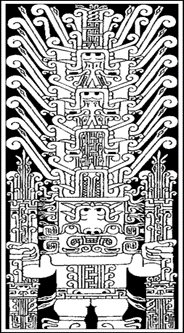
**UNIVERSIDAD NACIONAL FEDERICO VILLARREAL**

**FACULTAD DE INGENIERIA INDUSTRIAL Y SISTEMAS**

**ESCUELA DE INGENIERIA DE SISTEMAS**

****

**SEMINARIO DE TESIS**

**TITULO**

**IMPLEMENTAR LA SEGURIDAD DE LA INFORMACION CONTRA RIESGOS DE ATAQUES CIBERNETICOS Y LA CIBERSEGURIDAD EN LAS PYMES Y MICOEMPRESAS**

**AUTOR: ANGEL IVAN CERVANTES RONDON**

**CODIGO: 2016705024**

**INDICE**

[**TÍTULO: 5**](#_Toc435478154)

[**AUTOR 5**](#_Toc435478155)

[**LUGAR DONDE SE VA A REALIZAR LA INVESTIGACIÓN: 5**](#_Toc435478156)

[**1.** **DESCRIPCIÓN DEL PROYECTO 6**](#_Toc435478157)

[1.1. ANTECEDENTES 7](#_Toc435478158)

[1.2. PLANTEAMIENTO DEL PROBLEMA 13](#_Toc435478164)

[1.2.1. DESCRIPCIÓN DE LA PROBLEMÁTICA 13](#_Toc435478165)

[1.2.2. DESCRIPCIÓN DEL PROBLEMA 16](#_Toc435478166)

[1.2.3. FORMULACIÓN DEL PROBLEMA 16](#_Toc435478167)

[1.2.3.1. PROBLEMA GENERAL 16](#_Toc435478168)

[1.2.3.2. PROBLEMA ESPECÍFICO 17](#_Toc435478169)

[1.3. OBJETIVOS 17](#_Toc435478170)

[1.3.1. OBJETIVO GENERAL 17](#_Toc435478171)

[1.3.2. OBJETIVO ESPECÍFICOS 17](#_Toc435478172)

[1.4. JUSTIFICACIÓN E IMPORTANCIA 18](#_Toc435478173)

[1.4.1. JUSTIFICACIÓN 18](#_Toc435478174)

[1.4.2. IMPORTANCIA 19](#_Toc435478175)

[1.5. ALCANCES Y LIMITACIONES 20](#_Toc435478176)

[1.5.1. ALCANCE 20](#_Toc435478177)

[1.5.2. LIMITACIÓN 20](#_Toc435478178)

[1.5.2.1. DELIMITACION ESPACIAL 21](#_Toc435478179)

[1.5.2.2. DELIMITACION TEMPORAL 21](#_Toc435478180)

[**2.** **MARCO TEÓRICO 22**](#_Toc435478181)

[2.1. TEORÍAS GENERALES RELACIONADAS CON EL TEMA 23](#_Toc435478182)

[**3.** **HIPÓTESIS Y OPERACIONALIZACIÓN DE LAS VARIABLES. 69**](#_Toc435478198)

[3.1. HIPÓTESIS GENERAL 69](#_Toc435478199)

[3.2. HIPÓTESIS ESPECÍFICAS 69](#_Toc435478200)

[3.3. VARIABLES 69](#_Toc435478201)

[3.3.1. VARIABLES INDEPENDIENTE 69](#_Toc435478202)

[3.3.2. VARIABLES INTERVINIENTE 70](#_Toc435478203)

[3.3.3. VARIABLE DEPENDIENTE 70](#_Toc435478204)

[3.3.4. OPERACIONALIDAD DE LAS VARIABLES. 70](#_Toc435478205)

[3.4. TIPO 76](#_Toc435478206)

[3.5. POBLACIÓN: 76](#_Toc435478207)

[3.6. UNIVERSO SOCIAL: 76](#_Toc435478208)

[3.7. MUESTRA: 76](#_Toc435478209)

[**4.** **MÉTODO. 77**](#_Toc435478210)

[4.1. DISEÑO DE INVESTIGACIÓN 77](#_Toc435478211)

[4.2. ESTRATEGIA DE PRUEBA DE HIPÓTESIS 78](#_Toc435478212)

[4.3. TÉCNICAS DE RECOLECCIÓN DE DATOS 79](#_Toc435478213)

[4.3.1. INSTRUMENTOS DE RECOLECCIÓN DE DATOS. 79](#_Toc435478214)

[**5.** **CRONOGRAMA 83**](#_Toc435478215)

[**6.** **PRESUPUESTO 85**](#_Toc435478216)

[**7.** **REFERENCIAS BIBLIOGRÁFICAS 86**](#_Toc435478217)

**TITULO DE LA TESIS**

**IMPLEMENTAR LA SEGURIDAD DE LA INFORMACION CONTRA RIESGOS DE ATAQUES CIBERNETICOS Y LA CIBERSEGURIDAD EN LAS PYMES Y MICOEMPRESAS**

**CERVANTES RONDON ANGEL IVAN**

**CODIGO ALUMNO 2016705024**

**LIMA METROPOLITANA**

**LIMA PERU**

**1.- DESCRIPCION DEL PROYECTO**

**1.1. ANTECEDENTES.**

El objetivo de la seguridad de la información, es el conjunto de medidas preventivas y correctivas implementados en las organizaciones, lo cual permiten proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

