UNIVERSIDAD
SAN IGNACIO
DE LOYOLA

FACULTAD DE INGENIERIA

Ingeniería Empresarial y de Sistemas

GESTIÓN DE LA CIBERSEGURIDAD Y PREVENCIÓN DE LOS ATAQUES CIBERNÉTICOS EN LAS PYMES DEL PERÚ, 2016

Tesis para optar el grado de Bachiller en Ingeniería Empresarial y de Sistemas

ANTONIO INOGUCHI ROJAS

ERIKA LIZET MACHA MORENO

Asesor:

Lida Vasquez Pajuelo

Lima – Perú

2017

Dedicatoria

A Dios, por permitirnos llegar a este momento tan especial en nuestras vidas. Por fortalecer nuestros corazones y habernos puesto en el camino a personas que nos apoyaron durante el tiempo de estudio.

A nuestros padres por su apoyo incondicional y sus consejos para hacer de nosotros mejores personas.

A nuestros profesores del programa de CPEL, por su tiempo, por su apoyo, así como por la sabiduría que nos transmitieron en el desarrollo de nuestra formación profesional.

Agradecimiento

A Dios por brindarnos protección y fortaleza para superar los obstáculos que se presentan en nuestra vida.

A nuestros padres, que como personas ejemplares nos han enseñado a no rendirnos y perseverar para cumplir nuestros sueños.

Al personal del área de sistemas de la Empresa Transporte Zavala Cargo S.A.C. que con entusiasmo colaboraron en realizar las encuestas, parte fundamental para el desarrollo de nuestra investigación.

Gracias a todas las personas que ayudaron directa e indirectamente en la realización de esta tesis.

Presentación

El presente trabajo de investigación ayudará a las PYMES del Perú a tomar conciencia en la protección de su data informática y sistemas informáticos, teniendo en cuenta que cuando nos referimos a la data informática, es toda la información virtual que se encuentra almacenada y disponible en la red privada de las pymes, siendo dicha información fundamental y vital para que las pymes funcionen correctamente y alcance sus objetivos propuestos.

El objetivo es de obtener un nivel considerable de seguridad para las pymes, el cual se logrará con los resultados obtenidos en la investigación y posteriormente recomendando e indicando una propuesta para gestión y prevención de seguridad informática, la cual podrá ser aplicable para la mayoría de pymes de diferentes rubros o giros de negocio, el único requisito es que la pyme se proponga implementar la propuesta de seguridad informática resultante.

Nuestro trabajo de investigación se desenvolverá con los capítulos explicados a continuación.

En el primer capítulo se explicará la problemática, la cual nos habla de los motivos de una fácil intromisión a la información en una red privada, la importancia de plasmar criterios de seguridad de la información para mantener una red privada segura. Así como también teóricamente el objetivo, los antecedentes e hipótesis de esta investigación.

En el segundo capítulo se desarrollará la metodología con la que se ha llevado a cabo la investigación como la operacionalización de las variables y técnicas de recolección de datos hasta los métodos que emplearemos para el análisis del mismo.

En el tercer capítulo se da a conocer y explicar los resultados de esta investigación, posterior a ello se procederá de igual forma a explicar las conclusiones y por último se brindara todas las recomendaciones posibles de la práctica realizada en fin de tener pymes en el Perú con una alto conocimiento de protección de su información en las redes de internet privadas y así evitando la intromisión y robo de su data virtual por parte de extraños a la pyme.

ÍNDICE

Introducción

La ciencia de la informática hoy en día es un elemento esencial para cualquier país que desea el progreso y mejora del mismo, toda información virtual que esté presente en la red interna privada de una pyme es considerada un activo. Este activo debería de ser considerada y resguardado como algo muy apreciado por una pyme ya que esto puede hacer que surja adelante o fracase, es por ello que debemos darle toda seguridad posible a la información virtual que existe en la red privada de una empresa.

Un gran número de las pymes no conocen el gran problema con el que luchan día a día considerando así a la seguridad informática como algo no necesario y secundario, por los general ni se preocupan en invertir en personal capacitado, ni el financiero para minimizar riesgos de ataques y robos de información, la cual puede ser destruida, vendida a la competencia de la pyme o solicitar una suma de dinero para devolver la información.

La principal amenaza que afecta a la seguridad de la información de una pyme es el desconocimiento del concepto de la misma, la confidencialidad, la integridad y los niveles de disponibilidad de la información que se deben manejar no son los adecuados. Dejando así las pymes con serios inconvenientes como el retraso de su continuidad operacional diaria la cual tiene como consecuencia una significativa pérdida de ingresos monetarios y contratiempos no pronosticados en la producción esperada.

Hoy en día existen muchos factores que amenazan la seguridad de información de las pymes y por lo general el presupuesto destinado para la proteger y resguardar la información de las redes de internet externas no es el suficientes, tener identificadas y controladas las vulnerabilidades de la información interna en la red se logra con un correcto plan de seguridad generado gracias a un análisis de riesgo previo.

Con las ansias de lograr este objetivo el cual se basa en que las pymes del Perú conozcan la importancia de salvaguardar la información virtual en sus redes privadas, es que se presenta esta investigación.

CAPITULO I

PROBLEMA DE INVESTIGACIÓN

1. Problema de Investigación

1.1. Planteamiento del Problema

Como sabemos, el desarrollo tecnológico ha transformado las operaciones de las empresas e instituciones y la forma en cómo interactúan las personas, pero a la vez han traído riesgos y dificultades en cuanto a la seguridad de la información.

Según el informe sobre riesgos globales para 2016 del Foro Económico Mundial, los ataques cibernéticos se han considerado como uno de los principales riesgos globales entre los más probables de ocurrir y con mayores consecuencias, en los últimos años han aumentado rápidamente atacando a los negocios en todo tipo de sectores empresariales, para ello se necesitarán implementar nuevas directivas que garanticen la seguridad minimizando los riesgos de ataques cibernéticos.

1.2. Formulación del Problema

Gran parte de las PYMES en el Perú son consideradas las más vulnerables a los ciberataques porque desconocen el impacto que pueden tener sobre su negocio. Esto lleva a que muchas no implementen las acciones necesarias para protegerse de manera efectiva.

El impacto de una pérdida de información puede ser muy grande y recuperarse puede demandar mucho tiempo. Los ciberataques pueden causar daño a la marca y pérdida de clientes.

1.2.1. Problema

1.2.1.1. Problema Principal

¿En qué medida se relaciona la gestión de la ciberseguridad con la prevención de los ataques cibernéticos en las PYMES del Perú, 2016?

1.2.1.2. Problemas Específicos

- ¿Cuáles son los problemas de gestión de la ciberseguridad en las PYMES del Perú, 2016?
- ¿Cómo prevenir los riesgos de los ataques cibernéticos en las PYMES del Perú, 2016?

1.2.2. Objetivos

1.2.2.1. Objetivo Principal

Determinar la gestión de la ciberseguridad con la prevención de los ataques cibernéticos en las PYMES del Perú, 2016.

1.2.2.2. Objetivos Específicos

- Identificar los problemas de gestión de la ciberseguridad en las PYMES del Perú, 2016.
- Prevenir los riesgos de los ataques cibernéticos en las PYMES del Perú, 2016.

1.3. Justificación de la Investigación

1.3.1. Justificación Metodológica

Con esta investigación ayudaremos a fomentar una cultura de prevención y detección de riesgos cibernéticos en las PYMES del Perú, se dará a conocer sobre el peligro que representa no estar preparado para los diferentes ataques cibernéticos que existen actualmente y se brindará información de cómo elaborar los planes de acción y estrategias basadas en minimizar los riesgos.

