UNIVERSIDAD ESTATAL DE MILAGRO

VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO

PROYECTO DE INVESTIGACIÓN Y DESARROLLO
PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGÍSTER EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

TÍTULO DEL PROYECTO:

ANÁLISIS DE UN PLAN CON ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS.

TUTOR
LSI, JESSICA JANINA CABEZAS QUINTO, MSIG

AUTOR
SEGUNDO ARTURO PÉREZ ALVAREZ

MILAGRO, enero del 2023

ACEPTACIÓN DEL TUTOR

En calidad de Tutor de Proyecto de Investigación, nombrado por el Comité Académico del Programa de Maestría en Gerencia de Tecnologías de la Información

CERTIFICO

Que he analizado el Proyecto de Investigación con el tema **ANÁLISIS DE UN PLAN CON ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS,** elaborado por **SEGUNDO ARTURO PÉREZ ALVAREZ,** el mismo que reúne las condiciones y requisitos previos para ser defendido ante el tribunal examinador, para optar por el título de **MAGÍSTER EN GERENCIA DE TECNOLOGIAS DE LA INFORMACIÓN**

Milagro, 12 de enero del 2023

Firmado electrónicamente por:
JESSICA JANINA CABEZAS QUINTO

_____

LSI, JESSICA JANINA CABEZAS QUINTO, MSIG

C.I: 1203461544

DECLARACIÓN DE AUTORÍA DE LA INVESTIGACIÓN

El / la autor/a de esta investigación declara ante el Comité Académico del Programa de Maestría en Gerencia de Tecnologías de la Información de la Universidad Estatal de Milagro, que el trabajo presentado de mi propia autoría, no contiene material escrito por otra persona, salvo el que está referenciado debidamente en el texto; parte del presente documento o en su totalidad no ha sido aceptado para el otorgamiento de cualquier otro Título de una institución nacional o extranjera

Milagro, 12 de enero del 2023

Firmado electrónicamente por:
SEGUNDO ARTURO
PEREZ ALVAREZ

Segundo Arturo Pérez Alvarez
C.I.1804344305

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO
DIRECCIÓN DE POSGRADO
CERTIFICACIÓN DE LA DEFENSA

El TRIBUNAL CALIFICADOR previo a la obtención del título de **MAGÍSTER EN GERENCIA DE TECNOLOGIAS DE LA INFORMACION**, presentado por **ING. PEREZ ALVAREZ SEGUNDO ARTURO**, otorga al presente proyecto de investigación denominado "ANÁLISIS DE UN PLAN CON ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS", las siguientes calificaciones:

TRABAJO DE TITULACION	50.67
DEFENSA ORAL	37.67
PROMEDIO	**88.33**
EQUIVALENTE	**Muy Bueno**

Firmado electrónicamente por:
MIRELLA AZUCENA
CORREA PERALTA

Mgti. CORREA PERALTA MIRELLA AZUCENA
PRESIDENTE/A DEL TRIBUNAL

Firmado electrónicamente por:
JOSUE JESUS
CABRERA
RUILOVA

Mba CABRERA RUILOVA JOSUE JESUS
VOCAL

Firmado electrónicamente por:
LUIS EDUARDO
SOLIS GRANDA

M.A.E. SOLIS GRANDA LUIS EDUARDO
SECRETARIO/A DEL TRIBUNAL

DEDICATORIA

Dedico esta tesis en primer lugar a Dios que ha hecho posible culminar este proceso tan anhelado, a mi madre por siempre ser mi soporte y motivación a lo largo de toda esta etapa.

A mis hermanos que siempre han estado ahí para apoyarme, en especial a mi hermana que siempre ha estado dispuesta a brindarme su ayuda incondicional, lo cual ha influido mucho en alcanzar este objetivo.

AGRADECIMIENTO

Mi agradecimiento está dirigido en primer lugar a Dios que me ha permitido lograr esta meta anhelada, a mi familia y a mi novia que han sabido comprenderme y apoyarme durante todo el desarrollo de mi trabajo.

Así también agradezco a mi tutora por guiarme adecuadamente durante el desarrollo de mi tesis y a todos mis formadores que en parte aportaron en mi formación.

CESIÓN DE DERECHOS DE AUTOR

Sr. Dr.
Jorge Fabricio Guevara Viejó
Rector de la Universidad Estatal de Milagro

Presente.

Mediante el presente documento, libre y voluntariamente procedo a hacer entrega de la Cesión de Derecho del Autor del Trabajo realizado como requisito previo para la obtención de mi Título de Cuarto Nivel, cuyo tema fue **ANÁLISIS DE UN PLAN CON ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS**, y que corresponde al Vicerrectorado de Investigación y Posgrado.

Milagro, 12 de enero del 2023

Segundo Arturo Pérez Alvarez
C.I 1804344305

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Anexos

Resumen

El presente trabajo busca analizar la seguridad de la información en las pequeñas y medianas empresas, considerando el contexto actual en el que se desenvuelven, para determinar el diseño con estrategias de seguridad adecuado.

Las empresas están inmersas en una era digital por lo que es necesario que cuenten con un plan de contingencia ante la perdida de información, más aún que determinen todas las brechas de seguridad existentes, esto es necesario al momento de procesar datos importantes para los diversos procesos de las empresas. Por ello se realizará una investigación de campo aplicando el método descriptivo, para poder determinar procesos de seguridad aplicables en base a las encuestas realizadas.

El estudio se limita a las pequeñas y medianas empresas de la ciudad de Milagro, el cual sen centra en 69 empresas. El levantamiento de información tiene como objetivo determinar el comportamiento de cada una, para en torno a ello disminuir los riesgos asociados a la seguridad de la información.

Palabras Clave:
Seguridad de la información, pequeñas y medianas empresas, brechas de seguridad.

Abstract

The present work seeks to analyze information security in small and medium-sized companies, considering the current context in which they operate, to determine the design with adequate security strategies.

Companies are immersed in a digital age, so it is necessary for them to have a contingency plan for the loss of information, even more so that they determine all existing security breaches, this is necessary when processing important data for the various processes. of the companies. For this reason, a field investigation will be carried out applying the descriptive method, in order to determine applicable security processes based on the surveys carried out.

The study is limited to small and medium-sized companies in the city of Milagro, which focuses on 69 companies. The purpose of collecting information is to determine the behavior of each one, in order to reduce the risks associated with information security.

Key words: Information security, small and medium enterprises, security breaches.

Introducción

Los avances tecnológicos actuales han generado que las empresas deban incorporarse en un ambiente globalizado y competitivo, haciéndolas depender cada vez más de la tecnología, esto ha generado una brecha de seguridad en las pequeñas y medianas empresas, las cuales pueden o no contar con los recursos necesarios para costear un sistema de seguridad que proteja la información de peligros internos y externos.

En efecto las pequeñas y medianas empresas pueden requerir un sistema de seguridad que proteja la información de los ataques cibernéticos y de las eventualidades diarias que pueden surgir en una empresa, tales como: daños equipos, servidores y discos duros. Además de proteger la información, esta debe estar disponible en todo momento para que las empresas no detengan sus operaciones y continúen con normalidad.

Para las empresas el proteger la información puede entenderse como un gasto desmesurado que no pueden cubrir, sin embargo, a pesar de los diversos servicios de seguridad de paga que existen, también se pueden utilizar otros métodos que no requieren de mucha inversión. Es por ello que la presente investigación tiene como objetivo analizar como incide un plan con estrategias de seguridad de la información en las pequeñas y medianas empresas.

CAPÍTULO I: EL PROBLEMA DE LA INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

El uso de las herramientas tecnológicas ha facilitado mucho el manejo de la información, sin embargo, en toda operación o proceso está latente la posibilidad de un evento no programado a causa de un desastre o una contingencia mayor, las cuales pueden representar la no disponibilidad o pérdidas potenciales de información.

Las empresas en la actualidad necesitan que su información esté protegida ante cualquier amenaza, ya que de esto depende su correcto funcionamiento. Por lo cual los datos deben estar disponibles en todo momento para permitir la continuidad de sus procesos.

La transformación de los mercados ha obligado a que las PYME incorporen diversas adaptaciones tecnológicas, sin embargo, estas pueden no contar con un proceso definido que le permita proteger su información ante cualquier eventualidad, es por ello que los sistemas deben incluir procesos de seguridad que ayuden a proteger las mismas.

Existen estándares definidos como las normas ISO/IEC 27000, la cual presenta un grupo de estándares para la gestión de seguridad de cualquier empresa. Sin embargo, en muchas de las pequeñas y medianas empresas pueden no conocer estas normativas y por ende omitir su aplicación que pueden repercutir en Pérdida de información valiosa para cualquier empresa.

1.1.1 Delimitación del problema

La presente investigación tiene como objeto de estudio a las pequeñas y medianas empresas del cantón Milagro, de la Provincia del Guayas.

1.1.2 Formulación del problema

- ¿Cómo incide un plan con estrategias de seguridad de la información en las pequeñas y medianas empresas?

1.1.3 Preguntas de investigación

- ¿Cómo afecta una instalación eléctrica deficiente en los daños de los computadores?
- ¿Qué impacto tiene la falta de dispositivos de respaldo de energía en el daño de las Bases de Datos?
- ¿Cómo incurre no contar con un proceso de seguridad de la información en la pérdida de la información relevante para la empresa?

1.1.4 Determinación del tema

- Análisis de un plan con estrategias de seguridad de la información para las pequeñas y medianas empresas.

1.2 OBJETIVOS

1.2.1 Objetivo general

- Definir cómo incide un plan con estrategias de seguridad de la información en las empresas mediante un análisis de los procesos de seguridad que poseen, para evitar la pérdida de información.

1.2.2 Objetivos específicos

- Identificar los distintos tipos de amenazas de seguridad de la información que puede tener una empresa examinando diversas situaciones presentadas, para disminuir su impacto.
- Distinguir qué impacto tienen los escasos respaldos de información y de energía, mediante encuestas al personal de tecnología, para determinar los procesos adecuados que ayuden a proteger la integridad de la información.

- Identificar cómo incurre contar con políticas y procesos de seguridad de la información en la pérdida de la información relevante para la empresa.

1.2.3 Hipótesis general

Un plan con estrategias de seguridad de la información en las empresas incide en el resguardo de la información.

1.2.4 Hipótesis específica

- Identificar los distintos tipos de amenazas de seguridad de la información que puede tener una empresa y su impacto en la misma.
- Los escasos respaldos de información y energía inciden en los procesos adecuados para proteger la integridad información.
- Los escasos procesos de seguridad inciden en la pérdida de información relevante en una empresa.

1.2.5 Declaración de las variables

En la tabla 1, se expone el cuadro de operacionalización de las variables, en donde se describe la variable independiente y dependiente, su conceptualización, categorías, indicadores, ítems de preguntas, la unidad de análisis y la técnica e instrumento con el cual se realizará el levantamiento de información.

Tabla 1:

Declaración de las variables

OPERACIONALIZACIÓN DE LAS VARIABLES						
VARIABLES	**CONCEPTUALIZACIÓN**	**CATEGORÍAS**	**INDICADORES**	**ÍTEMS PREGUNTAS**	**UNIDAD DE ANÁLISIS**	**TÉCNICA E INSTRUMENTO**
Variable Independiente Seguridad de la información	Eventos preventivos que permiten proteger la información.	**Licenciamiento**	Número de licencias de sistemas operativos.	¿Las computadoras y servidores cuentan con sistemas operativos con licencias?	Administrativos departamento de tecnología.	Encuesta
			Número de licencia de antivirus.	¿Con cuántas licencias de antivirus cuenta la empresa?		
		Respaldos	Número de respaldos anuales.	¿Cada cuánto tiempo se realiza respaldo de la información?	Administrativos departamento de tecnología	Encuesta
			Número de respaldos eléctricos	¿La empresa cuenta con un respaldo de energía?		
		Políticas de seguridad de la información	Número de estrategias preventivas para resguardar la información	¿La empresa cuenta con un plan preventivo ante la Pérdida de información?	Administrativos departamento de tecnología.	Encuesta
			Número de capacitaciones recibidas	¿Cuántas veces se capacito al personal sobre las normas de		

				seguridad de la información?		
Variable Dependiente Pérdida de información	Situación donde Información ya no se encuentra disponible para acceder a ella.	**Pérdida de información**	Número de veces que se ha perdido la información.	¿Cuántas veces se ha perdido información relevante para la empresa?	Administrativos departamento de tecnología.	Encuesta
		Vulnerabilidad de la información	Número de ataques cibernéticos.	¿La empresa ha sufrido de ataques cibernéticos en el año en curso?	Administrativos departamento de tecnología.	Encuesta
			Tipos de ataques cibernéticos.	En caso de haber sufrido un ataque cibernético seleccionar el tipo.	Administrativos departamento de tecnología.	Encuesta
		Estado de equipos informático	Fallos en los equipos informáticos.	¿Los fallos en los equipos informáticos han ocasionado pérdida de información?	Administrativos departamento de tecnología.	Encuesta
			Mantenimiento de equipos informáticos.	¿Cada que tiempo recibe mantenimiento los equipos de cómputo de la empresa?	Administrativos departamento de tecnología.	Encuesta

Tabla 1: *Declaración de las variables*

Elaborado por: Pérez, 2022

1.3 Justificación

El siguiente trabajo analizará un plan de contingencia para la recuperación de la información digitalizada, debido a que la información es imprescindible para toda organización y es de vital importancia protegerla ante cualquier suceso interno o externo que amenace a esta.

Como sabemos la tecnología no está exenta de fallas y la empresa tiene que estar preparada para reponerse lo más pronto posible, porque de esto dependen las consecuencias que generan estos fallos.

Este análisis está dirigido a evitar la pérdida total de la información definiendo mejoras y desarrollando procesos que ayuden a la pronta recuperación de la información digitalizada ya que de eso dependerá el continuo funcionamiento de la empresa.

Para el desarrollo de este trabajo se realizará una investigación de campo, los métodos a utilizar serán deductivo e inductivo, recurriendo como técnica a las encuestas, debido que a través de este instrumento se lograra conseguir información que aporte a estipular una propuesta acertada ante el tema planteado.

1.3.1 Alcance y limitaciones

El alcance del estudio involucra a las pequeñas y medianas empresas de la ciudad de Milagro, ubicada en la Provincia del Guayas. Para ello se procederá a realizar el levantamiento de información en torno a los permisos que otorguen las distintas empresas.

CAPÍTULO II: MARCO REFERENCIAL

2.1 MARCO TEÓRICO

2.1.1 Antecedente histórico

Es importante establecer la importancia de la seguridad de la información en torno a sus sistemas, considerando los avances tecnológicos actuales y sus amenazas, por tal motivo en el desarrollo de la investigación se busca explorar las brechas de seguridad en torno al sistema de información de las empresas.

Las empresas están conformadas por los sistemas de información, los cuales parten del estudio de su organización, del contexto y las implicaciones del ambiente en el que se desenvuelve la entidad, para lo cual incluyen un conjunto de componentes, que buscan recolectar, almacenar, procesar datos para proporcionar información de los productos o procesos que se desarrollan. En lo relacionado a los componentes principales de un sistema de información se puede encontrar a los componentes físicos, los programas, la infraestructura de comunicaciones, las bases de datos y sus servidores, por último, están los recursos humanos y procesos (Pablos Heredero et al., 2019). El sistema de información de una empresa permite un adecuado funcionamiento, porque de ahí surgen los reportes que ayudan a definir mejoras enfocadas en optimizar la productividad.

Todo sistema de información involucra la existencia de distintos tipos información, la cuales que son imprescindibles para las empresas, por ello existen estándares que se sugieran a las empresas para proteger la información como los definidos por el Organismo Internacional de Estandarización, el cual establece procedimientos básicos que toda empresa debe seguir para proteger la información

a través de las normativas ISO que se actualizan cada determinado tiempo. Actualmente se encuentran vigente las normativas ISO 27002:2022 las cuales se acoplan al contexto actual de las empresas.

Con el pasar de los años han surgido diversos estudios referentes al sistema de seguridad uno de ellos es el estudio presentado por Topanta, et al. (2019) el cual presentó un estudio de la primera edición Seguridad de la Información – Ecuador 2017, midiendo las principales tendencias en cuanto a seguridad de la información. Participaron más de 50 empresas nacionales y multinacionales de diversas industrias. El 79% de las empresas tenía a cargo un responsable de seguridad de la información. Un 62% de las empresas no contaba con un presupuesto para la gestión de la seguridad de la información.

Para el 2018, el 42% de las empresas, según el estudio realizado, mantendrían el mismo presupuesto asignado para la seguridad de la información. El 60% de las empresas no contaba con un SOC (Centro de Operaciones de Seguridad), punto importante para la gestión de seguridad de la información, dado que reúne el personal y herramientas necesarias para soportar la seguridad que la actividad de la organización requiere. El 54% aseguró haber experimentado robo de información, mientras que un 46%, sufrió ataques de software malicioso como el ransomware WannaCry, responsable de incidentes a escala mundial (Marín et al., 2020). La implementación de un sistema de seguridad de la información requiere de un presupuesto definido por cada empresa dependiendo de la actividad que realice, más que todo en la actualidad donde las empresas tuvieron que acoplarse a los diversos cambios digitales debido a la pandemia dejando con ellos ciertos datos expuestos a ataques cibernéticos.