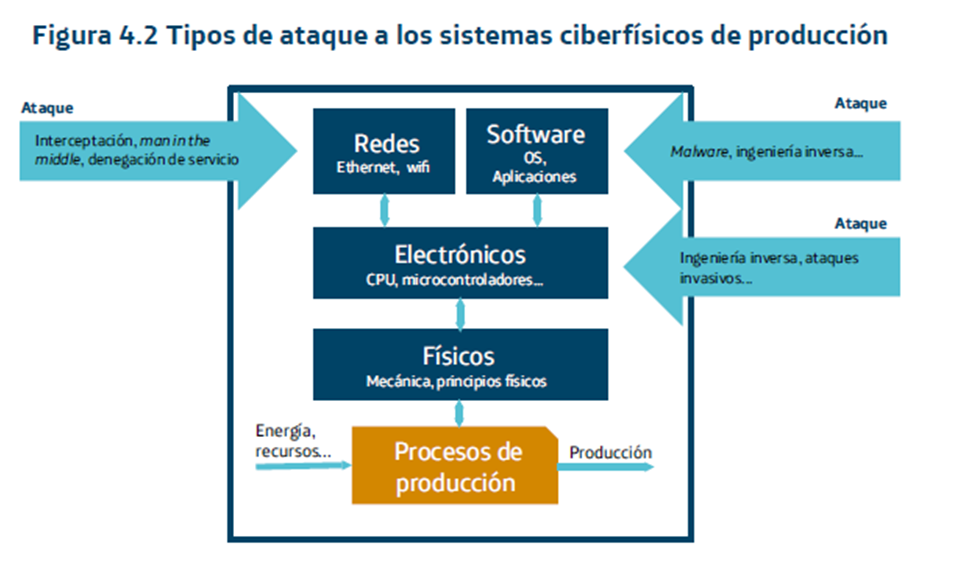
Las empresas con el tiempo se han ido perfeccionando en tecnología, en sistemas informáticos. Esta evolución de los sistemas computacionales, se ha ido ejercido a través del comercio electrónico, los sistemas computacionales en las nubes (internet) y de las comunicaciones se han abierto para las empresas y las personas, descubriendo el valor de la información y la facilidad de accesos a los datos.

Las microempresas, que han comenzado a incursionar en el mercado de la tecnología en la nube, deben considerar la importancia de la seguridad de la información en el contexto de internet, del cual en gran mayoría no le dan mayor importancia a su información que publican en la red no diferencian lo privado de lo público.

Por otro lado, la tecnología que va en constante cambio, ha repercutido que formas de comunicación surgiendo nuevas amenazas contra la seguridad de la información, entre ello tenemos la delincuencia informática, como por ejemplo ciberataques, hackers, etc. Esto es un flagelo, que se ha ido en aumento en estas épocas de pandemia, como lo informa la DIVINDAT-PNP, donde los fraudes, el robo de cuentas, etc., ha ido en aumento, por lo que el nivel de protección de la información corre un alto riesgo de pérdida de información tanto para los negocios y a la vez su ventaja competitiva en el mercado.

“Durante los últimos años, la aparición de noticias sobre problemas relacionados con la privacidad que afectaban tanto a empresas como a personas, así como el robo de información personal o fotografías, ha despertado la conciencia en una parte muy importante de la sociedad respecto a la importancia que tiene proteger la información personal en Internet.

Se trata además de una situación compleja, en la que el número y la variedad de ciber-amenazas es cada vez más elevado dado el proceso de digitalización de toda la economía y el avance de nuevas tendencias tecnológicas, como la computación en la nube o el Internet de las cosas.” (fuente: Fundación Telefónica; Ciberseguridad, la protección de la información en un mundo digital, pág. 9, 2016, España).



Este mundo del comercio electrónico contiene diferentes plataformas que permiten facilitar todo lo relacionado a la logística, inventarios, pagos entre otras funciones, de transacciones realizada de manera online (INTERNET), del cual se puede realizar compra – venta de productos o servicios.

Esto ha crecido de manera importante, que cada vez es más accesible el internet, mucha gente prefiere adquirir productos o servicios online, más en esta nueva normalidad generada por el impacto del COVID-19, muchas más empresas y negocios se están inclinando por crear su tienda online.



(Fundacion Telefonica, 2016)

Como observamos, en el cuadro la ciberseguridad, para la navegación de un negocio que use la nube (internet) es indispensable, porque con los tiempos, el avance tecnológico ha conllevado también a degenerarse por usuarios o personas que delinquen por este medio aprovechando la vulnerabilidad de algunas redes de comunicación, hoy más que todo se ha visto la débil ciberseguridad que existe en el Perú.

De acuerdo a los comentarios de OPTICAL NETWORS en su página web: “Ciberseguridad en el Perú: 5 factores que debes conocer para proteger los datos de tu empresa” (losc cambios ocasionados por la covid19, 2020)

“…… los ataques informáticos en Perú son uno de los peligros latentes más preocupantes en el sector corporativo, debido a que cada año surgen nuevas y más avanzadas amenazas orientadas a dañar y robar información empresarial……”

“La emergencia sanitaria ocasionada por la COVID-19 significa cambios en todos los aspectos de nuestra sociedad, de manera irreversible. Por lo que es innegable que, hechos como el crecimiento del comercio electrónico, la promoción de métodos de pago digitales y la implementación de trabajo remoto seguro sean parte de la nueva realidad.

Por ello, el panorama de ciberseguridad ha cambiado y generado nuevas necesidades en los sectores de comercio, finanzas, administrativo, educativo y de servicios que puedan realizarse de forma remota……”

“Crecimiento del Ecommerce en Perú. La inmovilización social ocasionada por el virus desató un incremento del comercio electrónico nunca antes visto en nuestro país: se estima que esta forma de venta aumentó en 131%, en mayor de 2020, ante la necesidad de los peruanos por comprar en línea.

