahora existen los llamados sistemas de información estratégicos. Antes, los sistemas de información empresariales se veían como una herramienta que simplificaba las actividades de la empresa y reducía la burocracia al llevar la contabilidad y procesar documentos operativos.

De acuerdo con Briones, Molina & Avilés (2020), con el desarrollo de la informática y las telecomunicaciones, se logró aumentar la eficacia de las tareas, ahorrar tiempo y espacio

de almacenamiento de información, lo que llevó a un mayor interés en los sistemas de información. Con el tiempo, las empresas se dieron cuenta de que los sistemas de información podían ofrecer una ventaja competitiva y permitirles diferenciarse de sus competidores, lo que los convirtió en una cuestión estratégica importante en los procesos de planificación empresarial.

Al examinar el avance de los sistemas de información, un trabajo crucial fue presentado por Gibson y Nolan (1974). Su estudio delineó la progresión de los sistemas de información en consonancia con los progresos de las tecnologías de la información (véase tabla 2). A medida que los equipos informáticos, el software, el hardware, las bases de datos y las telecomunicaciones evolucionaron, los sistemas de información adquirieron una importancia cada vez mayor en las organizaciones, pasando a ser considerados un elemento esencial en el proceso de planificación.

Tabla 2

Etapas de la Evolución de los sistemas de información

Etapas	**Características**
Iniciación	a) Introducción de la informática en la empresa b) Aplicaciones informáticas orientadas a la mecanización y automatización de los procesos ordinarios c) Escaso gasto en informática y escasa formación del personal
Contagio	a) La aplicación de las tecnologías de información b) originan resultados espectaculares c) Difusión de las tecnologías de información en todas las áreas de la empresa d) Aumenta la cualificación del personal e) Existe gran descoordinación y poca planificaciónen el desarrollo de los sistemas de información

Control	a) La alta dirección de la organización se preocupa b) de los sistemas de información como consecuenciadel alto coste en ellos c) Centralización de los proyectos de inversión entecnologías de información
Integración	a) Se controla el incremento del gasto b) Se produce la integración de los sistemas de información existentes en las distintas áreas de la empresa c) Mejora y perfeccionan los sistemas de información
Administración de lainformación	a) El sistema de información adquiere unadimensión estrategia en la empresa b) Descentralización de ciertas aplicaciones informáticas
Madurez	a) Desarrollo de los Sistemas de información en los b) niveles superiores de la organización apareciendo losSistemas Estratégicos de información c) Adquiere gran importancia la creatividad y la innovación

Nota; Fuente: Gibson y Nolan 1974

De acuerdo con Andreu, Ricart y Valor (1991), se pueden identificar cuatro etapas en la evolución de los sistemas de información. En la primera etapa, la informática se introduce en la organización para simplificar y automatizar los procesos administrativos, y se utilizan las computadoras y los sistemas informáticos para mejorar la contabilidad, las nóminas y la facturación, con el objetivo de ahorrar costes y tiempo. Sin embargo, en esta etapa, hay una falta de formación en los empleados y la organización carece de profesionales capacitados para resolver los problemas relacionados con los sistemas de información.

En la segunda etapa, se produce un "contagio" de las aplicaciones informáticas en

diferentes departamentos de la empresa, sin una planificación adecuada, lo que resulta en un aumento significativo de los costes. En esta etapa, se observa un aumento en la formación del personal en tecnologías de información y aplicaciones informáticas, y la organización cuenta con profesionales capaces de solucionar los problemas relacionados con el manejo de los sistemas de información.

En la tercera etapa, los sistemas de información se utilizan en toda la organización y la dirección los considera un elemento fundamental de la empresa. Se empiezan a elaborar procedimientos de planificación de los sistemas de información y se reconoce la necesidad de utilizarlos para cumplir con los objetivos de la empresa.

En la cuarta etapa, los sistemas de información se valoran como una fuente de ventaja competitiva sostenible y se establecen como un aspecto clave en el proceso directivo para elaborar la estrategia general de la compañía. Se planifica y desarrolla los sistemas de información para que sean coherentes con la estrategia general de la organización.

2.1.2. Modelos de Sistema de Información

Implementar un sistema de información puede ser clave para que una organización obtenga mejores resultados que sus competidores en la economía. Esta implementación puede traer beneficios como la reducción de costos de fabricación del producto, disminución de los costos de comunicación entre las diferentes áreas de la empresa, mejor coordinación entre los diferentes niveles jerárquicos de la organización, una mayor conectividad con los proveedores y clientes, adaptación rápida a las necesidades del consumidor y disminución del tiempo de entrega del producto, entre otros. Estos beneficios pueden ayudar a fortalecer la estrategia que la empresa haya elegido seguir, como el liderazgo en costos, la diferenciación del producto y la concentración.

Por otro lado, las organizaciones que no den la debida importancia a los sistemas de

información y no los desarrollen coherentemente con su estrategia empresarial podrían enfrentar problemas diversos. Por ejemplo, podrían perder poder en las negociaciones con competidores, proveedores y clientes, establecer objetivos empresariales inalcanzables, duplicar esfuerzos, tener sistemas inexactos, manejar mal la información y elegir tecnologías de información inadecuadas. En cambio, si se utilizan sistemas estratégicos de información, se puede ayudar a la empresa a sobrevivir en entornos altamente competitivos y lograr un crecimiento de la organización. Para ello, se puede emplear el modelo de fuerzas competitivas de Porter (1982), que permitirá relacionar las amenazas y oportunidades que la empresa puede encontrar con los agentes externos y actuar en consecuencia.

Figura 7

Modelo de Sistema de Información organizacional

Nota: Esquema ilustrativo de las cinco fuerzas identificadas por Porter

2.1.3. Desarrollo De Los Sistemas De Información

El desarrollo de sistemas de información se compone de siete fases principales.

a. La primera fase implica la definición del proyecto, en la que se evalúan los problemas de la empresa y se determina cómo se pueden resolver mediante la implementación de un sistema de información. Además, se identifican los objetivos

de la utilización de estos sistemas y se integran dentro de la estrategia global de la compañía. Es importante que la alta dirección considere los sistemas de información como una herramienta estratégica y tenga fe en su éxito.

b. La siguiente etapa es el análisis de sistemas, en la que se investigan los diferentes problemas de la organización y se identifican sus causas, proponiendo diversas soluciones. En este proceso se lleva a cabo un estudio de factibilidad, evaluando si las soluciones son viables considerando los recursos de la empresa. Se analizan tres tipos de factibilidad: técnica, económica y operativa.
c. La tercera fase es el diseño de sistemas, en la que se detalla cómo el sistema de información cumplirá con los requisitos de la organización. Se determinan los componentes que se utilizarán (hardware, software y tecnología de las telecomunicaciones) y cómo se relacionarán entre sí. De esta forma, se establecen las especificaciones del sistema de información.
d. La cuarta etapa es la programación, en la que se traducen las especificaciones del sistema desarrolladas en la fase anterior, llevando a cabo la programación y el desarrollo del software.
e. La quinta fase es la de pruebas, en la que se evalúa exhaustivamente el correcto funcionamiento del sistema de información en diferentes condiciones. Se realizan tres tipos de pruebas: pruebas de programas, pruebas al sistema y pruebas de aceptación.
f. La fase de conversión implica la implementación del sistema de información o la sustitución del antiguo por el nuevo. En este proceso, las empresas pueden optar por diversas estrategias.
g. La última fase es el mantenimiento, en la que se lleva a cabo la revisión y actualización periódica del sistema de información para asegurar su correcto

funcionamiento y adecuación a las necesidades de la organización.

El ciclo completo de las fases examinadas es lo que se denomina ciclo de vida de los sistemas de información. Sin embargo, para muchas empresas, seguir todas las etapas anteriores puede resultarles muy costoso en términos de tiempo y dinero. Además, los continuos cambios en los requisitos de la información pueden hacer que un sistema de información se vuelva obsoleto incluso durante su desarrollo. Por esta razón, las empresas pueden elegir otro conjunto de estrategias para desarrollar un sistema de información que les permita obtener resultados igualmente satisfactorios que los obtenidos mediante el ciclo de vida de los sistemas de información.

Existen varias estrategias que las empresas pueden adoptar en cuanto al desarrollo de sistemas de información, entre ellas se incluyen:

1. Elaboración de prototipos: se trata de la creación de una versión preliminar del sistema de información total para reducir el tiempo y los costos de desarrollo. Los prototipos son evaluados por los empleados y se adaptan continuamente a sus necesidades. Una vez que se comprueba su correcto funcionamiento, se extienden a otras áreas de la empresa. Sin embargo, el principal problema de esta estrategia es la superficialidad y la falta de documentación y pruebas adecuadas para garantizar su correcto funcionamiento. Además, no son recomendables para grandes organizaciones.
2. Paquetes de software de aplicaciones: se trata de adquirir software ya existente en el mercado para manejar la información. Es una solución sencilla y útil para las empresas que no tienen suficiente capital para desarrollar su propio sistema de información. Sin embargo, estos paquetes suelen ser inflexibles para adaptarse a las necesidades específicas de la empresa.
3. Desarrollo por los usuarios finales: los propios usuarios pueden desarrollar sus

propios sistemas de información utilizando herramientas informáticas como hojas de cálculo, editores de texto y bases de datos. Esta solución permite un mayor control del sistema por parte de los usuarios y ahorra costos, pero también puede resultar en la proliferación de sistemas de información sin control y sin cumplir los mínimos de calidad.

4. Subcontratación de los sistemas de información: las empresas pueden contratar a empresas externas para desarrollar sus sistemas de información. Esta estrategia permite aprovechar las economías de escala del proveedor y asegurar la calidad del servicio, pero también puede suponer una pérdida de control y dependencia del proveedor, así como la revelación de información estratégica a terceros.

2.1.4. Modelo PDCA

El ciclo de Deming, también conocido como PDCA (Planificar-Hacer-Verificar-Actuar, por sus siglas en inglés), es un enfoque metodológico creado por Shewart y Deming para abordar proyectos de mejora en procesos internos y externos. En la actualidad, muchas normas ISO y estándares se basan en este ciclo de mejora.

Una novedad en la norma ISO 27001:2013 es la eliminación del ciclo PDCA como marco obligatorio para la gestión de mejora continua. En su lugar, solo se menciona en la sección 10.2 que "la organización debe mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información". Sin embargo, el ciclo PDCA está implícito en la estructura misma de la norma. A continuación, se presenta este modelo de mejora continua que consideramos necesario conocer.

El modelo PDCA consta de las siguientes fases, que permiten establecer un modelo comparativo a lo largo del tiempo y medir el grado de mejora alcanzado:

Planificar: En esta fase se realiza la planificación de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI). Se define el contexto de la organización,

se establecen los objetivos y las políticas necesarias para alcanzarlos.

Hacer: En esta fase se lleva a cabo la implementación y puesta en marcha del SGSI. Se aplican las políticas y controles seleccionados según el análisis de riesgos realizado. Se deben establecer procedimientos claros que indiquen quién debe realizar cada tarea, garantizando la capacitación necesaria.

Verificar: En esta fase se realiza el monitoreo y la revisión del SGSI. Se verifica que los procesos se ejecuten según lo planificado y que permitan alcanzar los objetivos de la manera más eficiente posible.

Actuar: En esta fase se mantiene y mejora el SGSI. Se definen y ejecutan las acciones correctivas necesarias para rectificar cualquier fallo detectado en la fase anterior (Gómez Fernández & Fernández River, 2015).

2.1.5. MAGERIT VS 3.0

Magerit es el nombre corto de la "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas". Esta metodología fue creada por el Consejo Superior de Administración Electrónica (CSAE) y está destinada al uso público, siendo propiedad del Ministerio de Administraciones Públicas (MAP) de España. El objetivo principal de Magerit es abordar los riesgos asociados con los sistemas de información utilizados en medios electrónicos, informáticos y telemáticos, ya que su uso es cada vez más común en la actualidad. Se busca evitar estos riesgos a través de medidas preventivas para generar confianza en su uso.

Es fundamental analizar los riesgos antes de implementar medidas de seguridad adecuadas. Esto implica considerar los riesgos existentes, el estado de la tecnología y los costos asociados tanto con la falta de seguridad como con las salvaguardas necesarias. Magerit, como Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones Públicas, proporciona un enfoque formal para investigar los riesgos

que enfrentan los sistemas de información y recomendar las medidas apropiadas para controlar estos riesgos (Gaona Vásquez, 2013, pág. 28).

Los objetivos de Magerit, según se describen en el libro I de la versión 3, son los siguientes:

Objetivos directos:

Crear conciencia entre los responsables de las organizaciones de información sobre los riesgos existentes y la necesidad de gestionarlos.

Proporcionar un método sistemático para analizar los riesgos asociados con el uso de tecnologías de la información y comunicación (TIC).

Ayudar a descubrir y planificar el tratamiento adecuado para mantener los riesgos bajo control.

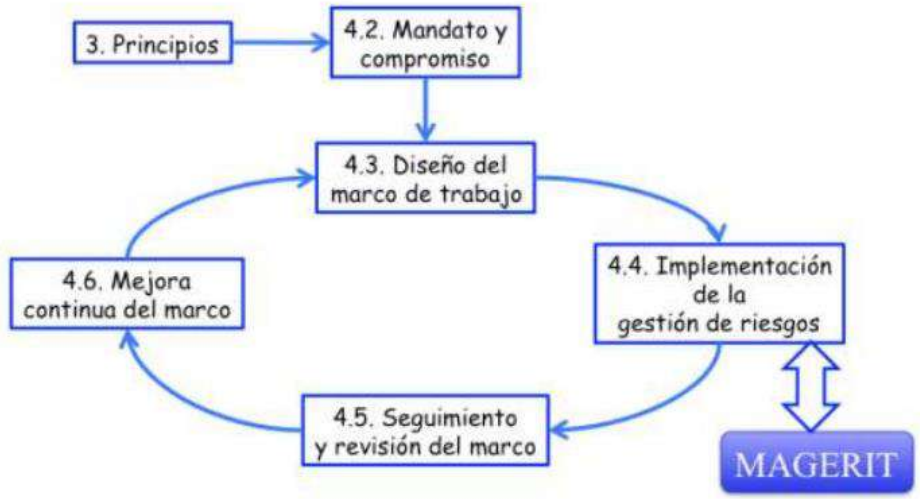
Objetivos indirectos:

Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

La metodología MAGERIT versión 3 se basa en el "Proceso de Gestión de Riesgos" definido en la normativa ISO 31000, este implementa este proceso dentro de un marco de trabajo para permitir que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos asociados con el uso de tecnologías de la información. (Amutio Gómez, Candau, & Mañas, 2012).

Figura 8

ISO 31000 - Marco de trabajo para la gestión de riesgos



Nota: desarrollado por Niño (2018)

En las "Directrices de la OCDE para la seguridad de sistemas y redes de información - Hacia una cultura de la seguridad", el principio 6 establece lo siguiente:

6) Evaluación del riesgo. Los participantes deben llevar a cabo evaluaciones de riesgo.

Existen diversas formas de analizar los riesgos que pueden afectar a los sistemas y tecnologías de la información y comunicación, como guías formales, enfoques metodológicos y herramientas de apoyo. Todos ellos tienen como objetivo determinar el nivel de seguridad o inseguridad de los sistemas. Se deben considerar varios elementos para obtener resultados óptimos. Por esta razón, MAGERIT se basa en un enfoque metódico que elimina la improvisación y no depende de la arbitrariedad del analista.

2.2. Estándares Y Normas Para Asegurar La Información

2.2.1.1. ISO Serie 27000

Al igual que otras normas ISO, la norma 27000 es una serie de estándares que comprende definiciones de vocabulario (ISO 27000), requisitos para sistemas de gestión de seguridad de la información (ISO 27001), guía de buenas prácticas en objetivos de control y

controles recomendables de seguridad de la información (ISO 27002), guía de implementación de un Sistema de Gestión en Seguridad de la Información (SGSI) con información sobre el uso del esquema PDCA (Planificar, Hacer, Verificar, Actuar) (ISO 27003), especificación de métricas para evaluar la eficacia del SGSI (ISO 27004), guía de técnicas de gestión de riesgos (ISO 27005), especificación de requisitos para la acreditación de entidades de auditoría y certificación de SGSI (ISO 27006), guía de auditoría de SGSI (ISO 27007), guía de gestión de seguridad de la información para telecomunicaciones (ISO 27011), guía de continuidad de negocio en relación con las tecnologías de la información y las comunicaciones (ISO 27031), guía de ciberseguridad (ISO 27032), guía de seguridad en redes (ISO 27033), guía de seguridad en aplicaciones (ISO 27034) y guía de seguridad de la información en el sector sanitario (ISO 27799). ISO/IEC 27001 (Burgos Salazar & G. Campos, 2010). (Antunes, Maximiano, Gomes, & Pinto, 2021)

2.2.1.2. Familias ISO 27000

ISO 27000 incluye términos y definiciones utilizados en toda la serie 27000. Es fundamental contar con un vocabulario preciso cuando se aplica cualquier estándar.

ISO 27001 es la norma principal de esta serie y establece los requisitos para el "Sistema de Gestión de Seguridad de la Información". En su Anexo A, presenta de manera resumida los objetivos de control y los controles desarrollados en ISO 27002:2013, los cuales las organizaciones pueden seleccionar al desarrollar sus propios Sistemas de Gestión de Seguridad de la Información (SGSI).

La norma ISO/IEC 27001:2013, desarrollada por la ISO (Organización Internacional de Normalización) y la IEC (Comisión Electrotécnica Internacional), es un sistema de estandarización reconocido a nivel mundial. Esta norma establece los requisitos para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI). Además, especifica los controles

de seguridad que deben implementarse según las necesidades de una organización, sector o proceso, en función del alcance del SGSI. Para obtener la certificación, se requiere la documentación adecuada y el cumplimiento de todos los requisitos.

No obstante, a pesar de que la norma sugiere un enfoque para su cumplimiento, no proporciona una metodología concreta para lograr los productos y la documentación requerida, ni especifica un flujo de trabajo con procesos bien definidos.