Las PYMES en Ecuador representan el 99,55%, y ello se debe al dinámico proceso de emprendimiento que existe, sin embargo muchas de las empresas consideran que poseen una correcta protección de su información, RSM US (2018), encontró en su estudio que el 95% de las pymes encuestadas consideran que poseen mecanismos de seguridad informática superior al promedio, y su riesgo de sufrir ataques informáticos es muy bajo (Sánchez, et al., 2021); sin embargo, el estado real de preparación y madurez en ciberseguridad de estas pymes puede ser bastante insatisfactorio. Esto se evidencia en el estudio de Cyber Security Breaches Survey 2019, donde se señala que solo el 15% de las pymes poseen un proceso formal de gestión de incidentes cibernéticos,(Llano, et al.,2021), y el 50% de los líderes de TI dicen que no saben por dónde empezar para mejorar su postura de seguridad. Bajo este panorama, las organizaciones no realizan evaluaciones permanentes, sistemáticas y exhaustivas del riesgo cibernético. (Rodríguez-Mendoza y Aviles-Sotomayor, 2020)

Debido a los avances tecnológicos y a la falta de concientización en ciberseguridad, se han generado brechas de seguridad fáciles de vulnerar, un ejemplo característico son el uso de plataformas digitales como las videoconferencias, conexiones remotas, medios y redes sociales, de los cuales, se hace énfasis tanto en las aplicaciones web como en las móviles, que son los más vulnerables para un ataque de ciberseguridad. Muchas de las pequeñas y medianas empresas utilizan diversos aplicativos de seguridad sin embargo este puede no ser eficiente por ello la investigación busca establecer procesos que garanticen la disponibilidad de la información y así mejorar la continuidad de sus funciones cotidianas.

2.1.2 Antecedentes referenciales

Dentro de la investigación realizada encontramos diversos estudios que se enfocan en la seguridad de la información.

Para Tundidor et al. (2019) la seguridad de la información tributa a una disciplina que se encarga de proteger la información mediante la implementación de técnicas, el despliegue de tecnologías que establecen de forma que se aseguran las situaciones de fallas parciales o totales, cuando la información es aquel activo que se encuentra en riesgo, es la disciplina que nos habla de los riesgos, amenazas, análisis de escenarios, buenas prácticas y esquemas normativos, los mismos que exigen niveles de aseguramiento de procesos y de tecnología para elevar el nivel de confianza en la creación, utilización, almacenaje, transmisión, recuperación y disposición de la información.

Es común que la seguridad de la información se resguarde en las políticas de desarrolladas a través de la elaboración de un plan preventivo. Las empresas serán la encargada de marcar todas las líneas de actuación en materia de seguridad y mediante el plan preventivo determinar las medidas tanto técnicas como procedimentales que garantice los objetivos marcados por la política de seguridad.

Aquellas medidas técnicas serán llevadas a cabo por el equipo de seguridad informática y los administradores de sistemas, estos implantarán las medidas necesarias para el cumplimiento de políticas y realizarán el análisis de riesgos en el que se debería basar (Altamirano, 2019).

Es así que se debe tener en cuenta que la protección de seguridad de la información mediante la aplicación de políticas, las cuales se llevan a cabo solo a través de una perspectiva tecnológica, es decir, tendrá un enfoque incompleto, ya que, según los estudios realizados hasta la fecha, se ha demostrado que es

fundamental el poder tener una visión más amplia a través de un enfoque interdisciplinario, en donde el factor principal como lo es el humano, es quien jugará un papel fundamental durante este enfoque.

Según Cano y Almanza, (2020) en su estudio indican que las empresas deben adoptar un enfoque multifacético, apalancando personas, procesos y tecnología, con la finalidad de crear un entorno de confianza respaldadas por la supervisión y el análisis. Sin embargo, la tecnología no puede garantizar solamente un entorno seguro para la información; deben tenerse en cuenta tanto los aspectos humanos de la seguridad de la información, como los aspectos tecnológicos.

Es importante recordar que el incumplimiento ya sea total o parcial de las políticas de seguridad establecidas o las violaciones al sistema de información conlleva a una pérdida económica de la organización, aquello que resulta significativo para la gestión del mismo.

2.1.3 Fundamentación

Mantener segura la información es un proceso ligado a protegerla ante la pérdida, alteración no autorizada y/o de la divulgación inapropiada. La Seguridad de la Información tiene como objetivo, la confidencialidad, la integridad y la disponibilidad de la información.

La primera se enfoca en mantener la información fuera del conocimiento de aquellas personas que no se encuentran autorizadas para tener acceso a ella. La integridad asegura que la información permanezca inalterada y completa; y por último, la disponibilidad consiste en que la información y los sistemas de comunicación permanezcan accesibles para sus usuarios oportunamente.

Anteriormente, las empresas consideraban sus productos como el activo clave de sus negocios, actualmente más de uno están reconociendo que sus activos claves

más valiosos es la información. Independientemente de que la información sea una base de datos de sus clientes o registros contables, la habilidad de almacenarla, recuperarla y manipularla de manera segura es crucial para el éxito en los negocios.

Toda información es valiosa por tres razones. La primera es que toda información representa básicamente dinero, un ejemplo evidente es la propiedad intelectual. Una segunda razón es que la información es la materia prima para poder tomar decisiones, por lo general, la información suele funcionar como un activador de negocios con el cual muchas organizaciones simplemente no podrían funcionar y, por último, la confiabilidad de la información en línea, considerada como un prerrequisito de la expansión de los negocios virtuales.

2.2 MARCO CONCEPTUAL

Información

La información es un recurso necesario y de gran valor para las empresas que la gestionan adecuadamente. La información implica un proceso de interpretación y transformación cuyo principal objetivo es la minimización de la incertidumbre en la toma de decisiones, en un entorno de creciente complejidad e incertidumbre. (Lapiedra et al., 2021)

Dentro de una empresa todos los empleados generan y captan información importante para el desempeño de sus funciones, la cual le permite tomar decisiones acertadas en frente de cualquier proceso, es por ello que la información debe estar siempre disponible para no afectar la productividad de una empresa.

Sistemas de información

Son un conjunto de elementos o componentes interrelacionados que recaban, manipulan, almacenan y distribuyen datos e información y proporciona una reacción correctiva si no se ha logrado cumplir un objetivo.(Arevalo et al., 2020)

Dentro de una empresa es el sistema central que ayuda a recopilar toda la información y a procesarla de forma adecuada para mejorar los procesos internos que lleva toda empresa. En la actualidad en los sistemas de información se encuentran implícitos todas las herramientas digitales, como las redes sociales.

Seguridad de la información

Son registros y procedimientos que requieren la integración de la tecnología, los ordenamientos y el comportamiento del usuario humano de tal manera que se logren los objetivos de asegurar la información, logrando que esta se encuentre disponible, integra y sea confidencial.(Muñoz et al., 2021)

Esto implica que se deben emplear controles tanto de los sistemas de información como en los procesos operativos de una empresa, con la finalidad de proteger los datos de tal forma que nadie más tenga acceso a determinada información confidencial.

Ciberseguridad

Comprende en proteger la información mediante la incorporación de herramientas tecnológicas con el objetivo de proteger datos confidenciales, actualmente las empresas mantienen información digital la cual puede ser infringida mediante ataques informáticos, los cuales en los últimos años han ganado importancia debido al uso de diversas plataformas web gratuitas que no son muy seguras (Morán, 2021). Las empresas requieren invertir en ciberseguridad que les

ayude a proteger la información de diversos ataques cibernéticos los cuales están latentes en la actualidad.

ISO 27002:2022

Son normas establecidas como una guía para el la ejecución de controles de seguridad de la información dentro de una empresa. Según Vargas & Marchan, (2019) las normas ISO proporcionan procedimientos para la administración de seguridad de la información

CAPÍTULO III: METODOLOGÍA

3.1. TIPO Y DISEÑO DE INVESTIGACIÓN

Para la elaboración del siguiente trabajo de investigación, se tomó en consideración a las medianas y pequeñas empresas de la ciudad de Milagro de la Provincia del Guayas. Para ello se realizó una investigación descriptiva, con la finalidad de analizar el estado actual en que se encuentran las empresas en lo referente a la seguridad de información.

3.2. LA POBLACIÓN Y LA MUESTRA

3.2.1. Características de la población

En el estudio se tomará en consideración a todas las empresas medianas y pequeñas del cantón Milagro de la Provincia del Guayas, como no existe una cantidad especifica de las empresas en la actualidad, se procederá a realizar un levantamiento de información considerando a todas las empresas que cuenten con una cantidad de trabajadores comprendidas entre 9 hasta 199.

3.2.2. Delimitación de la población

La investigación se limita específicamente al área de tecnología de las pequeñas y medianas empresas del Cantón Milagro, debido a que la cantidad de empresas no se ha definido se procederá a estudiar a todas las empresas directamente.

3.3. LOS MÉTODOS Y LAS TÉCNICAS

Para la presente investigación se aplicará el método descriptivo enfocándose puntualmente en una recolección de información de forma cuantitativa. El método descriptivo detalla características esenciales de la población que se estudia, ayudando en el registro y análisis de la información. Esto permite establecer la estructura o el comportamiento de los fenómenos estudiados, proporcionando información sistemática y comparable con la de otras fuentes.(Guevara et al., 2020)

Para nuestro estudio es importante establecer el comportamiento de cada empresa esto ayudara a estudiar de manera más específica los problemas de seguridad de la información que tienen en la actualidad.

Muñoz et al. (2021) define a las encuestas como una secuencia en la que se emplea un instrumento, el cual tiene como objetivo la consolidación de datos, con el fin de conseguir una aproximación de la realidad. Para la ejecución del análisis de este trabajo investigativo se hará uso de la técnica de la encuesta, la misma que se aplicará mediante la herramienta de formularios proporcionada por Google, “GoogleForms”.

3.4. PROPUESTA DE PROCESAMIENTO ESTADÍSTICO DE LA INFORMACIÓN.

Posterior a le ejecución de la encuesta se clasifico la información obtenida, para que esta sea procesada estadísticamente a través del software SPSS Statistics y así poder validar las hipótesis planteadas durante el desarrollo de esta investigación.

CAPÍTULO IV: ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. ANÁLISIS DE DESCRIPTIVO DE LOS RESULTADOS

En los resultados obtenidos de las encuestas realizadas a 59 empresas del cantón Milagro, se pudo determinar a las pequeñas y medianas empresas conforme al número de empleados con las que contaban cada una.

Tabla 2:

Número de colaboradores por empresa.

		Frecuencia	Porcentaje
Válido	10-49 colaboradores	26	44,1
	50-199 colaboradores	27	45,8
	Mas de 200 colaboradores	6	10,2
	Total	59	100,0

Tabla 2: *Número de colaboradores por empresa.*

Elaborado por: Pérez, 2022

Figura 1:

Número de colaboradores por empresa.

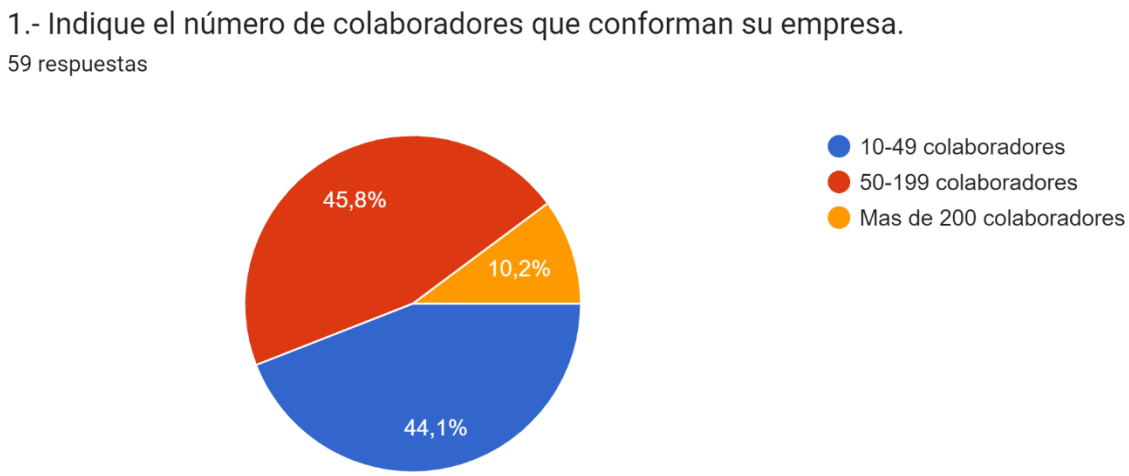


Figura 1: *Número de colaboradores por empresa.*

Elaborado por: Pérez, 2022

Conforme a la figura 1 se puede visualizar que 26 de las empresas son consideradas pequeñas debido a que cuentan con una cantidad de 10 a 49 empleados, 27 se clasifican como medianas debido a que tienen entre 50 y 199 empleados y 6 corresponden a las grandes empresas que tienen 200 empleados en adelante.

Tabla 3:

Sistemas operativos que cuentan con licenciamiento en las empresas.

		Frecuencia	Porcentaje
Válido	No	32	54,2
	SI	27	45,8
	Total	59	100,0

Tabla 3: *Sistemas operativos que cuentan con licenciamiento en las empresas.*

Elaborado por: Pérez, 2022

Figura 2:

Numero de computadores con sistema operativo licenciado.

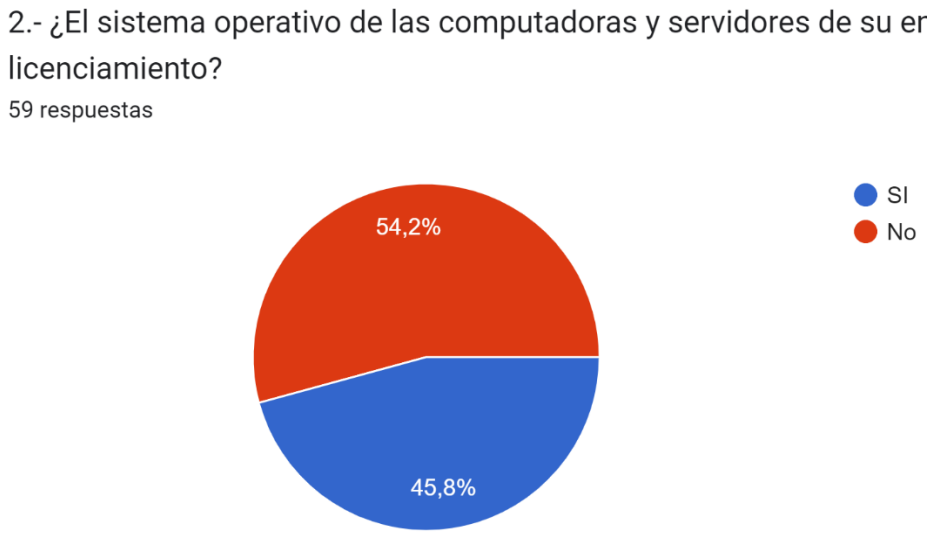


Figura 2: *Numero de computadores con sistema operativo licenciado.*

Elaborado por: Pérez, 2022

Según la figura 2 podemos visualizar que el 45,8% de las empresas cuentan con sistema operativo con licencia, mientras que el 54,2% no posee el licenciamiento adecuado.

Tabla 4:

Antivirus que cuentan con licenciamiento en las empresas.

		Frecuencia	Porcentaje
Válido	No	32	54,2
	SI	27	45,8
	Total	59	100,0

Tabla 4: *Antivirus que cuentan con licenciamiento en las empresas.*

Elaborado por: Pérez, 2022

Figura 3:

Numero de computadores con antivirus licenciado.

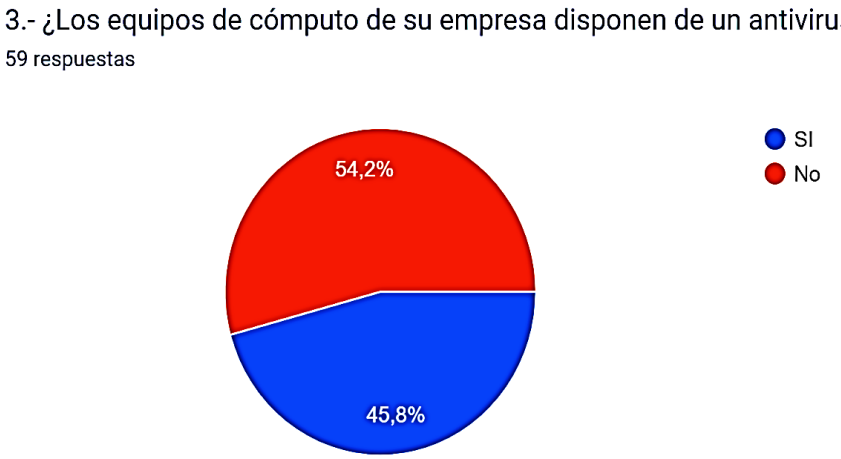


Figura 3: *Numero de computadores con antivirus licenciado.*

Elaborado por: Pérez, 2022

En la figura 3 se puede observar que el 45,8% de las empresas encuestada cuentan con un antivirus con licencia instalados en sus equipos, mientras que el 54,2% no cuentan con uno.