Esta nueva modalidad de consumo también genera nuevas preocupaciones, ya que las empresas se ven en la necesidad de proteger sus sitios webs de las diversas vulnerabilidades que puede presentar un Ecommerce…… (losc cambios ocasionados por la covid19, 2020)

Como vemos, OPTICAL NETWORS, es una de las tantas empresas que han visto las vulnerabilidades existentes en el manejo de las redes y del software de comercio electrónico, para esto, es necesario para que las empresas al ofrecer sus productos, bienes o servicios a los clientes, también de resguardar la seguridad de los datos de sus clientes. Las plataformas facilitan operaciones como exhibición de productos, pagos, envíos, logística y todo lo necesario para que tanto el comerciante como el cliente tengan una experiencia bastante eficiente.

Los comerciantes con el auge del internet y redes sociales, sus tiendas han pasado al comercio electrónico, abarcando a un público más extenso, esto implica que las plataformas deberán ser perfectamente optimizada, en base de datos de clientes para ofrecerles promociones nuevas o generar más fidelidad.

“El delito informático pertenece a la clasificación genérica de delitos contra el patrimonio. En los últimos años, la sociedad está experimentando un constante progreso tecnológico, esto supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos. Esta realidad ha originado un debate en torno a la necesidad de distinguir o no los delitos informáticos del resto….

En el Perú, el total de delitos informáticos registrados entre los meses de enero y setiembre 2020 alcanzó 2 mil 512; por trimestre, entre el segundo y tercer trimestre las denuncias se incrementan en 101,9%..........”

(INFORME SEGURIDAD CIUDADANA, 2020)

Barrantes Porras, Carlos Eduardo y Hugo Herrera, Javier Roberto (2012) en su tesis “Diseño e Implementación de un sistema de gestión de seguridad de información en procesos tecnológicos (Perú)”.

En la implementación de un sistema de gestión de seguridad de la información se redujo los riesgos relacionados a los activos de información de los procesos que se encuentran bajo la gerencia de tecnología de Card Perú S.A. que se encontraba en peligro los recursos, servicios y continuidad de los procesos tecnológicos.

Implementaron una política de seguridad de información que, involucrado los procesos de TI, la gestión y monitoreo de los incidentes y vulnerabilidades de seguridad de la información, esto implico los procesos de TI por lo que la seguridad de la información se pudo controlar con la documentación del SGSI.

Ampuero Chang, Carlos Enrique (2011) en su tesis: “Diseño de un Sistema de Gestión de Seguridad de Información para una Compañía de Seguros (Perú)”

Concluye la implementación de un sistema de gestión de seguridad de la información, lo cual esto permitió la gestión en la implementación de controles y procedimientos cumpliendo las normas relacionadas a la gestión de riesgos, gestión de seguridad de información y gestión del negocio, reguladas por la Superintendencia de Banca, Seguros y AFP (SBS), para las entidades financieras, seguros y empresas privadas de sistemas de pensiones.

Las microempresas u organizaciones establezcan entandares, procedimientos, políticas y controles garantizando la protección de su información y la de sus clientes, obteniendo su ventaja competitiva en el mercado, y evitar pérdidas económicas.

Es necesario que el hardware de procesamientos, debe garantizar el perfeccionamiento de los sistemas informáticos en su manipulación física que incluyan un gran criterio de seguridad a la información, resguardando y limitando la exposición de los datos de las personas que dan uso a las tiendas virtuales.

Estos conjuntos de normas, procedimientos y mecanismos de seguridad deben garantizar la integración, confiabilidad y disponibilidad en los sistemas de procesamiento de los datos usados por las personas y las organizaciones.

Para este propósito, la inversión de equipos de cómputos con seguridad, para el uso de las redes en las nubes, para que no vulneren la data de información valiosas para las empresas y que afectan a sus clientes, lo cual es el activo más importante para todas las empresas que optan incursionar en este mundo cibernético con la intensión no dejar de vender y producir.

Tener un software adecuado, con funcionalidad no complicada, con base instructiva y segura, con protección de intrusos o de usuarios que intente vulnerar la información, normas y políticas de seguridad de la información.

**1.2. PLANTEAMIENTO DEL PROBLEMA**

**1.2.1. DESCRIPCION DE LA PROBLEMÁTICA.**

Las empresas que incursionan en estos tiempos en al ámbito de las tecnologías de información, en exclusividad de las microempresas en el ámbito de Lima Metropolitana, ha afrontado riesgos que atentan contra la información crítica para su negocio, la cual es soportada por hardware, software, personas, redes, etc. La necesidad que abarca la utilización de la internet, que no se puede obviar en ninguna empresa, de exponer información al público en general, a sus socios de negocios, fuente de ingresos, en cuenta que esta información día a día va aumentando como una estrategia competitiva de presencia en la red y de rapidez en las negociaciones, esto provoca un mayor grado de exposición y por lo tanto de vulnerabilidades, que enfrenta el responsable de la seguridad de la información en diferentes organizaciones en la gestión de los incidentes de seguridad y sus riesgos.

La situación actual presentada en el mundo, en exclusive en el Perú, por consecuencia de la pandemia del COVID, que afecto a las microempresas en lo concerniente a la tecnología, que afecta el procesamiento y seguridad de la información, por la conectividad remotas improvisadas, esta condición presentada, que no cumplen la seguridad de la información requería, esto afecto el mantenimiento y continuidad de la funcionalidad del negocio y atención comercial.

La viabilidad de las ventas por internet y redes sociales se presentan como una buena alternativa, ante la medida anunciada por el gobierno de prohibir la afluencia de público, pero a estas consecuencias algunas empresas no se encontraron preparadas para afrontarla tecnológicamente.