Este estándar internacional también adopta el modelo Planificar-Hacer-Verificar-Actuar (PHVA), que implica un ciclo de mejora continua. Consiste en planificar, desarrollar, verificar y actuar en función de los resultados obtenidos durante las verificaciones. De esta manera, se busca refinar la gestión, haciéndola más eficaz y efectiva.

La norma se aplica a todo tipo de organizaciones, independientemente de su tamaño o actividad, ya sean empresas privadas, públicas o entidades sin ánimo de lucro. Establece los requisitos para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un SGSI documentado, teniendo en cuenta los riesgos empresariales generales. Sin embargo, no proporciona orientación sobre los procedimientos específicos para su implementación. Por ejemplo, requiere un análisis de riesgos con características objetivas y precisas, pero no indica el mejor método para llevarlo a cabo. Puede realizarse utilizando herramientas comerciales, aplicaciones personalizadas, reuniones, entrevistas, tablas u otros métodos apropiados. Siempre que se cumplan los requisitos de objetividad del método, se obtengan resultados repetibles y se documente la metodología, estos recursos serán válidos para cumplir con la norma.

2.2.2. Análisis de la seguridad informática en Ecuador

En 2019, se llevó a cabo un estudio en la ciudad de Santo Domingo de los Tsáchilas para analizar la seguridad de la información en las pequeñas y medianas empresas. El objetivo era proporcionar datos estadísticos sobre los problemas a los que estas empresas

están expuestas y las medidas que deben tomar para proteger tanto su información física como digital. En muchos casos, los empresarios de las PyMEs solo toman medidas de seguridad informática después de sufrir un incidente, lo que resulta en costos más altos que una inversión inicial (Sampedro et al., 2019).

En 2020, se realizó una investigación sobre la seguridad informática en las PyMEs de la ciudad de Quevedo. El objetivo era evaluar el uso de reglas, normas y protocolos de seguridad informática. Mediante una encuesta, se encontró que existe un alto porcentaje de desconocimiento o falta de conocimiento sobre los mecanismos, políticas y normas de seguridad informática (Zuñiga et al., 2020). Es necesario conocer y comprender la seguridad informática en las PyMEs para prevenir posibles ataques informáticos o pérdida de información.

También en 2020, en la ciudad de Riobamba, se llevó a cabo un estudio sobre el desarrollo de medidas de seguridad informática en dispositivos móviles para la gestión de la información en las PyMEs. Se utilizó la metodología basada en las normas ISO/IEC 27001:2015 y se determinó que las empresas carecían de normas o procedimientos de seguridad de la información (Vizuete, 2021). Para garantizar una gestión segura de la información en una empresa, es importante socializar las políticas de seguridad con el personal.

En 2021, se publicó un artículo que destacaba la importancia de las políticas de seguridad informática según las normas ISO 27001 para las pequeñas y medianas empresas en Ecuador. El objetivo era identificar las amenazas y riesgos utilizando la matriz de análisis de riesgos de tecnología de la información, y luego abordarlos mediante la elaboración de políticas de seguridad informática para garantizar la confiabilidad, integridad y disponibilidad de la información y los recursos informáticos de las PyMEs (Llano et al., 2021). La implementación de políticas de seguridad informática en las PyMEs permitirá regular los

procesos y la gestión de los servicios informáticos más comunes.

2.2.3. Marco Legal de las PyMES en el Ecuador

El Marco Legal de las Pequeñas y Medianas Empresas (PyMES) en Ecuador se establece a través de dos leyes principales: la Ley de compañías y el código orgánico de la producción.

La Ley de compañías es la normativa legal que regula a todas las empresas, ya sean pequeñas, medianas o grandes, constituidas en Ecuador. Fue publicada en el registro oficial el 5 de noviembre de 1999, y ha sido modificada por última vez el 23 de octubre de 2018. Esta ley consta de 460 artículos que establecen las normas y regulaciones para la actividad empresarial en el país. La Superintendencia de Compañías es la entidad encargada de supervisar y garantizar el cumplimiento de las disposiciones establecidas en esta ley.

Por otro lado, el código orgánico de la producción, comercio e inversiones (COPCI) es una normativa publicada en el registro oficial el 29 de diciembre de 2010, con su última modificación realizada el 31 de diciembre de 2019. El COPCI tiene como objetivo regular la producción y proporcionar incentivos para las iniciativas empresariales y empresas que se acojan a este código. El libro III del COPCI, titulado "Desarrollo empresarial de las micro, pequeñas y medianas empresas y democratización de la producción", contiene las disposiciones que rigen específicamente a las PyMES en el país, desde el artículo 53 hasta el artículo 66.

Dentro del reglamento de inversiones del código orgánico de la producción, en su artículo 106 sobre la clasificación de las Micro, Pequeñas y Medianas Empresas (MIPYMES), se establecen las siguientes categorías para su consideración:

Clasificación	Números de Trabajadores	Valor de Ventas Anuales (USD)
Microempresa	Entre 1 a 9	Iguales o menores a $300.000,00
Pequeña empresa	Entre 10 a 49	Entre $300.001,00 y $1’000.000,00
Mediana empresa	Entre 50 a 199	Entre $1’000.001,00 y $5’000.000,00

En la actualidad, las empresas de diferentes tamaños ya sean pequeñas, medianas o grandes, dependen en gran medida de la tecnología para llevar a cabo sus actividades y procesos comerciales. Por esta razón, es fundamental contar con un departamento de tecnología e informática (TI) en las empresas, el cual tiene la responsabilidad de proporcionar y facilitar soluciones informáticas y herramientas necesarias para la gestión de los sistemas informáticos, brindar soporte a los usuarios de los equipos informáticos y administrar la infraestructura tecnológica de la empresa.

2.2.3.1. Actividades del Departamento de TI

Una de las principales fortalezas que una empresa debe tener es la capacidad de automatizar tareas diarias y garantizar la seguridad de la información que maneja. Esto es posible gracias al trabajo del departamento de Tecnología de la Información (TI). Según Bambú Mobile (2022), el departamento de TI desempeña diversas funciones y servicios, que incluyen:

a. Administración: Su tarea consiste en supervisar todas las infraestructuras informáticas de la empresa. Ayudan al personal a resolver problemas con equipos y programas, capacitan a los empleados sobre los sistemas utilizados, aseguran el cumplimiento de las normas y políticas de seguridad de la información, entre otros servicios.
b. Soporte técnico: Se encargan de reparar equipos y programas dañados, instalar nuevo software o hardware, realizar copias de seguridad y recuperar elementos

digitales, solucionar problemas de la red, entre otras funciones relacionadas con el mantenimiento y el soporte técnico.

c. Comunicación: Su responsabilidad radica en administrar y mantener las redes de comunicación de la empresa. Configuran las redes de correo electrónico y gestionan la incorporación o salida de usuarios de los sistemas de comunicación.

d. Programación: Se enfocan en el desarrollo de software o aplicaciones necesarias para la empresa, con el objetivo de mejorar la eficiencia y satisfacer las necesidades específicas del negocio.

2.2.3.2. Rol del Departamento de TI

El diseño de un organigrama para un departamento de Tecnología de la Información (TI) variará según las necesidades específicas de la empresa, lo que significa que no existe un organigrama perfecto para dicho departamento. No obstante, se pueden ofrecer pautas para organizar el departamento y formar un equipo eficiente que se ajuste a las necesidades de la empresa (Pinto, 2020). El departamento de TI podría incluir las siguientes funciones o áreas:

a. Área de Comunicaciones
b. Centro de Planificación, Gestión y Estrategia de Servicios
c. Área de Gestión de Riesgos
d. Centro de Negocio y Aplicaciones Empresariales
e. Centro de Atención al Cliente
f. Área de Sistemas e Infraestructuras
g. Gestión del Desarrollo de Nuevas Tecnologías
h. Director del Departamento

El tamaño de la estructura del departamento de TI dependerá de las necesidades y recursos de la empresa.

2.2.3.3. Amenazas a la Seguridad

Un sistema informático se enfrenta a numerosas amenazas y ataques. Con el fin de identificar estas amenazas, se pueden realizar tres clasificaciones: la primera se refiere a los tipos de atacantes, la segunda a los tipos de ataques que pueden ocurrir y la tercera a las formas en que se llevan a cabo dichos ataques (Universidad Veracruzana, 2022). A continuación, se presenta en la Tabla 4 una lista de los términos utilizados para describir a las personas que llevan a cabo los ataques informáticos, junto con una breve definición que los caracteriza.

Nombre de los atacantes	Definición
Hackers	Profesionales en el campo de la informática con una notable curiosidad por descubrir vulnerabilidades en los sistemas, pero sin ninguna motivación económica ni intención maliciosa.
Crackers	Un hacker, por otro lado, es alguien que rompe la seguridad de un sistema con intenciones maliciosas, ya sea para dañarlo o para obtener ganancias económicas.
Phreakers	Existen los crackers telefónicos, quienes sabotean las redes de telefonía con el objetivo de realizar llamadas de forma gratuita.
Sniffers	Expertos en redes que analizan el tráfico con el fin de obtener información, extrayéndola de los paquetes transmitidos a través de la red.
Lammers	Jóvenes inexpertos en informática que se autodenominan hackers y se jactan de ello, a pesar de tener pocos conocimientos en la materia.
Newbie	Hacker novato.
Ciberterrorista	Un experto en informática y en intrusiones a redes que trabaja como espía o saboteador informático para países u organizaciones
Programadores de virus	Expertos en programación, redes y sistemas que desarrollan programas dañinos que causan efectos no deseados en los sistemas o aplicaciones
Carders	Personas que se dedican a atacar sistemas de tarjetas, como los cajeros automáticos.

Además de la clasificación de las amenazas a la seguridad, existen diversos tipos de ataques informáticos que un sistema puede enfrentar cuando se aprovechan sus vulnerabilidades, como se detalla a continuación.

Nombre del ataque	Definición
Interrupción	Ocurre cuando un recurso del sistema o de la red se vuelve inaccesible debido a un ataque.
Intercepción	Se produce cuando un intruso obtiene acceso a la información de nuestro equipo o a la que transmitimos a través de la red.
Modificación	Consiste en la alteración no autorizada de la información, lo que invalida su veracidad o integridad.
Fabricación	Se refiere a la creación de un producto, como una página web, que es difícil de distinguir del auténtico y puede ser utilizado para obtener información confidencial del usuario.

2.2.3.4. Mecanismos Preventivos en Seguridad Informática

Los mecanismos de prevención son una serie de controles periódicos y mejoras que se aplican en diversos aspectos, como hardware, software y otros elementos de los sistemas y procesos. Estos controles están adaptados a los procesos específicos de cada empresa (Romero et al., 2018).

Es importante destacar que muchas amenazas cibernéticas pueden evitarse si se implementan medidas preventivas en seguridad informática. Sin embargo, una empresa se enfrenta al desafío de obtener el consentimiento y el compromiso de todos los participantes al intentar implementar dichas medidas (Torres, 2022).

A continuación, se mencionan algunos ejemplos de mecanismos preventivos utilizados en seguridad informática:

Mecanismos de Prevención	Acción
Respaldo de Información	La política de respaldos tiene en cuenta varios aspectos importantes: los formatos de archivos que se almacenan, el horario en que se realizan los respaldos, el control de los medios utilizados y el respaldo de la información en un lugar considerado seguro.
Actualización de sistemas	Es necesario actualizar periódicamente el sistema operativo, ya que estas actualizaciones incluyen correcciones de errores, parches de seguridad y otras mejoras.
Antivirus	Además, se recomienda instalar antivirus en los equipos tecnológicos para proteger los datos de la empresa. Esto es parte de un control de seguridad y un filtro para prevenir posibles amenazas.
Firewall	Es un control de seguridad y filtro.

Mecanismos Correctivos en Seguridad Informática

Se deben implementar medidas correctivas de seguridad para reducir o minimizar los efectos de eventos que afecten a los sistemas. Estas medidas incluyen la creación de contenedores de seguridad al bloquear direcciones IP identificadas como amenazas, el bloqueo de eventos sospechosos y la implementación de un proceso de desbloqueo por parte del administrador, entre otras acciones (Samaniego & Ponce, 2021).

En cuanto a los pasos necesarios en los mecanismos correctivos, se deben realizar inventarios detallados de los problemas de seguridad informática para buscar posibles soluciones. También es importante estudiar los problemas identificados para plantear soluciones efectivas y documentar todos los procesos llevados a cabo (Romero et al., 2018).

6.3.8. Mecanismos de Detección en Seguridad Informática

Los mecanismos de detección se basan en la premisa de que un atacante es capaz de violar la seguridad y puede haber realizado una intrusión total o parcial en un recurso específico. Estos mecanismos tienen como objetivos detectar el punto exacto del ataque,

identificar actividades sospechosas y comprender lo sucedido (Torres, 2022).

6.4. Plan Estratégico de Seguridad Informática

Un plan estratégico de seguridad informática es una herramienta que guía al departamento de TI de una institución o empresa. Está compuesto por procedimientos, reglas, políticas, normas y estándares destinados a evaluar y minimizar los riesgos futuros. La elaboración de este plan debe adaptarse a las necesidades, actividades, funciones y tecnología de la institución o empresa (Paladines et al., 2021).

El desarrollo de un plan estratégico de seguridad informática consta de tres fases o etapas que buscan prevenir, detectar y responder a amenazas que afecten los procesos informáticos de las empresas. Estas etapas son: análisis, evaluación y tratamiento de riesgos.

6.4.1. Análisis de Riesgos

El análisis de riesgos tiene como objetivo identificar los activos de información de un sistema y estimar su vulnerabilidad y el impacto que un ataque podría tener. Este análisis proporciona una línea base para identificar áreas vulnerables y garantizar que las medidas de protección sean adecuadas. Además, ofrece un marco estratégico para gestionar recursos, amenazas e impactos, siendo esencial para controlar las actividades (Holguín & Lema, 2019).

En el análisis de riesgos, es necesario entender los siguientes términos:

Activos: Recursos o elementos relacionados con los sistemas de información que tienen valor para la empresa.

Amenazas: Operaciones que pueden causar daños significativos o no a la empresa.

Impacto: Resultado de una amenaza en un activo.

Probabilidad: Estimación de la posibilidad de que un recurso informático esté expuesto a un evento.

Vulnerabilidades: Características o condiciones débiles de un recurso que permiten la materialización de amenazas.

2.2.3.5. ISO 27001:2013

Es una norma internacional establecida por la Organización Internacional de Normalización (ISO) que proporciona un marco para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) dentro de una organización. Esta norma está diseñada para ayudar a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de su información.

Las organizaciones están invirtiendo cada vez más en abordar los riesgos asociados con la seguridad de la información, en vista de la importancia de preservar la confidencialidad, integridad y disponibilidad de los datos. Estas inversiones se reflejan en proyectos que van desde implementaciones tecnológicas específicas para la seguridad de la información, hasta la definición e implementación de modelos de seguridad que permiten una gestión continua de una estrategia de seguridad de la información, la cual debe evolucionar y mejorar con el tiempo.

La norma internacional ISO/IEC 27001 se ha presentado como un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información. Esto implica que se puede crear un marco formal para gestionar la seguridad de la información en las organizaciones. Volviendo a lo básico, es interesante preguntarse: ¿Qué es la seguridad de la información? ¿Qué implica gestionar la seguridad de la información?

Contexto de la organización: La norma requiere que una organización identifique y comprenda el contexto en el que opera, incluyendo sus partes interesadas relevantes y los requisitos legales, regulatorios y contractuales aplicables.

Liderazgo: El liderazgo y el compromiso de la alta dirección son fundamentales para establecer y mantener un SGSI efectivo. La norma exige que la alta dirección proporcione un enfoque estratégico para la seguridad de la información y demuestre su liderazgo y

compromiso.

Planificación: Las organizaciones deben desarrollar una estrategia de seguridad de la información basada en la evaluación de riesgos, estableciendo objetivos y planes para alcanzarlos. También deben considerar los requisitos legales y contractuales, así como los controles de seguridad necesarios.

Soporte: La norma ISO 27001:2013 requiere que las organizaciones proporcionen los recursos necesarios, incluyendo personal competente, infraestructura y entorno de trabajo adecuados, para implementar y mantener el SGSI.

Operación: Esta sección se refiere a la implementación de los controles y procesos necesarios para gestionar los riesgos de seguridad de la información. Incluye el establecimiento de políticas y procedimientos, la gestión de activos, el control de acceso, la gestión de cambios y la adquisición de servicios y productos.

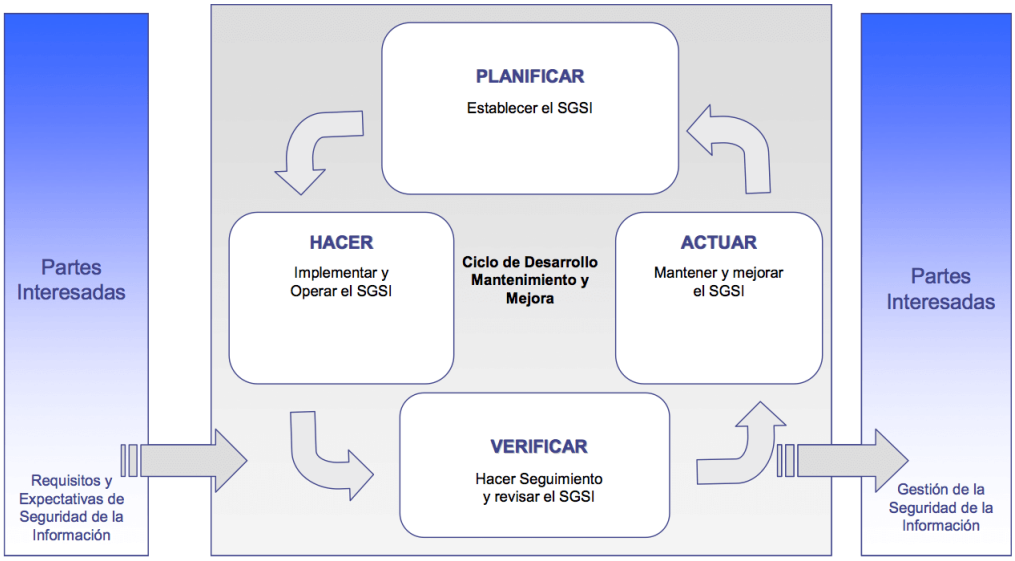
Evaluación del desempeño: Las organizaciones deben realizar evaluaciones periódicas para medir el desempeño de su SGSI y tomar medidas correctivas cuando sea necesario. Esto implica la monitorización, el análisis de datos, las auditorías internas y la revisión por la dirección.