1.3.2. Justificación Práctica

Esta investigación es importante porque los estudios realizados por empresas especialistas en ciberseguridad señalan que los ataques cibernéticos han evolucionado, los hackers están desarrollando software maliciosos cada vez más sofisticados con el fin de buscar vulnerabilidades en los sistemas interconectados para sustraer información digital con el fin de lograr su objetivo.

Para ello con el nuevo conocimiento acerca de la importancia de elaborar planes de acción y estrategias para minimizar los riesgos, las empresas tendrán el enfoque necesario para establecer una nueva gobernanza y directivas que garanticen la seguridad cibernética.

1.3.3. Justificación Legal

Los ataques cibernéticos no es solo un problema de las empresas, también el Estado se involucra en este tema, por ello con el objetivo de fortalecer la seguridad informática, el 22 de octubre del año 2013 el presidente Ollanta Humala aprobó la ley N°30096 – Ley de Delitos Infor máticos.

Capítulo II, Art. 2 Acceso ilícito a la información:

“El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado”.

Capítulo II, Art. 3 Atentado contra la integridad de datos informáticos:

“El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos

informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

Capítulo II, Art. 4 Atentado contra la integridad de sistemas informáticos.

"El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

1.4. Viabilidad de la Investigación

La investigación la consideramos viable puesto que contamos con el apoyo del personal del área de Sistemas que labora en La Empresa Trasporte Zavala Cargo S.A.C. quienes se han ofrecido de manera desinteresada para poder colaborar en la ejecución de técnicas de recopilación de datos necesarios para poder analizar la gestión de la ciberseguridad y prevención de los Ataques Cibernéticos en su empresa, con ello habremos seleccionado una muestra de todas las PYMES del Perú con el fin de analizar los datos obtenidos y exponerlos.

2. Marco Referencial

Los sistemas empresariales con la ayuda de la tecnología salen al mundo exterior para mantener a las empresas y su negocio interconectado con los

clientes, con los proveedores, para mantener data actualizada en tiempo real, etc. La tecnología evoluciona tan rápido día a día que permite optimizar todos los procesos y reducir los costes de las empresas, pero en esta marcha de evolución las empresas se descuidan de tener segura toda la información digital que tanto esfuerzo les ha costado producirla, es por ello que se debe enfatizar y profundizar la idea de prevención contra los ataques cibernéticos a las empresas y así puedan considerar presupuestar en planes de ciberseguridad de su información si no desean sufrir la perdida y/o manipulación de sus sistemas produciéndose así cibercrímenes clasificados en dos grandes grupos:

- **Riesgos a la información cibernética privada**, estos riesgos generan un robo, manejo inadecuado o divulgación prohibida de la ciberinformación de una empresa. Se encuentran los siguientes riesgos a tomar en cuenta:

    - Investigación de información cibernética privada ya se a un país o a una empresa.
    - Hurto y divulgación de ciberinformación privada de una empresa tipo económica, nuevos proyectos, etc.
    - Hurto y divulgación de información personal de los trabajadores de la empresa.
    - Hurto de identificaciones autorizadas a la empresa.
    - Fraude fiscal.

- **Riesgos a la infraestructura tecnológica de ciberinformación**, estos riesgos generan y provocan la paralización total o parcial y por lapsos de tiempo indefinidos de operaciones, servicios o sistemas vitales para una empresa o País. Se encuentran los siguientes riesgos a tomar en cuenta:

  - Intromisiones a sistemas de una red privada manipulando infraestructuras críticas para la operación de una empresa o Estado.
  - Intromisiones a las redes privadas con la finalidad de detener procesos de producción automatizados en la empresa.
  - Intromisiones a las redes privadas contra servicios de Internet vitales para las operaciones de la empresa.
  - Intromisiones a sistemas de control y redes industriales.
  - Infección con malware a toda la red de la empresa.
  - Intromisiones a redes privadas, sistemas o servicios a través de servicios de empresas terceras.

2.1. Antecedentes

Dichas intromisiones cibernéticos siempre están presente y cada vez se habla más del tema en distintos congresos o foros mundiales todos llegando a la conclusión que los ataques cibernéticos evolucionan de forma muy frecuente.

Dichas intromisiones logran avanzado desde simples modificaciones de página Web, hasta estafas, o temas más complicados como actividades de espionajes.

En febrero de 2015, la firma Kaspersky quien es una empresa que se dedica crear soluciones de seguridad así como un antivirus quien es su producto estrella que lleva el mismo nombre de la empresa. Esta firma dio a conocer su comentario acerca el ciber-crimen logrado ejecutarse por The Carbanak group, este grupo realizó un sinfín hurtos a casi cien bancos, robando alrededor de Un billón de dinero americano en todo el mundo. Lo que se analizo fue, que dichos asaltantes cibernéticos descubrieron las flaquezas de los sistemas en la redes privadas, en otras palabras podían ingresar a sus a sus protocolos de seguridad sin mayores problemas con la finalidad de ingresar a la red privada de la empresa sin autorización alguna. Los delincuentes lograron realizar registros y transacciones falsas que aparentemente eran transacciones normales para los funcionarios del banco y de forma no lograron ser detectadas por procesos antifraude que tenía la empresa.

Así mismo a finales del 2014, la firma Sony Pictures fue víctima de un ataque cibernético donde los hackers ingresaron al núcleo de la propiedad intelectual de una empresa. Entre los daños ocasionados a la firma Sony se detectó la sustracción de 100 Tera bitios (Mil catorce bitios) de ciber-información, conteniendo de mails, trailers de películas nuevas y próximos guiones a estrenarse en nuevos proyectos.

Según un informe de la firma Digiware señala que el Perú es el quinto país de América Latina que más recibe ataques cibernéticos. Según el estudio, el Perú concentra el 11.22% de recepción de ataques cibernéticos, luego aparecen Colombia 21.73%, Brasil con el 19% de recepción de ataques cibernéticos,

Argentina con el (13.94%), mientras que Ecuador tiene un porcentaje similar que el Perú (11.25%).

2.2. Bases Teóricas

A continuación se desarrollan los fundamentos teóricos de los ataques cibernéticos:

Ataques Cibernéticos de Países; Los problemas del mundo donde vivimos se extienden en el mundo del ciberespacio. Pocas años atrás se viene registrando ciberataques estratégicos como por ejemplo, el ciberataque al País de Estonia en 2007 que produjo la inhabilitación pasajera de muchas instalaciones militares críticas, otro caso es el ciberataque del País de Rusia al País Georgia en 2008 el cual trajo como consecuencia la invasión terrestre, otro caso es el ciberataque al País de EEUU, el cual se descubrió que la base del ataque se encontraba en el territorio del País de China.

En los últimos años se ha revelado que muchos países invierten grandes recursos monetarios, infraestructurales y personas para lograr dar grandes pasos de innovación de amenazas cibernéticas muy avanzadas que logran realizar ataques de forma agresiva y que pueden escoger blancos de infraestructura tecnológica muy específicos logrando estar insertado en redes cibernéticas privadas de la víctima sin ser descubiertos.

Estamos convencidos que existen muchos otros ataques cibernéticos sufridos a muchos países pero estos mismo son clasificadas para no ser divulgados ya

que con ello los países atacados quedarían como débiles en seguridad de la información ante otros posibles ataques de países en conflictos o guerras.

Ataques Cibernéticos de Empresas Privadas; Muchas empresas privadas tienen como obtener a como dé lugar obtener los procesos técnicos operarios industriales de otras empresas privadas o estatales las cuales representan una rivalidad.

Este tipo de amenaza y de igual forma que los ataques entre países se realiza invirtiendo grandes recursos monetarios, infraestructurales y personas en el objetivo de innovar nuevas amenazas cibernéticas muy avanzadas para lograr realizar ataques de forma agresiva y que pueden escoger sus blancos de infraestructura tecnológica muy específicos manteniendo una constante presencia insertada en las redes privadas cibernéticas de otra empresa sin ser descubiertos.