Esta situación conlleva a la realidad que se encuentra a nivel tecnológico algunas microempresas, al no encontrarse preparados para afrontar situaciones extremas tecnológicamente, a todo esto, también conllevo a la informalidad existente a nivel empresarial. La virtualidad presentada ha sido improvisada, para mantenerse dentro del mercado, que se han tenido que valer en la suspensión perfecta de labores parando su producción y servicios o improvisando plataformas vulnerables, como en la educación actual que hay muchos no han podido ser beneficiados.

Las microempresas y el área educativa del estado y algunos privados, no están previstos de servidores, programas basados en esta virtualidad, seguridad de su información para ser compartida en la nube (internet), a todo esto, la baja y escasa viabilidad de medios informáticos y de telecomunicación de información de data (internet) que no llegan a la gran mayoría.

Al no existir una tecnología adecuada, estos medios tecnológicos improvisados vulneran el medio de seguridad de accesos, esto podría ser vulnerados por hackers, troyanos, etc.; que pueden distorsionar información, comunicación, etc.

Durante los periodos de pandemia (2020 -2021), las microempresas de Lima Metropolitana, que se abocaron a ofertar sus productos, en las nubes (Internet), más en común las empresas del comercio de productos de enseres y alimentos, no consideraron el riesgo que existiría así su clientes o personas que usarían sus plataformas, lo cual esto conllevo a un alto índice delictivo, que genero vulneración y extracción de información y estafas procesados por los ciberdelincuentes.

Las amenazas en el riesgo de la tecnología informática, es la vulneración de la información, que se vio vulnerada por ciberdelincuentes, por la extracción de información (datos personales) de los clientes, la clonación de páginas para la vulnerabilidad de la base de datos. Todo esto, es producto de la imprevisión de equipos informáticos y software, que no avalan la seguridad de la información.

La información y los datos de los clientes, los pagos electrónicos fueron vulnerados, por hackers, que aprovecharon las redes sociales, vulnerando páginas y cuentas, subiendo el grado de delito cibernético en la nube, por la que la base de datos de muchos clientes y cibernautas fueron estafados y vulnerados con sus cuentas de créditos y ahorros, por existir paginas vulnerables, a los hackers, que aprovecharon el alto volumen de compra por estos medios y la poca seguridad de la información de datos que algunas páginas electrónicas ofrecieron durante la confinación social.

**1.2.2. DESCRIPCION DEL PROBLEMA.**

El propósito de esta investigación es gestionar la seguridad de la información y el riesgo vulnerable que existe en las redes de internet si no se cuenta con equipos adecuados y software de seguridad adecuadas, en las ventas de bienes y servicios, que facilita la internet a través de los sistemas tecnológicos, dando a conocer la utilización de este método de compra y venta. Para poder llegar a los clientes con el propósito de tener en cuenta las causas y el perfeccionamiento de este método moderno y qué relación existe entre los clientes del mismo, entre consumidor - empresa y empresa - tecnología.

De esta manera mantener la seguridad de su información dentro de las redes, conllevando a las normas establecidas de seguridad de la información para que estos no sean vulnerados y afecte los negocios establecidos y sus clientes.

**1.2.3. FORMULACION DEL PROBLEMA**

**1.2.3.1.- PROBLEMA GENERAL**

¿En qué medida se relaciona la gestión de la seguridad y riesgo de la información con la prevención de los ataques cibernéticos en los micros empresas y/o PYMES de Lima Metropolitana 2020 - 2021?

**1.2.3.2.- PROBLEMA ESPECIFICO**

¿Cuáles son los problemas de gestión de la seguridad y riesgo de la información en el comercio electrónico de los micros empresas de Lima Metropolitano 2020 - 2021?

¿Cómo prevenir los riesgos y la seguridad de la información de los ataques cibernéticos en las microempresas de Lima Metropolitana 2020 - 2021?

¿Cómo definir normas y aplicar los estándares de seguridad en las microempresas de Lima Metropolitana 2020 - 2021?

**1.3. OBJETIVOS**

**1.3.1. OBJETIVO GENERAL**

Definir la implementación de seguridad de la información para proteger la prevención de los ataques cibernéticos por medio de la gestión de la ciberseguridad y diseñar modelos de seguridad aplicando los estándares y normas de seguridad de la información en diferentes ambientes de empresas pymes y/o microempresas.

**1.3.2. OBJETIVO ESPECIFICO**

- Identificar los riesgos potenciales y amenazas que puedan afectar la seguridad de la información de una organización pymes y/o microempresa para prevenir los ataques cibernéticos.

- Identificar los riesgos y problemas de gestión de la ciberseguridad de la información.

- Definir modelos de normas de seguridad aplicando los estándares y normas ISO para la seguridad de tecnológica de la información.

**1.4. JUSTIFICACION E IMPORTANCIA**

**1.4.1. JUSTIFICACION.**

Las microempresas para ser competitivas dentro del mercado, deberán apuntar a los mercados virtuales con medios de seguridad de la información, plataformas viables para explotar los nuevos mercados con una tecnología adecuada, fiable y puedan mantener a sus clientes potenciales, lo cual le permitiría buscar nuevos mercados y ofertar nuevos productos.

En estos tiempos la tecnología de la información es uno de los recursos considerado lo más importante a nivel empresarial, además en estas épocas de incertidumbre mundial, para mantener el mercado muchas empresas han recurrido a las ventas virtuales, ocasionando vulnerabilidad en la información, aprovechado por delincuentes cibernéticos como los phishing, dedicados a realizar fraudes cibernéticos y entre otras modalidades que hoy se presentan en el ciberespacio.