Mejora: La norma promueve un enfoque de mejora continua para el SGSI. Las organizaciones deben identificar oportunidades de mejora, implementar acciones correctivas y preventivas, y revisar regularmente el sistema para asegurar su eficacia.

En resumen, el análisis teórico de ISO 27001:2013 muestra que es una norma integral que aborda la seguridad de la información desde una perspectiva holística. Proporciona un marco sólido para establecer un SGSI efectivo y garantizar la protección de la información dentro de una organización. Al seguir los requisitos de esta norma, las organizaciones pueden fortalecer su postura de seguridad, reducir los riesgos y mejorar la confianza de sus partes interesadas.

Figura 9

Procesos basados en la aplicación de la ISO 27001



2.2.3.6. ISO/IEC 27002

ISO/IEC 27002, también conocida como "Tecnología de la información - Técnicas de seguridad - Código de práctica para el control de la seguridad de la información", es una norma internacional que proporciona directrices y mejores prácticas para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) dentro de una organización.

El objetivo principal de esta norma es establecer controles y salvaguardias para proteger la confidencialidad, integridad y disponibilidad de la información en una organización. Estos controles abarcan una amplia gama de áreas, incluyendo la gestión de activos de información, el control de acceso, la seguridad física, la seguridad de los recursos humanos, la gestión de incidentes, la continuidad del negocio y la conformidad legal.

Un análisis teórico de la norma implica comprender su estructura y contenido, así como evaluar su relevancia y aplicabilidad en diferentes contextos organizativos. A continuación, se presentan algunos aspectos clave para considerar en dicho análisis:

Alcance y estructura: La norma ISO/IEC 27002 proporciona un conjunto de controles de seguridad de la información organizados en 14 secciones. Estas secciones abarcan diferentes aspectos relacionados con la seguridad de la información y se pueden adaptar según las necesidades de la organización.

Marco de referencia: La norma se basa en un marco de referencia de gestión de riesgos. Proporciona directrices para identificar, evaluar y tratar los riesgos de seguridad de la información de manera sistemática y efectiva.

Mejores prácticas: esta norma se basa en las mejores prácticas y experiencia acumulada en el campo de la seguridad de la información. Incorpora enfoques probados y recomendaciones para abordar los desafíos y amenazas actuales en este ámbito.

Enfoque basado en controles: La norma se centra en la implementación de controles de seguridad de la información. Estos controles están diseñados para reducir los riesgos identificados y abordar las necesidades de seguridad específicas de la organización.

2.2.3.7. Gestión de Activos de Información

En esta gestión se requiere la identificación, valoración y clasificación de los activos de información más importantes para el negocio. Según la norma ISO/IEC 27001, un activo de información es algo al que la organización asigna directamente un valor y, por lo tanto, debe proteger.

Sin embargo, para evitar una definición demasiado amplia, es necesario establecer criterios que permitan identificar los activos de información y definir las diferentes formas en que se pueden reconocer en la organización.

Principalmente, se considera como activo de información cualquier conjunto de datos creado o utilizado por un proceso de la organización, así como el hardware y software utilizados para su procesamiento o almacenamiento, los servicios utilizados para su transmisión o recepción, y las herramientas/utilidades para el desarrollo y soporte de sistemas

de información. En casos especiales, también se puede considerar como activo de información a personas que manejen datos, transacciones o tengan conocimientos específicos muy importantes para la organización (por ejemplo, secretos industriales, manejo de claves importantes o conocimiento especializado).

Bajo esta gestión, se busca cumplir con tres puntos principales:

Inventario de Activos: Es necesario identificar claramente todos los activos y elaborar y mantener un inventario de los activos de información importantes de la organización. Este inventario debe incluir la valoración de cada activo, utilizando una escala definida por la organización, como alto, medio o bajo valor. Además, es importante indicar las propiedades más importantes para proteger de cada activo en términos de confidencialidad, integridad y disponibilidad, asignando un valor a cada propiedad. También se debe indicar la ubicación del activo de información y los procesos que lo utilizan. (Cárdenas, 2021)

Propiedad de los Activos: Toda la información y los activos asociados con los servicios de procesamiento de información deben ser propiedad de una parte designada de la organización. En este sentido, se pueden determinar entidades que interactúen con los activos de información, como:

a. Propietario de la Información: Se refiere a una entidad específica dentro de la organización, ya sea un cargo, un proceso o un grupo de trabajo, que tiene la responsabilidad de establecer y regular el acceso a la información, así como determinar los requisitos necesarios para garantizar la protección contra accesos no autorizados, modificaciones, pérdida de confidencialidad o destrucción intencionada. Además, también se encarga de definir el manejo de la información una vez que ya no es necesaria, incluyendo los plazos de retención asociados.
b. Custodio Técnico: Hace referencia a una entidad designada dentro de la

organización, como un cargo, un proceso o un grupo de trabajo, cuya responsabilidad es administrar y aplicar los controles de seguridad establecidos por el propietario de la información. Esto implica tareas como realizar copias de seguridad, asignar privilegios de acceso, modificaciones y borrado, y utilizar los recursos de seguridad y control disponibles en la organización.

c. Usuario: Se trata de cualquier persona que genera, adquiere, transforma, almacena o utiliza información de la organización, ya sea en formato físico o digital, tanto de manera presencial como a través de redes de datos y sistemas de información. Los usuarios son aquellos que utilizan la información en el desempeño de sus funciones laborales y tienen el derecho explícito de acceder a los activos de información según lo establecido en el inventario de información. Para cada usuario, se deben definir los derechos y niveles de acceso al activo de información, incluyendo la capacidad de lectura, escritura, borrado, entre otros.

Figura 10

Responsables de la Información

Directrices de la Información: La información debe ser clasificada teniendo en cuento a su valor, requisitos legales, sensibilidad y su importancia para la organización. La clasificación de la información puede variar según cada organización y generalmente se basa en la confidencialidad, aunque también puede incluir la disponibilidad y la integridad. Por ejemplo, un esquema simple de clasificación podría tener dos niveles: información pública e información confidencial. Sin embargo, algunas organizaciones pueden requerir más niveles, como información pública, de uso interno, confidencial y altamente confidencial.

Es responsabilidad de cada organización definir el significado de cada nivel de clasificación y establecer los procedimientos necesarios para garantizar un tratamiento y manejo seguro de la información en cada nivel. Esto incluye determinar los niveles de acceso permitidos, los métodos de distribución y transmisión, las condiciones de almacenamiento, las condiciones de entrega a terceros y la destrucción de la información.

En este sentido, se deben aplicar las mejores prácticas de seguridad para cada nivel de clasificación en general, abarcando todos los activos de información de ese nivel. Sin embargo, si se requiere un tratamiento y manejo específico para un activo de información en particular, esto debe estar respaldado y justificado mediante la identificación de un riesgo específico asociado a dicho activo en el proceso de Gestión de Riesgos.

2.2.3.8. Gestión de la Estrategia de seguridad de la información

Para poder supervisar y dirigir todas estas actividades, es necesario que la organización implemente las siguientes acciones desde el nivel más alto de la estructura:

Declaraciones formales de intención y compromiso: La alta dirección debe presentar políticas organizativas, como la política de seguridad de la información, que reflejen su compromiso con la seguridad. Todos los demás documentos relacionados con la seguridad de la información, como normas, procedimientos y guías, deben estar alineados y respaldar estas declaraciones de alto nivel para garantizar la coherencia y operatividad en todas las áreas de

seguridad.

Definición de roles, responsabilidades y recursos: Es importante determinar quién será responsable de las diferentes actividades del ciclo PHVA (Planificar, Hacer, Verificar, Actuar) en cada gestión. Más que enfocarse en una estructura organizativa específica, es crucial identificar a las personas responsables en todos los niveles, desde la alta dirección hasta los usuarios finales. Una estructura organizativa rígida puede limitar la asignación de responsabilidades a aquellos que ejecutan los procesos de la organización, lo cual asegura que las actividades de seguridad formen parte de la rutina diaria y sean adoptadas por todos.

Medición y control: Los resultados y el estado de la seguridad de la información deben ser incluidos en los mecanismos y herramientas de apoyo a la toma de decisiones de la organización. Cada gestión debe tener indicadores de desempeño que reflejen sus actividades más relevantes y que estén alineados con los indicadores de nivel superior, los cuales contribuyen al logro de los objetivos organizacionales. Es fundamental utilizar herramientas de medición y control, como cuadros de mando gerenciales y metodologías organizativas, como el Balanced Scorecard (BSC).

Modelo de gobierno de la seguridad de la información: Se busca establecer un marco de gestión formal para la estrategia de seguridad de la información. Esto puede lograrse a través de la decisión de cumplir con uno o más modelos ampliamente reconocidos a nivel mundial. La elección de este marco dependerá del tipo de organización, su tamaño, sus objetivos de seguridad y el nivel de madurez que se desee alcanzar en la gestión de la seguridad de la información. Algunos de estos marcos o modelos incluyen COBIT, ISO/IEC 27001, ISM3, ITIL, las series del NIST, SABSA, TOGAF, entre otros. Estos marcos o modelos influirán en la implementación de las diferentes gestiones presentadas anteriormente.

En resumen, al implementar estas acciones, se establecerá un modelo de seguridad de

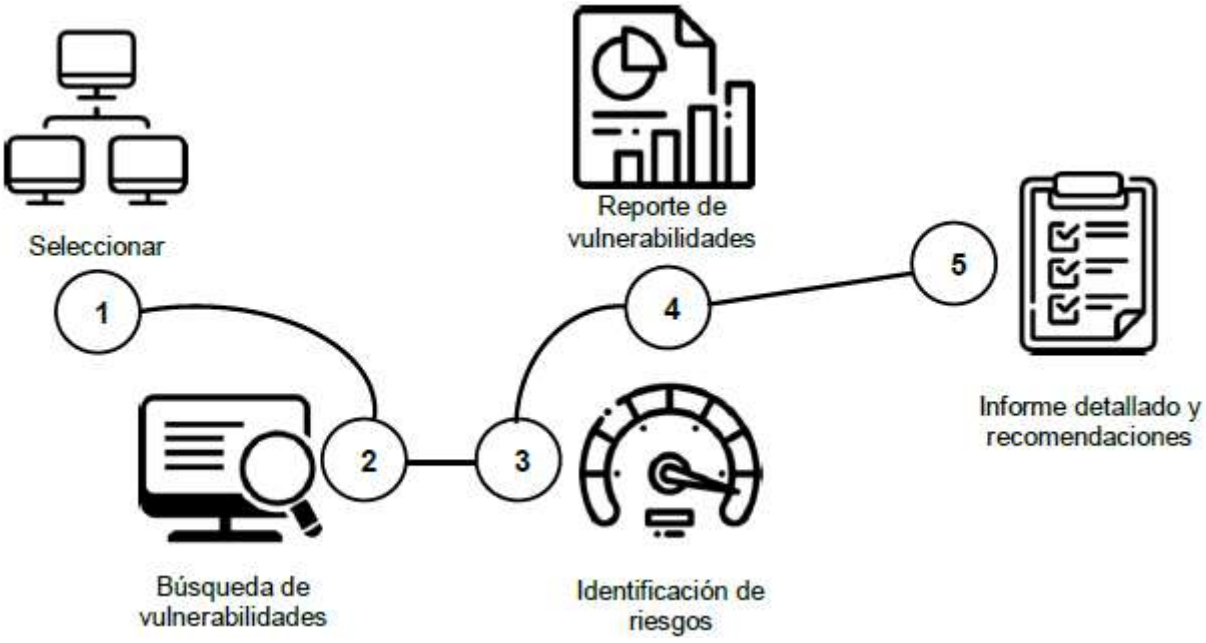
la información integral y se dirigirá su implementación y mejora continua. (Cárdenas, 2021)

2.2.3.9. Búsqueda de vulnerabilidad de la informción

En esta investigación se eligieron los paquetes de software comerciales más comúnmente utilizados en las PYMEs en Colombia para identificar vulnerabilidades relacionadas con el software y su versión. La estrategia propuesta para desarrollar una herramienta de búsqueda de vulnerabilidades cibernéticas en las PYMEs se basa en un proceso sistémico y sistemático, que se inicia con la definición y declaración inicial de un proyecto de investigación (García-González y Sánchez-Sánchez, 2020). El modelo sistémico de la herramienta se representa en la Figura 1, y el código fuente de la herramienta se encuentra disponible en el repositorio (Sánchez-Sánchez, 2020)

Figura 11

Esquema búsqueda de debilidades cibernéticas en pymes



Selección de equipos: en esta etapa inicial se seleccionan los equipos y dispositivos dentro de la PYME que serán analizados en busca de vulnerabilidades. Se recomienda evaluar todos los equipos, especialmente aquellos conectados a través de una red, como sistemas, servidores, computadoras portátiles, máquinas virtuales, dispositivos móviles y

computadoras de escritorio. (Sánchez & García, 2021)

Búsqueda de vulnerabilidades: este proceso es el núcleo de la herramienta desarrollada y se basa en el uso de agentes de búsqueda inteligentes que identifican el software instalado, sus versiones y buscan vulnerabilidades en el CVE (Common Vulnerabilities and Exposures) para cada uno de ellos en los equipos y dispositivos seleccionados. El objetivo de este proceso es crear una lista completa de las vulnerabilidades en las diferentes aplicaciones instaladas en cada equipo. CVE Details (CVSS, 2019) recopila las principales vulnerabilidades encontradas por proveedores de software, hardware e investigadores, asignándoles un número de identificación CVE-ID, una descripción de la vulnerabilidad, las versiones del software afectadas y una posible solución. Sin embargo, CVE Details no ofrece una API de consulta automática, por lo que es necesario realizar consultas individuales. Por lo tanto, se requiere un proceso automatizado que evalúe todos los programas instalados en cada equipo seleccionado. Para automatizar este proceso de búsqueda, se utilizó un agente inteligente con tres componentes: captura de la lista de programas de software, consulta en un diccionario unificado de nombres y Web Scraping.

Marco Conceptual

En el marco conceptual de seguridad informática para redes empresariales en las PYMEs, es necesario considerar los siguientes términos:

Identificación de los activos críticos: es importante identificar los activos críticos de la empresa, tales como la información confidencial, los datos financieros, la propiedad intelectual, entre otros, y determinar su valor y su impacto en la organización.

Evaluación de riesgos: se debe realizar una evaluación de riesgos para identificar las posibles amenazas y vulnerabilidades de la empresa, y establecer medidas para mitigarlas.

Políticas de seguridad: se deben establecer políticas de seguridad que definan las medidas de protección necesarias para asegurar la integridad y confidencialidad de la información, así como la disponibilidad de los sistemas informáticos.

Controles de acceso: se deben establecer controles de acceso adecuados para proteger los sistemas y la información de accesos no autorizados, incluyendo la autenticación de usuarios, la gestión de contraseñas, el control de privilegios y la auditoría de acceso.

Protección contra malware: se deben implementar medidas de protección contra malware, incluyendo la instalación y actualización de software antivirus, antispyware y antimalware, así como la implementación de políticas de uso de internet y correo electrónico.

Copias de seguridad: se deben establecer políticas de copias de seguridad para garantizar la disponibilidad y la recuperación de la información en caso de fallos o desastres.

Plan de contingencia: se debe elaborar un plan de contingencia que establezca los procedimientos a seguir en caso de un incidente de seguridad, para minimizar su impacto y garantizar la continuidad del negocio.

Capacitación y concientización: se debe capacitar y concientizar al personal de la empresa sobre las políticas de seguridad y las medidas de protección, para evitar errores y comportamientos inadecuados que puedan poner en riesgo la seguridad de la información y

los sistemas.

Sistemas de Información Transaccionales: Estos sistemas se utilizan para procesar transacciones comerciales diarias, como ventas, compras, pagos y devoluciones. Estos sistemas están diseñados para capturar, procesar y almacenar datos transaccionales en tiempo real.

Sistemas de Información de Soporte a la Toma de Decisiones: Estos sistemas proporcionan información que se utiliza para tomar decisiones empresariales importantes. Estos sistemas utilizan técnicas analíticas para procesar grandes cantidades de datos y presentar información útil y significativa para los tomadores de decisiones.

Sistemas de Información de Gestión: Estos sistemas se utilizan para gestionar y coordinar los recursos y procesos de una organización. Estos sistemas incluyen la planificación de recursos empresariales (ERP), la gestión de la cadena de suministro (SCM) y los sistemas de gestión de relaciones con los clientes (CRM).

Sistemas de Información de Gestión de Conocimiento: Estos sistemas se utilizan para ayudar a las organizaciones a recopilar, almacenar y distribuir información y conocimientos específicos de la empresa. Estos sistemas incluyen bases de datos de conocimientos, sistemas de gestión documental y sistemas de gestión de contenido empresarial.

Riesgo: El riesgo se refiere a la probabilidad de que un evento adverso ocurra y cause daño o pérdida. Puede ser el resultado de una decisión, acción o evento aleatorio, y puede tener consecuencias negativas para individuos, organizaciones o la sociedad en general. El riesgo puede ser medido y gestionado a través de diversas estrategias y herramientas.

Riesgo informático: El riesgo informático se refiere a la posibilidad de que un sistema informático o los datos almacenados en él sean dañados o comprometidos por virus, hackers, errores de programación u otros factores. La seguridad informática se centra en la

prevención, detección y respuesta a los riesgos informáticos para proteger los activos digitales de una organización.

Información: La información se refiere a datos que han sido procesados y organizados para que tengan significado y sean útiles para las personas. Puede ser transmitida y almacenada en diversos formatos, como texto, imágenes o audio, y puede ser utilizada para tomar decisiones, resolver problemas o crear conocimiento.

Datos: Los datos se refieren a hechos y cifras sin procesar que se recopilan y almacenan en un formato digital o analógico. Los datos pueden ser estructurados o no estructurados y pueden ser utilizados para analizar patrones, tendencias y relaciones.