Ataques Cibernéticos Terroristas, Absolutismo o extremismo de Política o de Ideología; Dichos terroristas y agrupaciones fanática extremistas emplean el espacio cibernético para planear sus operaciones, luego ejecutarlas y al final publicitarlas para demostrar su superioridad intelectual cibernética contra sus oponentes, esto con el fin de reclutar más partidarios para continuar con los ataques. Estos grupos son conscientes de lo importante que es una buena estratégica y táctica de ataque en el ciberespacio para sus beneficios. Y medio por el cual divulgan muchos de las acciones extremistas son las grupos

sociales en redes de internet y/o foros sociales en internet estos mismo han sido trasformado en la primordial herramienta usada por estos grupos.

Ataques Cibernéticos de Bandas Criminales Organizadas; Las bandas del crimen organizado también conocidas como cibergangs han emprendido acciones en las redes de internet, básicamente en redes de internet privadas de empresas. Las empresas privadas o estatales comúnmente siempre sufren ataques de seguridad de su información desde el anonimato, este modelo de ataque que usan las bandas tienen como prioridad el robo de información extremadamente sensible para luego usarla para el fraudes, venta a otras empresas o extorciones económicas para devolución de la información robada.

Ataques Cibernéticos de Hacktivistas; Desde el 2011, los hacktivistas han creado un movimiento masivo denominado “el hacktivismo”. Dicho movimiento se ha transformado en una de los riesgos más grandes para todas las organizaciones privadas y estatales de muchos países.

Este movimiento hacktivista tiene como prioridad actuar desde el anonimato, logrando así cometer el robo de la información de las empresas y posterior a ello la libre distribución de la misma por medio de las redes de internet masivas, esencialmente a través de foros grupales concurridos, Facebook, twitter, y otras aplicaciones de celular comunes. Los hacktivistas suelen agruparse de manera dispersa para planificar y coordinar usando la red de internet conocida como el under-ground, que básicamente es una red donde no se puede rastrear con facilidad de que país o localidad estas conectado.

Existen mucho de estos estos grupos hacktivistas entre los más conocidos se encuentran Anonymous o Luzsec. Estos grupos hacktivistas tienen como mira asaltar el ciberespacio privado de empresas u organizaciones del rubro de las comunicaciones televisivas, proveedores de instalaciones vitales, proveedores de internet services, bancos, etc.

Ataques Cibernéticos de Bajo perfil; Estos ataques son realizados comúnmente por individuos de un alto saber en las ciencias de la informática, y ello les permite llevar a cabo sus ciberataques por razones muy diversa como los son venganzas, sabotaje, rivalidades, investigación, cólera e ira de despido de la empresa, siempre son temas de motivo personal.

Ataques Cibernéticos de Personas con Accesos Autorizados; También conocidos como insiders, intruders o privilegiados, este segmento son unas de las mayores amenazas para la seguridad de la información en la entidades privadas y estatales de todos los países, por lo general son personas que están infiltradas en un una entidad o grupo y está descontenta o disconforme como el modo de pensar de la misma agrupación a la que pertenece, pero esta como integrante para poder robar la información sin mucho esfuerzo ya que cuenta con accesos a la red privada donde la información se encuentra. También se les pude señalar como espía infiltrado por un Estado enemigo de otro, también hay casos de empleados de la organización que son cautivados y contratados por bandas de terroristas o cibercriminales.

3. Hipótesis

3.1. Hipótesis General

Existe relación en la gestión de la ciberseguridad con la prevención de los ataques cibernéticos en las PYMES del Perú, 2016.

3.2. Hipótesis Específicas

- Existen problemas de gestión en la ciberseguridad en las PYMES del Perú, 2016.
- Existen estrategias de prevención de riesgos de ataques cibernéticos en las PYMES del Perú, 2016.

CAPITULO II

METODOLOGÍA

4. Tipo y diseño de la Investigación

4.1. Tipo de la Investigación

Para el desarrollo de este trabajo se aplicarán los siguientes tipos de Investigación:

Según el enfoque: Investigación Cuantitativa

De acuerdo a Hernández, Fernández y Baptista (2006, p. 4), la investigación cuantitativa “Usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías”.

Según el Nivel: Investigación Cuantitativa – Descriptiva

De acuerdo a Hernández, Fernández y Baptista (2006, p. 80), la investigación descriptiva “Busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice. Describe tendencias de un grupo o población”.

El objetivo de esta investigación es conocer cuál es el nivel de madurez actual en la que se encuentran las PYMES del Perú con respecto a la ciberseguridad y cuál es el nivel de impacto de un ciberataque a una PYME, ya que este tipo de empresas son los objetivos preferidos de los ciberdelincuentes porque no cuentan con sistemas de protección ni con el conocimiento adecuado para evitar los ataques que llegan a través de la red, para conocer estos datos con

exactitud serán necesario analizar los puntos débiles y hacer auditoria de seguridad en las PYMES.

4.2. Diseño de la Investigación

Para esta investigación utilizaremos el diseño **Cuantitativo No Experimental**, porque según Hernández, Fernández y Baptista (2006) (p. 205), el diseño No Experimental “se realiza sin manipular deliberadamente variables” es decir, no se hace variar en forma intencional las variables independientes, para observar su efecto sobre otras variables; sino que se observan los fenómenos“

Para mostrar los resultados de la investigación seguiremos estos pasos:

1. Recolección de datos.
2. Clasificación de datos.
3. Presentación de datos (tablas y gráficos).
4. Análisis descriptivo.

A partir de los resultados del análisis sobre la gestión de la seguridad de la información se diseñará un plan estratégico de seguridad informática y un programa de concientización en seguridad de información empresarial, con la finalidad de brindarles a los integrantes de las empresas, conocimientos tecnológicos y las diversas aplicaciones que se pueden utilizar para tener segura la información y reducir los riesgos de los ciberataques.

5. Operacionalización de las Variables

Tabla 1. Operacionalización de la Variable Ciberseguridad.

Variable	Definición Conceptual	Definición Operacional	Indicadores	Ítems o Indice	Variabilidad
Gestión de la Ciberseguridad	Aplicación de un proceso de análisis de riesgos relacionados con el uso, procesamiento, almacenamiento, transmisión de información o datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados. (Chamorro, 2011).	Factores de Conocimiento: 1. Nivel de Conocimiento de la Gestión de la Ciberseguridad.	Escala de Niveles: Niveles Básico Niveles Intermedio Niveles Avanzado	Índices: 1= Niveles Básico 2= Niveles Intermedio 3= Niveles Avanzado	Puntuación mínima: 1 Puntuación máxima: 3

Tabla 2. Operacionalización de la Variable Ataques Cibernéticos.

Variable	Definición Conceptual	Definición Operacional	Indicadores	Ítems o Indice	Variabilidad
Prevención de los Ataques Cibernéticos	Acción de impulsar la implantación de la normativa sobre la protección de infraestructuras críticas y de las capacidades necesarias para la protección de los servicios esenciales. (Presidencia del Gobierno de España, 2013).	Frecuencia de Ataques Cibernéticos anuales.	Cantidad de Ataques anuales: De 0-3 4-7 8-11 12-15 16 a más	Índices: 1= 0-3 2= 4-7 3= 8-11 4= 12-15 5= 16 a más	Puntuación mínima: 1 Puntuación máxima: 5

6. Población, muestra y muestreo

Población: según las últimas cifras del Instituto Nacional de Estadística e Informática(INEI), en el Perú hay en total 1.713.272 empresas, de las cuales el 99.6% son consideradas micro, pequeñas y medianas empresas (MIPYME), de este total, el 96.2% (1.648.167 empresas) está integrada por las microempresas, siguen las pequeñas empresas que son el 3.2% (54,824 empresas) y las medianas empresas, que son el 0.2% (3,426 empresas) y en último lugar están las grandes empresas, que son el 0.4% (6,853 empresas).