Los puntos críticos de vulneración han sido la información, los procesos, la seguridad de las bases de datos, etc. Por lo tanto, se tiene que definir diseños e implementación de una plataforma para la gestión de los clientes y proporcionar a las empresas las siguientes ventajas:

- Facilitar los accesos adecuados dando la seguridad de la información y accesos, sin que sean vulnerables a los servicios y/o aplicaciones que estén en la nube.

- La administración adecuada de la infraestructura en la nube por parte de las empresas, debe brindar seguridad, procesamiento de la información adecuada con equipos de hardware y software adecuados, que no sean vulnerables.

- La gestión de procesamiento y seguridad de la información debe efectuarse de manera sencilla y centralizada reduciendo la necesidad de desplegar y entrenar a un gran equipo de operadores y administradores que controlen adecuadamente los accesos y los procesamientos de la información.

- Debe estar orientada a la seguridad de información y al procesamiento de la misma orientada a la utilización de tecnología Web, no requerirá de configuraciones especiales a nivel de los clientes para lograr la gestión de los servidores.

- La disponibilidad de la plataforma, debe de minimizar la pérdida de oportunidades de negocio.

- Se debe prevenir o resolver los problemas presentes o futuros en el área de seguridad de la información y procesamiento de la misma, con base de datos no vulnerables y seguros.

**1.4.2. IMPORTANCIA**

La importancia de mantener una seguridad de la información en los servidores y tener equipos de cómputo que brinden seguridad a los clientes sin que estos no sean afectados en sus cuentas bancarias, tarjetas de créditos y mantener un servicio seguro.

**1.5. ALCANCES Y LIMITACIONES.**

**1.5.1. ALCANCE.**

En el mercado tecnológico existen equipos con alta capacidad de mantener la información respaldad, con seguridad de respuesta oportuna y gestión adecuada. Para mantener la seguridad de los equipos de cómputo se tiene que tener un software adecuado que pueda satisfacer la seguridad de los usuarios finales, con software de antivirus que controle toda la vulnerabilidad existen en la nube, la información almacenada y gestionada es el alto índice activo para una empresa, institución, etc. Por ello se debe gestionar su seguridad y mantenimiento adecuada y seguro.

**1.5.2. LIMITACION.**

La limitación de esta investigación está en la parte interesada de implementar nuevas tecnologías de comercialización tecnológica vía internet, con software y hardware que no vulneren la seguridad y el riesgo de la información.

En estas limitaciones, se afianza la inversión que estaría disponibles de invertir los micros empresas en Lima metropolitana, en la comercialización de servicios y bienes a través de la nube (internet), obteniendo cultura de gestión del conocimiento y herramientas tecnológica para su publicidad, venta y comercialización de sus productos.

Otras de las limitaciones, es la ilegalidad e informalidad que algunas micro empresas trabajan, tanto en la parte de tecnología, usando software y equipos no seguros y vulnerables, con el cual no hay una cultura de inversión y futurismo tecnológico.

**1.5.2.1. DELIMITACION ESPACIAL.**

Esta investigación se realizó en las empresas y micro empresas de Lima Metropolitana, que en estas épocas han decido incursionar en el mundo tecnológico de la Internet, para mantener sus ventas, por condiciones obligadas por la situación presentada.

**1.5.2.2. DELIMITACION TEMPORAL.**

La investigación se realizó desde el año 2020 cuando surgió la condición del COVID19, que impulso a muchos micro empresarios a entrar al mundo tecnológico de la internet, sin ningún asesoramiento técnico, del cual el índice de vulneraciones delictivas en la red aumento.

**2.- MARCO TEORICO**

**2.1. TEORÍAS GENERALES RELACIONADAS CON EL TEMA**

En esta investigación es establecer interés de permitir la evaluación objetiva del posible impacto de los riesgos de seguridad de la información, vulneración de los ataques cibernéticos y sus efectos en la gestión de Información de medianas empresas de Lima Metropolitana.

**DEFINICION**:

La seguridad de la información indica percepción del nivel de protección de los sistemas informáticos, es decir que está libre de todo peligro, daño o riesgo.

Un ataque cibernético es la acción delictiva y malintencionada que se ocasiona al realizar acceder a información privada, bien para apropiarse de ella o bien para inutilizarla y pedir dinero a cambio de liberarla.

En la ley 30096 de delito informáticos en su en su capítulo DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS dentro de los siguientes artículos:

Artículo 2: “El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad ………”.

Artículo 3: “El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos ……”.

**CONTROL DE RIESGO DE LA INFORMACION**.

Es el riesgo es representación errónea, que no sea prevenida o detectada y corregida oportunamente por los sistemas informáticos.

Estos riesgos generan un robo, manejo inadecuado o divulgación prohibida de la información sistemática de la empresa. Se encuentran los siguientes riesgos a tomar en cuenta:

- Hurto y divulgación de la información privada de una empresa

- Hurto y divulgación de información personal de los trabajadores de la empresa.

- Hurto y divulgación de información personal de los clientes de la empresa.

- Hurto de identificaciones autorizadas a la empresa.

- Intromisiones a las redes privadas contra servicios de Internet vitales para las operaciones de la empresa.

**OPERATIVIDAD DE LOS ATAQUES CIBERNETICOS:**

Estos ataques son producidos cuando la vulnerabilidad o debilidad en el software o en el hardware son detectados por delincuentes o personas que se valen de esta circunstancia para obtener beneficios, por lo general, es de índole económicos. Esto causan un efecto negativo en la seguridad de los sistemas comprometidos, derivándose de los activos de la organización.

Los daños que provocan son:

– Daños menores: son tipo de virus que borran algunos programas, pero que sólo bastará con volver a instalarlos, ya que el daño no es grave.

– Daños moderados: Se produce cuando los virus formatean un disco duro y sobrescriben el mismo. En este caso, se puede reinstalar el sistema operativo y utilizar el último backup, lo que debería tomar horas de restituirlo.