Sistemas: Los sistemas son conjuntos de componentes interconectados que trabajan juntos para lograr un objetivo común. Los sistemas pueden ser físicos o digitales y pueden ser diseñados para cumplir diversas funciones, como la gestión de datos, la producción de bienes y servicios o la comunicación.

Virus: Un virus informático es un programa o código malicioso que se inserta en un sistema informático sin el conocimiento o consentimiento del usuario. Los virus pueden causar daño al sistema o a los datos almacenados en él, y pueden propagarse de un sistema a otro a través de la red.

Hacker: Un hacker es una persona que tiene habilidades avanzadas en el uso de la tecnología y el software y que utiliza estas habilidades para acceder a sistemas informáticos sin autorización. Los hackers pueden ser benignos (white hat) o maliciosos (black hat) y pueden tener diferentes motivaciones para acceder a sistemas.

Pequeñas empresas: Las pequeñas empresas son organizaciones comerciales que tienen un número limitado de empleados y que operan con recursos limitados. Las pequeñas empresas pueden ser de propiedad individual o tener varios propietarios y pueden operar en una variedad de industrias.

Riesgos empresariales: Los riesgos empresariales se refieren a los peligros que enfrentan las empresas en el curso de sus operaciones. Estos pueden incluir riesgos financieros, operativos, legales y de seguridad. La gestión de riesgos empresariales implica identificar y mitigar los riesgos potenciales para garantizar la continuidad del negocio y proteger los activos de la empresa.

Control de riesgos de información: se refiere a un conjunto de medidas y procesos que se implementan para identificar, evaluar y reducir los riesgos relacionados con la información en una organización. El objetivo principal del control de riesgos de información es garantizar la seguridad, confidencialidad, integridad y disponibilidad de los datos, minimizando así los riesgos asociados con el uso de la información.

Administración de la información: se refiere a la gestión de información dentro de una organización. La administración de la información implica la recopilación, organización, almacenamiento, protección y análisis de la información para mejorar la toma de decisiones y el rendimiento de la organización. La administración de la información también se ocupa de la calidad de los datos, la integridad y la seguridad de la información.

Información financiera: se refiere a la información relacionada con la situación financiera de una organización, como sus estados financieros, balances, cuentas de resultados y flujo de caja. La información financiera es importante para los inversionistas, los accionistas, los reguladores y otros interesados en la salud financiera de la organización.

Procesos informáticos: se refiere a las actividades y tareas relacionadas con el uso de la tecnología de la información en una organización. Los procesos informáticos incluyen la planificación, el diseño, la implementación, la operación y el mantenimiento de sistemas y aplicaciones informáticas.

Sistemas informáticos: se refiere a los componentes de hardware, software y redes que se utilizan para procesar, almacenar y comunicar información en una organización. Los

sistemas informáticos pueden ser tan simples como una computadora personal o tan complejos como un sistema de gestión de bases de datos empresariales. Los sistemas informáticos son importantes para el éxito de la organización, ya que permiten la automatización de procesos, la mejora de la eficiencia y la toma de decisiones basada en datos.

Datos digitales: incluyen información personal, financiera, legal, de investigación y desarrollo, estratégica, comercial, correos electrónicos, contestadores automáticos, bases de datos, unidades lógicas y copias de seguridad. Los activos tangibles incluyen los mismos tipos de información, pero en formato físico, como llaves de oficina y otros medios de almacenamiento

Activos tangibles: incluyen conocimiento, relaciones, secretos comerciales, licencias, patentes, experiencia, conocimientos técnicos, imagen corporativa, marca, reputación comercial, confianza de los clientes, ventaja competitiva, ética y productividad.

Activos intangibles: entre ellos aparecen una serie de activos como el conocimiento, Secretos comerciales, licencias o Patentes, conocimientos técnicos, imagen corporativa, marca, reputación comercial, confianza de los clientes, ventaja competitiva, Productividad.

Software de aplicación: incluye software desarrollado por la organización, software de cliente, planificación de recursos empresariales, gestión de la información, utilidades, herramientas de bases de datos, aplicaciones de comercio electrónico y middleware

Sistemas operativos: entre los más importantes se pueden incluir servidores, ordenadores de sobremesa, ordenadores centrales, dispositivos de red y dispositivos de mano e incrustados.

Activos Físicos Infraestructura de TI: incluyen infraestructura de TI, como edificios, centros de datos, habitaciones de equipos y servidores, armarios de red, oficinas, escritorios, cajones, archivadores, salas de almacenamiento de medios físicos, cajas de

seguridad, dispositivos de identificación, autenticación, control de acceso al personal y otros dispositivos de seguridad

Controles de entorno de TI: incluyen equipos de alarma, supresión contra incendio, sistemas de alimentación ininterrumpida, alimentación de potencia, acondicionadores, filtros, supresores de potencia, deshumificadores, refrigeradores, alarmas de aire y alarmas de agua.

El hardware de TI: entre estos se encuentran dispositivos de almacenamiento, ordenadores de mesa, estaciones de trabajo, ordenadores portátiles, equipos de mano, servidores, módems, líneas de terminación de red, dispositivos de comunicaciones y equipos multifunción.

Los activos de servicios de TI: incluyen servicios de autenticación de usuario, administración de procesos, enlaces, cortafuegos, servidores proxy, servicios de red, servicios inalámbricos, anti-spam, virus, spyware, detección y prevención de intrusiones, teletrabajo, seguridad, correo electrónico, mensajería instantánea, servicios web, contratos de soporte y mantenimiento de software.

Capítulo 3: Modelo De Aseguramiento De La Información Empresarial Para Salvaguardar el Activo Intangible

3.1. Presentación de los Resultados Empresas Pymes de Guayaquil

Para la presente investigación y la determinación del cumplimiento de los objetivos se realizó un estudio de caso enfocado en las pequeñas y medianas empresas, específicamente los empresarios, dueños o gerentes de los establecimientos, con el objetivo de analizar los resultados de la investigación, los datos se presentaran de forma agrupada o resumen presentando las preguntas de mayor relevancia para la investigación, que corresponden a diferentes aspectos del entorno a la seguridad informática, se abordaran preguntas que permiten conocer el entorno de la empresa en relación sus personal, capacidad instala, equipos informáticos, servidores para respaldo de información y seguridad de la información.

3.2. Análisis Descriptivo de los Resultados

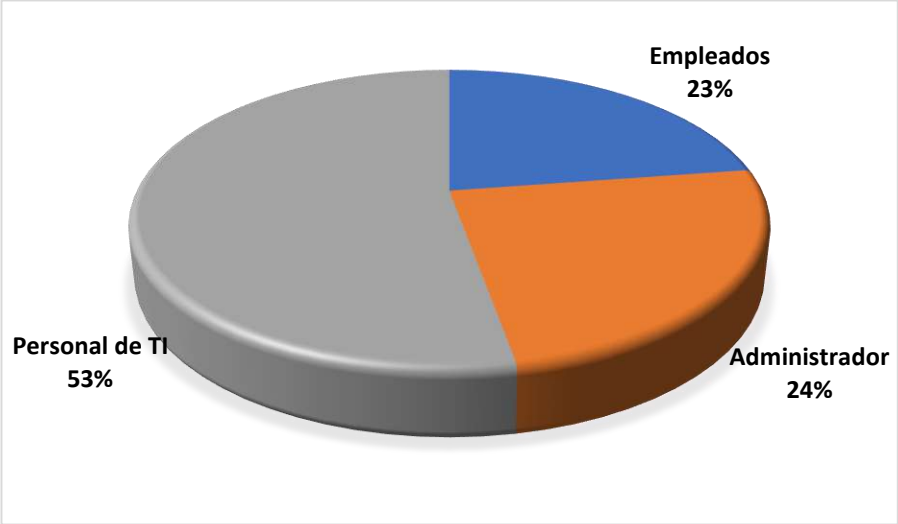
Tabla 3

1. ***¿Cuál es la persona encargada de implementar y preservar el software de seguridad en los dispositivos informáticos de la organización?***

Encargado	Respuestas	Porcentaje
Empleados	12	22,64%
Administrador	13	24,53%
Personal de TI	28	52,83%
Total	53	100,0%

Figura 12

Respuestas pregunta 1



Según los resultados de la encuesta realizada a las pequeñas y medianas empresas (PyMES), se encontró que un significativo 59,09% de las personas encargadas de instalar y mantener el software de seguridad en los equipos de cómputo pertenecen al departamento de Tecnología de la Información (TI). Este dato revela que los requisitos relacionados con la instalación y el mantenimiento de los equipos de cómputo son gestionados por el personal especializado del área de TI, como se evidencia en la tabla 3.

Esta estadística resalta la importancia que las PyMES le otorgan a la seguridad informática, al asignar esta responsabilidad a profesionales capacitados en el campo de la tecnología. Al contar con personal de TI dedicado a la instalación y mantenimiento de los softwares de seguridad, las empresas demuestran una conciencia consciente de los riesgos asociados con los ataques cibernéticos y la protección de los datos confidenciales de la organización.

La Figura 12, a la que se hace referencia, proporciona una visualización gráfica de los resultados obtenidos en la encuesta, confirmando la destacada presencia del personal de TI en el proceso de gestión de la seguridad informática en las PyMES. Esta representación visual

respalda aún más la importancia asignada a la inversión en recursos y talento especializado para proteger los sistemas informáticos y salvaguardar la integridad de la información empresarial.

En resumen, la investigación revela que el departamento de TI asume la responsabilidad principal en la instalación y mantenimiento del software de seguridad en los equipos de cómputo de las PyMES encuestadas. Esto indica una respuesta adecuada a los requisitos de seguridad, ya que el personal especializado está involucrado en la tarea crucial de proteger la infraestructura tecnológica de la organización. La Figura 12 proporciona una representación gráfica de estos hallazgos, respaldando aún más la importancia de la participación del personal de TI en la gestión de la seguridad informática.

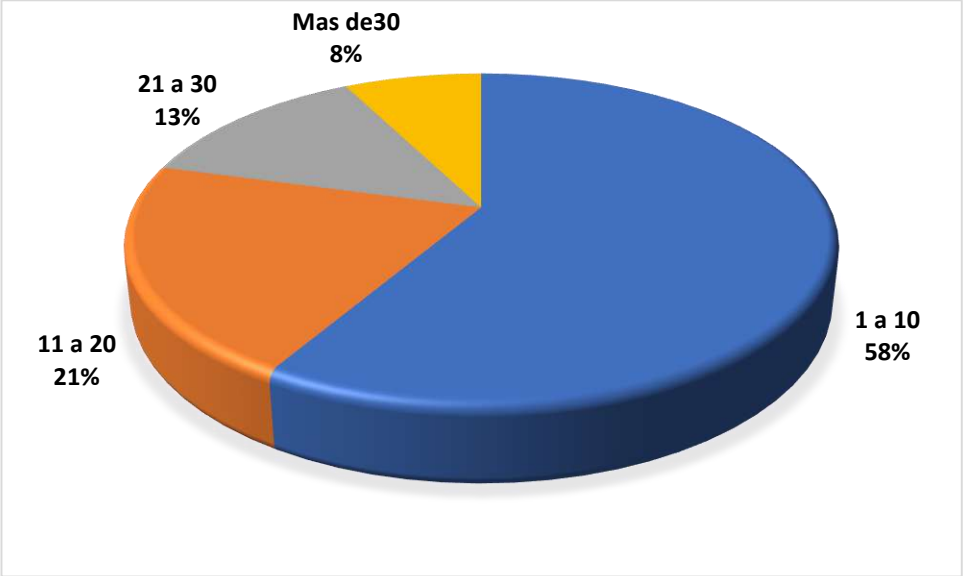
Tabla 4

2. ¿Cuántas computadoras tiene la compañía a su disposición para el trabajo relacionado al manejo de la información Contable-Financiera?

Equipos	Cantidad	Porcentaje
1 a 10	31	58,49%
11 a 20	11	20,75%
21 a 30	7	13,21%
Mas de30	4	7,55%
Total	**53**	**100,0%**

Figura 13

Cantidad de equipos por empresa



Los resultados estadísticos presentados muestran la distribución de la cantidad de computadoras en las pequeñas y medianas empresas (PyMES) encuestadas. Analicemos los datos:

Para el rango de 1 a 10 computadoras, se observa que 31 empresas, lo que representa un 58,49% del total, se encuentran dentro de este rango. Esto indica que la mayoría de las PyMES encuestadas tienen una cantidad relativamente baja de computadoras. En el siguiente rango, de 11 a 20 computadoras, se encontraron 11 empresas, lo que equivale a un 20,75% del total. Esto sugiere que una proporción significativa de las PyMES posee una cantidad moderada de computadoras, pero aún no alcanza los niveles más altos.

En el rango de 21 a 30 computadoras, se identificaron 7 empresas, lo que representa un 13,21%. Esta cifra indica que una menor proporción de PyMES encuestadas posee una cantidad más sustancial de computadoras en este rango. Por último, se encontraron 4 empresas, que representan un 7,55% del total, con más de 30 computadoras. Esto demuestra que una minoría de las PyMES encuestadas tiene un número considerable de computadoras,

lo que podría indicar un mayor tamaño o una mayor necesidad de recursos informáticos.

En general, se puede inferir que la mayoría de las PyMES encuestadas tienen una cantidad limitada de computadoras, con la mayoría de ellas cayendo en el rango de 1 a 10. Sin embargo, también se identificaron algunas empresas con un número más considerable de computadoras, aunque estas representan una proporción menor del total. Estos datos proporcionan una perspectiva de la distribución de recursos informáticos en las PyMES encuestadas y pueden ser útiles para comprender las necesidades y los desafíos tecnológicos a los que se enfrentan.

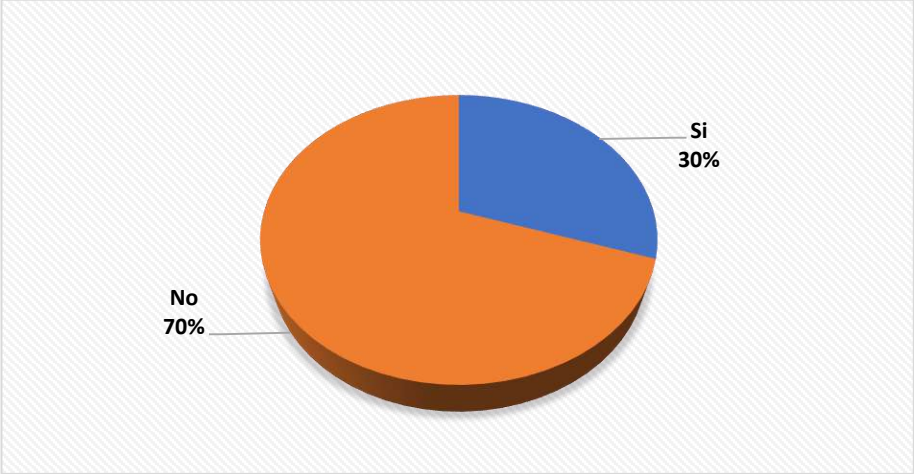
Tabla 5

3. ¿La empresa cuenta con servidores centrales de datos disponibles, de su propiedad o instalados dentro de ella?

Ítems	Respuesta	Porcentaje
Si	16	30,19%
No	37	69,81%
Total	**53**	**100,00%**

Figura 14

Existen servidores dentro de la Empresa



Los resultados estadísticos proporcionados muestran la distribución de las pequeñas y

medianas empresas (PyMES) encuestadas en relación con la posesión de servidores de datos propios:

De las PyMES encuestadas, se encontró que 16 empresas, lo que equivale a un 30,19% del total, tienen servidores de datos de su propiedad. Esto indica que una proporción significativa de las PyMES encuestadas ha invertido en la adquisición y mantenimiento de sus propios servidores, lo que les permite gestionar y controlar directamente sus datos.

Por otro lado, se observa que 37 empresas, lo que representa un 69,81% del total, no tienen servidores de datos propios. Esto indica que la mayoría de las PyMES encuestadas dependen de otros medios o proveedores externos para el almacenamiento y la gestión de sus datos. Este análisis sugiere que una proporción considerable de las PyMES encuestadas ha optado por tener sus propios servidores de datos, lo que puede implicar una mayor autonomía y control sobre la infraestructura tecnológica y los datos confidenciales de la empresa. Sin embargo, la mayoría de las PyMES aún no han adquirido servidores propios, lo que podría indicar una dependencia de servicios externos o una menor inversión en infraestructura de TI.

Estos datos son relevantes para comprender la distribución de los recursos tecnológicos en las PyMES y las decisiones que toman en cuanto a la gestión de sus datos. Además, pueden servir como punto de partida para evaluar las necesidades y los desafíos en términos de almacenamiento y gestión de datos en el contexto de estas empresas.

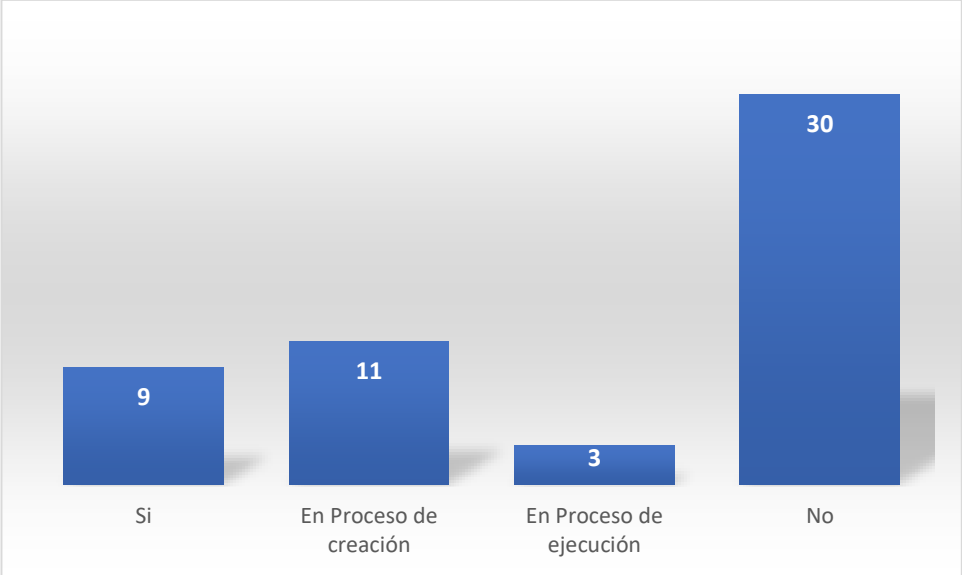
Tabla 6

4. ¿La empresa cuenta actualmente con políticas de seguridad informática que se encuentre expresadas en manuales de políticas y procesos?