Tabla 5:

Tipos de software utilizados por la empresa.

		Frecuencia	Porcentaje
Válido	No aplica, la empresa si cuenta con licenciamiento.	24	40,7
	Utiliza software con parches informáticos.	9	15,3
	Utiliza software libre gratuito.	26	44,1
	Total	59	100,0

Tabla 5: *Tipos de software utilizados por la empresa.*

Elaborado por: Pérez, 2022

Figura 4:

Tipos de licencias utilizadas

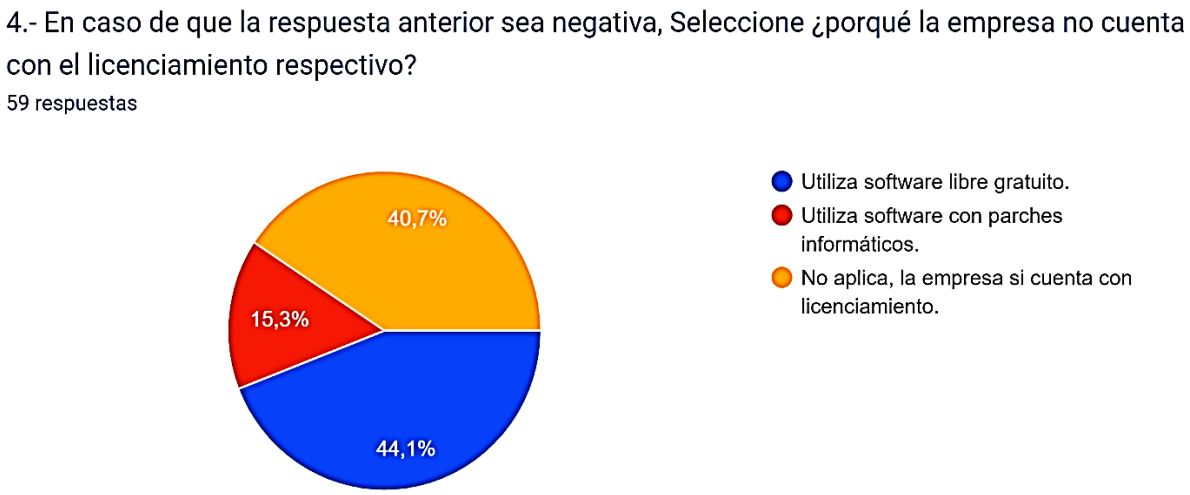


Figura 4: *Tipos de licencias utilizadas*

Elaborado por: Pérez, 2022

Según lo expuesto en el siguiente diagrama, se determina que las empresas que indicaron no estar compuestas de un antivirus con licencia es porque del 100% el 44,1% utilizan un software libre gratuito y el 15,3% utiliza un software con parches informáticos; por lo cual se comprende que el porcentaje restante si cuenta con licenciamiento.

Tabla 6:

Utilización de respaldo de energía.

		Frecuencia	Porcentaje
Válido	No	29	49,2
	Si	30	50,8
	Total	59	100,0

Tabla 6: *Utilización de respaldo de energía.*

Elaborado por: Pérez, 2022

Figura 5:

Respaldo de energía

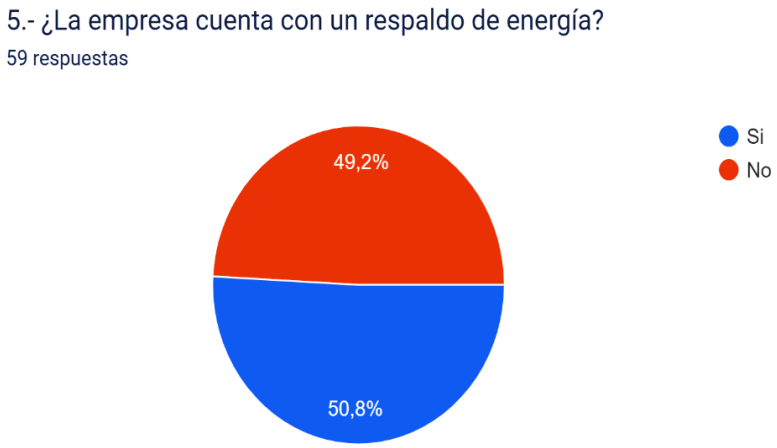


Figura 5: *Respaldo de energía*

Elaborado por: Pérez, 2022

Se puede observar que de las 59 empresas 30 están preparadas con un respaldo de energía mientras que 29 de ellas, no.

Tabla 7:

Aplicación de respaldo de información.

		Frecuencia	Porcentaje
Válido	Al menos dos veces por semana	7	11,9
	Al menos una vez por semana	10	16,9
	De vez en cuando	21	35,6
	Diariamente	18	30,5
	Nunca	3	5,1
	Total	59	100,0

Tabla 7: *Aplicación de respaldo de información.*

Elaborado por: Pérez, 2022

Figura 6:

Respaldo de información

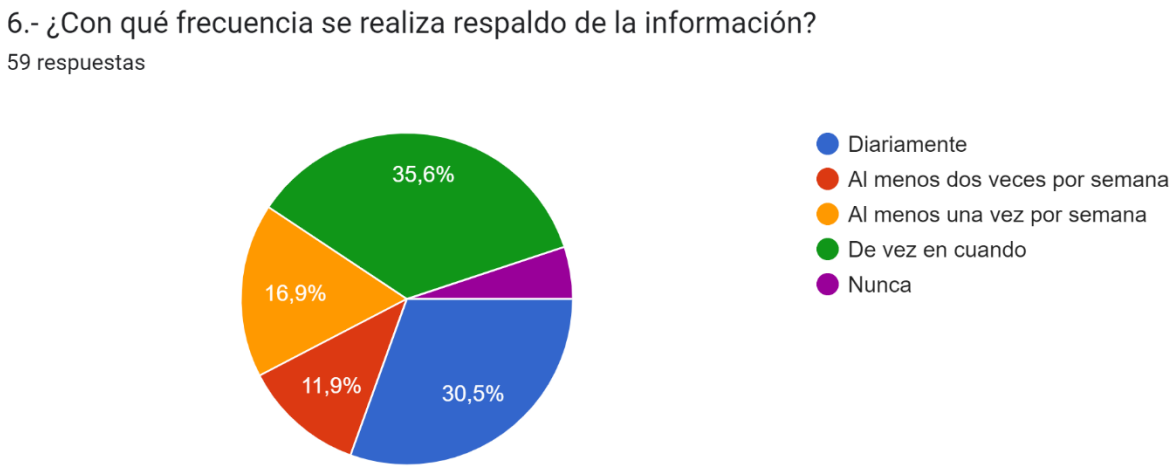


Figura 6: *Respaldo de información*

Elaborado por: Pérez, 2022

En la figura 5 se puede apreciar que solo 18 empresas realizan respaldo diariamente, 7 lo hacen dos veces por semana, 10 una vez por semana, 21 lo realizan de vez en cuando y 3 empresas no realizan ningún tipo de respaldo de su información.

Tabla 8:

Plan preventivo ante la Pérdida de información de la empresa.

		Frecuencia	Porcentaje
Válido	No	27	45,8
	Si	32	54,2
	Total	59	100,0

Tabla 8: *Plan preventivo ante la Pérdida de información de la empresa.*

Elaborado por: Pérez, 2022

Figura 7:

Plan preventivo ante la Pérdida de información.

Figura 7: *Plan preventivo ante la Pérdida de información.*

Elaborado por: Pérez, 2022

En la figura 7 se puede visualizar que de las empresas encuestadas el 54,2% cuenta con un plan preventivo ante la Pérdida de información y el 45,8% no cuenta con ningún plan de acción ante ello.

Tabla 9:

Capacitación de políticas de seguridad de la información a empleados.

		Frecuencia	Porcentaje
Válido	Dos veces al año.	10	16,9
	Mas de tres veces en el año.	10	16,9
	Nunca.	18	30,5
	Una vez al año.	21	35,6
	Total	59	100,0

Tabla 9: *Capacitación de políticas de seguridad de la información a empleados.*

Elaborado por: Pérez, 2022

Figura 8:

Capacitaciones políticas de seguridad de la información.

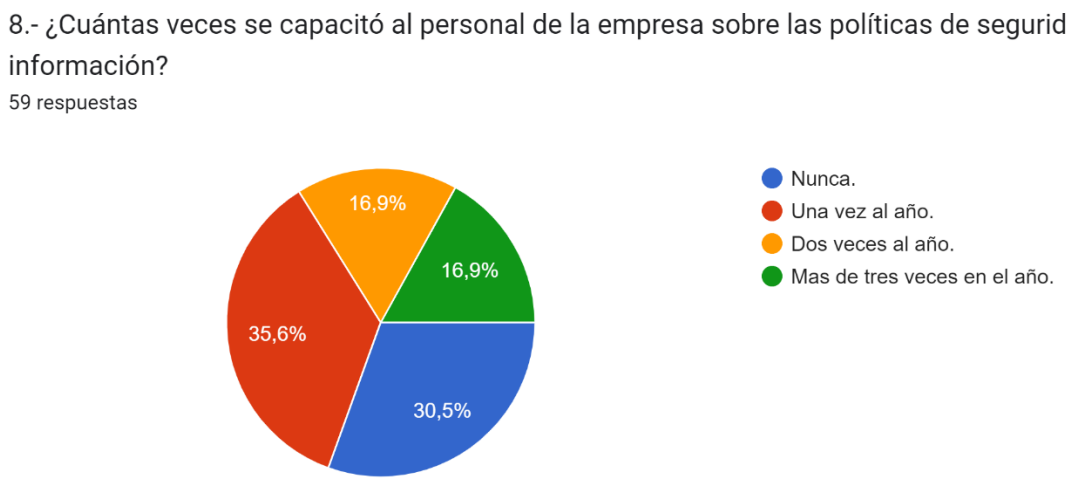


Figura 8: *Capacitaciones políticas de seguridad de la información.*

Elaborado por: Pérez, 2022

En la figura 8 se puede visualizar la frecuencia con la que se capacito al personal de las empresas sobre las normas de seguridad de la información, donde se tiene que 10 de ellas lo hacen trimestralmente, 10 de forma semestral, 21 anualmente y 18 no ha ejecutado capacitaciones hacia su personal de acuerdo a las normativas correspondientes.

Tabla 10:

Pérdida de información en la empresa.

		Frecuencia	Porcentaje
Válido	No	23	39,0
	Si	36	61,0
	Total	59	100,0

Tabla 10: *Pérdida de información en la empresa.*

Elaborado por: Pérez, 2022

Figura 9:

Pérdida de información

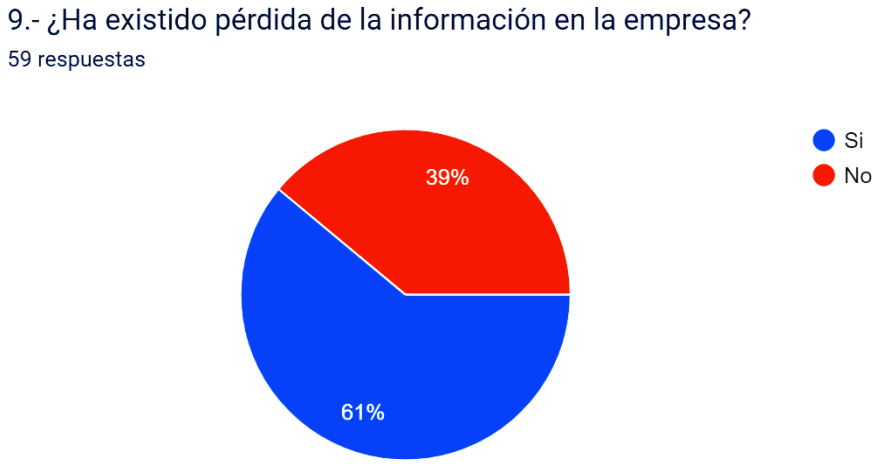


Figura 9: *Pérdida de información*

Elaborado por: Pérez, 2022

En la siguiente pregunta se busca identificar si ha existido pérdida de información en las empresas encuestas, aquello que en este gráfico se proyecta que el 61% ha perdido información mientras que el 39% no.

Tabla 11:

Integridad de la información en la empresa.

		Frecuencia	Porcentaje
Válido	Al menos dos veces por semana	6	10,2
	Al menos una vez por semana	5	8,5
	De vez en cuando	31	52,5
	Diariamente	3	5,1
	Nunca	14	23,7
	Total	59	100,0

Tabla 11: *Integridad de la información en la empresa.*

Elaborado por: Pérez, 2022

Figura 10:

Integridad de la información

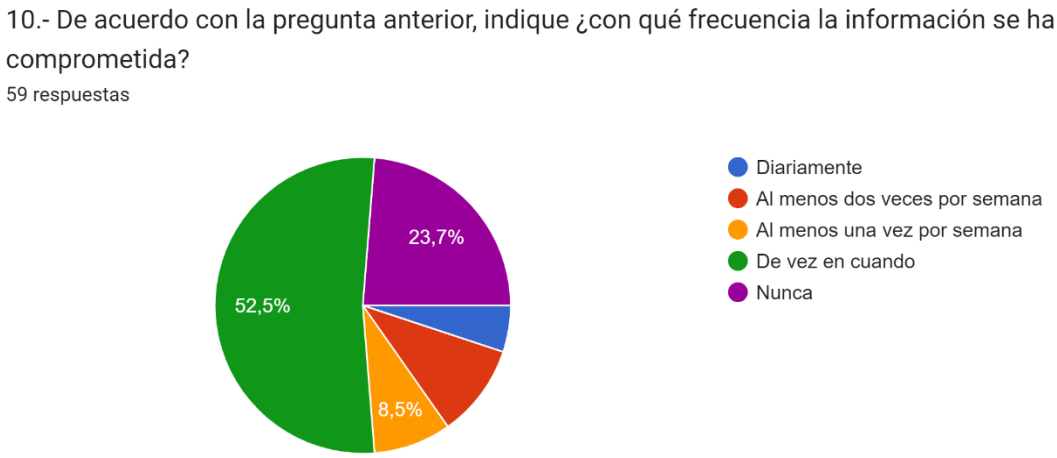


Figura 10: *Integridad de la información*

Elaborado por: Pérez, 2022

En la figura 10 se puede apreciar que, en 3 empresas, la información se ha visto comprometida diariamente, 6 indican que dos veces por semana, 5 ha presenciado la pérdida de información al menos una vez por semana, 31 (más del 50% de los encuestados) especifican que este problema surge de vez en cuando y 14 mencionan que nunca han presentado este tipo de inconvenientes.

Tabla 12:

Ataques cibernéticos a la empresa.

		Frecuencia	Porcentaje
Válido	No	42	71,2
	Si	17	28,8
	Total	59	100,0

Tabla 12: *Ataques cibernéticos a la empresa.*

Elaborado por: Pérez, 2022

Figura 11:

Ataques cibernéticos

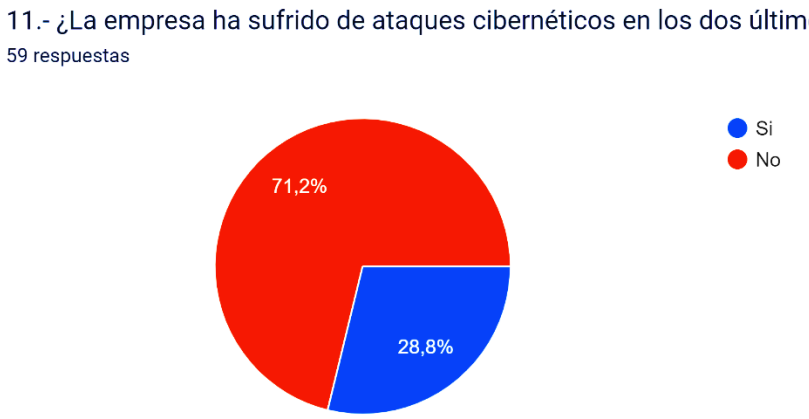


Figura 11: *Ataques cibernéticos*

Elaborado por: Pérez, 2022

En la figura 11 se puede observar que 17 empresas han sufrido de ataques cibernéticos en los dos últimos años, mientras que 42 manifiestan que no.

Tabla 13:

Tipos de ataques cibernéticos que ha sufrido la empresa.