– Daños mayores: Son virus que pueden pasar completamente desapercibidos y generar daños profundos, que ni siquiera pueden repararse con el backup.

– Daños severos: Cuando un virus realiza cambios mínimos y que son progresivos, el usuario no tiene mayor idea cuando los datos son correctos o han sido modificados.

**CIBERSEGURIDAD:**

Es el conjunto de procedimientos, normas y herramientas que se aplican para proteger la información generada y procesada por los sistemas electrónicos. En la practica es salvaguardar las computadoras, los servidores, los sistemas electrónicos, las redes y los datos de ataques maliciosos, más comúnmente conocido como seguridad de tecnología de la información o seguridad de la información electrónica.

Esta estará encargada de proteger la integridad de la infraestructura computacional, protección de los archivos o datos, con el objetivo de evitar que todo tipo de amenazas que puedan poner en riesgo la información que reside almacenada en cualquier dispositivo.

**IMPLEMENTACION DE UN SISTEMA DE SEGURIDAD DE LA INFORMACION**.

La Norma ISO 27001 ofrece la seguridad de la información basándose en un método de evolución y tratamiento del riesgo, proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Las medidas de seguridad se van a implementar por lo general en forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos), la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales necesarias para prevenir violaciones de la seguridad, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, antivirus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

* Identificando el sus activos y responsables
* La vulnerabilidad de los activos las debilidades susceptibilidad de sufrir ataques y daños
* Identificar las amenazas que puedan dañar la información por virus y ataques cibernéticos
* Identificar las condiciones legales como obligaciones con sus clientes, usuarios, etc.
* Identificar los riesgos y las probabilidades de amenazas que puedan afectar y dañar la información
* Planificar el tratamiento del riesgo definiendo políticas de riesgos en función de los puntos anteriores y de la política definida por la dirección seleccionando los controles adecuados para cada riesgo de asumir, reducir, eliminar y transferir el riesgo.

**3. HIPÓTESIS Y OPERACIONALIZACIÓN DE LAS VARIABLES**

**3.1. HIPOTESIS GENERAL**

Mediante la instalación una plataforma de comercio electrónico, se tendrá que evaluar la transacción electrónica entre las personas y una empresa comercial u de otro rubro de ventas de bienes y servicios, para garantizar la privacidad e integridad de la información, evitando riesgos y posibles ataques cibernéticos a la información.

Los protocolos, equipos y codificaciones adecuadas, que aseguren la confiabilidad y seguridad de los comercios electrónicos, que en futuro sea un elemento de ventas y comercialización de éxito para las microempresas.

La seguridad debe basarse en las normas ISO TEC 27001, que establece el mecanismo adecuado para controlar los riesgos que se presenten en el uso de los sistemas de información.

**3.2. HIPOTESIS ESPECCIFICAS**

- Determinar los riesgos potenciales y amenazas que puedan afectar la seguridad de la información de una organización pymes y/o microempresa para prevenir los ataques cibernéticos.

- Determinar los riesgos y problemas de gestión de la ciberseguridad de la información.

- Determinar aplicación de los modelos de normas de seguridad aplicando los estándares y normas ISO para la seguridad de tecnológica de la información.

**3.3. VARIABLES**

**3.3.1. VARIABLES INDEPENDIENTES**

Riesgo de la seguridad:

**3.3.2. VARIABLES INTERVEN**IENTE

Modelos de normas de seguridad aplicando los estándares y normas ISO

**3.3.3. VARIABLES DEPENDIENTE**

Ciberseguridad

**3.3.4. OPERACIONALIDAD DE LAS VARIABLES**

|  |  |  |  |
| --- | --- | --- | --- |
| **VARIABLE** | **DEFINICION CONCEPTUAL** | **DIMENSIONES** | **INDCADORES** |
| RIESGO DE LA SEGURIDAD | Controlar la seguridad de la información | Medir la seguridad de la información | Políticas de seguridad que se debe conocer y aplicar |
| Política de seguridad | Medios determinantes de política de seguridad de comunicación |
| verificación de las medidas de seguridad |
| Determinar la evaluación interna |
| Ciberseguridad | Conjunto de software y hardware que dan soporte al procesamiento y almacenamiento de datos | La seguridad de los sistemas de procesamiento, transmisión y almacenamiento de datos | La configuración de seguridad de los equipos de almacenamientos de datos |
| Evaluar la seguridad de los sistemas de información de procesamientos de datos |
| Seguridad de los sistemas de comunicación |
|  |  |  | La confidencialidad en el acceso a la información por quienes estén autorizados. |
| aplicación de los modelos de normas de seguridad aplicando los estándares y normas ISO | Es una norma internacional que permite la seguridad, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. | El modelo ISO consta de las dimensiones de La confidencialidad, la disponibilidad, La integridad. | La disponibilidad al acceso de la información y a los sistemas que procesan la misma de parte de los usuarios autorizados cuando lo requieran. |
|  |  |  | La integridad es el mantenimiento exacto de la información y sus métodos de proceso. |

**3.4. TIPO**

Tipo de Investigación: APLICADA

Nivel de Investigación: Descriptivo Interpretativo.

El tipo de investigación que se desarrollará es de tipo APLICADA y el nivel de investigación es de tipo descriptivo e interpretativo, porque trataremos de demostrar la vulnerabilidad de riesgo de la información que existe tecnológicamente en el internet y la negoción electrónica.

**3.5. POBLACION**

Para el estudio se ha considerado una muestra de 50 micros empresas del total que existe en Lima metropolitana.

**3.6. UNIVERSO SOCIAL**

Microempresas de Lima Metropolitano.