Muestra: se seleccionó como muestra representativa de las PYMES a la empresa Transporte Zavala Cargo S.A.C. del sector Transporte de Carga a nivel nacional, que por su estructura organizacional es considerada como Mediana empresa. Las Medianas Empresas del sector Transporte de Carga, tienen de 6 a 25 vehículos, cuentan con una estructura para el embarque y desembarque de carga, hay concertación de carga que anualmente se estima en 21,000 TN de carga transportada.

Además contamos con el apoyo de sus trabajadores para poder realizar la encuesta, porque se ha observado que es una de las empresas que tienen muy poca cultura en seguridad informática y dentro de sus activos tiene entre 2 y 60 equipos informáticos.

Muestreo: la técnica de muestreo que utilizaremos será *No Probabilístico-Por Conveniencia*, debido a que la muestra elegida está más accesible a nosotros para poder realizar nuestro estudio.

7. Técnicas de Recolección de Datos

Técnica: para la recolección de datos utilizaremos la Técnica Indirecta.

Instrumento: utilizaremos La Encuesta como instrumento de recolección de datos.

La encuesta se realizó en el mes de octubre de 2016, en la empresa Transporte Zavala Cargo S.A.C.

Formulación de las preguntas de acuerdo a las variables

Se han identificado preguntas relacionadas a las variables de Gestión de la Ciberseguridad y Prevención de los Ataques Cibernéticos, se plantearon nueve preguntas en la encuesta, orientadas a obtener resultados que definan si la organización conoce y tiene implementado el concepto de ciberseguridad y a la vez analizar el nivel de madurez en la que se encuentran la empresa Transporte Zavala Cargo S.A.C. con respecto a la Ciberseguridad.

*Tabla 3. Preguntas relacionadas a las v*ariables del trabajo de Investigación.

VARIABLES	PREGUNTAS RELACIONADAS A LAS VARIABLES
Gestión de la Ciberseguridad	¿En su empresa existen normas o prácticas enfocadas a la ciberseguridad?
	¿Cree usted que la Ciberseguridad sea importante en su empresa?
	¿Dentro de su empresa existe algún personal encargado de la ciberseguridad?
	¿En su empresa se realizan análisis y gestión de riesgos informáticos?
Prevención de los Ataques Cibernéticos	¿Existe en su empresa planes de contingencia ante un ciberataque?
	¿Sabe usted qué medidas tomar ante un ciberataque?
	¿En su empresa existen herramientas que aseguren su información digital?
	¿En su empresa asignan presupuesto destinado a la ciberseguridad?
	¿Su empresa realiza capacitación sobre temas de ciberseguridad y prevención ante amenazas cibernéticas?

Calificación de las Variables

Para calificar las variables se eligió la escala de Likert, el cual tiene los siguientes valores:

Tabla 4. Calificación de variables en escala de Likert.

Muy de acuerdo	**1**
De acuerdo	**2**
Ni en acuerdo ni en desacuerdo	**3**
En desacuerdo	**4**
Muy en desacuerdo	**5**

8. Métodos de Análisis de Datos

Se realizó el trabajo de investigación en la empresa Transporte Zavala Cargo S.A.C., encuestando a cinco trabajadores que pertenecen al área de Sistemas, solicitándoles que fueran lo más sinceros posibles para dar validez al trabajo.

En cada gráfico se muestra el resultado de cada pregunta de la encuesta.

1. ¿En su empresa existen normas o prácticas enfocadas a la ciberseguridad?

Tabla 5. Encuesta uno de normas o prácticas de ciberseguridad.

Criterio	Personas	Porcentaje
Muy de acuerdo	0	0%
De acuerdo	1	20%
Ni en acuerdo ni en desacuerdo	0	0%
En desacuerdo	0	0%
Muy en desacuerdo	4	80%
Total	**5**	**100%**

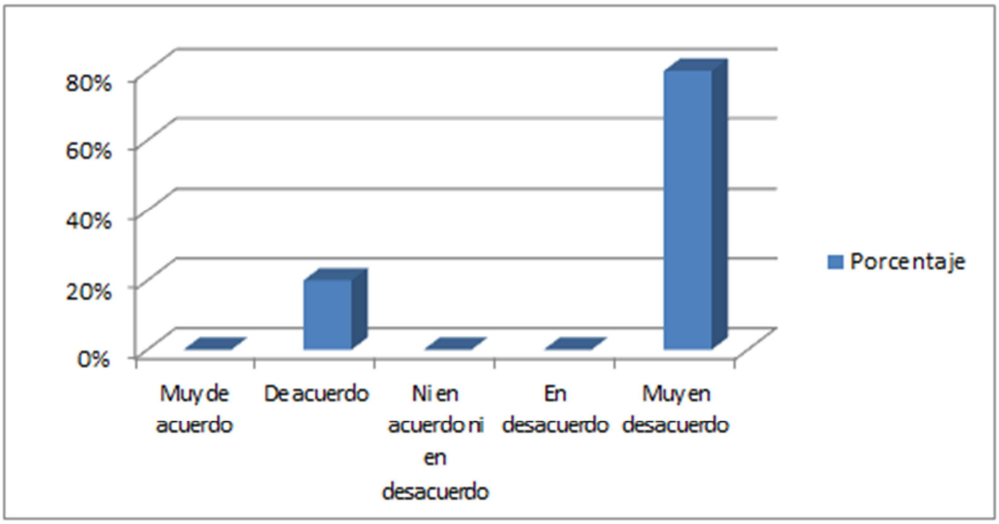


Figura 1. Resultado en la encuesta uno.

Según la muestra, el 80% confirma que en la empresa no existen normas o prácticas orientadas a la ciberseguridad, en tanto el 20% de los consultados consideran que la empresa si cuenta con políticas o prácticas de ciberseguridad.

2. ¿Cree usted que la Ciberseguridad sea importante en su empresa?

Tabla 6. Encuesta dos de la importancia de la ciberseguridad.

Criterio	Personas	Porcentaje
Muy de acuerdo	5	100%
De acuerdo	0	0%
Ni en acuerdo ni en desacuerdo	0	0%
En desacuerdo	0	0%
Muy en desacuerdo	0	0%
Total	**5**	**100%**

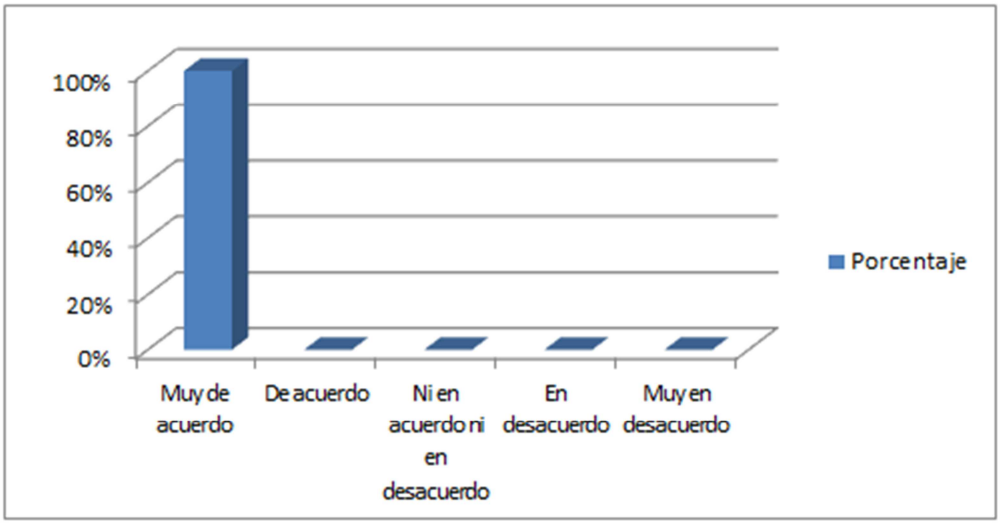


Figura 2. Resultado en la encuesta dos.