Ítems	Frecuencia	Porcentaje
Si	9	16,98%
En Proceso de creación	11	20,75%
En Proceso de ejecución	3	5,66%
No	30	56,60%
Total	**53**	**100,00%**

Figura 15

Existen políticas de Seguridad Informática



Los resultados estadísticos presentados muestran la situación actual de las políticas de seguridad informática en las pequeñas y medianas empresas (PyMES) encuestadas:

Un total de 9 empresas, lo que equivale al 16,98% del total, indican que cuentan actualmente con políticas de seguridad informática expresadas en manuales de políticas y procesos. Esto sugiere que estas empresas han establecido formalmente políticas y procedimientos para garantizar la seguridad de la información y proteger sus activos digitales.

Por otro lado, se encontraron 11 empresas, lo que representa un 20,75% del total, que están en proceso de creación de políticas de seguridad informática. Esto implica que estas empresas están conscientes de la importancia de contar con políticas de seguridad, y están trabajando activamente en su desarrollo. Es un indicador positivo, ya que demuestra un esfuerzo por establecer medidas de protección y mitigar riesgos en el ámbito de la seguridad informática.

Solo 3 empresas, correspondientes al 5,66% del total, se encuentran en proceso de ejecución de las políticas de seguridad informática. Esto sugiere que han avanzado más allá de la etapa de creación y han comenzado a implementar y aplicar sus políticas de seguridad. Estas empresas están tomando medidas concretas para asegurar sus sistemas y datos. Por último, se identificó que 30 empresas, lo que representa el 56,60% del total, no cuentan actualmente con políticas de seguridad informática. Esto es preocupante, ya que indica una falta de enfoque y atención en la protección de los activos digitales y la seguridad de la información.

En resumen, los resultados muestran una diversidad en la adopción de políticas de seguridad informática en las PyMES encuestadas. Mientras que un pequeño porcentaje ya ha implementado políticas y procesos, una proporción significativa se encuentra en proceso de creación o ejecución. Sin embargo, la mayoría de las empresas aún no cuentan con políticas de seguridad informática, lo que sugiere la necesidad de una mayor conciencia y esfuerzo para fortalecer las medidas de seguridad en el ámbito digital.

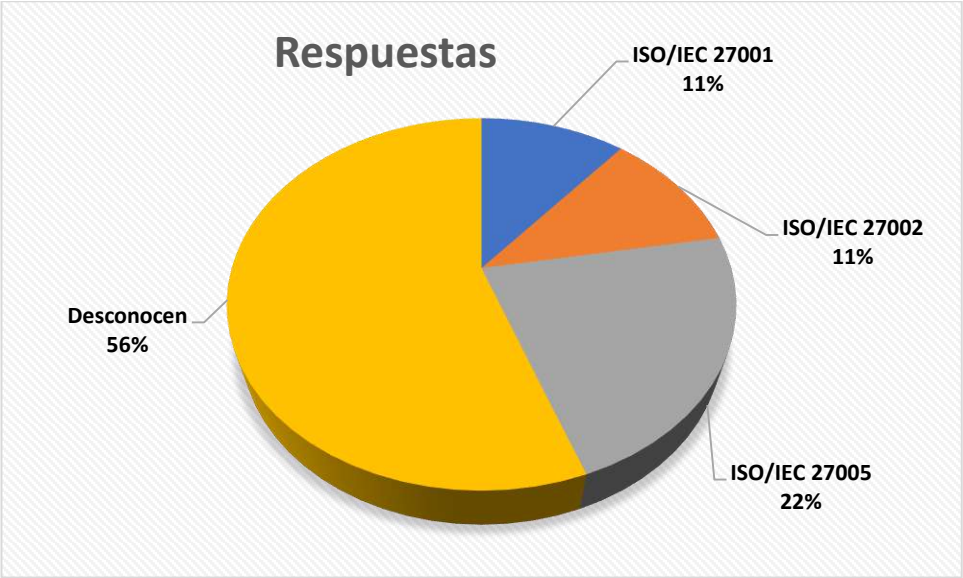
Tabla 7

5. Si respondió de forma afirmativa a la pregunta anterior ¿Conoce usted bajo que Norma o Estándar fueron diseñadas las políticas de seguridad informática?

Norma	Respuestas	Porcentaje
ISO/IEC 27001	1	11,11%
ISO/IEC 27002	1	11,11%
ISO/IEC 27005	2	22,22%
Desconocen	5	55,56%
TOTAL	**9**	**100,0%**

Figura 16

Se aplican normas o estándares a las políticas de seguridad



De acuerdo con los datos se encontró que ISO/IEC 27001 esta norma o estándar fue utilizado para diseñar las políticas de seguridad informática en un caso, lo cual representa el 11,11% del total de los casos analizados. Que la ISO/IEC 27002 al igual que en el caso anterior, esta norma o estándar también fue utilizado en un caso para diseñar las políticas de seguridad informática, lo cual representa el 11,11% del total de los casos. Que la ISO/IEC

27005 se utilizó en dos casos, las políticas de seguridad informática fueron diseñadas bajo la norma o estándar ISO/IEC 27005. Esto representa el 22,22% del total de los casos analizados. Finalmente, en cinco casos, no se especifica bajo qué norma o estándar fueron diseñadas las políticas de seguridad informática o si se utilizó alguna de ellas, esto representa el 55,56% del total de los casos analizados.

En resumen, según los datos proporcionados, se puede observar que la mayoría de los casos analizados (55,56%) desconocen bajo qué norma o estándar fueron diseñadas las políticas de seguridad informática. Sin embargo, hubo algunos casos (11,11% cada uno) en los que se utilizó ISO/IEC 27001 y ISO/IEC 27002, y en dos casos (22,22%) se utilizó ISO/IEC 27005.

Tabla 8

6. ¿El personal de la empresa ha recibido información sobre las políticas de seguridad informática?

Ítems	Respuestas	Porcentaje
Si	2	22,22%
Parcialmente	3	33,33%
No	4	44,44%
Total	**9**	**100,0%**

En la tabla 8 podemos observar que quienes implementaron algún tipo de políticas de seguridad de la información a penas el 22,22% de ellos recibieron la capacitación o al menos la información de las políticas, sin embargo, el 44,44 es decir el doble de los anteriores no recibieron o desconocen esos procedimientos, y quienes no recordaban o recibieron parcialmente la información de las políticas de seguridad fueron el 33,33%. Esto nos dice la importancia que están teniendo el cuidado de forma general de la información que las pequeñas y mediana empresas tienen sobre su activo intangible

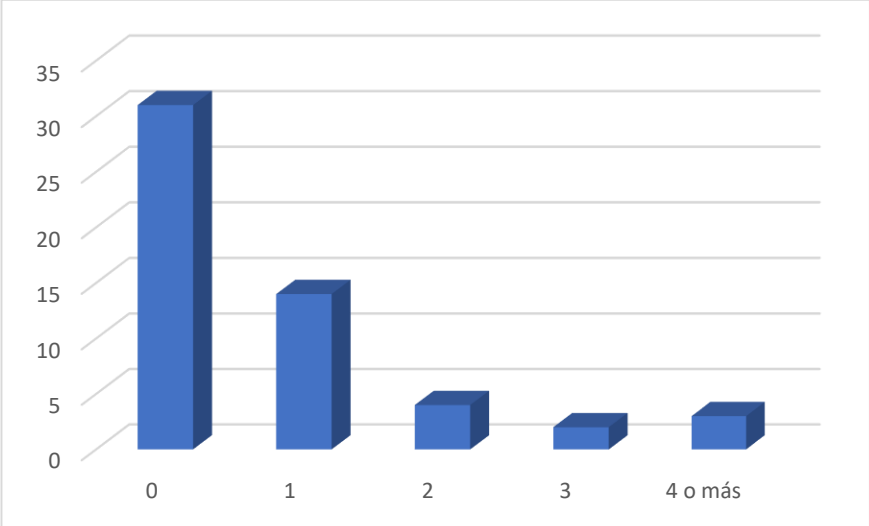
Tabla 9

7. ¿Existen programas de capacitación para el manejo y la seguridad Información en la empresa, indique cuantas al año realizan?

Cantidad	Respuestas	Porcentaje
0	31	58,5%
1	14	26,4%
2	4	7,5%
3	2	3,8%
4 o más	2	3,8%
Total	**53**	**100,0%**

Figura 17

Programas de Capacitación para la seguridad informática



Como demuestran los datos la información sobre la existencia de programas de capacitación para el manejo y la seguridad de la información en las pequeñas y medianas empresas (PyMES) encuestadas. A continuación, analicemos los datos:

El 58,5% de las PyMES encuestadas (31 empresas) indicaron que no tienen programas de capacitación para el manejo y la seguridad de la información en la empresa. Esta cifra representa la mayoría de las empresas encuestadas y sugiere una falta de enfoque en la capacitación específica en esta área.

Un 26,4% de las PyMES (14 empresas) mencionaron tener un programa de capacitación. Esto indica que un poco más de una cuarta parte de las empresas encuestadas reconocen la importancia de la capacitación en el manejo y la seguridad de la información y han implementado programas específicos para abordar esta necesidad. Solo el 7,5% de las PyMES (4 empresas) informaron contar con dos programas de capacitación en esta área. Esto indica que una pequeña proporción de las empresas encuestadas ha invertido en múltiples programas de capacitación para mejorar el manejo y la seguridad de la información.

El 3,8% de las PyMES (2 empresas) afirmaron tener tres programas de capacitación. Esto demuestra que una minoría aún más pequeña ha llevado a cabo esfuerzos considerables para brindar múltiples programas de capacitación en el manejo y la seguridad de la información. Otro 3,8% de las PyMES (2 empresas) mencionaron tener cuatro o más programas de capacitación. Esto indica que un número muy reducido de empresas encuestadas ha invertido significativamente en múltiples programas para mejorar sus conocimientos y habilidades en este ámbito.

En general, los resultados revelan que la mayoría de las PyMES encuestadas no cuentan con programas de capacitación específicos para el manejo y la seguridad de la información en la empresa. Sin embargo, una proporción considerable ha implementado al menos un programa de capacitación, con una minoría aún más pequeña invirtiendo en múltiples programas. Estos hallazgos resaltan la necesidad de fomentar la conciencia y la inversión en capacitación en materia de seguridad de la información para garantizar una gestión efectiva de los datos en las PyMES. También hay que considerar que los encuestados mencionaban que en ocasiones para cumplir con algún indicador generan capacitaciones inexistentes que solo están en el papel mas no en conocimiento real de los trabajadores.

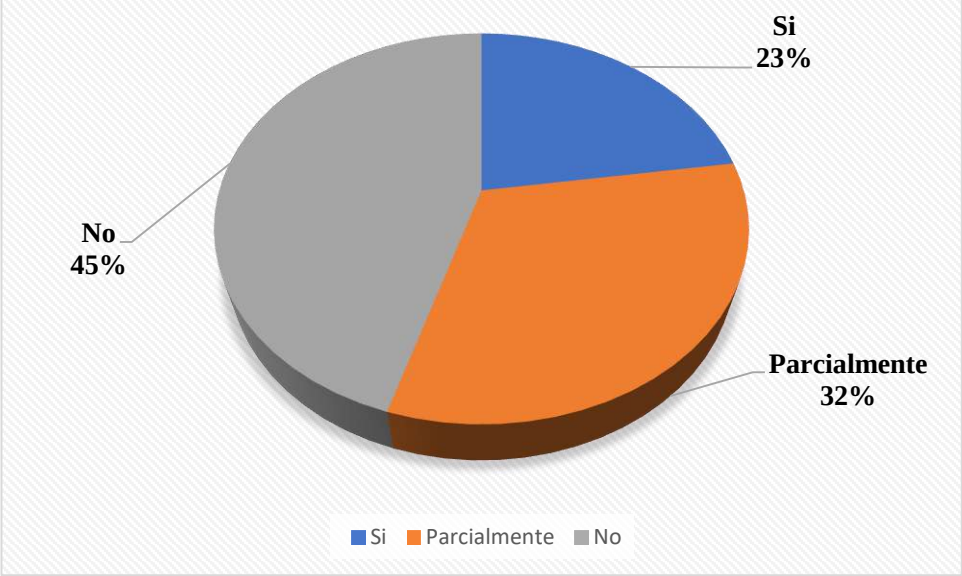
Tabla 10

8. ¿Se ha realizado la identificación y clasificación de los activos de información más importantes dentro de la empresa?

Ítems	Respuestas	Porcentaje
Si	12	22,64%
Parcialmente	17	32,08%
No	24	45,28%
Total	**53**	**100,0%**

Figura 18

Información de importancia para la empresa



Los resultados que se muestran en la tabla 10 muestran la identificación y clasificación de los activos de información más importantes dentro de la empresa. Analicemos los datos:

Para la opción Sí, se observa que 12 empresas, lo que representa un 22,64% del total, han realizado la identificación y clasificación de los activos de información más importantes. Esto indica que un porcentaje relativamente bajo de las empresas encuestadas ha llevado a cabo este proceso. En la opción Parcialmente, se encontraron 17 empresas, lo que equivale a un 32,08% del total. Esto sugiere que una proporción significativa de las empresas ha

realizado un avance parcial en la identificación y clasificación de sus activos de información, pero aún no ha completado el proceso en su totalidad.

En la opción No, se identificaron 24 empresas, lo que representa un 45,28% del total. Esta cifra indica que una proporción considerable de las empresas encuestadas aún no ha realizado la identificación y clasificación de los activos de información más importantes dentro de su organización.

En general, se puede inferir que un porcentaje notablemente bajo de las empresas encuestadas ha llevado a cabo la identificación y clasificación de los activos de información de manera completa. La mayoría de las empresas se encuentran en las categorías Parcialmente o No, lo que indica que aún queda trabajo por hacer en términos de proteger y gestionar adecuadamente los activos de información en estas organizaciones. Estos resultados resaltan la importancia de implementar políticas y prácticas sólidas de gestión de la información, así como la necesidad de concientización y capacitación en materia de seguridad de la información. Identificar y clasificar los activos de información es fundamental para establecer medidas de protección adecuadas y tomar decisiones informadas sobre la asignación de recursos para la seguridad cibernética.

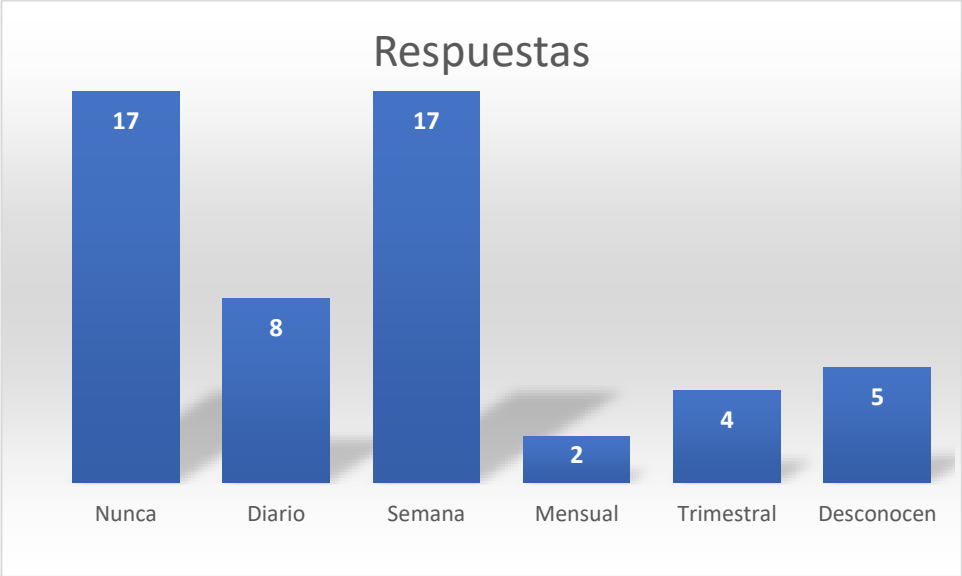
Tabla 11

9. Al respaldar la información de la empresa de forma general se lo realiza cada que tiempo:

Ítems	Respuestas	Porcentaje
Nunca	17	32,08%
Diario	8	15,09%
Semana	17	32,08%
Mensual	2	3,77%
Trimestral	4	7,55%
Desconocen	5	9,43%
Total	**53**	**100,0%**

Figura 19

Periodos de respaldo de información



Los resultados estadísticos presentados en la tabla 11 muestran la frecuencia con la que las empresas respaldan su información de forma general. Veamos el análisis de los datos:

El 32,08% de las empresas encuestadas indicaron que nunca respaldan su información. Esto es una preocupación significativa, ya que implica que estas empresas no cuentan con ninguna medida de respaldo para proteger sus datos en caso de pérdida o daño.

Un 15,09% de las empresas realizan respaldos diarios. Esta frecuencia diaria es positiva, ya que garantiza que los datos estén respaldados de forma regular y reduce el riesgo de pérdida de información valiosa. Otro 32,08% de las empresas realizan respaldos semanales. Aunque no es tan frecuente como el respaldo diario, sigue siendo una práctica razonablemente buena para garantizar la protección de los datos en caso de problemas.

Solo un 3,77% de las empresas realizan respaldos mensuales. Esta frecuencia es menos común y puede implicar un mayor riesgo, ya que los datos pueden perderse o dañarse antes de que se realice el próximo respaldo.

Un 7,55% de las empresas realizan respaldos trimestrales. Esta frecuencia es aún menos frecuente y puede ser insuficiente para garantizar una protección adecuada de los datos, ya que hay un período prolongado entre los respaldos. Un 9,43% de las empresas desconocen la frecuencia con la que realizan respaldos de su información. Esta falta de conocimiento puede ser preocupante, ya que indica una falta de conciencia o de una política establecida en relación con la protección de datos.