		Frecuencia	Porcentaje
Válido	Malware	5	8,5
	No aplica, no ha existido ataques cibernéticos.	37	62,7
	Phishing	8	13,6
	Ransomware	3	5,1
	Whaling	6	10,2
	Total	59	100,0

Tabla 13: *Tipos de ataques cibernéticos que ha sufrido la empresa.*

Elaborado por: Pérez, 2022

Figura 12:

Tipo de ataque cibernético

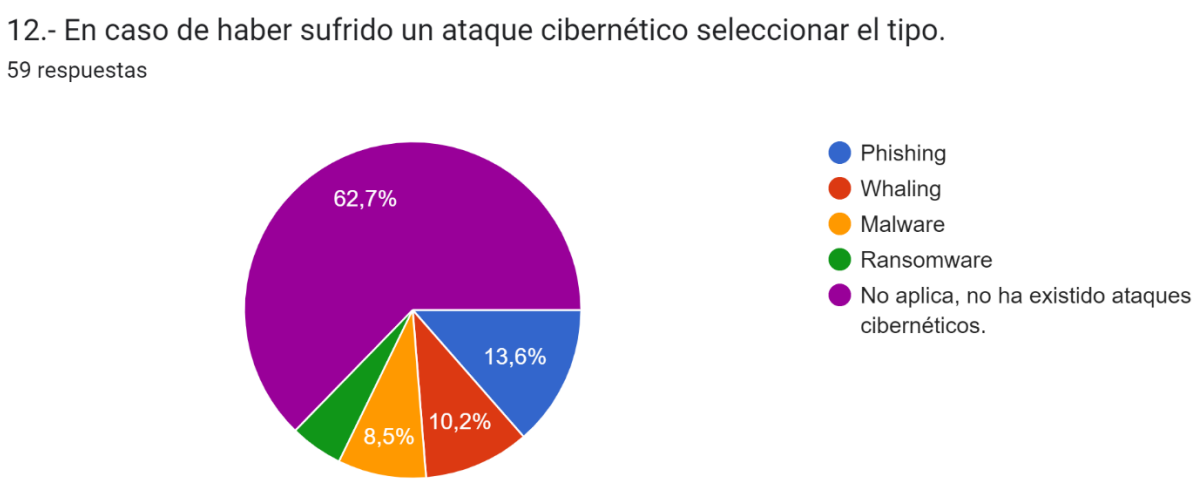


Figura 12: *Tipo de ataque cibernético*

Elaborado por: Pérez, 2022

Dentro de la figura 12 se proyecta el tipo de ataque cibernético que han sufrido las 17 empresas, de las cuales 8 indican que han sufrido de phishing, 6 de whaling, 5 de malware y 3 de rasomware.

Tabla 14:

Pérdida de información por fallos en equipos informáticos de la empresa.

		Frecuencia	Porcentaje
Válido	No	25	42,4
	Si	34	57,6
	Total	59	100,0

Tabla 14: *Pérdida de información por fallos en equipos informáticos de la empresa.*

Elaborado por: Pérez, 2022

Figura 13:

Pérdida de información por fallos en equipos

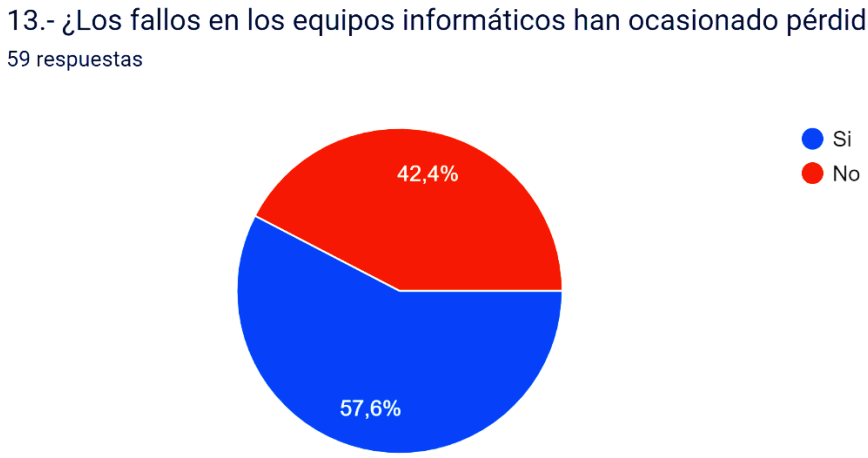


Figura 13: *Pérdida de información por fallos en equipos*

Elaborado por: Pérez, 2022

En la figura 13 se especifica que 34 empresas han perdido información por fallos en sus equipos informáticos, por otro lado, 25 mencionan que esta no ha sido la causa.

Tabla 15:

Mantenimiento de los equipos de cómputo.

		Frecuencia	Porcentaje
Válido	Cada dos años.	1	1,7
	Cuando los equipos presentan fallos.	24	40,7
	Dos veces al año.	14	23,7
	Una vez al año.	20	33,9
	Total	59	100,0

Tabla 15: *Mantenimiento de los equipos de cómputo.*

Elaborado por: Pérez, 2022

Figura 14:

Mantenimiento de los equipos de cómputo.

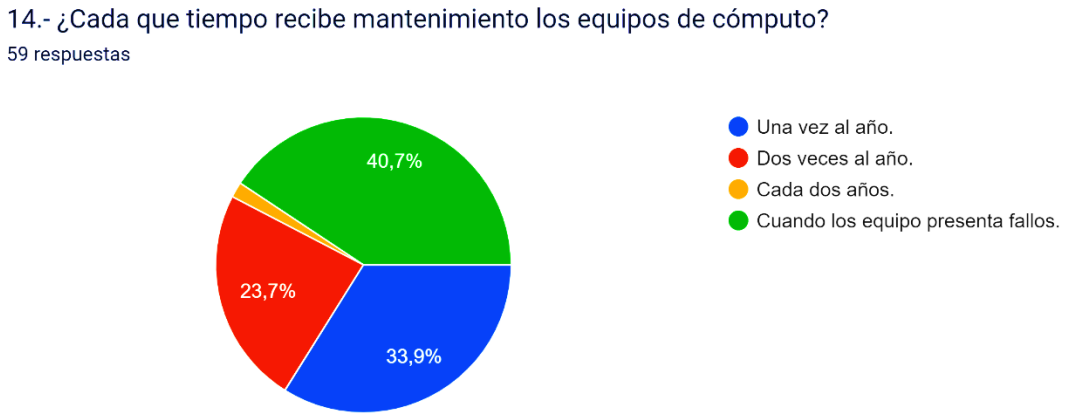


Figura 14: *Mantenimiento de los equipos de cómputo*

Elaborado por: Pérez, 2022

Para la última pregunta se intenta identificar la frecuencia con la que reciben mantenimiento los equipos de cómputo de las empresas, aquellas que como se visualiza en la figura 14, 20 empresas indicaron que brindan mantenimiento a sus equipos, una vez al año; 14 lo hacen dos veces al año; 1 cada dos años y el mayor porcentaje, es decir, 24 empresas dan mantenimiento a sus equipos cuando estos presenten fallas.

Análisis General

Conforme al análisis realizado se puede constatar que no todas las empresas cuentan con el licenciamiento respectivo en los equipos informáticos que usan, esto se da tanto para el sistema operativo como en el antivirus utilizado. Cuando los equipos informáticos no cuentan con el debido licenciamiento se encuentran mas vulnerables a sufrir un ataque informático, por tanto, existe más riesgo de pérdida de información.

Los cortes de energías son otros aspectos a considerar que en ocasiones pueden producir la Pérdida parcial de información. Resguardar la información implica estar preparado ante cualquier evento que pueda ocasionar su Pérdida, sin embargo, no todas las empresas consideran importante este aspecto al no contar con un respaldo de energía.

Así también es muy importante que los equipos informáticos donde se almacena la información de los diversos procesos que lleva la empresa, cuenten con una revisión periódica, con el fin de identificar algún problema en sus compontes para evitar un fallo imprevisto que ocasione la Pérdida de la información. Conforme a las encuestas realizadas una de las causas que compromete la seguridad de la información son los fallos en los equipos de cómputo.

De igual forma el respaldo de la información es imprescindible debido a que esto nos ayuda a tener nuestra copia de seguridad disponible en caso de que exista alguna Pérdida de la misma, por ello se sugiere que el respaldo sea diario para que el impacto sea menor, conforme a las encuestas realizadas se puede visualizar que una parte de las empresas realiza el respaldo de la información diariamente, seguido de un porcentaje que establece que se ejecuta un respaldo de información de vez en cuando, las que no lo hacen corren el riesgo de perder información imprescindible para el desarrollo de sus operaciones.

Las normas de seguridad en las empresas son de suma importancia por ello es imprescindible que los empleados sean capacitados sobre este tema, para que hagan el uso adecuado de los medios digitales y de los equipos informáticos, sobre todo en una era digital donde las amenazas en la web se han incrementado.

Conforme a los datos recopilados se puede determinar que muchas de las empresas han sufrido Pérdida de información, esto se ha dado por diversos motivos y no solamente por ataques informáticos sino por fallos en sus equipos como se lo ha mencionado anteriormente, por ello es importante contar con un plan de estrategias de seguridad de la información, que contemple los diversos escenarios que puedan ocasionar la vulnerabilidad de datos importantes.

4.2. ANÁLISIS CORRELACIONAL DE LOS RESULTADOS

Para analizar las respuestas de la encuesta se aplicó el análisis correlacional de Pearson con la finalidad de medir la relación entre dos variables.

Para efectuar el análisis correlacional de las variables primero se ingresó toda la información a al aplicativo estadístico SPSS, información que fue recopilada de las encuestas realizadas a 59 empresas del canto Milagro. Posterior a ello se procedió a realizar el cálculo de la variable considerando la variable dependiente e independiente para cada una de las dimensiones.

Realizado el proceso estadístico en el aplicativo SPSS, se consiguieron los siguientes resultados, para analizar y verificar cada una de las hipótesis planteadas en la investigación.

4.2.1. Contrastación de la Hipótesis General

Un plan con estrategias de seguridad de la información en las empresas incide en el resguardo de la información.

Tabla 16:

Contrastación de la Hipótesis General

Correlaciones			
		VINDEPENDIENTE	VDEPENDIENTE
VINDEPENDIENTE	Correlación de Pearson	1	-,319
	Sig. (bilateral)		,014
	N	59	59
VDEPENDIENTE	Correlación de Pearson	-,319	1
	Sig. (bilateral)	,014	
	N	59	59

Tabla 16: *Contrastación de la Hipótesis General*

Elaborado por: Pérez, 2022

Conforme con los resultados obtenidos en la tabla 15, entres las variables estrategias y seguridad de la información existe una relación directa significativa (r=,014), lo cual indica que las estrategias para proteger la información garantizan la integridad de la misma por lo que se considera la hipótesis general.

4.2.2. Contrastación de la Hipótesis Específica 1

Identificar los distintos tipos de amenazas de seguridad de la información que puede tener una empresa y su impacto en la misma.

Tabla 17:

Contrastación de la Hipótesis Específica 1

Correlaciones			
		Ataques cibernéticos	Pérdida de la información
Ataques cibernéticos	Correlación de Pearson	1	,112
	Sig. (bilateral)		,397
	N	59	59
Pérdida de la información	Correlación de Pearson	,112	1
	Sig. (bilateral)	,397	
	N	59	59

Tabla 17: *Contrastación de la Hipótesis Específica 1*

Elaborado por: Pérez, 2022

Conforme con los resultados obtenidos en la tabla 16, entres la dimensión ataques cibernéticos y pérdida de la información no existe una relación directa significativa (r=,397), esto se da por lo que los ataques informáticos no son el único motivo de perdida de la información, por lo cual no se acepta la hipótesis.

4.2.3. Contrastación de la Hipótesis Específica 2

Los escasos respaldos de información y energía inciden en los procesos adecuados para proteger la integridad información.

Tabla 18:

Contrastación de la Hipótesis Específica 2

Correlaciones			
		Respaldo de energía e información	**Perdida de la información**
Respaldo de energía e información	Correlación de Pearson	1	-,470*
	Sig. (bilateral)		,000
	N	59	59
Perdida de la información	Correlación de Pearson	-,470*	1
	Sig. (bilateral)	,000	
	N	59	59

Tabla 18: *Contrastación de la Hipótesis Específica 2*

Elaborado por: Pérez, 2022

De acuerdo con los resultados obtenidos y presentados en la tabla 17, entre la dimensión respaldo de energía y uso de la tecnología existe una relación significativa (r= ,000), esto denota que los respaldos de energía y de información ayudan a resguardar la información de la empresa, por ello se acepta la hipótesis especifica.

4.2.4. Contrastación de la Hipótesis Específica 3

Los escasos procesos de seguridad de la información, inciden en la pérdida de información relevante en una empresa.

Tabla 19:

Contrastación de la Hipótesis Específica 3

Correlaciones			
		Procesos de seguridad de la información	**Perdida de la información**
Procesos de seguridad de la información	Correlación de Pearson	1	-,306*
	Sig. (bilateral)		,018
	N	59	59
Perdida de la información	Correlación de Pearson	-,306*	1
	Sig. (bilateral)	,018	
	N	59	59

Tabla 19: *Contrastación de la Hipótesis Específica 3*

Elaborado por: Pérez, 2022

De acuerdo con los resultados obtenidos y presentados en la tabla 18, entre los procesos de seguridad de la información y perdida de la información existe una relación significativa (r=,018), debido a que mientras los empleados mas conozcan sobre ciertos procesos de seguridad de la información, habrá mayor resguardo de la misma.

CONCLUSIONES

Una vez analizada la información recopilada en la investigación, se puede concluir que la seguridad de la información depende de multiplico factores, teniendo entre uno de los principales: contar con estrategias de seguridad de la información para evitar alguna pérdida importante.

Es ineludible considerar los diferentes tipos de amenazas existentes en la web, los cuales están en constante cambio conforme al avance de la tecnología digital. En el estudio realizado los ataques cibernéticos no son la principal causa de la perdida de información, sin embargo, también se debe tener en consideración para disminuir en lo posible las brechas de seguridad que pueden existir en las empresas.

Los respaldos de información y energía que llevan las empresas son concluyentes para que los datos almacenados en las computadoras y servidores no se pierdan en su totalidad ya que esta puede ser relevante para los diversos procesos que llevan.

En cada empresa existen escasos procesos de seguridad empezando desde el punto más básico, partiendo desde el licenciamiento de su sistema operativo y antivirus, hasta el mantenimiento periódico de sus equipos informáticos.

RECOMENDACIONES

Se recomienda establecer políticas de seguridad de la información para cada empresa y que estos sean socializados con todo el personal para el debido cumplimiento del mismo.

Se debe capacitar periódicamente al personal de la empresa sobre las diversas normas de seguridad de información en la web, con la finalidad de concientizar el uso y la protección de la información.

Se recomienda contar con un plan de mantenimiento preventivo para los equipos informáticos que usan las empresas para evitar la pérdida de información por el daño de algún equipo informático.

Se recomienda realizar los respaldos de información de forma diaria y de preferencia contratar un repositorio en la nube para que la información esté disponible en todo momento.

CAPÍTULO V: PROPUESTA

5.1 TEMA

Plan con estrategias de seguridad de la información para las pequeñas y medianas empresas.

5.2. JUSTIFICACIÓN

Las diversas tecnologías han proporciona a las PYMES más de una manera para mejorar su productividad y su competitividad en el mercado, debido a la interacción y al acercamiento con los clientes que las herramientas tecnológicas proporcionan.

Esto les ha permitido recopilar información necesaria para mejorar sus procesos y servicios, sin embargo, no todas las empresas se han visto en la necesidad de aplicar en ciertas herramientas tecnológicas porque no lo requerían, aunque debido al confinamiento ocasionado por la pandemia, las empresas se vieron en la necesidad de incorporar de forma más implícita las TIC.

Por ello las Pymes deben adecuar sus procesos con la incorporación de diversas tecnologías emergentes que ayudan a mejorar sus procesos, sin embargo, la incorporación de nuevas tecnologías ha creado la necesidad de implementar nuevos controles que protejan la información en todo momento.

La información es una activo muy importante en cada empresa, la cual puede estar amenazada ante cualquier eventualidad, entre los cuales se debe considerar amenazas externas e internas. Por ello las empresas deben contar con un plan con

estrategias que contemplen la seguridad de la información desde todos sus aspectos.

.

5.3 FUNDAMENTACIÓN

La aplicación de un plan con estrategias de seguridad de la información para las pequeñas y medianas empresas se basa en las normativas de seguridad definidas por las normas ISO 27002:2022 la cual aplica distintos controles clasificados por atributos.

El primer atributo contempla los distintos tipos de controles a aplicarse cuando se presenta algún incidente de seguridad, este contempla los valores de prevención detección y corrección. Estos valores son fundamentales a la hora de aplicar determinados controles en una empresa.

El segundo atributo observa las propiedades de la seguridad de la información, enfocándose específicamente en la confidencialidad, integridad y disponibilidad. Cada control determina lo que se debe proteger en base a la necesidad de cada empresa.

Como otro atributo se considera la ciberseguridad, este aporta una estructura con estándares definidos por las normativas ISO/IEC TS 27110. Se definen diferentes fases para identificar las amenazas cibernéticas, proteger la información, detectar las brechas de seguridad, responder ante cualquier tipo ataque y estar preparado para recuperar la información en el menor tiempo posible y de forma íntegra.

Las capacidades operativas es un atributo importante a contemplar, donde se especifican diversos criterios de seguridad entre ellos tenemos: la parte física que

considera la protección de los equipos informáticos mediante los cuales se transmite y almacena la información, los sistemas de seguridad con los que cuenta la empresa y finalmente considera la parte humanos que intervienen en la protección física de la información.

Finalmente, los dominios de la seguridad contemplaran la aplicación de los controles estándar para proteger y recuperar la información el cual es el objetivo de la propuesta la cual se aplicará para las PYMES de la ciudad de Milagro.