El 100 % de los encuestados afirman que la ciberseguridad es muy importante y debe ser implementado para evitar riesgos.

3. **¿Dentro de su empresa existe algún personal encargado de la ciberseguridad?**

Tabla 7. Encuesta tres de personal encargado de la ciberseguridad.

Criterio	Personas	Porcentaje
Muy de acuerdo	0	0%
De acuerdo	0	0%
Ni en acuerdo ni en desacuerdo	0	0%
En desacuerdo	0	0%
Muy en desacuerdo	5	100%
Total	**5**	**100%**

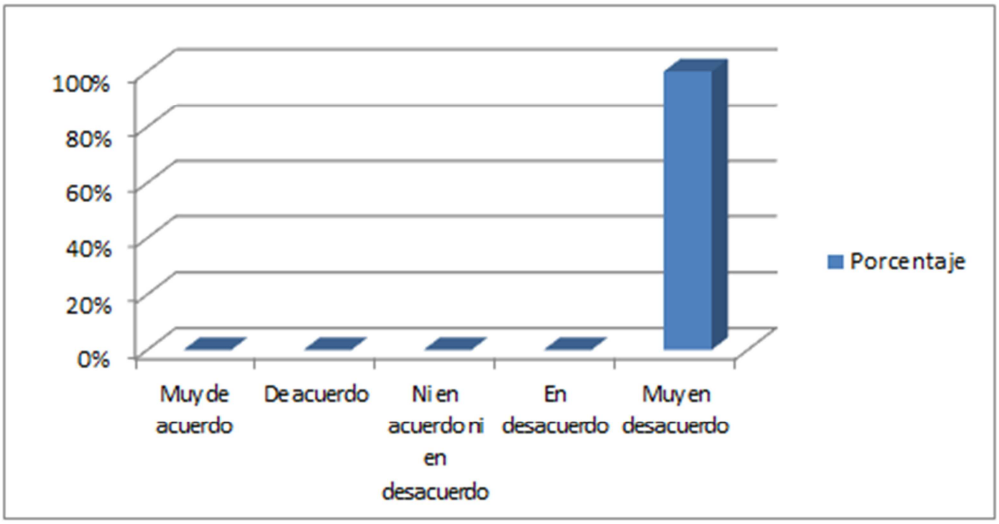


Figura 3. Resultado en la encuesta tres.

Según la muestra, el 100% de los encuestados respondieron que no existe personal capacitado en ciberseguridad dentro de la empresa.

4. **¿En su empresa se realizan análisis y gestión de riesgos informáticos?**

Tabla 8. Encuesta cuatro de análisis y gestión de riesgos informáticos.

Criterio	Personas	Porcentaje
Muy de acuerdo	0	0%
De acuerdo	2	40%
Ni en acuerdo ni en desacuerdo	0	0%
En desacuerdo	3	60%
Muy en desacuerdo	0	0%
Total	**5**	**100%**

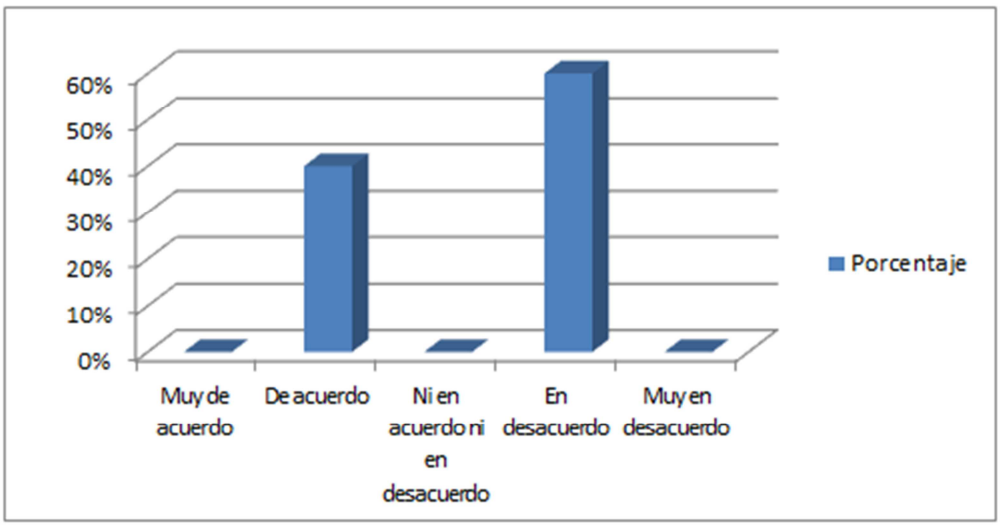


Figura 4. Resultado en la encuesta cuatro.

Ante esta pregunta, tan solo el 40% respondió que si se utilizan métodos de análisis de riesgos informáticos, mientras que el 60% respondió que no se realizan.

5. ¿Existe en su empresa planes de contingencia ante un ciberataque?

Tabla 9. Encuesta cinco de planes de contingencia ante un ciberataque.

Criterio	Personas	Porcentaje
Muy de acuerdo	0	0%
De acuerdo	0	0%
Ni en acuerdo ni en desacuerdo	0	0%
En desacuerdo	5	100%
Muy en desacuerdo	0	0%
Total	**5**	**100%**

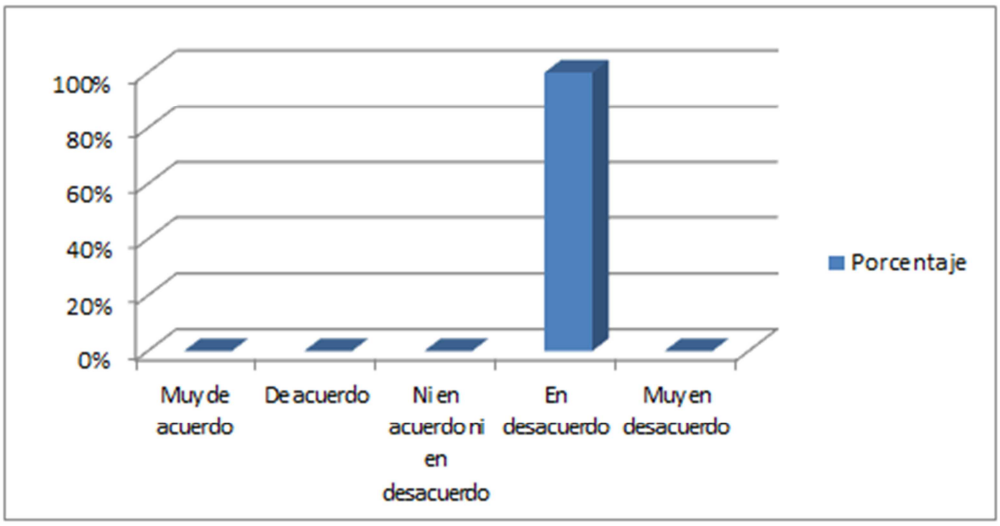


Figura 5. Resultado en la encuesta cinco.

Ante la pregunta, el 100% de los consultados respondió que no cuentan con procedimientos para afrontar ataques cibernéticos.

6. ¿Sabe usted qué medidas tomar ante un ciberataque?

Tabla 10. Encuesta seis de medidas a tomar ante un ciberataque.