En general, estos resultados revelan una variedad de prácticas de respaldo de información en las empresas encuestadas. Aunque algunas empresas realizan respaldos diarios o semanales, una proporción considerable no realiza respaldos o tiene una frecuencia de respaldo baja. Esto resalta la importancia de concienciar a las empresas sobre la necesidad de implementar estrategias de respaldo de datos regulares y confiables para proteger su información empresarial.

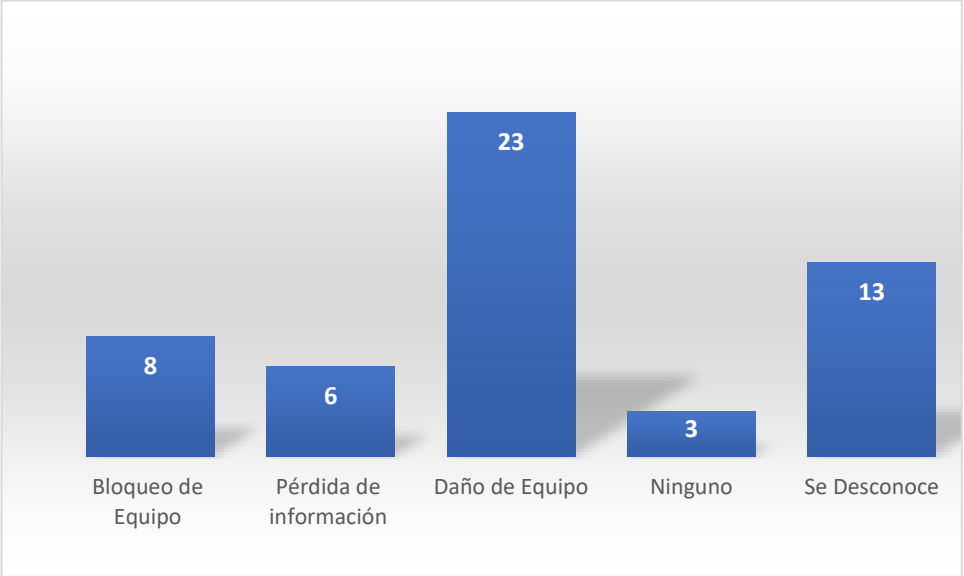
Tabla 12

10. ¿Cuáles de los siguientes incidentes de seguridad informática se han presentado en la empresa en los últimos años?

Ítems	**Respuestas**	**Porcentaje**
Bloqueo de Equipo	8	15,09%
Pérdida de información	6	11,32%
Daño de Equipo	23	43,40%
Ninguno	3	5,66%
Se Desconoce	13	24,53%
Total	**53**	**100,00%**

Figura 20

Incidentes ocurridos con la información



Analicemos los datos se observan que el Bloqueo de Equipo según los resultados, se registraron 8 incidentes de bloqueo de equipo, lo que representa un 15,09% del total. Esto implica que un número significativo de equipos de la empresa experimentaron bloqueos o fallas que impidieron su funcionamiento normal. Estos bloqueos pueden haber sido causados por diversos factores, como malware, fallas técnicas o errores humanos.

En cuanto a Pérdida de información los datos muestran que se reportaron 6 incidentes de pérdida de información, lo que corresponde a un 11,32%. Este tipo de incidente implica la eliminación accidental o no autorizada de datos importantes de la empresa, lo cual puede tener consecuencias graves en términos de pérdida de información confidencial o crítica.

Para Daño de Equipo se registraron 23 incidentes de daño de equipo, lo que representa un 43,40% del total. Esto indica que un número considerable de equipos de la empresa sufrió daños físicos o técnicos. Estos daños pueden ser causados por diversos factores, como fallos en hardware, condiciones ambientales adversas o acciones maliciosas. Para la opción

Ninguno, se encontraron 3 respuestas indicando que no se ha experimentado ningún incidente de seguridad informática en la empresa en los últimos años. Esto representa un 5,66% del total de respuestas. Es importante destacar que esta cifra puede ser positiva, ya que indica que la empresa ha logrado mantener un entorno relativamente seguro en términos de incidentes de seguridad.

Finalmente tenemos la opción se Desconoce con 13 respuestas indicaron desconocimiento de los incidentes de seguridad informática que se han presentado en la empresa. Esto representa un 24,53% del total de respuestas. Esta falta de conocimiento puede deberse a la falta de registro o seguimiento adecuado de los incidentes, lo cual puede ser preocupante, ya que dificulta la evaluación y respuesta efectiva ante posibles problemas de seguridad.

En resumen, los resultados muestran que la empresa ha experimentado una variedad de incidentes de seguridad informática en los últimos años, incluyendo bloqueo de equipo, pérdida de información y daño de equipo. Estos incidentes resaltan la importancia de implementar medidas de seguridad sólidas para proteger los sistemas y datos de la empresa. Además, es relevante mejorar la conciencia y el registro de los incidentes de seguridad para una gestión más efectiva de la seguridad informática.

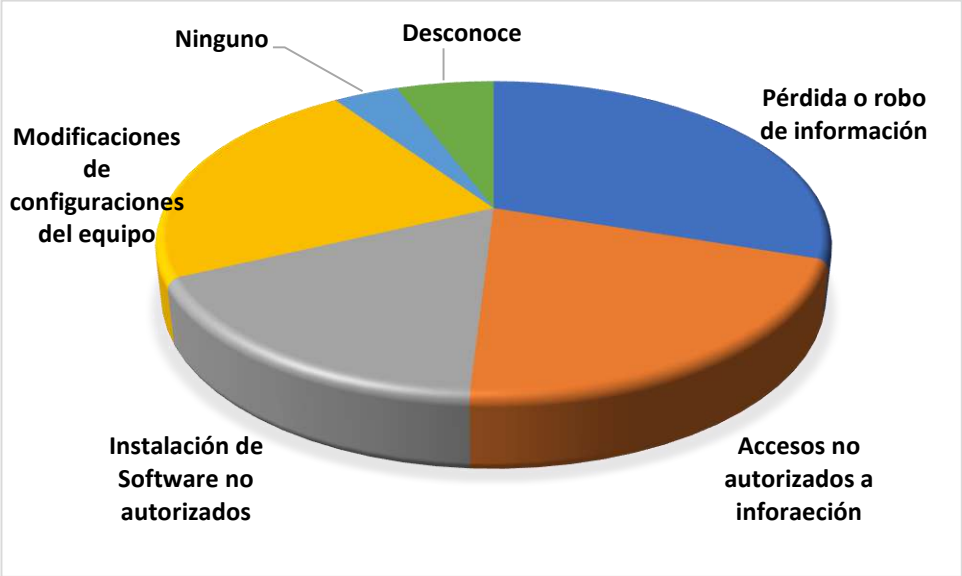
Tabla 13

11. Al desarrollar sus actividades diarias ¿Qué tipo de riesgos informáticos fueron informados en la empresa?

Ítems	**Respuestas**	**Porcentaje**
Pérdida o robo de información	16	30,19%
Accesos no autorizados a información	11	20,75%
Instalación de Software no autorizados	9	16,98%
Modificaciones de configuraciones del equipo	12	22,64%
Ninguno	2	3,77%
Desconoce	3	5,66%
Total	**53**	**100,00%**

Figura 21

Riesgos informáticos informados por empleados



De acuerdo con los resultados obtenido de la data podemos observar en la tabla 13 que la categoría más comúnmente informada es la Pérdida o robo de información, con un total de 16 casos, lo que representa el 30,19% del total. Esto indica que la empresa ha experimentado incidentes en los que se ha producido la pérdida o el robo de información, lo que puede tener un impacto significativo en la confidencialidad y la integridad de los datos. En segundo lugar, de riesgo informado con mayor frecuencia es el de Accesos no autorizados a información, con 11 casos, lo que equivale al 20,75% del total. Esto sugiere que la empresa ha enfrentado problemas relacionados con personas que intentan acceder a información sensible o confidencial sin tener la autorización correspondiente.

En tercer lugar, se encuentra la "Instalación de Software no autorizado", con 9 casos, lo que representa el 16,98%. Esto indica que la empresa ha enfrentado desafíos relacionados con la instalación de software no autorizado en los equipos, lo cual puede introducir vulnerabilidades y riesgos de seguridad. Otro tipo de riesgo informado es el de

"Modificaciones de configuraciones del equipo", con 12 casos, lo que equivale al 22,64%. Esto sugiere que la empresa ha experimentado incidentes en los que se han realizado cambios no autorizados en la configuración de los equipos, lo que puede comprometer su funcionamiento y la seguridad de los datos almacenados.

Un número pequeño de casos informados, 2 en total (3,77%), indican que no se han reportado riesgos informáticos en la empresa. Además, se registraron 3 casos (5,66%) en los que se desconoce qué tipos de riesgos informáticos han sido informados. Esto puede deberse a una falta de información o registro adecuado de los incidentes.

En general, estos datos proporcionan una visión de los riesgos informáticos enfrentados por la empresa en cuestión. Los resultados destacan la importancia de abordar y mitigar estos riesgos para proteger la información y los sistemas de la empresa contra pérdidas, accesos no autorizados y otros incidentes. Estos resultados también pueden servir como base para la implementación de medidas de seguridad adecuadas y la concientización sobre la importancia de proteger los recursos informáticos de la organización.

Para aportar criterios que les permitan un modelo básico para el aseguramiento de la información se pude considerar los siguientes aspectos de seguridad de la información para PYMEs (Pequeñas y Medianas Empresas). Este modelo se basa en las mejores prácticas y estándares de seguridad de la información. Recuerda que es importante adaptar este modelo a las necesidades y características específicas de tu empresa.

Evaluación de riesgos: Realiza una evaluación de riesgos para identificar las amenazas y vulnerabilidades de seguridad de la información en tu empresa. Considera aspectos como acceso no autorizado, pérdida de datos, ataques cibernéticos, desastres naturales, etc.

Política de seguridad de la información: Desarrolla una política clara de seguridad de la información que establezca los objetivos, principios y responsabilidades en relación con

la protección de la información. Asegúrate de que todos los empleados comprendan y acepten esta política.

Gestión de accesos: Implementa un sistema de gestión de accesos para controlar quién tiene acceso a los sistemas y datos de la empresa. Asigna privilegios de acceso basados en los roles y responsabilidades de cada empleado.

Protección de datos: Utiliza medidas de protección adecuadas para los datos de tu empresa, como cifrado de datos, contraseñas seguras, autenticación de dos factores, etc. Además, realiza copias de seguridad regularmente y almacena los datos de forma segura.

Concientización y capacitación: Educa a tus empleados sobre las mejores prácticas de seguridad de la información, incluyendo la importancia de contraseñas seguras, la detección de correos electrónicos de phishing y el uso seguro de los recursos informáticos de la empresa.

Gestión de incidentes: Establece un proceso claro para la gestión de incidentes de seguridad de la información. Define cómo se deben reportar y gestionar los incidentes, así como los roles y responsabilidades de los equipos encargados de ello.

Actualizaciones y parches: Mantén tus sistemas operativos, aplicaciones y dispositivos actualizados con los últimos parches de seguridad. Esto ayudará a proteger tu empresa contra las vulnerabilidades conocidas.

Auditoría y monitoreo: Realiza auditorías periódicas de seguridad de la información para evaluar el cumplimiento de las políticas y estándares establecidos. Implementa herramientas de monitoreo que te permitan detectar actividades sospechosas o no autorizadas en tus sistemas.

Contratos y proveedores: Si trabajas con proveedores externos, asegúrate de que cumplan con los estándares de seguridad de la información. Incluye cláusulas de seguridad en los contratos para garantizar la protección de los datos compartidos.

Evaluación continua: La seguridad de la información debe ser un proceso continuo. Realiza evaluaciones y mejoras constantes en función de los cambios tecnológicos, las amenazas emergentes y las necesidades de tu empresa.

Aplicación de ISO/IEC 27001: Que al menos que trate de implementar una de las normas ISO, que le permitan garantizar los procesos del aseguramiento de la información, con ello la empresa se sienta comprometida en mantener los indicadores apropiados.

3.3. Contribuciones Teóricas

Podemos decir que, el estudio puede hacer contribuciones teóricas al identificar las necesidades de seguridad, evaluar las prácticas existentes, desarrollar recomendaciones específicas y validar la eficacia de las medidas de seguridad en las PYMES de la ciudad de Guayaquil. Estas contribuciones pueden ayudar a mejorar la comprensión y la implementación de la seguridad informática en el contexto empresarial de las PYMES.

Identificación de las necesidades de seguridad en las PYMES: El estudio puede proporcionar una comprensión más profunda de las necesidades y desafíos específicos de seguridad informática que enfrentan las PYMES en la ciudad de Guayaquil. Esto puede ayudar a llenar un vacío de conocimiento existente y proporcionar información valiosa sobre las áreas en las que las PYMES necesitan mejorar su seguridad informática.

Evaluación de prácticas y marcos de seguridad existentes: El estudio puede evaluar las prácticas y marcos de seguridad informática que se utilizan actualmente en las PYMES de la ciudad de Guayaquil. Esto puede permitir una comparación entre las prácticas actuales y las mejores prácticas teóricas y marcos de seguridad reconocidos internacionalmente. Además, el estudio puede identificar las brechas existentes entre la teoría y la práctica en términos de seguridad informática en las PYMES.

Desarrollo de recomendaciones y directrices específicas: Basándose en los hallazgos del estudio, se pueden desarrollar recomendaciones y directrices específicas para mejorar la

seguridad informática en las PYMES de la ciudad de Guayaquil. Estas recomendaciones pueden ser personalizadas para abordar las necesidades y desafíos únicos de las PYMES en esta región. Esto puede ayudar a las PYMES a implementar medidas de seguridad efectivas y mejorar su capacidad para proteger sus redes empresariales.

Validación de la eficacia de las medidas de seguridad: El estudio puede incluir una evaluación de la eficacia de las medidas de seguridad implementadas en las PYMES de la ciudad de Guayaquil. Esto puede ayudar a determinar si las medidas existentes son efectivas en la protección de las redes empresariales contra amenazas de seguridad. Además, el estudio puede identificar áreas en las que se necesitan mejoras y proporcionar recomendaciones para fortalecer la seguridad informática en las PYMES.

Podemos decir que, el estudio puede hacer contribuciones teóricas al identificar las necesidades de seguridad, evaluar las prácticas existentes, desarrollar recomendaciones específicas y validar la eficacia de las medidas de seguridad en las PYMES de la ciudad de Guayaquil. Estas contribuciones pueden ayudar a mejorar la comprensión y la implementación de la seguridad informática en el contexto empresarial de las PYMES.

3.4. Limitaciones

Para el presente trabajo de investigación se presentaron las siguientes limitaciones:

Tamaño y representatividad de la muestra: Si el estudio se basa en una muestra pequeña y no representa adecuadamente a todas las PYMES de la ciudad de Guayaquil, los resultados pueden no ser generalizables y limitar su aplicabilidad a otras empresas en la misma región o en diferentes contextos, debido al tiempo de investigación y a las respuestas obtenidas entre el total de las empresas y las que respondieron podría afectar los resultados esperados para generalizar a todos los sectores.

El aporte de las empresas encuestas que mostraron el interés por mejorar la seguridad de su información podría generar un sesgo de selección. Por tanto, si la selección

de las PYMES participantes fue aleatoria, pero se recibió las respuestas aquellas que ya estaban interesadas, puede haber un sesgo en los resultados y no reflejar la situación general de todas las PYMES en la ciudad.

Limitaciones de tiempo y recursos, el estudio se llevó a cabo en un período de tiempo limitado y con recursos limitados, lo que no permitió un mayor abordaje todos los aspectos relevantes de la seguridad informática a nivel físico, ciber y de las redes empresariales de las PYMES. Esto podría afectar la profundidad y la amplitud de los resultados.

Basado en el punto anterior los datos recopilados se basan únicamente en cuestionarios o entrevistas auto informadas, que permitan comprender el tratamiento y manejo de la información general y empresarial de las PYMES, lo que no permitió correlacionar algunos aspectos cualitativos y puede llegar a genera algún tipo de impresión en las respuestas.

Hay que recordar que este tipo de estudios es necesario realizar un seguimiento a largo plazo, si este para conocer las medidas que se implemente y poder ampliar los resultados analizados a lo largo del tiempo, puede haber limitaciones en la evaluación del impacto sostenido de las acciones tomadas para mejorar la seguridad informática en las PYMES.

CONCLUSIONES

Se ha detectado que las principales problemáticas relacionadas con la seguridad informática en las pequeñas y medianas empresas (PyMES) en la ciudad de Guayaquil se generan por lo siguiente: el 56,60,18% de los encuestadas no tienen una política de seguridad implementada en sus operaciones, el 44.44% de estas no brindan a su personal la información necesaria de sus políticas, el 58,5% no brinda capacitación regular a sus empleados sobre seguridad informática de hecho el porcentaje antes mencionado corresponde a cero capacitaciones al año y el 45,28% no lleva un registro de eventos o activos informáticos dentro de la empresa. Estas situaciones se deben a la falta de recursos y a la toma de decisiones inoportunas. Sin embargo, si la parte administrativa de las PyMES continúa tratando la seguridad informática como algo de poca relevancia, el problema podría complicarse aún más en el futuro, ya que los ciberataques están aumentando en gran medida.

Entre los riesgos informáticos identificados en este estudio se encuentran la pérdida o el robo de información, la instalación de software no autorizado y el daño a los equipos informáticos. Tanto la información como los equipos informáticos son activos valiosos para las PyMES y, por lo tanto, deben ser protegidos contra amenazas que puedan comprometer su disponibilidad, privacidad y veracidad. Para reducir el nivel de riesgo informático, es necesario considerar medidas adecuadas y establecer controles de seguridad informática apropiados según las necesidades de las PyMES, esto se contrasta con el estudio realizado por Antunes, Maximiano, Gomes, & Pinto (2021), dende expresa que las pequeñas y medianas empresas no se preocupan de salvaguardar los activos intangibles es decir la información general de la empresa.