5.4 OBJETIVOS GENERAL Y ESPECIFICOS

Objetivo General

Desarrollar un plan con estrategias de seguridad de la información para las pequeñas y medianas empresas, enfocándose en las necesidades presentadas en la actualidad.

Objetivos específicos

Definir los controles de seguridad necesarios para proteger la información de la empresa.

Establecer políticas de seguridad de acceso a la información para que no exista perdida ni daño de la información.

Determinar los equipos informáticos y softwares adecuados para que no exista ninguna brecha de seguridad.

5.5 UBICACIÓN

La propuesta se aplicar en la pequeñas y medianas empresas perteneciente a la ciudad de Milagro.

5.6 ESTUDIO DE FACTIBILIDAD

La ejecución de la propuesta es factible desde los aspectos organizacional, TIC y físicos, conforme se detalla a continuación.

Organizacional

La propuesta es factible porque las empresas conocen la necesidad de proteger la información, con ello se busca definir una estructura organizacional donde se considere todos los recursos y se limite el acceso a los mismos, con la finalidad de proteger la información ante cualquier amenaza que suscite.

La información deberá ser resguardada considerando el mal uso de los recurso o acceso no autorizado por personal no autorizado.

TIC

En cuanto a la tecnología de la información y comunicación la propuesta es aplicable ya que existen diversas herramientas que permiten implementar varios controles que ayudan a proteger la información ante cualquier amenaza.

Así también es factible que el departamento ejecute diversos procesos preventivos, que los ayuden a estar preparados ante la pérdida de la información en cualquier departamento de la empresa.

FÍSICO

La aplicabilidad de propuesta es viable consideran la restricción de acceso a las distintas áreas en base a las funciones de cada empleado, esto garantizara la seguridad de los equipos donde se almacena información imprescindible para la empresa.

5.7 DESCRIPCIÓN DE LA PROPUESTA

El siguiente plan con estrategias de seguridad de la información contempla la aplicación de diversos procesos que ayuden a prevenir la perdida de la información, definiendo controles a aplicarse en las PYMES. Para la ejecución de este plan se tomará como referencia la normas ISO 27002:2022.

Alcance y limites

Esta propuesta se enfocará netamente al área de sistemas, sin embargo, los procesos serán de aplicación para toda la empresa.

Políticas de seguridad de la información

En este punto se define las diversas políticas de seguridad que se deben seguir para evitar la pérdida de la información.

Tabla 20: *Políticas de seguridad*

Descripción	Aplicación
Perfiles para acceso a la información.	El personal de tecnología se encargará de crear restricciones de acceso a los equipos informáticos conforme al perfil de cada empleado.
Confidencialidad de la información.	El encargado del área o de la empresa deberá asegurarse que el personal a su cargo cumpla la política.
Integridad de la información.	Establecer parámetros de seguridad con sistemas debidamente licenciados, para que la información no este comprometida por amenazas externas.

Tabla 20: *Políticas de seguridad*

Elaborado por: Pérez, 2022

Acción preventiva a la pérdida de la información.

En este punto se definirá los controles preventivos que cada empresa debe seguir para evitar la pérdida de la información.

Tabla 21: *Acciones preventivas*

Descripción	**Aplicación**
Respaldo de información.	El personal de tecnología deberá ejecutar y monitorear que se realicen respaldo de información diarios y esto deberán estar en algún equipo con acceso restringido o en la nube.
Respaldo de energía.	Deberá implementar un respaldo de energía en todos los equipos o al menos en el equipo donde reposa los respaldos de información.
Mantenimiento de equipos informáticos.	El personal de tecnología establecerá cronogramas de mantenimientos preventivos de los equipos informáticos a cumplirse.
Instalación y configuración de antivirus.	Determinar el antivirus a utilizar en la empresa dependiendo de la capacidad económica de la misma y configurarlo con las debidas restricciones para que no pueda ser manipulado por personas ajenas al departamento de TIC.

Tabla 21: *Acciones preventivas*

Elaborado por: Pérez, 2022

Acción de recuperación de la información

Es importante conocer los procesos que se deben seguir cuando ha existido perdida de la información.

Tabla 22: *Acción de recuperación*

Descripción	**Departamento o persona encargada.**	**Aplicación**
Evaluación de la situación.	TIC	El encargado de TIC deberá analizar y registrar el suceso que ha comprometido la información, para proceder a ejecutar el respaldo.
Tiempo estimado de la recuperación	TIC	Dependiendo de cada empresa se deberá definir el tiempo de ejecución conforme a la necesidad de cada una.
Acciones correctivas a seguirse.	TIC	Se deberá analizar la situación y plantear mejoraras en los procesos de seguridad de la información .

Tabla 22: *Acción de recuperación*

Elaborado por: Pérez, 2022

5.7.1 Actividades

Para la aplicación de la propuesta se deberá solicitar el respectivo permiso

a cada empresa para que mediante con el jefe de sistema se ejecute los controles respectivos. Así también se encargará de exponer la importancia de la seguridad de la información en la empresa y dará a conocer las políticas vigentes.

Para que el plan con estrategias de seguridad cumpla su cometido, deberá existir una persona encargada de verificar el cumplimiento de todos los controles aplicados. La aplicación del monitoreo deberá realizarse de forma periódica cada 15 o 30 días.

5.7.2 Recursos, análisis financiero

Los Recursos financieros fue financiado directamente por el investigador, contemplando un monto aproximado de $710 dólares americanos, el que se detalla a continuación.

Tabla 23: *Datos generales*

<table>
<tr><td>Título del proyecto</td><td colspan="2">Plan con estrategias de seguridad de la información para las pequeñas y medianas empresas.</td></tr>
<tr><td>Director del Proyecto</td><td colspan="2">Segundo Arturo Pérez Alvarez</td></tr>
<tr><td>Duración del Proyecto

3 meses</td><td>Costo Total del proyecto

$ 710</td><td>Lugar de Ejecución del Proyecto
Pequeñas y medianas empresa del cantón Milagro.</td></tr>
<tr><td colspan="3">Fecha de Inicio estimada: 12 de septiembre del 2022
Fecha fin estimada : 12 de diciembre del 2022</td></tr>
</table>

Tabla 23: *Datos generales*

Elaborado por: Pérez, 2022

Tabla 24: *Talento Humano*

NOMBRE	Actividad	DURACIÓN	COSTO PARCIAL	COSTO TOTAL
Segundo Arturo Pérez Alvarez	Recolección de Datos	3 meses	50	150

Tabla 24: *Talento Humano*

Elaborado por: Pérez, 2022

Tabla 25: *Equipos*

DESCRIPCIÓN DEL EQUIPO	PRECIO
Laptop	$500,00
Servicio de internet por 3 meses	$60,00
TOTAL	$560,00

Tabla 25: *Equipos*

Elaborado por: Pérez, 2022

5.7.3 Impacto

La presente propuesta tiene un impacto organizacional el cual se centra en la utilización de la tecnología en las empresas, detallando políticas necesarias para el manejo adecuado de la información.

Así también los controles de seguridad contribuyen a que las empresas mantengan la información segura, libre de peligros internos y externos, contando así con la disponibilidad de la información para la toma de decisiones y el desarrollo adecuado de todos los procesos.

5.7.4 Cronograma

Id	Actividad	Comienzo	Fin	Duración	Septiembre	Octubre	Noviembre
1	Investigación de estudios previos	12/09/2022	23/09/2022	Dos semanas	XXXX		
2	Encuestas a personal de TIC de las empresas.	26/09/2022	29/09/2022	Una semana	XX		

3	Tabulación de Resultados	3/10/2022	9/10/2022	Una semana		XX	
4	Desarrollo del modelo de propuesta	10/10/2022	2/11/2022			XXXX	X

Tabla 26: *Cronograma*

5.7.5 Lineamiento para evaluar la propuesta

Los lineamientos de evaluación que se consideraran para la propuesta son:

Funcionalidad

En este aspecto se evaluará todos los criterios de ejecución que considera la propuesta y determina que estén debidamente alineadas con las necesidades de la empresa.

Aplicabilidad

En la aplicabilidad se procura analizar si es posible emplear los distintos controles propuestos, tomando en consideración los recursos con los que cuenta cada empresa.

BIBLIOGRAFÍA

Altamirano, M. (2019). Modelo para la gestión de la seguridad de la información y los riesgos a sociados a su uso. Avances Centro de Información y Gestión Tecnológica. https://dialnet.unirioja.es/servlet/articulo?codigo=6989568

Arevalo, F., Ordoñez, I., Cortez, A., & Solís, J. (2020). Importancia de los sistemas de información. *Ciencias Económicas* . https://fipcaec.com/index.php/fipcaec/article/view/285/501

Arguezo, E. (2019). PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA PROTECCIÓN DE ACTIVOS DE INFORMACIÓN BASADO EN LA NORMA ISO 27001EN EL ÁREADEINFORMÁTICA DE LA MUNICIPALIDAD PROVINCIAL DE HUÁNUCO. http://repositorio.udh.edu.pe/bitstream/handle/123456789/2084/ARG%c3%9cEZO%20RAMIREZ%2c%20EDUARDO%20DANIEL.pdf?sequence=3&isAllowed=y

Baque, M., Cedeño, B., Chele, J., & Gaona, V. (2020). Fracasos de las Pymes. *FIPCAEC*. https://fipcaec.com/index.php/fipcaec/article/view/293/517

Cano, J. J., & Almanza, A. (2020). Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 - 2018. https://www.researchgate.net/publication/339629757_Estudio_de_la_evolucion_de_la_Seguridad_de_la_Informacion_en_Colombia_2000_-_2018

Christian Llano Casa, A., Lisseth Gaibor Gavilanez, M., Cristina Cruz Caiza, C., & Augusto Cadena Moreano, J. (2021). Importance of IT security policies in accordance with ISO 27001 for small and medium-sized companies in Ecuador. *Revista Ciencia de La Ingeniería y Aplicadas*. http://investigacion.utc.edu.ec/revistasutc/index.php/ciya/article/view/374

Díaz Pérez, J. S., Vicente, J., & Martínez, B. (2020). *Esquema Director de Seguridad para Empresas pymes del sector Construcción*. https://rua.ua.es/dspace/bitstream/10045/102087/1/Esquema_Director_de_Seguridad_para_Empresas_pymes_d_Diaz_Perez_Juan_Salvador.pdf

Espinoza, E., Espinoza, R., & Medina, D. (2017). *IDENTIDAD CORPORATIVA COMO FACTOR DIFERENCIADOR EN LA COMPETITIVIDAD DE LAS PYMES DEL CANTON MILAGRO EN LA ZONA 5 DEL ECUADOR*. http://www.eumed.net/cursecon/ecolat/ec/2017/pymes-milagro-ecuador.html

Guevara, G., Verdesoto, A., & Castro, N. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *Revista Científica Mundo de La Investigación y El Conocimiento*. https://www.recimundo.com/index.php/es/article/view/860/1363

Lapiedra, R., Forés, B., Puig-Denia, A., & Martínez-Cháfer, L. (2021). Introducción a la gestión de sistemas de información en las empresas. In *Introducción a la gestión de sistemas de información en las empresas*. Universitat Jaume I. https://doi.org/10.6035/sapientia178

Leyva, A. (2021). Propuesta de estrategias de seguridad cibernética. Aproximaciones teórico –prácticas hacia el aprestamiento en países latinoamericanos. Revista Científica Dominio de Las Ciencias. https://dialnet.unirioja.es/descarga/articulo/8385888.pdf

Marín, J., Patiño, A., & Acevedo, J. (2020). Implementación de un sistema de seguridad perimetral informático usando vpn, firewall e ids. *Revista Universidad Católica de Oriente*. https://revistas.uco.edu.co/index.php/uco/article/view/284/370

Morales, F., Toapanta, S., & Toasa, R. M. (2019). *Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información*. https://www.researchgate.net/profile/Renato-Mauricio-Toasa-G/publication/339956501_Implementacion_de_un_sistema_de_seguridad_perimetral_como_estrategia_de_seguridad_de_la_informacion/links/5e95ffa5a6fdcca78915c13f/Implementacion-de-un-sistema-de-seguridad-perimetral-como-estrategia-de-seguridad-de-la-informacion.pdf

Morán, N. (2021). *ESTADO DE LA CIBERSEGURIDAD EN LAS EMPRESAS DEL SECTOR PÚBLICO DEL ECUADOR: UNA REVISIÓN SISTEMÁTICA*. https://dspace.ups.edu.ec/bitstream/123456789/20243/1/UPS-GT003204.pdf

Muñoz, M., Rafael, R., Agüero, V., Martin, J., & De, L. (2021). *Teletrabajo y la gestión de seguridad de la información en la empresa Infoservicios, Lima-2020*. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/60728/Medina_MRR-SD.pdf?sequence=1&isAllowed=y

Organismo Internacional de Estandarización. (n.d.). *ISO-27002-2022*. Retrieved September 16, 2022, from https://r2sc.com/es/wp-content/uploads/2022/05/ISO-27002-2022.pdf

Rodríguez-Mendoza, R., & Aviles-Sotomayor, V. (2020a). Las PYMES en Ecuador. Un análisis necesario. *593 Digital Publisher CEIT*, *5–1*(5), 191–200. https://doi.org/10.33386/593dp.2020.5-1.337

Pablos Heredero, C., López Hermoso, J., Romo, S., & Medina, S. (2019). Organización y transformación de los sistemas de información en la empresa. UNIVERSIDAD REY JUAN CARLOS.

Sampedro, C., Machuca, V., Palma, R., & Carrera, C. (2019). PERCEPCIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LAS PEQUEÑAS Y MEDIANAS EMPRESAS ENSANTO DOMINGO. *REVISTA INVESTIGACIÓN*

OPÉRACIONAL. http://www.invoperacional.uh.cu/index.php/invop/article/download/685/645

Sánchez-Sánchez, P. A., García-González, J. R., Triana, A., & Perez-Coronell, L. (2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. *Información Tecnológica*, *32*(5), 121–128. https://doi.org/10.4067/s0718-07642021000500121

Sanchez, V., Camilo, J., Fernando, F., & Hurtado, O. (2021). *LA BRECHA Y EL DESARROLLO DIGITAL DE LAS PYMES EN LATINOAMÉRICA*. https://repository.unimilitar.edu.co/bitstream/handle/10654/38040/VARGASSANCHEZJOHANCAMILO2021.pdf?sequence=3&isAllowed=y

Tundidor, Lazaro, Medina, & Nogueira. (2019). Evaluación del sistema de seguridad de la información para empresas de proyectos. Holguín. https://www.redalyc.org/articulo.oa?

Valenzuela, G., Cintia, M., Huyhua, T., & Augusto, R. (2022). *Nuevos mecanismos de la reactivación de las PYMEs*. http://hdl.handle.net/10757/661103

Vaca López, A. (2021). El Marketing Digital para las Pymes en tiempos de pandemia. Lúmina, 22(2), E0014. https://doi.org/10.30554/lumina.v22.n2.4524.2021

Vargas, E., & Marchan, A. (2019). *Propuesta de diseño de un Sistema de Gestión de la Seguridad de la Información según la NTP ISO/IEC 27001:2014 para la Universidad del Pacífico"*. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/2786/Ernesto%20Vargas_Alexis%20Marchan_Trabajo%20de%20Investigacion_Bachiller_2019.pdf?sequence=1&isAllowed=y

Samantha Valdez Valdez, J. (2020). *PROTECCIÓN DE INFORMACIÓN E IMPLEMENTACIÓN DE SOLUCIÓN NAS EN TI DE PYMES*.

http://repositorio.ug.edu.ec/bitstream/redug/49488/1/B-CINT-PTG-N.569%20Valdez%20Valdez%20Jenny%20Samantha%20.pdf

Xavier Jurado Pruna, F., & Valeria Yarad Jeada, P. (2020). ANÁLISIS DE LAS CARACTERÍSTICAS DEL SECTOR MICROEMPRESARIAL EN LATINOAMÉRICA Y SUS LIMITANTES EN LA ADOPCIÓN DE TECNOLOGÍAS PARA LA SEGURIDAD DE LA INFORMACIÓN. Revista Científica Ecociencia, 7(1), 26. https://orcid.org/0000-0001-8689-0398

ANEXOS

Anexo 1: *Formato Encuesta para las pequeñas y medianas empresas del cantón Milagro.*

UNIVERSIDAD ESTATAL DE MILAGRO

ENCUESTA

TEMA:

ANÁLISIS DE UN PLAN CON ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS.

OBJETIVO 1: Identificar los distintos tipos de amenazas de seguridad que puede tener una empresa examinando diversas situaciones presentadas, para disminuir la posibilidad de que exista alguna.

1. Indique el número de colaboradores que conforman su empresa.
   - 10-49 colaboradores ( )
   - 50-199 colaboradores ( )
   - Mas de 200 colaboradores ( )

2. ¿El sistema operativo de las computadoras y servidores de su empresa cuentan con licenciamiento?
   - SI ( )
   - NO ( )

3. ¿Los equipos de cómputo de su empresa disponen de un antivirus con licencia?
   - SI ( )
   - NO ( )
4. En caso de que la respuesta anterior sea negativa, Seleccione ¿por qué la empresa no cuenta con el licenciamiento respectivo?
   - Utiliza software libre gratuito.
   - Utiliza software con parches informáticos.
   - No aplica, la empresa si cuenta con licenciamiento.