Criterio	Personas	Porcentaje
Muy de acuerdo	0	0%
De acuerdo	1	20%
Ni en acuerdo ni en desacuerdo	0	0%
En desacuerdo	4	80%
Muy en desacuerdo	0	0%
Total	**5**	**100%**

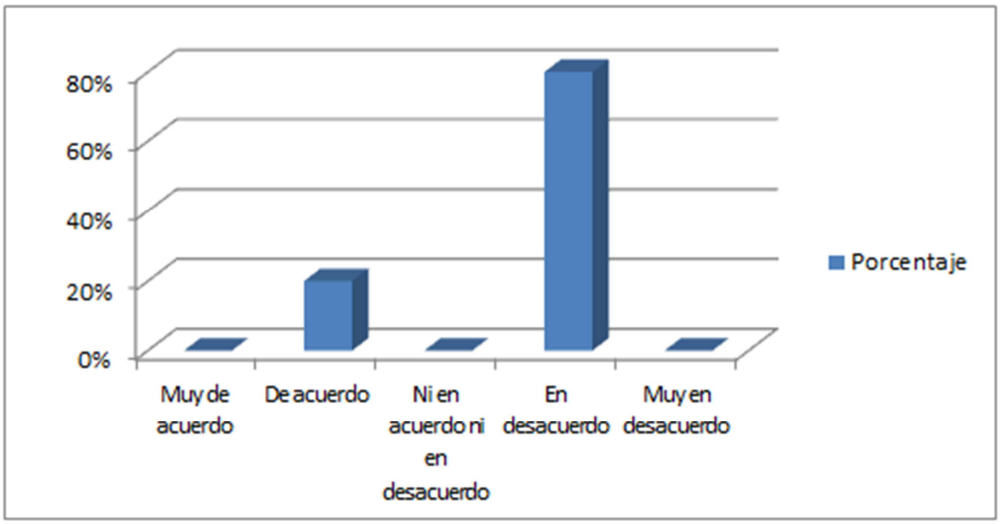


Figura 6. Resultado en la encuesta seis.

Frente a la pregunta de qué medidas tomar ante un ciberataque, el 80% de los consultados manifestaron que no saben cómo proceder ante un ciberataque, mientras que el 20% afirma que si sabe qué hacer ante un incidente de ciberataque.

7. ¿En su empresa existen herramientas que aseguren su información digital?

Tabla 11. Encuesta siete de herramientas de información digital.

Criterio	Personas	Porcentaje
Muy de acuerdo	0	0%
De acuerdo	1	20%
Ni en acuerdo ni en desacuerdo	0	0%
En desacuerdo	4	80%
Muy en desacuerdo	0	0%
Total	**5**	**100%**

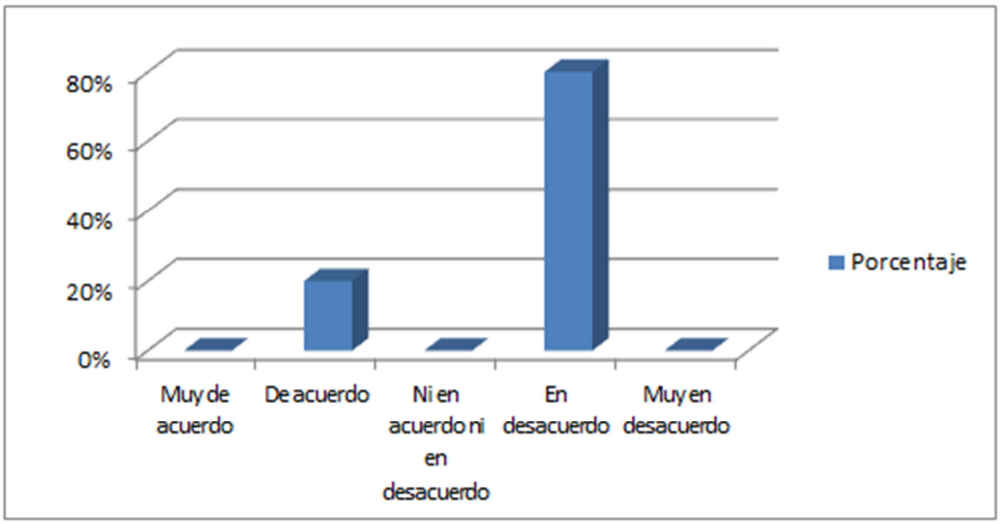


Figura 7. Resultado en la encuesta siete.

Ante esta pregunta, el 80% de los consultados respondieron que la empresa carece de herramientas que aseguren la información digital de la empresa, tan solo el 20% aseguró que la empresa si cuenta con herramientas tecnológicas, por ejemplo el antivirus.

8. ¿En su empresa asignan presupuesto destinado a la ciberseguridad?

Tabla 12. Encuesta ocho de presupuesto destinado a la ciberseguridad.

Criterio	Personas	Porcentaje
Muy de acuerdo	0	0%
De acuerdo	0	0%
Ni en acuerdo ni en desacuerdo	0	0%
En desacuerdo	0	0%
Muy en desacuerdo	5	100%
Total	**5**	**100%**

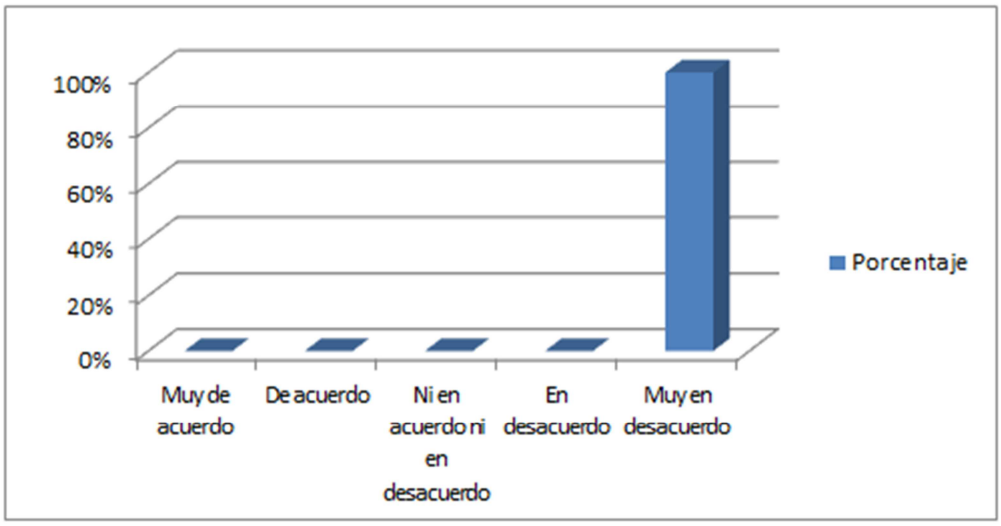


Figura 8. Resultado en la encuesta ocho.

Según la encuesta, el 100% de los encuestados respondió que en la empresa no se asigna presupuesto destinado a la ciberseguridad.

9. **¿Su empresa realiza capacitación sobre temas de ciberseguridad y prevención ante amenazas cibernéticas?**

Tabla 13. Encuesta nueve de capacitación y prevención de la ciberseguridad.