Para desarrollar una guía de seguridad informática efectiva, se debe tener en cuenta que sea útil, sencilla, práctica y adaptada a las necesidades de las PyMES. Para mejorar los

niveles de seguridad informática, se requiere implementar un conjunto de medidas y controles que abarquen tanto procesos como funciones de software y hardware. Estos deben ser supervisados no solo por especialistas en tecnologías de la información, sino también por los administradores de las PyMES y por todos aquellos que utilicen tecnologías de la información dentro de la empresa, con el objetivo de proteger la información y los equipos informáticos, como se demuestra en la encuesta las pequeñas y medianas empresas guayaquileñas apenas el 30,19% de estas cuenta con servidores propios para almacenar o respaldar la información, y que los encargados del cuidado de esta actividad son los empleados y administrador en 47,17% , es decir personal sin experiencia en el área de las nuevas tecnologías de la información, así lo afirma Huerta, Gaete, & Pedraja (2020), donde demuestra la importancia de contar no solo con el personal apropiado y un sistema de información para el mantenimiento y aseguramiento de la información.

En la validación de la guía de seguridad informática por parte de expertos, se promediaron las calificaciones obtenidas en la evaluación de 8 indicadores. El resultado obtenido en esta evaluación respalda la propuesta presentada en este trabajo, ya que se obtuvo una calificación de 5, considerada como "Muy buena".

LECCIONES APRENDIDAS

El aseguramiento de la información para cualquier organización en la actualidad no solo consiste en el respaldo de esta y el cuidado y mantenimiento de los equipos, hay que considerar como se ha observado y analizado que hay otros factores que inciden en afectaciones por el mal uso o cuidado de esta información, que ha pasado a ser un activo intangible para las pequeñas y medianas empresas.

Con relación al trabajo desarrollado, los objetivos fueron establecidos claramente desde y se centraron en proporcionar a las pequeñas y medianas empresas (PYMES) mejores un análisis y herramientas para gestionar la seguridad de la información y la ciberseguridad. Con respecto a la concientización del manejo de la información que se les debe brindar a los empleados para que estos conozcan y manejen la información basados en políticas y normas claras. La metodología adoptada para el marco ISO-27001:2013 está en línea con lo que se describe en la literatura. El alcance del trabajo de investigación se centra en las PYMES y las microempresas, y el objetivo es mejorar la seguridad de la información para evitar la pérdida o robo de esta, por parte de empleados o ciber ataques en general. Aunque existen otros marcos, como el Marco de Ciberseguridad del NIST, que podrían aplicarse a la auditoría de seguridad en las PYMES, se ha identificado en la literatura que el marco ISO-27001:2013 es una mejor práctica cuando se trata de seguridad de la información para este tipo de empresas.

En cuanto al impacto en las PYMES que estas puedan tener, es importante destacar las mejoras que puedan presentar, especialmente en aquellas empresas que se implemente políticas, capacitaciones y respaldo periódicos. Sin embargo, las PYMES guayaquileñas presentan indicadores muy bajos en las áreas informáticas de forma general, es decir tanto en la cantidad de equipos, políticas, encargados de respaldo, capacitaciones e información sobre la seguridad de la información.

La seguridad de la información es un tema muy amplio en los que se puede explorar

diferentes enfoques para implementar soluciones sólidas e integradas. La adopción de normas como la ISO-27001:2013 la cual se basa en la revisión de las mejores prácticas y marcos de seguridad de la información que deben aplicarse en las PYMES. Sin embargo, es importante tener en cuenta que es una herramienta para ampliar el objetivo de la investigación y puede considerarse una limitación en este estudio.

En este sentido, es necesario abordar, implementar y comparar otras mejores prácticas y marcos con el fin de evaluar la idoneidad total de ISO-27001:2013 para las PYMES de la ciudad de Guayaquil.

Bibliografía

Acuña, E. P. (2017). Ejercicio De La Revisoria Fiscal En La Actualidad. *Universidad Libre De Colombia* .

Almagro, L. (2019). Ciberseguridad Marco Nist Un Abordaje Integral. *Oea*.

Alzoubi, H., & Alshurideh, M. (2020). Do Perceived Service Value, Quality, Price Fairness And Service Recovery Shape Customer Satisfaction And Delight? A Practical Study In The Service Telecommunication Context . *Uncertain Supply Chain Management*.

Anser, M., & Zhang, Z. &. (2018). Moderating Effect Of Innovation On Corporate Social Responsibility And Firm Performance In Realm Of Sustainable Development. *Corporate Social Responsibility And Environmental*.

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information Security And Cybersecurity Management: A Case Study With Smes In Portugal. *Cybersecur. Privacy*.

Armenia, S., Angelini, M., & Nonino, F. (2021). A Dynamic Simulation Approach To Support The Evaluation Of Cyber Risks And Security Investments In Smes. *Sciencedirect Decision Support Systems*.

Bacinello, E. T. (2020). Influence Of Corporate Social Responsibility On Sustainable Practices Of Small And Medium-Sized Enterprises: Implications On Business Performance. *Corporate Social Responsibility And Environmental Management*.

Bahta, D., Yun, J., Islam, M. R., & & Ashfaq, M. (2020). Corporate Social Responsibility, Innovation Capability And Firm Performance: Evidence From Sme. Social Responsibility Journal. *Ahead-Of-Print*.

Bang, Y., & Lee, D. (2012). Improving Information Security Management:. *International Journal Of Information Management, 32,*, 409–418.

Barzanallana, R. (2019). ¿Introducción A La Seguridad Informática. *Umu.*

Batra, J., & Jain, R. (2021). A Comprehensive Study Of Spam Detection In E-Mails Using Bio-Inspired Optimization Techniques. *Journal Of Information Management Data Insights*.

Brâncoveanu, C. (2017). A Model Of Socially Responsible Organizational Culture. *University, Piteşti, Romania*, 48.

Briones, P., Molina, S., & Avilés, M. (2020). Modelo De Evaluación De Los Sistemas De Información. *Revista De Producción, Ciencias E Investigación,*.

Bukht, R., & Heeks, R. (2017). *Defining, Conceptualising And Measuring The Digital Economy.* University Of Manchester: Global Development Institute.

Cajal, A. (2019). Investigación De Campo: Características, Tipos, Técnicas Y Etapas. *Https://Www.Lifeder.Com/Author/Alberto-Cajal/*.

Cajiao, L. (2021). _Importancia_Clima_Organizaciónal_Dentro_Ambiente_Laboral_Empresa. *Universitaria Católica Lumen Gentium*.

Carpio, R. E. (2018). Modelo De Gestión Administrativo Para Empresas Familiarescaso Carvicaucho. *Pontificia Universidad Católica Del Ecuador* .

Castañeda, R., Ortega, P., & García, D. A. (2016). Información Desde El Punto De Vista De La Gestión Del Conocimiento . *Information Systems Success Measurement*.

Cepal. (2021). Transformación Digital De Las Mipymes. *Cepal Elementos Para El Diseño De Políticas*.

Chávez, J. D., & Loaiza, C. A. (2018). El Aseguramiento De La Información Como Método De Calidad Para La Auditoria Y Valoración Financiera. *Universidad Cooperativa De Colombiavalle Del Cauca*.

Chávez, J., & Loaiza, C. (2018). El Aseguramiento De La Información Como Método De Calidad Para La Auditoria Y Valoración Financiera. *Universidad Cooperativa De*

Colombia Valle Del Cauca.

Cuba, C. N. (2019). Responsabilidad Social Y Rendimiento Laboral En Los Colaboradores De Los Programas Sociales De Lima, Perú. *Revista Conrado, ,* 278-285.

Economic Research-Ekonomska, I. (2022). Impact Of Corporate Social Responsibility On Social. *Economic Research-Ekonomska Istraživanja*.

Encuesta Mundial Sobre El Estado De La Seguridad De La Información, 2. (2017). Encuesta Mundial Sobre El Estado De La Seguridad De La Información 2017. *Pwc España*.

Espinosa, J. (2014). Seminario Internacional De Seguridad Informática Y Técnicas De Comunicación, Y Su Aplicación En Logística. *Universidad Eafit*.

Evans, N., & Price, J. (2020). Development Of A Holistic Model For The Management Of An Enterprise's Information Assets. *International Journal Of Information Management, 54*.

Fernández, L. M. (2016). Responsabilidad Social Corporativa Estratégica De Los Recursos Humanos Basada En Alto Compromiso Y Resultados Organizativos: Un Modelo Integrador. *Universidad Complutense De Madrid Facultad De Ciencias Económicas Y Empresariales*, 106.

Gurmendi, P. P. (2018). Gestión De Los Sistemas De Información En La Toma De Decisiones De La Municipalidad Distrital De El Tambo 2018. *Universidad Nacional Del Centro Del Perú* .

Harris, S., & Maymi, F. (2016). Chapter 1: Security And Risk Management. In Cissp All-In-One Exam Guide. *Mcgraw-Hill Education*.

Hernández, S. R. (2014). *Metodología De La Investigación.* Mexico: Mcgraw-Hill.

Huerta, P. C., Gaete, H. G., & Pedraja, L. M. (2020). Dirección Estratégica, Sistema De Información Y Calidad. El Caso De Una Universidad Estatal Chilena. *Scielo: Información Tecnológica*.

Ikrema, H., & Carballo, P. A. (2021). High-Performance Human Resource Management Practices And Readiness For Change: An Integrative Model Including Affective Commitment, Employees' Performance, And The Moderating Role Of Hierarchy Culture. *European Research On Management And Business Economics*.

Innovación En La Sociedad Digital, A. (2021). *Innovación En La Sociedad Digital*. Obtenido De Https://Blog.Mdcloud.Es/Inteligencia-Artificial-En-Las-Empresas-Definicion-Beneficios-Y-Riesgos/

Instituto Nacional De Seguridad, S. Y. (2018). Directrices Para La Gestión Preventiva En Las Pymes. *Instituto Nacional De Seguridad, Salud Y Bienestar En El Trabajo (Inssbt*.

Laudon, K. C., & Laudon, J. P. (2016). Sistemas De Información Gerencial. En K. C. Laudon, *Authorized Translation From The English Language Edition, Entitled Management Information Systems 14th Edition.* Maxico.

Leal, R. Y. (2021). Buenas Prácticas De Seguridad Informática Aplicado Al Comercio Electrónico Para Las Pymes Colombianas Asociada A La Norma Iso 27001:2013 Anexo A. *Universidad Nacional Abierta Y A Distancia – Unad*.

Leea, S., & Han, H. (2020). Corporate Social Responsibility (Csr) As A Customer Satisfaction And Retention Strategy In The Chain Restaurant Sector. *Journal Of Hospitality And Tourism Management*.

Leiva, A., Mantilla, L., & Córdoba, J. (2022). Propuesta De Un Modelo De Ciberseguridad Para La Pequeña Empresa En Costa Rica. *Universidad Latinoamericana De Ciencia Y Tecnología*.

López Et Al, R. P. (2015). *Metodología De La Investigación Social Cuantitativa.* Universitat Autònoma De Barcelona.

López, S., Ojeda, H. J., & Ríos, M. M. (2017). La Responsabilidad Social Empresarial Desde La Percepción Del Capital Humano. Estudio De Un Caso. *Sciencedirect Revista De*

Contabilidad Spanish Accounting Review.

Maino, V. (2021). Estrategia Nacional De Ciberseguridad Del Ecuador. *Ministerio De Telecomunicaciones Y Sociedad De La Información*.

Marcandella, E., & Garccia, B. (2016). *De Boeck Supérieur*.

Mendivil, C., Borja, S., & Gutierrez, A. (2022). Formación Y Concienciación En Ciberseguridad Basada En Competencias: Una Revisión Sistemática De Literatura. *Recyt.Fecyt.Es/Index.Php/Pixel/Article/View/91640*.

Molina, E. H. (2019). Las Normas De Aseguramiento En Colombia Y Sus Efectos En El Ejercicio De La Revisoría Fiscal. *Conejo Técnico De La Consejoria Pública* .

Muñoz, H., Zapata, L., & Vida, R. (2019). Riesgos Informáticos Y Alternativas Para La Seguridad Informática En Sistemas Contables En Colombia. *Revista Venezolana De Gerencia, Vol. 2*.

Niño, M. (2018). Modelo De Un Sistema De Gestión De Seguridad De Información – Sgsi, Para Fortalecer La Confidencialidad, Integridad, Disponibilidad Y Monitorear Los Activos De Información. *Universidad Nacional "Pedro Ruiz Gallo"*.

Orozco, S. J. (2018). Diseño De Solución Tecnológica En La Nube Para La Entrega Inmediata Y Confiable De Un Sistema De Gestión De Operaciones Para Freelancers. *Universidad De San Carlos De Guatemala.*

Otero, O. A. (2018). Enfoques De Investigación: Métodos Para El Diseño Urbano - Arquitectónico. *Currently Works At The Facultad De Arquitectura*.

Paul, K., & Colm, K. (2019). The Importance Of Data Backup Policies And What To Include. *Https://Www.Techtarget.Com/Searchdatabackup/Tip/The-Importance-Of-Backup-Policies*.

Pooja, C., Gupta, B. B., Chang, X., & Nedjah, N. (2021). Enhancing Big Data Security Through Integrating Xss Scanner Into Fog Nodes For Smes Gain. *Scenciedirect*

Technological Forecasting And Social Change.

Rodríguez, C. A. (2017). Responsabilidad Social Corporativa En La Red Hospitalaria De Utilización Pública De Cataluña. *Universitat De Lleida*.

Rodríguez, C., Rodrígueza, C., & Zöllera, D. G. (2021). Responsabilidad Social Corporativa En Los Centros De La Red Hospitalaria De Utilización Pública De Cataluna. *Journal Title: Gaceta Sanitaria*.

Romero, M., Figueroa, G., & Vera, D. (2018). *Introducción A La Seguridad Informática Y El Análisis De Vulnerabilidades.* Manabí: Universidad Del Sur De Manabí.

Samonas, S., & Coss, D. (2014). *The Cia Strikes Back: Redefining Confidentiality, Integrity And Availability In Security*. Obtenido De Url: Http://Www. Proso.Com/Dl/Samonas.Pdf

Shafat, M., & Nasir, Z. (2018). Corporate Social Responsibility And Financial Performance: An Empirical Analysis Of Indian Banks. *Sciencedirect*.

Stallings, W. (2017). *Fundamentos De Seguridad En Redes. Aplicaciones Y Estándares.* Pearson Prentice Hall.

State Of Cyber Security, A. (2017). Pruebas De Penetración Para La Seguridad Informática Al Servidor Web Del Laboratorio De Ciberseguridad. *Sathir Sembrador*.

Trávez, C. F. (2018). El Clima Organizacional Y El Desempeño Laboral En El Departamento Simtel Del Gobierno Autónomo Desecntralizado Municipal Del Cantón Latacunga Provincia De Cotopaxi. *Universidad Técnica De Ambato*.

Vargas, A., Cristancho, L., & Michael, M. (2019). Modelo De Aseguramiento De La Información Y Revisoría Fiscal En Colombia. *Universidad Libre De Colombia*.

Vargas, P. A., & Cristancho, D. L. (2018). Modelo De Aseguramiento De La Información Y Revisoría Fiscal En Colombia. *Universidad Libre De Colombia*.

Whitman, M., Mattord, H., & Green, A. (2014). *Hands-On Information Security Lab Manual.*

Cengage Learning.

Yang, A. (2019). Price Differentiation Model: Its Challenges And Solutions. *J Revenue Pricing Manage*.

Ynzunza, C., Izar, J., & Bocarando, J. (2017). El Entorno De La Industria 4.0: Implicaciones Y Perspectivas Futuras. *Conciencia Tecnológica, Núm. 54, 2017*.

Yu, M.-C. M.-B. (2018). An Empirical Study On The Organizational Trust, Employee-Organization Relationship And Innovative Behavior From The Integrated. *Mdpi*.

Zenck, M. C., Ríos, I., & Pogo, L. (2017). Análisis De La Transparencia Sobre Las Políticas Locales De Responsabilidad Social En Ecuador: Estudio De Los Casos De Quito, Guayaquil Y Machala. *Rigc*.

Zuña, M. E., Arce, R. Á., & Romero, B. W. (2019). Análisis De La Seguridad De La Información En Las Pymes De La Ciudad De Milagro. *Revista Científica De La Universidad De Cienfuegos*.

Apéndice 1 Encuesta

Se diseño un cuestionario compuesto por once preguntas concretas con el fin de respaldar la propuesta y evaluar la situación actual de la seguridad informática en las pequeñas y medianas empresas (PYMES) de Guayaquil, Ecuador.

Se diseñó un formulario utilizando la herrmienta Google Forms y se distribuyó entre los contactos de las PYMES en la ciudad de Guayaquil que cuentan con un departamento de Tecnología e Informática. Las preguntas incluidas en el cuestionario fueron las siguientes:

1. ¿Cuál es el individuo encargado de implementar y preservar el software de seguridad en los dispositivos informáticos de la organización?

2. ¿Cuántas computadoras tiene la compañía a su disposición para el trabajo relacionado al manejo de la información Contable-Financiera?

3. ¿La empresa cuenta con servidores centrales de datos disponibles, de su propiedad o instalados dentro de ella?

4. ¿En la actualidad existen Políticas de Seguridad Informática documentadas y gestionadas en la empresa?

5. Si respondió de forma afirmativa a la pregunta anterior ¿Conoce usted bajo que Norma o Estándar fueron diseñadas las políticas de seguridad informática?

6. ¿El personal de la empresa ha recibido información sobre las políticas de seguridad informática?

7. ¿Cuántas capacitaciones en este año han recibido los empleados acerca de la Seguridad Informática?

8. ¿Se ha realizado la identificación y clasificación de los activos de información más importantes dentro de la empresa?

9. Al respaldar la información de la empresa de forma general la respaldan:

10. ¿Cuáles de los siguientes incidentes de seguridad informática se han presentado en la empresa en los últimos años?

11. ¿Qué tipo de riesgos informáticos fueron detectados?