OBJETIVO 2: Distinguir qué impacto tienen los escasos respaldos de energía en el daño de los servidores, mediante encuestas para optimizar el número de equipos de respaldos.

5. ¿La empresa cuenta con un respaldo de energía?
   - SI ( )
   - NO ( )

6. ¿Con que frecuencia se realiza respaldo de la información?
   - Diariamente ( )
   - Al menos dos veces por semana ( )
   - Al menos una vez por semana ( )
   - De vez en cuando ( )
   - Nunca ( )

7. ¿La empresa cuenta con un plan preventivo ante la posible pérdida de información?
   - SI ( )
   - NO ( )

8. ¿Cuántas veces se capacitó al personal de la empresa sobre las políticas de seguridad de la información?
   - Nunca. ( )
   - Una vez al año. ( )
   - Dos veces al año. ( )
   - Mas de tres veces en el año. ( )

9. ¿Ha existido pérdida de la información en la empresa?
   - SI ( )
   - NO ( )

10. De acuerdo con la pregunta anterior, indique ¿con qué frecuencia la información se ha visto comprometida?
    - Diariamente ( )
    - Al menos dos veces por semana ( )
    - Al menos una vez por semana ( )
    - De vez en cuando ( )
    - Nunca ( )

OBJETIVO 3: Identificar cómo incurre contar con políticas y procesos de seguridad de la información en la pérdida de la información relevante para la empresa.

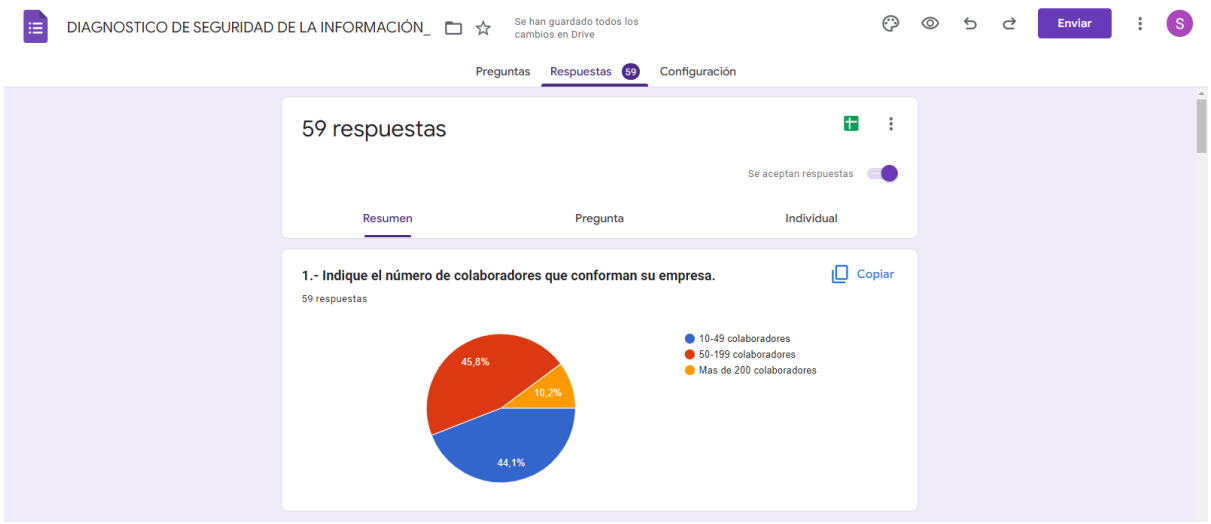
11. ¿La empresa ha sufrido de ataques cibernéticos en los dos últimos años?
    SI ( )
    NO ( )

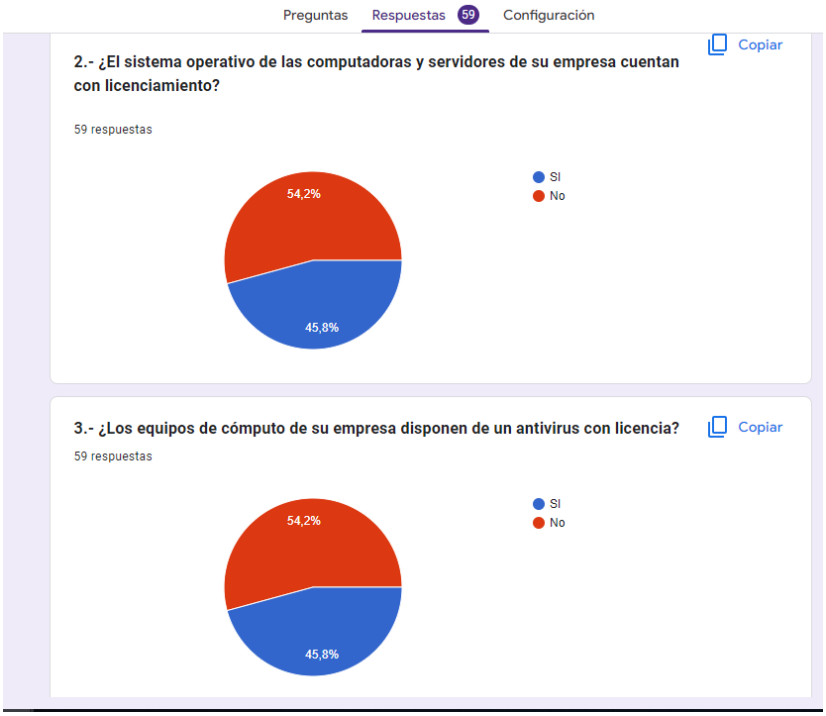
12. En caso de haber sufrido un ataque cibernético seleccionar el tipo.
    - Phishing ( )
    - Whaling ( )
    - Malware ( )
    - Ransomware ( )
    - No aplica, no ha existido ataques cibernéticos. ( )

13. ¿Los fallos en los equipos informáticos han ocasionado pérdida de información?
    - SI ( )
    - NO ( )

14. ¿Cada que tiempo recibe mantenimiento los equipos de cómputo de la empresa?
    - Una vez al año ( )
    - Dos veces al año ( )
    - Cada dos años ( )
    - Cuando los equipos presentas fallos ( )

Anexo 2: *Formulario de la encuesta*

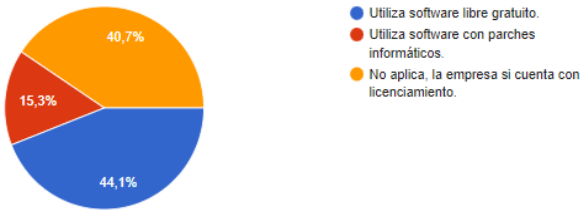




Copiar

4.- En caso de que la respuesta anterior sea negativa, Seleccione ¿porqué la empresa no cuenta con el licenciamiento respectivo?

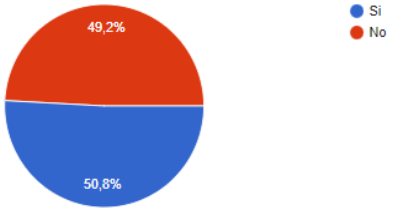
59 respuestas



Copiar

5.- ¿La empresa cuenta con un respaldo de energía?

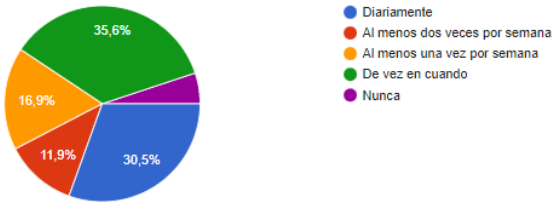
59 respuestas



Copiar

6.- ¿Con qué frecuencia se realiza respaldo de la información?

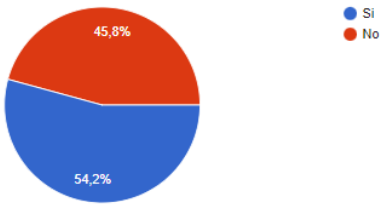
59 respuestas



Copiar

7.- ¿La empresa cuenta con un plan preventivo ante la posible pérdida de información?

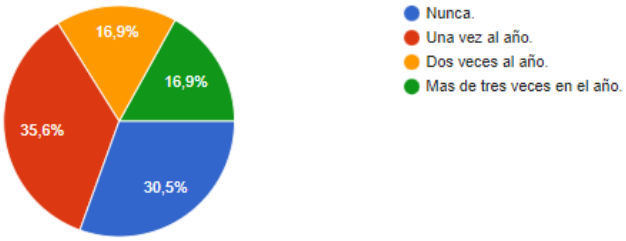
59 respuestas



Copiar

8.- ¿Cuántas veces se capacitó al personal de la empresa sobre las políticas de seguridad de la información?

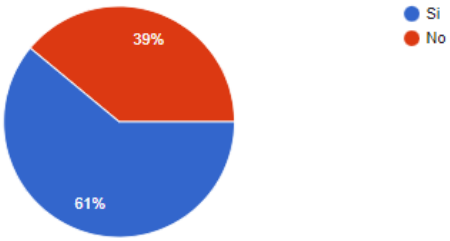
59 respuestas



Copiar

9.- ¿Ha existido pérdida de la información en la empresa?

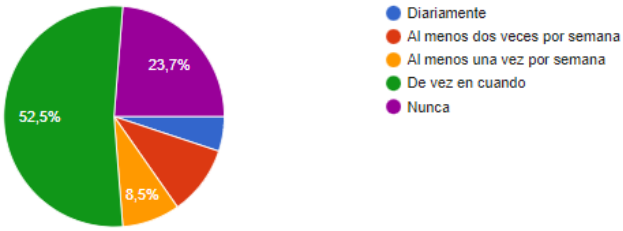
59 respuestas



Copiar

10.- De acuerdo con la pregunta anterior, indique ¿con qué frecuencia la información se ha visto comprometida?

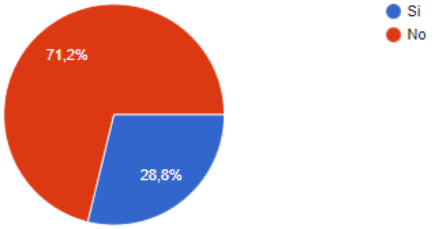
59 respuestas



Copiar

11.- ¿La empresa ha sufrido de ataques cibernéticos en los dos últimos años?

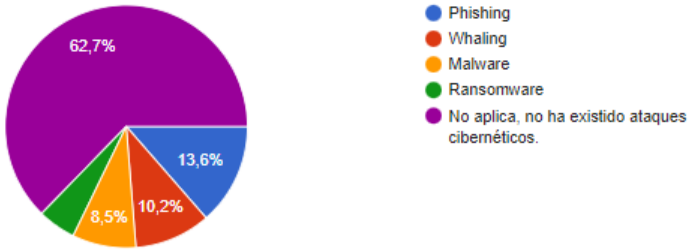
59 respuestas



12.- En caso de haber sufrido un ataque cibernético seleccionar el tipo.

Copiar

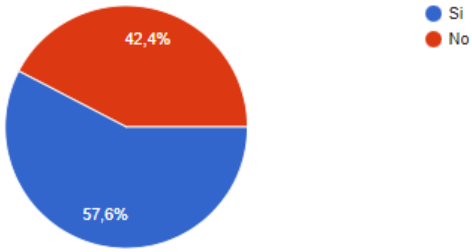
59 respuestas



13.- ¿Los fallos en los equipos informáticos han ocasionado pérdida de información?

Copiar

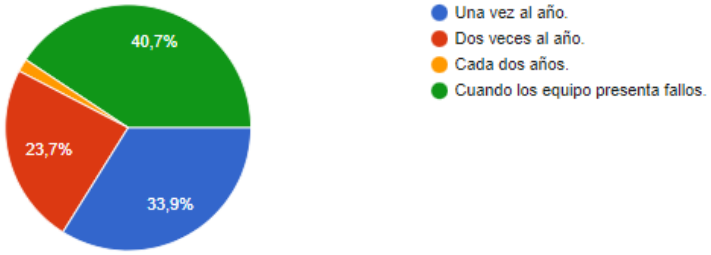
59 respuestas



14.- ¿Cada que tiempo recibe mantenimiento los equipos de cómputo?

Copiar

59 respuestas



Anexo 3: *Análisis de Jueces y Expertos Validación de Instrumento – Experto*

UNIVERSIDAD ESTATAL DE MILAGRO
DIRECCIÓN DE INVESTIGACIÓN Y POSGRADO
MAESTRÍA EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

Hoja de registro para la validación por expertos

Maestrante: Segundo Arturo Pérez Alvarez
Tutor: Lsi, Jessica Janina Cabezas Quinto, Msig

Datos del Experto

Nombres y Apellidos	Manuel Rodas Pérez
Última titulación académica	Magíster en Comunicación Estratégica
Institución de adscripción	Universidad Tecnologica Ecotec
Cargo	Docente / Director de proyecto de investigación cientifica
Teléfono celular	0981539995
Dirección de correo	manurodasperez@gmail.com

Instrumento.

Formato de encuesta para pequeñas y medianas empresas.

Sobre el instrumento.

Se presenta, para su validación, el formato de encuesta para pequeñas y medianas empresas, cuyo objetivo es: "Definir cómo incide un plan con estrategias de seguridad de la información en las empresas mediante un análisis de los procesos de seguridad que poseen, para evitar la pérdida de información.".

El presente cuestionario se ha elaborado a partir del Cuadro de operacionalización de variables, que a continuación se expone:

OPERACIONALIZACIÓN DE VARIABLES

Tema	Variables	Dimensión	Indicadores	Items	Instrumento
Análisis de un plan con estrategias de seguridad de la información para las pequeñas y medianas empresas.	VI: Estrategias	Licenciamiento	Sistemas operativos con licenciamiento Antivirus con licenciamiento.	**ENCARGADO DE TIC** ¿El sistema operativo de las computadoras y servidores de su empresa cuentan con licenciamiento? ¿Los equipos de cómputo de su empresa disponen de un antivirus con licencia? Seleccione porque la empresa no cuenta con el licenciamiento respectivo.	Encuesta
		Respaldos	Número de respaldos de información. Respaldo de energía.	**ENCARGADO DE TIC** ¿La empresa cuenta con un respaldo de energía? ¿Con que frecuencia se realiza respaldo de la información?	Encuesta
		Normativas y procesos de seguridad de la información. Políticas de seguridad de la información	Plan preventivo ante la pérdida de información. Personal capacitado	**ENCARGADO DE TIC** ¿La empresa cuenta con un plan preventivo ante la posible pérdida de información? ¿Cuántas veces se capacitó al personal de la empresa sobre las políticas de seguridad de la información?	Encuesta
	VD: Seguridad de la información	Pérdida de información	Número de veces que se ha perdido la información.	**ENCARGADO DE TIC** ¿Ha existido pérdida de la información en la empresa? ¿Con que frecuencia ha existido pérdida de información en la empresa?	Encuesta
		Vulnerabilidad de la información	Ataques cibernéticos. Tipos de ataques cibernéticos.	**ENCARGADO DE TIC** ¿La empresa ha sufrido ataques cibernéticos en los dos últimos años? En caso de haber sufrido un ataque cibernético seleccionar el tipo.	Encuesta
		Estado de equipos informático	Fallos en los equipos informáticos Mantenimiento de equipos informáticos	**ENCARGADO DE TIC** ¿Los fallos en los equipos informáticos han ocasionado pérdida de información? ¿Cada qué tiempo reciben mantenimiento los equipos de cómputo de la empresa?	Encuesta

La definición conceptual y operacional de la variable independiente *estrategias*:

Las estrategias son procedimientos que la empresa debe seguir para lograr resguardar la información de cualquier acontecimiento que ponga en peligro su integridad.

La definición conceptual y operacional de la variable dependiente *seguridad de la información*:

Conjunto de medidas tecnológicas que se aplican en una empresa para proteger la información que manejan en sus diversos procesos.

Sobre la validación

A continuación, se presentan dos tablas, con la referencia numérica de los ítems o aspectos sobre los que se indaga a través de cada cuestionario.

Por favor, valore cada ítem de acuerdo con los siguientes criterios:

- **(S) Suficiencia:** Los ítems que evalúan el mismo componente bastan para obtener la medición de este.
- **(Cl) Claridad:** El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.
- **(Co) Coherencia:** El ítem tiene relación lógica con el componente sobre el que se supone que indaga.
- **(R) Relevancia:** El ítem es esencial o importante, es decir debe ser incluido.

Para ello, coloque en la casilla correspondiente un número del uno (1) al cuatro (4) de acuerdo con la siguiente escala:

1. No cumple con el criterio	**2.** Bajo nivel	**3.** Moderado nivel	**4.** Alto nivel

Además de su valoración, por favor, agregue las observaciones que explican su valoración o ayudan a la mejora de la pregunta.

Instrumento: Encuesta dirigida al personal de TIC de las pequeñas y medianas empresas del cantón Milagro.