Criterio	Personas	Porcentaje
Muy de acuerdo	0	0%
De acuerdo	0	0%
Ni en acuerdo ni en desacuerdo	0	0%
En desacuerdo	0	0%
Muy en desacuerdo	5	100%
Total	**5**	**100%**

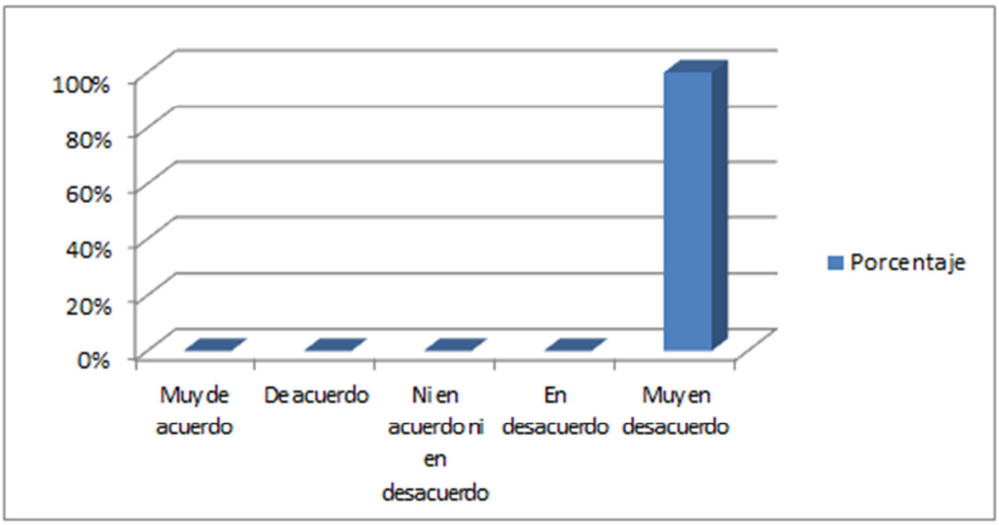


Figura 9. Resultado en la encuesta nueve.

Ante esta pregunta, el 100% respondió que no reciben capacitación ni formación en ciberseguridad.

CAPITULO III

RESULTADOS

9. Resultados Descriptivos

Los resultados generales que se derivan de la encuesta demuestran que para el personal consultado de la Empresa Transporte Zavala Cargo S.A.C., la ciberseguridad es importante; sin embargo la empresa no cuenta con procedimientos ni políticas que orienten a las buenas prácticas en el uso de la tecnología, no ha formado a sus empleados en materia de ciberseguridad para prevenir y evitar posibles amenazas; no invierten en herramientas de ciberseguridad y no tienen personal responsable de la seguridad de la empresa en la red.

10. Prueba de Hipótesis

En este trabajo de investigación los resultados de la encuesta realizada en la empresa Transporte Zavala Cargo (muestra), arrojaron que la empresa no cuenta con políticas ni metodologías de análisis y prevención de riesgos de ciberataques.

Por lo tanto se aprueba la hipótesis general planteada ya que si existe relación entre ambas variables, puesto que la gestión de la Ciberseguridad es un proceso de análisis de riesgos y amenazas, de decisión y ejecución de acciones, con el objetivo de prevenir y reducir el riesgo a un nivel aceptable y a un coste razonable.

Discusión

En nuestro estudio y el estudio realizado por Yamith Andrés Fernando Niño Wilches. Tesis Sobre La Importancia de la Implementación del Concepto de Ciberseguridad Organizacional en las Organizaciones Tipo Pymes. (2015). Bogotá, D.C. Se pudo encontrar que a pesar de que para todos los encuestados es importante la ciberseguridad, se evidencia desconocimiento del mismo por parte de la alta dirección, por tal motivo es importante que los líderes de las pymes conozcan, analicen e implementen los elementos que componen el concepto de ciberseguridad.

Análisis de riesgos: el cual busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de llegar a realizarse una amenaza. Por tal motivo se requiere identificarlos y analizarlos para determinar el nivel del riesgo y qué medidas se deben efectuar para tratarlos de forma adecuada.

Conclusiones

1. La Empresa Zavala Cargo S.A.C. tiene una falta del uso de planes contra ataques de Seguridad Cibernética, que resguarden su información cibernética permitiendo así una toma de decisiones más confiable.

2. La indiferencia de la Gerencia con temas de Ciberseguridad da como resultado la falta de apoyo económico al proceso de creación de medidas de seguridad informática dentro de una red privada, provocando así que la organización se exponga a mayores riesgos.

3. La Ciberseguridad de toda información que se maneja en una empresa es un compromiso compartido de todos los niveles jerárquicos en una empresa y que necesita el apoyo de todos los trabajadores de la misma, para ello se debe elaborar un plan adecuado de implantación de esquemas de Ciberseguridad con la adecuada coordinación de todas las áreas de la empresa.

4. Los resultados de las pruebas de seguridad informática que se hizo a la empresa Transporte Zavala Cargo S.A.C. nos permitió conocer la falta de conocimiento de seguridad de la información cibernética de todo el recurso humano que labora en la empresa. Dejando así a la empresa vulnerable a todos los riesgos cibernéticos de información vital y privada de la misma.

5. La realización de nuestro trabajo, permitió ayudar a que la empresa Transporte Zavala Cargo S.A.C en tener en cuenta la importancia que se debe de dar al resguardo de su información cibernética, ya que si dicha información fuese robada o manipulada por personas ajenas a la empresa conllevaría a resultados adversos para la empresa misma, a tal punto de quebrar.

6. Con la realización de nuestro trabajo se desea promover y motivar a las empresas en temas de seguridad cibernética y a la vez que los trabajadores tomen conciencia de como utilizan la tecnología en sus labores diarias.

Recomendaciones

Entre las medidas de ciberseguridad que deben adoptar las PYMES para garantizar la seguridad informática son:

1. Elaborar políticas de ciberseguridad en la empresa, con la finalidad de que su personal comprenda la importancia de esta materia.

2. Ejecutar Auditorías a la ciberseguridad de su empresa con la finalidad de conocer las flaquezas de seguridad informática y que procedimientos se debe realizar para menguar los riesgos.

3. Programar reuniones con gerencia y el área de sistemas con la finalidad de exponer las necesidades de herramientas necesarias para proteger la información cibernética de la empresa.

4. Diseñar un plan de contingencia en caso haya un incidente que comprometa los sistemas informáticos de la empresa. Contar con copias de respaldo (backup) de la información importante.

5. No es suficiente contar con un antivirus. Lo recomendable es contar con software licenciados que cuenten con protecciones oficiales y actualizadas, de tal modo que puedan repeler cualquier ataque de hackers o enviar alertas cuando ingresen intrusos a su red.

6. Realizar capacitaciones de carácter obligatorio de todo el personal que labora en la empresa puesto que es un filtro importante de información cibernética de la empresa la cual debe ser protegida y resguardada.

Referencias

Ciberespacio, Ciberseguridad y Ciberguerra. (25 de Mayo del 2015). Diario de la Mariana de Guerra del Perú. Recuperado de http://virtual.esup.edu.pe/bitstream/ESUP/113/1/pp.76-95.pdf

El 99.6% de las empresas son Mi pymes en el país. (12 de marzo de 2015). La Razón. Recuperado de https://www.inei.gob.pe/media/inei_en_los_medios/12_Marzo_Exitosa_13.pdf

Hernández, R. (2010). Metodología de la investigación. México: McGraw-Hill Interamericana.