**3.7. MUESTRA**

Para definir el tamaño de la muestra se ha utilizado el método probabilístico y aplicado la formula generalmente aceptada para poblaciones menores de 100000.



Donde:

N Es el tamaño de la muestra que se va a tomar en cuenta para el trabajo de campo. Es la variable que se desea determinar.

Pyq Representan la probabilidad de la población de estar o no incluidas en la muestra. De acuerdo a la doctrina, cuando no se conoce esta probabilidad por estudios estadísticos, se asume que p y q tienen el valor de 0.5 cada uno.

Z Representa las unidades de desviación estándar que en la curva normal definen una probabilidad de error= 0.05, lo que equivale a un intervalo de confianza del 95 % en la estimación de la muestra, por tanto, el valor Z = 1.96

N El total de la población. Este caso 50 personas, considerando solamente aquellas que pueden facilitar información valiosa para la investigación.

EE Representa el error estándar de la estimación, de acuerdo a la doctrina, debe ser 9.99% o menos. En este caso se ha tomado 5.00%.

Sustituyendo:



n = 50

**4. METODO**

**4.1. DISEÑO DE INVESTIGACION**

Se opta por una investigación aplicada, buscando la generación de conocimiento directo a los problemas del uso de la internet en las micro empresas, basándonos en el fundamentalmente de los problemas presentados en la parte tecnológica dentro de la investigación básica, ocupándose del proceso de enlace entre la teoría y el producto.

**4.2. ESTRATEGIA DE PRUEBA DE HIPOTESIS**

Se realiza la prueba bajo la recolección de datos bajo las fuentes teóricas y de observación usando el proceso probalistico, científico a la investigación descriptiva e interpretativa.

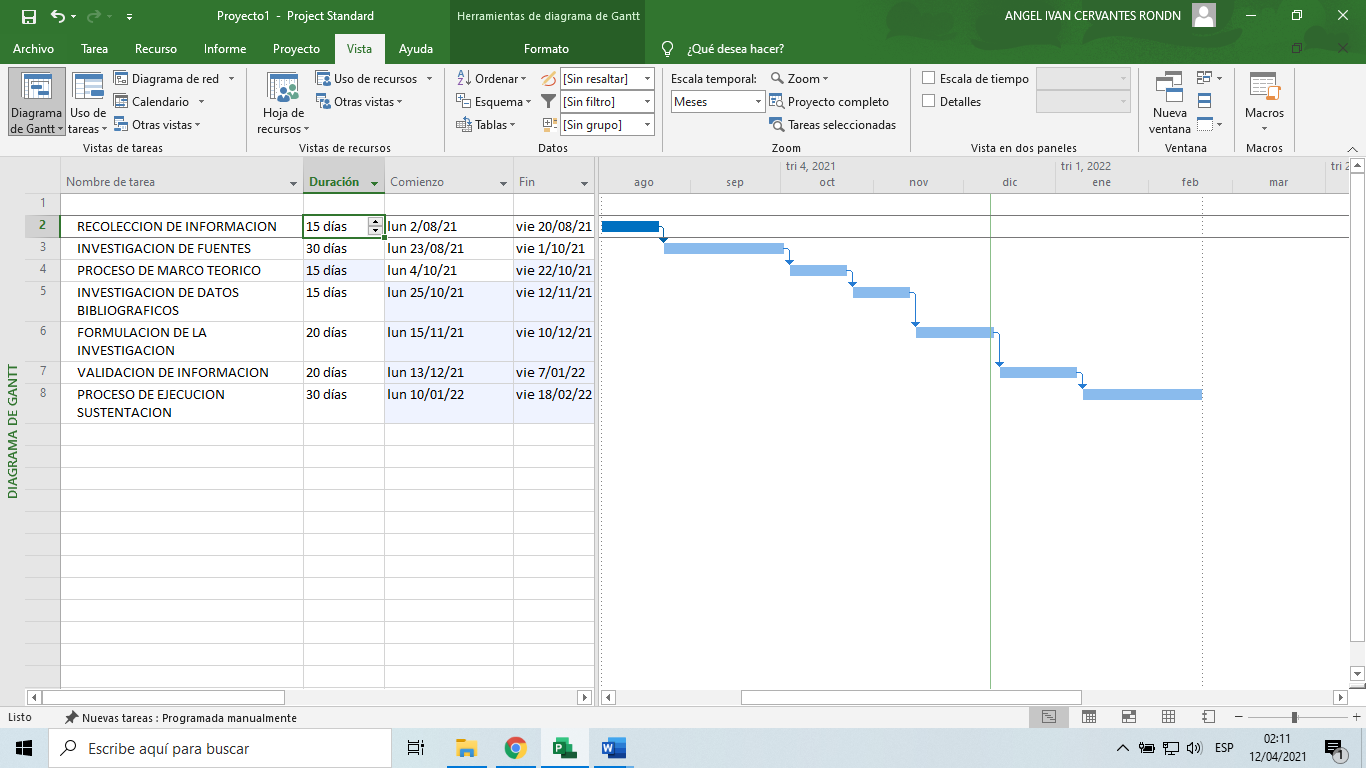
**4.3. TECNICAS DE RECOLECCION DE DATOS**

**4.3.1. INSTRUMENTOS DE RECOLECCION DE DATOS**

El procedimiento y técnicas para la recolección de datos, se basará en el uso de documentos obtenidos de las fuentes teóricas para poder ampliar el conocimiento y teorías que podrían ser de utilidad para la elaboración de la investigación que tengan relación con el objeto de estudio o problemática que se aborda en esta investigación.

De forma que se procederá a usar una técnica de observación indirecta, ya que se van a usar documentos, de modo que se van a analizar las teorías y las fuentes teóricas de forma cualitativa, por lo que no aplica el uso de encuestas ni de cuestionarios, en tanto que se trata de una investigación de tipo documental.