Pregunta por componente	(S)	(CI)	(Co)	(R)	Observación
1.- Indique el número de colaboradores que conforman su empresa. • 10-49 colaboradores. • 50-199 colaboradores. • Mas de 200 colaboradores.	4	3	4	3	
2.- ¿El sistema operativo de las computadoras y servidores de su empresa cuentan con licenciamiento?	4	4	4	3	
3.- ¿Los equipos de cómputo de su empresa disponen de un antivirus con licencia?	4	4	4	3	
4.- Seleccione porque la empresa no cuenta con el licenciamiento respectivo. • Utiliza software libre gratuito. • Utiliza software con parches informáticos. • No aplica, la empresa si cuenta con licenciamiento.	3	3	3	4	
5.- ¿La empresa cuenta con un respaldo de energía?	4	4	3	4	
6.- ¿Con que frecuencia se realiza respaldo de la información?	4	4	4	4	
7.- ¿La empresa cuenta con un plan preventivo ante la posible pérdida de información?	4	4	4	4	
8.- ¿Cuántas veces se capacitó al personal de la empresa sobre las políticas de seguridad de la información?	4	4	4	4	

Pregunta por componente	(S)	(CI)	(Co)	(R)	Observación
9.- ¿Ha existido pérdida de la información en la empresa?	4	4	4	4	
10.- ¿Con que frecuencia ha existido pérdida de información en la empresa?	3	3	4	3	
11.- ¿La empresa ha sufrido ataques cibernéticos en los dos últimos años?	4	4	4	4	
12.- En caso de haber sufrido un ataque cibernético seleccionar el tipo. • Phishing • Whaling • Malware • Ransomware • No aplica, no ha existido ataques cibernéticos.	4	4	4	4	
¿Los fallos en los equipos informáticos han ocasionado pérdida de información?	4	4	4	4	
¿Cada qué tiempo reciben mantenimiento los equipos de cómputo de la empresa? • Una vez al año • Dos veces al año • Cada dos años • Cuando los equipos presentan fallos	4	3	4	4	

Consideraciones sobre el instrumento revisado.
Las preguntas están acordes.
Sugerencias y recomendaciones.
Tal vez hubiera sido ideal buscar conectar a las PYMES en la encuestas

MANUEL
ANTONIO RODAS
PEREZ

MSC. Manuel Rodas Pérez

Firma

Anexo 4: *Base de Datos en el SPSS*

tab_Segundo_Perez.sav [ConjuntoDatos1] - IBM SPSS Statistics Editor de datos

Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

	Nombre	Tipo	Anchura	Decimales	Etiqueta	Valores	Perdidos	Columnas	Alineación	Medida	Rol
1	VAR00001	Cadena	64	0	1.- Indique el n...	Ninguna	Ninguna	64	Izquierda	Nominal	Entrada
2	VAR00002	Cadena	100	0	2.- ¿El sistema...	Ninguna	Ninguna	100	Izquierda	Nominal	Entrada
3	VAR00003	Cadena	80	0	3.- ¿Los equipo...	Ninguna	Ninguna	80	Izquierda	Nominal	Entrada
4	VAR00004	Cadena	128	0	4.- En caso de ...	Ninguna	Ninguna	128	Izquierda	Nominal	Entrada
5	VAR00005	Cadena	50	0	5.- ¿La empres...	Ninguna	Ninguna	50	Izquierda	Nominal	Entrada
6	VAR00006	Cadena	62	0	6.- ¿Con qué fr...	Ninguna	Ninguna	62	Izquierda	Nominal	Entrada
7	VAR00007	Cadena	85	0	7.- ¿La empres...	Ninguna	Ninguna	85	Izquierda	Nominal	Entrada
8	VAR00008	Cadena	108	0	8.- ¿Cuántas ve...	Ninguna	Ninguna	108	Izquierda	Nominal	Entrada
9	VAR00009	Cadena	57	0	9.- ¿Ha existid...	Ninguna	Ninguna	57	Izquierda	Nominal	Entrada
10	VAR00010	Cadena	110	0	10.- De acuerd...	Ninguna	Ninguna	110	Izquierda	Nominal	Entrada
11	VAR00011	Cadena	76	0	11.- ¿La empre...	Ninguna	Ninguna	76	Izquierda	Nominal	Entrada
12	VAR00012	Cadena	73	0	12.- En caso d...	Ninguna	Ninguna	73	Izquierda	Nominal	Entrada
13	VAR00013	Cadena	83	0	13.- ¿Los fallos...	Ninguna	Ninguna	83	Izquierda	Nominal	Entrada
14	VAR00014	Cadena	66	0	14.- ¿Cada que...	Ninguna	Ninguna	66	Izquierda	Nominal	Entrada
15											

*tab_Segundo_Perez.sav [ConjuntoDatos1] - IBM SPSS Statistics Editor de datos

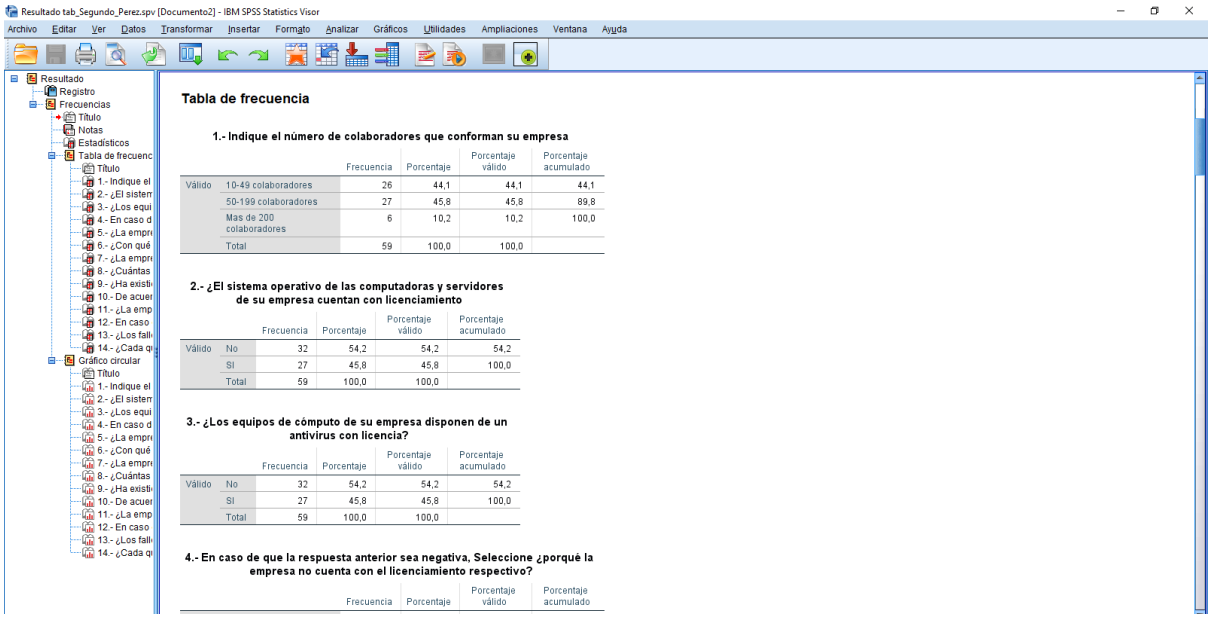
Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

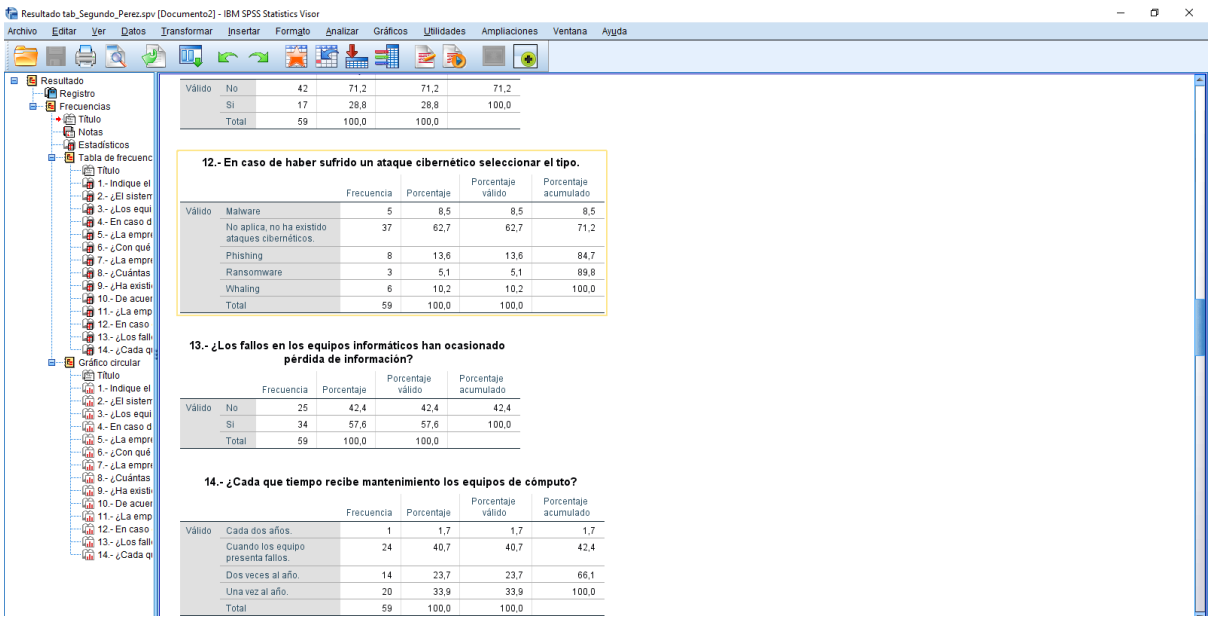
29 : VAR00003 | No | Visible: 14 de 14 variables

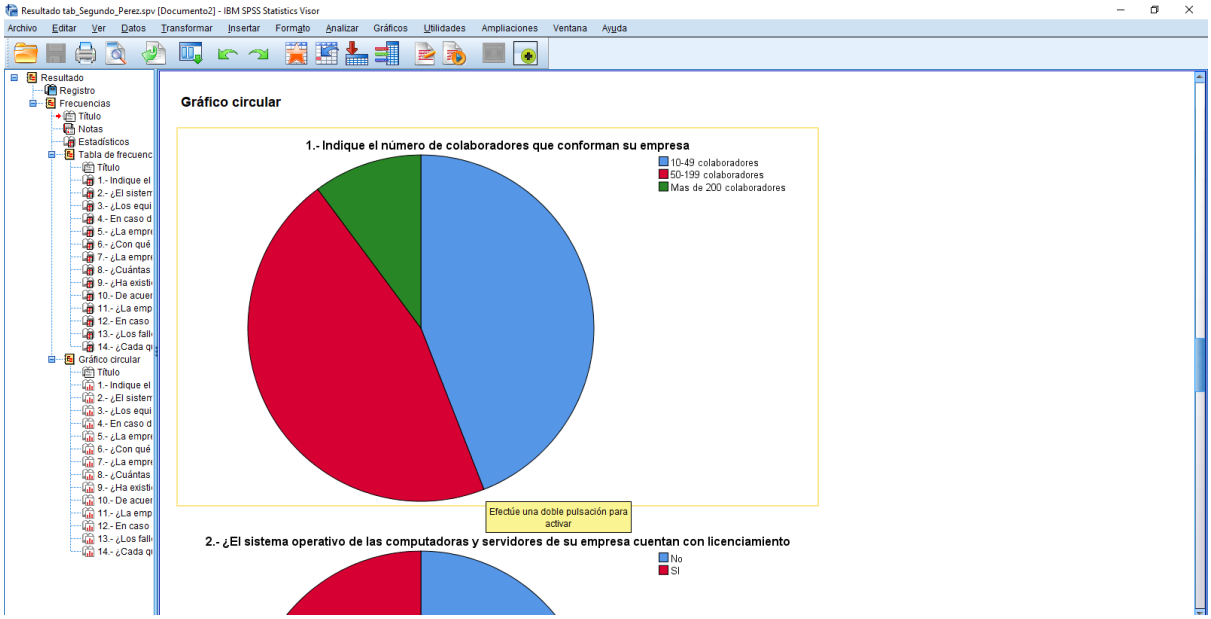
	VAR00001	VAR00002	VAR00003	VAR00004
1	50-199 colaboradores	No	SI	Utiliza software con parches informáticos.
2	10-49 colaboradores	SI	SI	No aplica, la empresa si cuenta con licenciamiento.
3	50-199 colaboradores	SI	SI	No aplica, la empresa si cuenta con licenciamiento.
4	10-49 colaboradores	SI	SI	Utiliza software libre gratuito.
5	50-199 colaboradores	SI	No	Utiliza software con parches informáticos.
6	50-199 colaboradores	No	No	Utiliza software con parches informáticos.
7	10-49 colaboradores	No	No	Utiliza software libre gratuito.
8	10-49 colaboradores	SI	SI	No aplica, la empresa si cuenta con licenciamiento.
9	50-199 colaboradores	No	No	Utiliza software con parches informáticos.
10	10-49 colaboradores	No	No	Utiliza software libre gratuito.
11	50-199 colaboradores	No	SI	No aplica, la empresa si cuenta con licenciamiento.
12	10-49 colaboradores	SI	SI	Utiliza software con parches informáticos.
13	50-199 colaboradores	No	No	Utiliza software libre gratuito.
14	10-49 colaboradores	No	No	Utiliza software libre gratuito.
15	10-49 colaboradores	No	No	No aplica, la empresa si cuenta con licenciamiento.
16	10-49 colaboradores	SI	SI	No aplica, la empresa si cuenta con licenciamiento.
17	50-199 colaboradores	No	No	Utiliza software libre gratuito.
18	50-199 colaboradores	No	No	Utiliza software libre gratuito.
19	50-199 colaboradores	No	SI	No aplica, la empresa si cuenta con licenciamiento.
20	10-49 colaboradores	SI	SI	No aplica, la empresa si cuenta con licenciamiento.
21	Mas de 200 colaboradores	SI	SI	Utiliza software con parches informáticos.
22	50-199 colaboradores	No	No	Utiliza software libre gratuito.
23	50-199 colaboradores	SI	SI	No aplica, la empresa si cuenta con licenciamiento.
24	50-199 colaboradores	No	No	Utiliza software libre gratuito.
25	10-49 colaboradores	SI	No	No aplica, la empresa si cuenta con licenciamiento.
26	50-199 colaboradores	No	No	Utiliza software libre gratuito.
27	50-199 colaboradores	SI	SI	No aplica, la empresa si cuenta con licenciamiento.
28	50-199 colaboradores	No	No	Utiliza software libre gratuito.
29	50-199 colaboradores	No	No	Utiliza software libre gratuito.