Norma Legal LEY N°30096. (22 de octubre de 2013). El Peruano. Recuperado de http://busquedas.elperuano.com.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Siete de cada diez bancos en Perú sufren fraudes de sus propios empleados. (31 de julio del 2014). Diario Gestión. Recuperado de http://gestion.pe/economia/siete-cada-diez-bancos-peru-sufren-fraudes-sus-propios-empleados-2104355

Anexos

La Encuesta

Responde las siguientes preguntas, marcando la respuesta que considere correcta

1. **¿En su empresa existen normas o prácticas enfocadas a la ciberseguridad?**

☐ Muy de acuerdo ☐ De acuerdo ☐ Ni en acuerdo ni en desacuerdo
☐ En desacuerdo ☐ Muy en desacuerdo

2. **¿Cree usted que la Ciberseguridad sea importante en su empresa?**

☐ Muy de acuerdo ☐ De acuerdo ☐ Ni en acuerdo ni en desacuerdo
☐ En desacuerdo ☐ Muy en desacuerdo

3. **¿Dentro de su empresa existe algún personal encargado de la ciberseguridad?**

☐ Muy de acuerdo ☐ De acuerdo ☐ Ni en acuerdo ni en desacuerdo
☐ En desacuerdo ☐ Muy en desacuerdo

4. **¿En su empresa se realizan análisis y gestión de riesgos informáticos?**

☐ Muy de acuerdo ☐ De acuerdo ☐ Ni en acuerdo ni en desacuerdo
☐ En desacuerdo ☐ Muy en desacuerdo

5. **¿Existe en su empresa planes de contingencia ante un ciberataque?**

☐ Muy de acuerdo ☐ De acuerdo ☐ Ni en acuerdo ni en desacuerdo
☐ En desacuerdo ☐ Muy en desacuerdo

6. **¿Sabe usted qué medidas tomar ante un ciberataque?**

☐ Muy de acuerdo ☐ De acuerdo ☐ Ni en acuerdo ni en desacuerdo
☐ En desacuerdo ☐ Muy en desacuerdo

7. **¿En su empresa existen herramientas que aseguren su información digital?**

☐ Muy de acuerdo ☐ De acuerdo ☐ Ni en acuerdo ni en desacuerdo
☐ En desacuerdo ☐ Muy en desacuerdo

8. **¿En su empresa asignan presupuesto destinado a la ciberseguridad?**

☐ Muy de acuerdo ☐ De acuerdo ☐ Ni en acuerdo ni en desacuerdo
☐ En desacuerdo ☐ Muy en desacuerdo

9. **¿Su empresa realiza capacitación sobre temas de ciberseguridad y prevención ante amenazas cibernéticas?**

☐ Muy de acuerdo ☐ De acuerdo ☐ Ni en acuerdo ni en desacuerdo
☐ En desacuerdo ☐ Muy en desacuerdo

Matriz de Consistencia

MATRIZ DE CONSISTENCIA DE LA INVESTIGACIÓN

Alumnos: Inoguchi Rojas Antonio
Macha Moreno Erika Lizet

Tema: La Ciberseguridad
Título de la Investigación: Gestión de la Ciberseguridad y Prevención de los Ataques Cibernéticos en las Pymes del Perú, 2016.
Línea de Investigación: Gestión de Tecnologías y Sistemas de Información

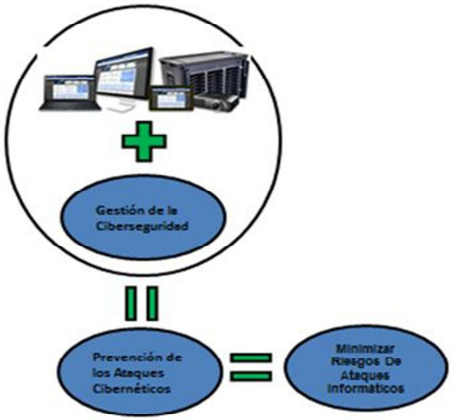
TÍTULO DE TESIS

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES
PROBLEMA GENERAL ¿En qué medida se relaciona la gestión de la ciberseguridad con la prevención de los ataques cibernéticos en las PYMES del Perú, 2016? **PROBLEMAS ESPECÍFICOS** • ¿Cuáles son los problemas de gestión de la ciberseguridad en las PYMES del Perú, 2016? • ¿Cómo prevenir los riesgos de los ataques cibernéticos en las PYMES del Perú, 2016?	**OBJETIVO GENERAL** Determinar la gestión de la ciberseguridad con la prevención de los ataques cibernéticos en las PYMES del Perú, 2016. **OBJETIVOS ESPECÍFICOS** • Identificar los problemas de gestión de la ciberseguridad en las PYMES del Perú, 2016. • Prevenir los riesgos de los ataques cibernéticos en las PYMES del Perú, 2016.	**HIPÓTESIS PRINCIPAL** Existe relación en la gestión de la ciberseguridad con la prevención de los ataques cibernéticos en las PYMES del Perú, 2016. **HIPÓTESIS ESPECÍFICAS** • Existen problemas de gestión en la ciberseguridad en las PYMES del Perú, 2016. • Existen estrategias de prevención de riesgos de ataques cibernéticos en las PYMES del Perú, 2016	**VARIABLE(S) DE ESTUDIO:** **VARIABLE A:** Gestión de la Ciberseguridad (Independiente) **VARIABLE B:** Prevención de los Ataques Cibernéticos (Dependiente) **OPERATIVIZACIÓN DE LAS VARIABLES**

Variables de Estudio	Dimensiones	Indicadores de desempeño	Puntaje de Ítem	Escala de Medición
VARIABLE "A" Gestión de la Ciberseguridad	Infraestructura Tecnológica.	Histórico de antigüedad o tiempo de uso.	Variables tipo cuantitativa, intervalor, independiente	Escala de Razón: tiempo (resultado en números positivos).
	Gestión de conocimiento sobre seguridad de información.	Diseminación e interpretación de la información.	Variables tipo cualitativa, nominal, independiente	Escala Ordinal: Mucho, Poco, Nada.
VARIABLE "B" Prevención de los Ataques Cibernéticos	Mecanismos de prevención y protección.	Histórico de tipos de defensas.	Variablestipo cualitativa, nominal, dependiente.	Escala Nominal: herramientas de protección (Antivirus, firewall, licencia de software, etc.)
	Tipos de ataques cibernéticos.	Probabilidad de amenaza y magnitud de daño.	Variablestipo cualitativa, nominal, dependiente.	Escala Ordinal: Alta, Media, Baja.

VARIABLES INTERVINIENTES

Dentro de las variables intervinientes se encuentran la adquisición de conocimientos tecnológicos y las diversas herramientas para tener segura la información de una empresa.

MÉTODO Y DISEÑO DE LA INVESTIGACIÓN	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS	TRATAMIENTO ESTADÍSTICO
Método del estudio **Tipo de Investigación** Según el Enfoque se aplicará una Investigación Cuantitativa, puesto que se busca definirlo, delimitar y saber exactamente donde se inicia el problema de los Ataques cibernéticos, adicional a ello deseamos conocer en qué dirección va la noción de la Pymes en cuanto a la Prevención de los Ataques Cibernéticos para minimizar riesgos de ataques. **Nivel de Investigación** Según el Nivel se aplicará una **Investigación Descriptiva**, puesto que el objetivo de esta investigación es conocer cuál es el nivel de madurez actual en la que se encuentran las pymes del Perú con respecto a la ciberseguridad y cuál es el nivel de impacto de un ciberataque a una pyme. **Diseño de la Investigación** **Cuantitativo – No experimental** **Esquema**  	**Población** El total de pequeñas y medianas empresas (Pymes) del Perú. **Muestra** Para la unidad de muestra se seleccionó a la empresa Transporte Zavala Cargo S.A.C. del sector Transporte. **Método de Muestreo** **No Probabilístico-Por Conveniencia**	**Técnica** **Indirecta** **Instrumento** • Encuesta de Gestión de la Ciberseguridad. • Encuesta de Prevención de los Ataques Cibernéticos.	**Método de análisis de datos** De acuerdo al diseño de Investigación y a las técnicas e instrumentos basados en una escala tipo likert donde se asignaron los siguientes valores: **Totalmente de acuerdo** 1 **De acuerdo** 2 **Ni en acuerdo ni en desacuerdo** 3 **En desacuerdo** 4 **Totalmente en desacuerdo** 5 Usando Encuestas como: ¿Su organización cuenta con normas o prácticas que orienten la forma de gestionar los activos de información? Criterio / Personas / Porcentaje Totalmente de acuerdo: 0 / 0% De acuerdo: 1 / 20% Ni en acuerdo ni en desacuerdo: 0 / 0% En desacuerdo: 0 / 0% Totalmente en desacuerdo: 4 / 80% Total: 5 / 100%