**5. CRONOGRAMA**



**6. PRESUPUESTO.**

Inversión de la investigación: 6500 soles

La variante de instalación del Proyecto de inversión de equipos es variante de acuerdo a lo requerido y cuanto valor agregado desea llegar en un comercio electrónico, como base se estima una inversión aproximada de 25000 dólares.

**7. REFERENCIAS BIBLIOGRAFICAS.**

# **BIBLIOGRAFÍA**

Fundación Telefónica.

Ciberseguridad, la protección de la información en un mundo digital,

Edición, 2016, España.

INEI

LIMA METROPOLITANA ENCUESTA DE OPINIÓN SOBRE EL IMPACTO DEL COVID-19 EN LAS EMPRESAS

Edición 2020, Lima Perú.

ISOTOOLS EXCELLENCE

La norma ISO 27001: Aspectos claves de su diseño e implantación

Banco Interamericano de Desarrollo

CIBERSEGURIDAD RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE

Edición 2020

Análisis y Gestión de Riesgos en los Sistemas de Información

J. Sánchez y otros. Departamento de Publicaciones, EUI-UPM.

Edición 2011.

**ANEXOS**

**MATRIZ DE CONSISTENCIA**

IMPLEMENTAR LA SEGURIDAD DE LA INFORMACION CONTRA RIESGOS DE ATAQUES CIBERNETICOS Y LA CIBERSEGURIDAD EN LAS PYMES Y MICOEMPRESAS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PROBLEMA | OBJETIVO | HIPOTESIS | VARIABLES | METODOS |
| PROBLEMA GENERAL | | | | |
| ¿En qué medida se relaciona la gestión de la seguridad y riesgo de la información con la prevención de los ataques cibernéticos en los micros empresas y/o PYMES de Lima Metropolitana 2020 - 2021? | Definir la implementación de herramientas tecnológicas para la gestión de incidentes de seguridad, procesamiento y control de la información en diferentes ambientes de la tecnología de la información (TI) de una determina empresa o microempresa. | la instalación una plataforma de comercio electrónico, evaluar la transacción electrónica entre las personas y una empresa comercial u de otro rubro de ventas de bienes y servicios, para garantizar la privacidad e integridad de la Información, evitando riesgos y posibles ataques cibernéticos a la información. | Riesgo de comunicación y tratamiento de la información | Tipo de investigación Aplicada |
| PROBLEMA ESPECÍFICO | | | | |
| ¿Cuáles son los problemas de gestión de la seguridad y riesgo de la información en el comercio electrónico de los micros empresas de Lima Metropolitano 2020 - 2021? | Evaluar las causas de los riesgos y ataques en la seguridad de la información | Definir los riesgos potenciales y amenazas que puedan afectar la seguridad de la información de una organización para prevenir los ataques cibernéticos. | Riesgos de seguridad de la información | Investigación aplicada |
| ¿Cómo prevenir los riesgos y la seguridad de la información de los ataques cibernéticos en las microempresas de Lima Metropolitana 2020 - 2021? | Gestionar la seguridad de los activos y la información contra los ataques y amenazas cibernéticos | Determinar los riesgos y problemas de gestión de la ciberseguridad de la información. | Ciberseguridad | Investigación aplicada |
| ¿Cómo definir normas y aplicar los estándares de seguridad en las microempresas de Lima Metropolitana 2020 - 2021? | Definir las políticas y normas de seguridad de la información | Determinar aplicación de los modelos de normas de seguridad aplicando los estándares y normas ISO para la seguridad de tecnológica de la información. | Modelos de normas de seguridad | Investigación aplicada |

**GLOSARIO**

**Internet**

Es un sistema de redes interconectadas mediante distintos protocolos que ofrece una gran diversidad de servicios y recursos.

**Ciberataques**

Es un conjunto de acciones ofensivas contra sistemas de información, estos pueden ser bases de datos, redes informáticas, etc. El objetivo es dañar, alterar o destruir organizaciones o personas. Además, pueden anular los servicios que prestan, robar datos o usarlos para espiar

**Hackers**

Es un individuo (persona) que tiene un alto grado de conocimiento de los sistemas y programas informáticos, y utiliza ese conocimiento para manipular de alguna manera esa tecnología, entonces un hacker con sombrero negro lo hace para robar algo valioso o por alguna otra razón maliciosa.

**Ecommerce**

Es el intercambio de productos o servicios usando redes computacionales, específicamente Internet

**comercio electrónico**

Se trata de la venta de servicios o productos a través de medios electrónicos actuales como páginas web, redes sociales o tiendas online.

**Troyanos**

Se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado

**Cibernautas**

Es la persona que usa lo servicios informáticos del ciberespacio Internet

**Cibernético**

Todo lo relacionado con la tecnología computacional interdisciplinaria usada para la extensión de las capacidades humanas

**servidores.**

Es un sistema que proporciona recursos, datos, servicios o programas a otros ordenadores, conocidos como clientes, a través de una red. En teoría, se consideran servidores aquellos ordenadores que comparten recursos con máquinas cliente.

**Backup**

Es una copia de seguridad o el proceso de copia de seguridad, que se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.

**Cortafuegos**

Es un sistema de seguridad para bloquear accesos no autorizados a un ordenador mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados.

**Antivirus**

Es un software o programa que se instala en una computadora, para cumplir con la función de actuar contra códigos o programas maliciosos

**Virus informático**

Es un sistema de software dañino, escrito intencionadamente para entrar en una computadora sin permiso o conocimiento del usuario. Tiene la capacidad de replicarse a sí mismo, continuando así su propagación.