Apéndice 2 Algunas de las Pequeñas y Medianas Empresas Guayas Personas Naturales

CATASTRO DEL RÉGIMEN DE MICROEMPRESAS VÁLIDO PARA EL PERÍODO FISCAL 2020 FECHA DE PUBLICACIÓN 23/10/2020			
NÚMERO DE RUC	RAZÓN SOCIAL	PROVINCIA	AÑO RÉGIMEN MICROEMPRESAS
0100002708001	LONDA JOSE BENJAMIN	GUAYAS	2021
0100008887001	TORAL VELEZ PAULINO RAFAEL	GUAYAS	2021
0100011915001	GARNICA GUTIERREZ BEATRIZ ERMOSINA	GUAYAS	2021
0100012103001	ORTEGA JOSE ERNESTO	GUAYAS	2021
0100033950001	VILLAVICENCIO PERALTA HERNAN AUGUSTO	GUAYAS	2021
0100037662001	QUEVEDO FLORES CARLOS ALBERTO	GUAYAS	2021
0100038629001	ZUMBA AYABACA MARIA DOLORES	GUAYAS	2021
0100042530001	SALAMEA CORDERO CARLOS EDMUNDO	GUAYAS	2021
0100046523001	VELEZ VILLACIS JORGE WASHINGTON	GUAYAS	2021
0100049725001	ALVAREZ ESPINOZA NESTORIO DE JESUS	GUAYAS	2021
0100062215001	PACHECO CASTRO JULIO MARIA	GUAYAS	2021
0100077890001	ORTIZ YUNGA MANUEL MESIAS	GUAYAS	2021
0100086958001	TOLEDO ECHEVERRIA SANTIAGO IVAN	GUAYAS	2021
0100090216001	POLO MORALES BOLIVAR ALEJANDRO	GUAYAS	2021
0100091362001	DUCHI JIMENEZ GERMAN LEOPOLDO	GUAYAS	2021
0100098839001	BRAVO CEDILLO HOMERO RENE	GUAYAS	2021
0100109412001	VALLADOLID QUITUISACA MANUEL REDENTOR	GUAYAS	2021
0100134113001	TAPIA MATUTE JORGE HONORATO	GUAYAS	2021
0100135169001	CHUCHUCA BRITO JAIME RAUL	GUAYAS	2021
0100140888001	VEINTIMILLA PACHECO ROGERIO ALONSO	GUAYAS	2021
0100141845001	SALAZAR MONTESINOS RUTH BALBINA	GUAYAS	2021
0100145341001	ROJAS ORELLANA BERTHA LEOPOLDINA	GUAYAS	2021
0100149871001	ROBLES PIÑA CARLOS ALFREDO	GUAYAS	2021
0100155373001	LIU LIMA LUIS SAN	GUAYAS	2021
0100156140001	CAJAMARCA GUACHICHULLCA JOSE LUIS	GUAYAS	2021
0100156900001	CAMPOVERDE MORALEZ JULIO FELICIO	GUAYAS	2021
0100157536001	URGILES LEON ALICIA MAGDALENA	GUAYAS	2021
0100163237001	ALARCON MEDINA ZOILA BIRMANIA	GUAYAS	2021
0100167899001	QUITENO SUMBA JOSE MOISES	GUAYAS	2021
0100172980001	GUZHÑAY ZUNA TARGELIO	GUAYAS	2021
0100191410001	MANCERO ALVARADO SERGIO MIGUEL	GUAYAS	2021
0100199660001	VASQUEZ LOPEZ GUILLERMO HERIBERTO	GUAYAS	2021
0100206549001	BERMEO RAFAEL MARIA	GUAYAS	2021
0100209113001	QUITO CABRERA DELIA GERARDINA	GUAYAS	2021
0100225937001	PEÑARANDA BARRIONUEVO JUAN LUIS	GUAYAS	2021
0100246735001	CABRERA MENDEZ TERESA DE JESUS	GUAYAS	2021
0100251065001	ORELLANA TAPIA ROSA ISABEL	GUAYAS	2021

0100252659001	MAYORGA AYALA MARIO GILBERTO	GUAYAS	2021
0100252840001	PEREZ VELASTEGUI FRANCISCO ENRIQUE	GUAYAS	2021
0100265370001	SUAREZ CEPEDA TERESA DE JESUS	GUAYAS	2021
0100266147001	TOLEDO FIGUEROA JORGE DE JESUS	GUAYAS	2021
0100267442001	RODRIGUEZ RODAS CARMITA ALICIA	GUAYAS	2021
0100277383001	MORA UZHCA JULIO CESAR	GUAYAS	2021
0100281773001	BERMEO MARIA FLORENCIA	GUAYAS	2021
0100283217001	GALARZA CAMPOVERDE GIL RODRIGO	GUAYAS	2021
0100288091001	PAUTA MONTALVAN JAIME LUCIANO	GUAYAS	2021
0100331677001	FRIAS ROMAN ALEX VICENTE	GUAYAS	2021
0100334978001	MANCERO JIMENEZ FAUSTO CESAR	GUAYAS	2021
0100341148001	GUANIN VEGA CARLOS ENRIQUE	GUAYAS	2021
0100341379001	PACHECO MENDEZ ADAN GUILLERMO	GUAYAS	2021
0100386424001	QUITO MOROCHO ENMA CONSUELO	GUAYAS	2021
0100409259001	ORELLANA LEON JAIME RODRIGO	GUAYAS	2021
0100410745001	SARMIENTO ORELLANA RUBEN ANTONIO	GUAYAS	2021
0100412816001	TOLEDO TOLEDO HUGO BOLIVAR	GUAYAS	2021
0100418763001	BENAVIDES PESANTEZ PURIFICACION EUDOCIA	GUAYAS	2021
0100418912001	GUACHUN QUITO LUIS ALEJANDRO	GUAYAS	2021
0100419217001	BARRERA MARQUINA ABEL VICENTE	GUAYAS	2021
0100419704001	RAMON LARRIVA CONRADO NEPTALI	GUAYAS	2021
0100420223001	PASTUZO MORENO JOSE MODESTO	GUAYAS	2021
0100421437001	MONTESDEOCA RODAS ERLINDA EMERITA	GUAYAS	2021
0100426410001	TORRES PESANTEZ INES VICTORIA	GUAYAS	2021
0100428630001	RODRIGUEZ TENEMAZA MANUEL GUILLERMO	GUAYAS	2021
0100431485001	GARNICA PAGUAY LUIS ANTONIO	GUAYAS	2021
0100433085001	PALOMEQUE VINTIMILLA ELOY ALBINO	GUAYAS	2021
0100434364001	MENDEZ RIERA LEON BENIGNO	GUAYAS	2021
0100436666001	ORELLANA LEON ROSA MATILDE	GUAYAS	2021
0100449032001	CAMPOVERDE INAMAGUA MARIANA DE JESUS	GUAYAS	2021
0100464957001	TACURI LOJA LUIS GONZALO	GUAYAS	2021
0100480904001	NACIPUCHA PAREDES MARIA ESTHER	GUAYAS	2021
0100487859001	MARQUEZ CARRASCO ESTEVAN EZEQUIEL	GUAYAS	2021
0100496587001	TOLEDO TOLEDO HUGO BOLIVAR	GUAYAS	2021
0100497593001	CEDILLO MARIA FLORINDA	GUAYAS	2021
0100497726001	RODRIGUEZ MARTINEZ LUZ AMERICA	GUAYAS	2021
0100499516001	PATIÑO MONTALVO MERCEDES YOLANDA	GUAYAS	2021
0100502525001	MATUTE LITUMA SIMON	GUAYAS	2021
0100508811001	PEÑARANDA ZHUNIO LUIS ALVINO	GUAYAS	2021
0100508951001	IÑIGUEZ ULLOA BEATRIZ DE LAS NUVES	GUAYAS	2021
0100516657001	COBOS ILLESCAS JOSE CESAREO	GUAYAS	2021
0100517374001	GUZMAN VILLAVICENCIO LUIS AURELIO	GUAYAS	2021
0100530641001	FARFAN URDIALES JORGE MANUEL	GUAYAS	2021

0100549740001	ESPADERO FAJARDO ANGEL FLORENCIO	GUAYAS	2021
0100553403001	CABRERA ALVARRACIN RUBEN	GUAYAS	2021
0100555622001	BERMEO VELEZ EFRAIN HOMERO	GUAYAS	2021
0100566165001	REYES ESPINOZA CARLOS RIGOBERTO	GUAYAS	2021
0100573351001	PALACIOS CASTRO ROSA IMELDA	GUAYAS	2021
0100603265001	UYAGUARI BUELE ANGEL MARIA	GUAYAS	2021
0100609528001	CABRERA SALINAS ELICENDO RODRIGO	GUAYAS	2021
0100619493001	MARCA OLEAS MIGUEL ANGEL	GUAYAS	2021
0100621390001	CASTRO TELLO CELIO RAFAEL	GUAYAS	2021
0100637313001	LOYOLA JACOME LEONOR PIEDAD	GUAYAS	2021
0100643675001	ROMERO SERRANO LUIS RODRIGO	GUAYAS	2021
0100648906001	TORO GALVEZ LUIS ANGEL	GUAYAS	2021
0100660398001	PEÑAHERRERA ASTUDILLO ELENA BEATRIZ	GUAYAS	2021
0100660703001	LEMA MONTESDEOCA JOSE REINALDO	GUAYAS	2021
0100667575001	GUEVARA TORRES EDGAR ANIBAL	GUAYAS	2021
0100676816001	CORONEL ZARUMA ZOILA DORINDA	GUAYAS	2021
0100687730001	LOYOLA ORELLANA MIGUEL CESAR	GUAYAS	2021
0100689660001	TERREROS SERRANO JORGE FERNANDO	GUAYAS	2021
0100697697001	ARAY VAZQUEZ JOSE HUMBERTO	GUAYAS	2021
0100698950001	CAMPOVERDE CAMPOVERDE MANUEL EMILIO	GUAYAS	2021
0100707207001	ESPADERO FAJARDO CARLOS RICARDO	GUAYAS	2021
0100723774001	GALLARDO CARRION ROSA MATILDE	GUAYAS	2021
0100729763001	TORAL AMADOR MARGARITA MARIA	GUAYAS	2021
0100741453001	ELJURI ANTON OLGUITA MARIA EULALIA	GUAYAS	2021
0100751171001	CONDO SANCHO MANUEL RODRIGO	GUAYAS	2021
0100752542001	VASQUEZ CALLE VICTOR ALBERTO	GUAYAS	2021
0100753540001	MALDONADO GARZON MARIA CRISOMITA	GUAYAS	2021
0100766492001	MENDIETA ALVARADO SEGUNDO LIZARDO	GUAYAS	2021
0100781681001	LEON LOPEZ ROSA SABINA	GUAYAS	2021
0100782044001	CANTOS LOPEZ JOSE RODOLFO	GUAYAS	2021
0100782721001	COBOS ALVAREZ HUGO ISAIAS	GUAYAS	2021
0100787688001	CAJAMARCA CUJI LUIS MARIA	GUAYAS	2021
0100796572001	BAUTISTA MACHUCA JORGE ALEJANDRO	GUAYAS	2021
0100797281001	CARRASCO MURILLO MANUEL XAVIER	GUAYAS	2021
0100802297001	ORELLANA RAMON ANGEL BENIGNO	GUAYAS	2021

Apéndice 3 Algunas de las Pequeñas y Medianas Empresas Guayas Personas jurídicas año 2021

Nombre	Ciudad	Tamaño
TECH MAHINDRA-ECUADOR S.A.	GUAYAQUIL	MEDIANA
NEGOCIOS GRAFICOS GRAFINPREN S.A.	GUAYAQUIL	MEDIANA
AVP. SISTEMAS S.A.	GUAYAQUIL	MEDIANA
ZAZAPRINT S.A.	GUAYAQUIL	MEDIANA
COMUNICADORES DEL ECUADOR COMUNIDOR S. A	GUAYAQUIL	PEQUEÑA
MENDOTEL S.A.	GUAYAQUIL	MEDIANA
DAKPOINT S.A.	GUAYAQUIL	MEDIANA
GRAFICAS JALON ENAJA S.A.	GUAYAQUIL	MEDIANA
MERCADOLIBRE ECUADOR CIA. LTDA.	QUITO	MEDIANA
PROYECTOS DEL ECUADOR S.A. PROYECSA	GUAYAQUIL	PEQUEÑA
TEKOCSA S.A.	GUAYAQUIL	MEDIANA
TICKETSHOW S.A.	GUAYAQUIL	PEQUEÑA
OBRAS DE INGENIERIA ELECTRICA Y TELEFONICA OBRET S.A.	GUAYAQUIL	MEDIANA
PANATEL DEL ECUADOR S.A.	GUAYAQUIL	MEDIANA
PREMIUMTECH S.A.	GUAYAQUIL	MEDIANA
COMPUHELP S.A.	GUAYAQUIL	MEDIANA
GLOBE IMPORT IMPORTGLOBE S.A.	GUAYAQUIL	PEQUEÑA
DVT DEL ECUADOR S.A.	GUAYAQUIL	MEDIANA
TECNIWASH S.A.	GUAYAQUIL	MEDIANA
FUORI S.A.	GUAYAQUIL	MEDIANA
IGUANA DIGITAL S.A. IGUDISA	GUAYAQUIL	PEQUEÑA
A-C DEPOT DEL ECUADOR S.A. ACDEPOT	GUAYAQUIL	MEDIANA
VIAMATICA S.A.	GUAYAQUIL	MEDIANA
CORPACK S.A.	GUAYAQUIL	MEDIANA
SOLUCIONES ESPECIALIZADAS DE EN TELEMÁTICA S.A. SESTEL	GUAYAQUIL	MEDIANA
TELECOMUNICATION - CITY S.A. TELECISA	GUAYAQUIL	PEQUEÑA
SUZUKI WASH S.A. SUWASH	GUAYAQUIL	PEQUEÑA
ONDU SOLUCIONES TECNOLOGICAS S.A.	GUAYAQUIL	PEQUEÑA
AEKANSA S.A.	GUAYAQUIL	MEDIANA
GAECO S.A.	GUAYAQUIL	PEQUEÑA
PROLOGIC S.A.	GUAYAQUIL	MEDIANA
LITOCOPIAS S.A.	GUAYAQUIL	PEQUEÑA
SERVIGANGA S.A.	GUAYAQUIL	MEDIANA
MARKETQUALITY S.A.	GUAYAQUIL	PEQUEÑA
RETAILPOINT DEL ECUADOR S.A.	GUAYAQUIL	MEDIANA
STILINDGRAF S. A.	GUAYAQUIL	PEQUEÑA
MODITEX S.A.	GUAYAQUIL	PEQUEÑA
DATILMEDIA S.A.	GUAYAQUIL	PEQUEÑA
DISEÑO E INSTALACIONES TELEFONICAS Y ELECTRICAS DINSTELEC	GUAYAQUIL	MEDIANA

S.A.		
DALO S.A.	GUAYAQUIL	PEQUEÑA
PACIFIC SERVICE ENTERPRISE PACENT S.A.	GUAYAQUIL	PEQUEÑA
IMPORTADORA-TECHZONE S.A.	GUAYAQUIL	MEDIANA
SISTEMAS Y SERVICIOS ERAZO C.A.	GUAYAQUIL	MEDIANA
SOLINTELSA SOLUCIONES INTEGRADAS EN INTERNET Y TELECOMUNICACIONES S. A.	GUAYAQUIL	PEQUEÑA
QUANTUMBIT S.A.	GUAYAQUIL	PEQUEÑA
SERVICENTURIOSA S.A.	GUAYAQUIL	MEDIANA
ILEMENSYS S.A.	GUAYAQUIL	PEQUEÑA
NANOITS S.A.	GUAYAQUIL	MEDIANA
SUPTRONIC S.A.	GUAYAQUIL	PEQUEÑA
TECNICA, MONTAJE Y MANTENIMIENTO CRUZ S.A. TECMOCRUZ	GUAYAQUIL	MEDIANA
COMPUDINER S.A.	GUAYAQUIL	PEQUEÑA
DESARROLLO TECNOLOGIA & SISTEMAS S.A. DESARTECSIS	GUAYAQUIL	MEDIANA
MAC CENTER S.A.	GUAYAQUIL	MEDIANA
ACTIVIDADES DE PRONOSTICOS DEPORTIVOS JUEGOS ON LINE SPORTBET S.A.	GUAYAQUIL	PEQUEÑA
ASESORAMIENTO GENERAL DE INGENIERIA AGI S.A.	GUAYAQUIL	MEDIANA
MALL DE TECNOLOGIA TECHMALL S.A.	GUAYAQUIL	MEDIANA
LEVEL PRINT S.A. LEPRINTSA	GUAYAQUIL	PEQUEÑA
ECOLOGIA EN IMPRESION S.A. ECOLOIMP	GUAYAQUIL	PEQUEÑA
PROCOMA ELECTRICO S.A.	GUAYAQUIL	PEQUEÑA
OFFNORT S.A.	GUAYAQUIL	PEQUEÑA
SISTECOM SISTEMAS DE COMPUTACION CA	GUAYAQUIL	PEQUEÑA
IMPRENTATOTAL S.A.	GUAYAQUIL	PEQUEÑA
NIKOTRON S.A.	GUAYAQUIL	PEQUEÑA
APPTELINK S.A.	GUAYAQUIL	PEQUEÑA
ZAMMPERS S.A.	GUAYAQUIL	PEQUEÑA
RP3 S.A. RETAIL POS 3	GUAYAQUIL	PEQUEÑA
LEXTECS S.A.	GUAYAQUIL	PEQUEÑA
HIDMOL S.A.	GUAYAQUIL	PEQUEÑA
EBESTPHONE ECUADOR S.A.	GUAYAQUIL	PEQUEÑA
GRAFIMAC S.A.	GUAYAQUIL	PEQUEÑA
BOSTONE S.A.	GUAYAQUIL	PEQUEÑA
COMERCIALIZADORA SERVI VELL COMSEVIVSA S.A.	GUAYAQUIL	PEQUEÑA
FC EMPRENDIMIENTO Y NETWORKING FCNETCORP S.A.	GUAYAQUIL	PEQUEÑA
OLEAS SANCHEZ INVERSIONES OLEXSAIMPORT S.A.	GUAYAQUIL	PEQUEÑA
EDITORIAL TINTA MORADA S.A. EDITCORP	GUAYAQUIL	PEQUEÑA