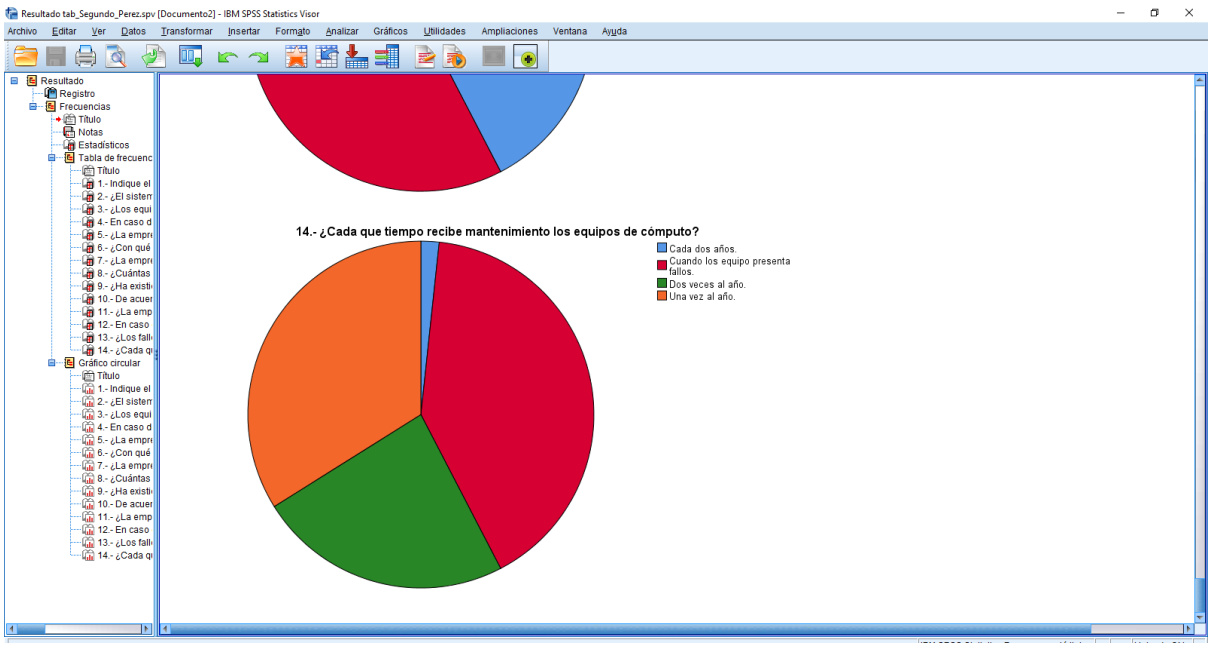
Vista de datos | Vista de variables

Anexo 5: *Tablas de Frecuencias y Gráficos para la tabulación de la encuesta*

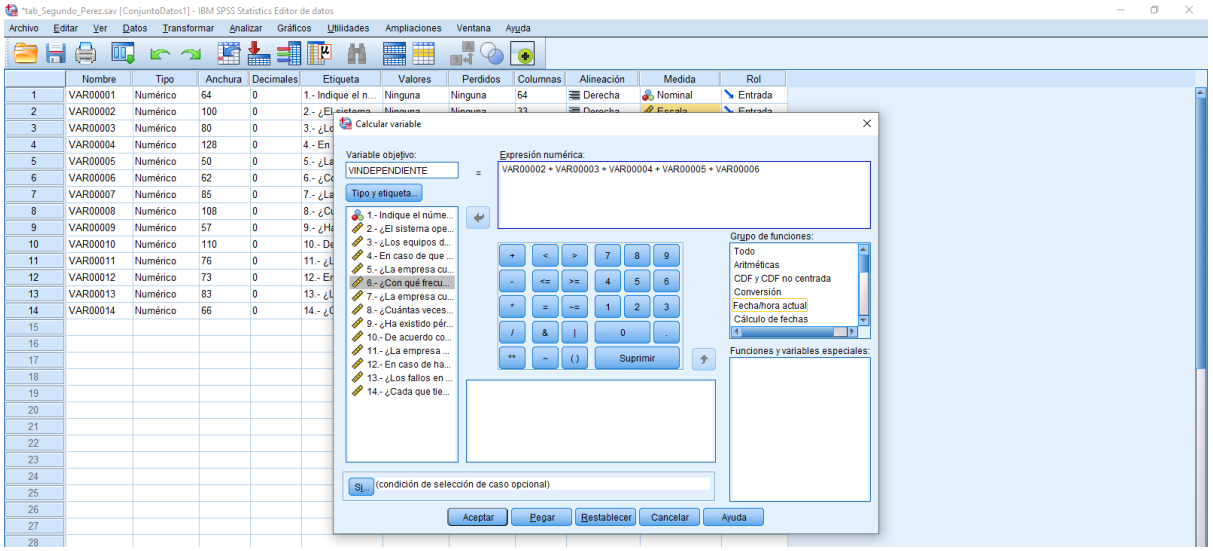


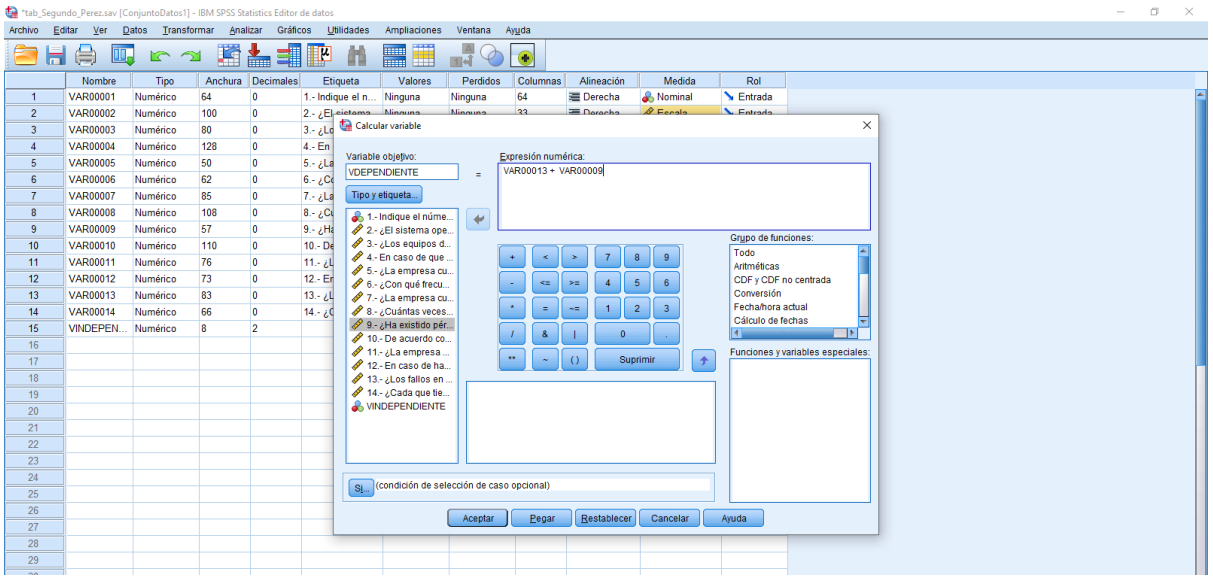



Resultado tab_Segundo_Perez.spv [Documento2] - IBM SPSS Statistics Visor
Archivo Editar Ver Datos Transformar Insertar Formato Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda
Gráfico circular
1.- Indique el número de colaboradores que conforman su empresa
10-49 colaboradores
50-199 colaboradores
Mas de 200 colaboradores
Efectúe una doble pulsación para activar
2.- ¿El sistema operativo de las computadoras y servidores de su empresa cuentan con licenciamiento
No
SI

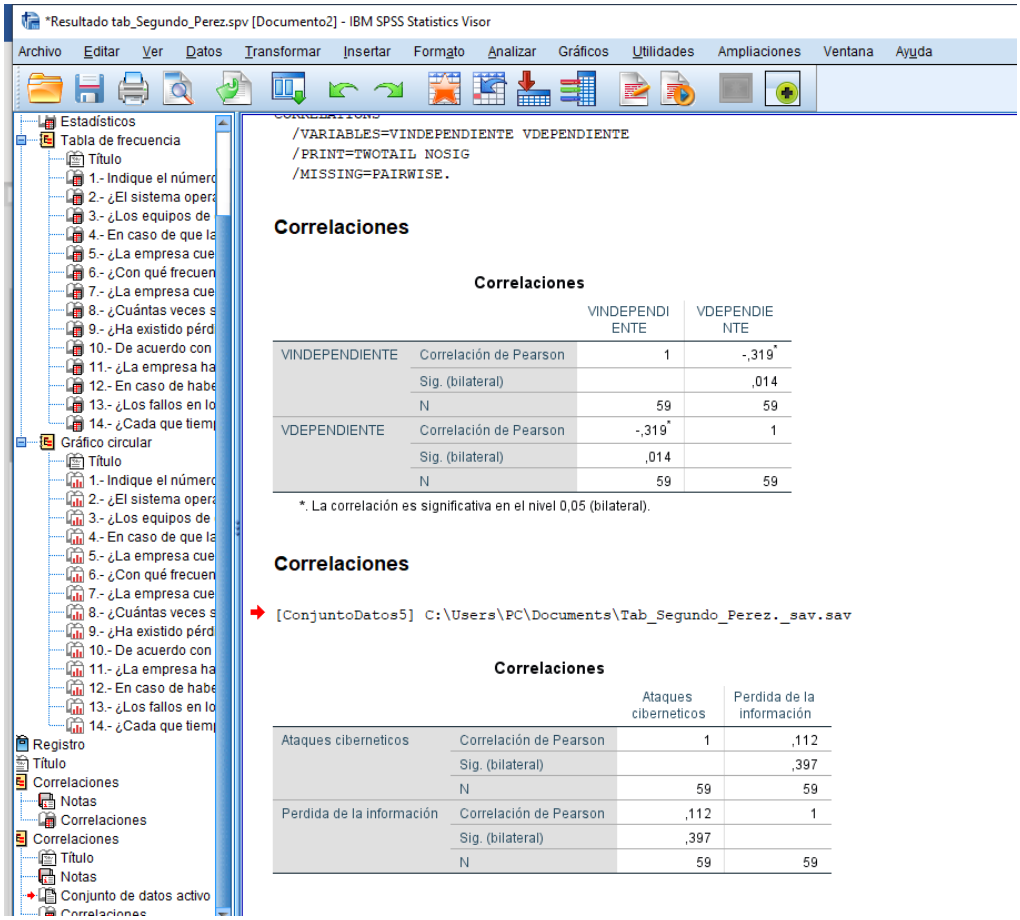

Resultado tab_Segundo_Perez.spv [Documento2] - IBM SPSS Statistics Visor
Archivo Editar Ver Datos Transformar Insertar Formato Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda
14.- ¿Cada que tiempo recibe mantenimiento los equipos de cómputo?
Cada dos años.
Cuando los equipo presenta fallos.
Dos veces al año.
Una vez al año.

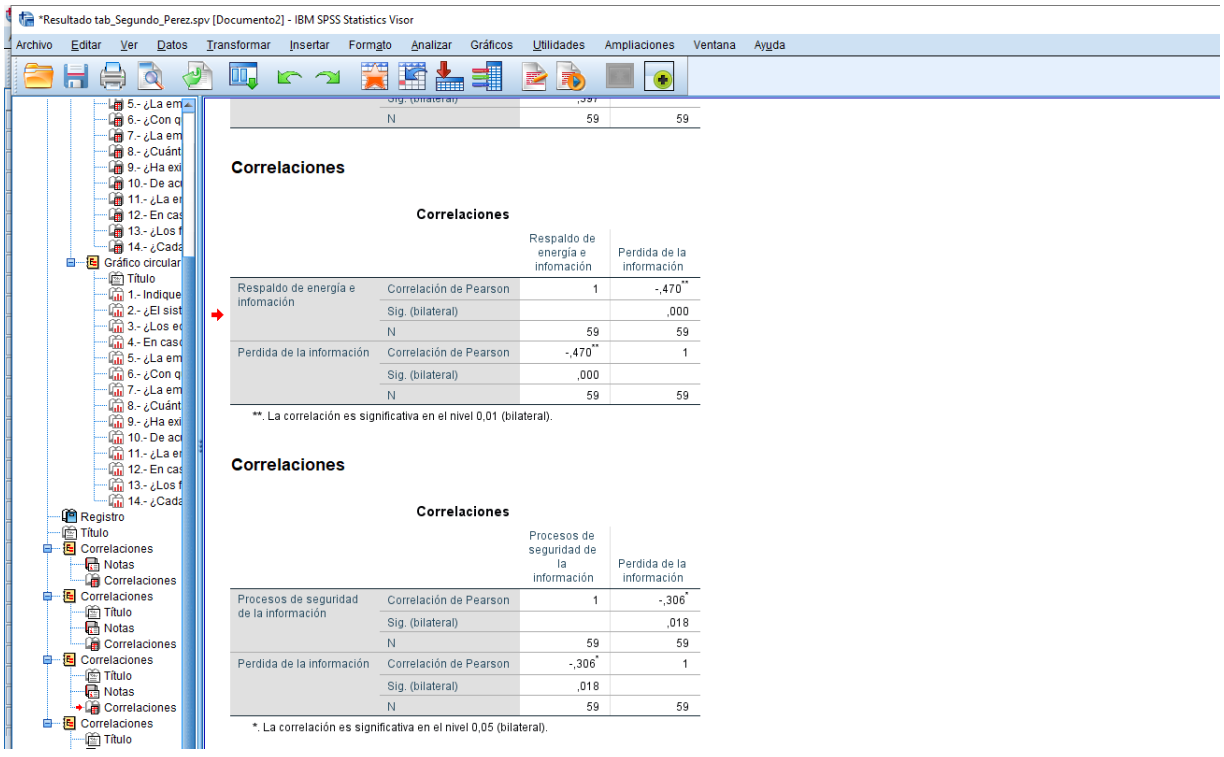
Anexo 6: *Cálculo de las Variables Independientes y Dependientes*





Anexo 7: *Resultados de la contrastación de las variables*





Anexo 8: *Informe del tutor*

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

INFORME DEL TUTOR

Milagro, 01 de noviembre del 2022

Sr. Ing.
Eduardo Espinoza S., Phd
Director de Posgrados

De mis consideraciones

Por medio de la presente certifico haber acompañado en el desarrollo del trabajo de Titulación en calidad de **profesor tutor**, al maestrante **PEREZ ALVAREZ SEGUNDO ARTURO,** con el tema: **"ANÁLISIS DE UN PLAN CON ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS"**. En el cual se realizaron 8 tutorías, las mismas que se encuentran registradas en el Sistema de Gestión Académica.

Además, notificó que el Trabajo de Titulación cumple con los parámetros de calidad y forma requeridos por el programa de maestría en **MAESTRÍA EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN EN MODALIDAD PRESENCIAL**, cumpliendo con el porcentaje de originalidad del 1 %.

Pongo de manifiesto que autorizo la entrega del documento desarrollado a los entes pertinentes para proceder a la revisión y posterior defensa del Trabajo de Titulación presentado por el maestrante.

Atentamente,

Firmado electrónicamente por:
JESSICA JANINA CABEZAS QUINTO

Lsi, Jessica Cabezas Quinto, Msc.
C.I. 1203461544

Anexo 9: *Informe de plagio*

Informe de originalidad

NOMBRE DEL CURSO
REV.TRABAJOS - POSGRADO

NOMBRE DEL ALUMNO
JESSICA JANINA CABEZAS QUINTO

NOMBRE DEL ARCHIVO
TESIS SEGUNDO PEREZ_INTRODUCCION

SE HA CREADO EL INFORME
31 oct 2022

Resumen

Fragmentos marcados	1	1 %
Fragmentos citados o entrecomillados	1	0,3 %

Coincidencias de la Web

scielo.cl	2	1 %

1 de 2 fragmentos

Fragmento del alumno MARCADO

Esto se evidencia en el estudio de Cyber Security Breaches Survey 2019, donde se señala que solo el 15% de las pymes poseen un proceso formal de gestión de incidentes cibernéticos, y el 50% de los...

Mejor coincidencia en la Web

Esto se evidencia en el estudio de Cyber Security Breaches Survey 2019, donde se señala que solo el 15% de las pymes poseen un proceso formal de gestión de incidentes cibernéticos, y el 50% de los...

Medida del nivel de seguridad informática de las pequeñas y ... https://www.scielo.cl/scielo.php?pid=S0718-07642021000500121&script=sci_arttext

2 de 2 fragmentos

Fragmento del alumno CITADO

...por dónde empezar para mejorar su postura de seguridad. **Bajo este panorama, las organizaciones no realizan evaluaciones permanentes**, sistemáticas **y exhaustivas del riesgo**

Mejor coincidencia en la Web

Bajo este panorama, las organizaciones no realizan evaluaciones permanentes, sistémicas **y exhaustivas del riesgo** cibernético

31/10/22, 10:45 TESIS SEGUNDO PEREZ_INTRODUCCION

Medida del nivel de seguridad informática de las pequeñas y ... https://www.scielo.cl/scielo.php?pid=S0718-07642021000500121&script=sci_arttext

Anexo 10: *Registro de acompañamiento*

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

Milagro, 31 de octubre del 2022

REGISTRO DE ACOMPAÑAMIENTOS

Inicio: 29-08-2022 **Fin** 01-11-2022

DIRECCIÓN DE POSGRADO

CARRERA: MAESTRIA EN GERENCIA DE TECNOLOGIAS DE LA INFORMACION

TEMA: ANÁLISIS DE UN PLAN CON ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS

ACOMPAÑANTE: CABEZAS QUINTO JESSICA JANINA

DATOS DEL ESTUDIANTE		
APELLIDOS Y NOMBRES	**CÉDULA**	**CARRERA**
PEREZ ALVAREZ SEGUNDO ARTURO	1804344305	MAESTRIA EN GERENCIA DE TECNOLOGIAS DE LA INFORMACION EN MODALIDAD PRESENCIAL

Nº	FECHA	HORA		Nº HORAS	DETALLE
1	31-08-2022	Inicio: 07:00 a.m.	Fin: 08:00 a.m.	1	REVISIÓN DEL CRONOGRAMA DE TRABAJO, Y ESTANDARIZACIÓN DE LOS FORMATOS Y DOCUMENTOS A UTILIZAR
2	07-09-2022	Inicio: 07:00 a.m.	Fin: 08:00 a.m.	1	REVISIÓN DEL CAPITULO1: PROBLEMATICA, OBJETIVOS GENERAL, OBJETIVO ESPECIFICO, JUSTIFICACIÓN, Y DEFINICIÓN DE VARIABLES
3	18-09-2022	Inicio: 15:00 p.m.	Fin: 16:00 p.m.	1	2DA REVISIÓN DEL CAPITULO 1, ANTECEDENTE DEL CAPITULO 2, Y CONTENIDO DEL MARCO TEÓRICO
4	25-09-2022	Inicio: 17:00 p.m.	Fin: 18:00 p.m.	1	REVISIÓN DEL CAPITULO 2
5	02-10-2022	Inicio: 17:15 p.m.	Fin: 18:15 p.m.	1	REVISIÓN DEL CAPITULO 3 Y ENCUESTA
6	13-10-2022	Inicio: 10:15 a.m.	Fin: 11:15 a.m.	1	REVISIÓN DEL CAPITULO 4
7	[illegible]	[illegible]	[illegible]	1	REVISIÓN DEL CAPITULO 4 Y

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

Firmado electrónicamente por:
JESSICA JANINA CABEZAS QUINTO

CABEZAS QUINTO JESSICA JANINA
PROFESOR(A)