**UNIVERSIDAD NACIONAL “SAN LUIS GONZAGA DE ICA”**

FACULTAD DE INGENIERIA DE SISTEMAS



TESIS:

“SEGURIDAD DE LA INFORMACION Y PREVENCIÓN DE LOS ATAQUES CIBERNÉTICOS EN LAS PYMES DEL PERÚ”

TESIS PARA OBTENER EL BACHILLER DE: INGENIERIA DE SISTEMAS

AUTORES:

AGUILAR OYOLO YORDI

MIREYA MANDUJANO BENDEZU

ASESOR: ING. EDGAR PEÑA CASAS.

ICA – PERÚ

2019

**Contenido**

[**INTRODUCCIÓN** 2](#_Toc10477150)

[**CAPITULO I: EL PROBLEMA OBJETIVOS E HIPOTESIS** 2](#_Toc10477151)

[1.1 El problema de investigación: 2](#_Toc10477152)

[**1 .1.1 Situación problemática** 2](#_Toc10477153)

[**1 .1.2 Formulación** **del problema** 2](#_Toc10477154)

[**1 .1.3 Delimitación del problema** 2](#_Toc10477155)

[1.2 JUSTIFICACIÓN E IMPORTANCIA 2](#_Toc10477156)

[1.3 OBJETIVO 2](#_Toc10477157)

[**CAPITULO II: MARCO TEORICO** 2](#_Toc10477158)

[2.1. Antecedentes 2](#_Toc10477159)

[**2.1.1 Antecedentes Nacionales** 2](#_Toc10477160)

[**2.1.2 Antecedentes Internacionales** 2](#_Toc10477161)

[2.2 Bases Teóricas 2](#_Toc10477162)

[2.3 Marco Conceptual 2](#_Toc10477163)

[3.1) Tipo nivel y diseño de la investigación 2](#_Toc10477164)

[**Tipo de investigación:** 2](#_Toc10477165)

[**Nivel de investigación:** 2](#_Toc10477166)

[**Diseño de investigacion:** 2](#_Toc10477167)

# **INTRODUCCIÓN**

Se estima que los ataques cibernéticos están en crecimiento, no solo a nivel nacional sino también a escala mundial, la empresa de seguridad RSA security calcula $9100 millones de dólares en pérdidas solo por el pichinga (Páginas web falsas clonadas) y un estudio realizado por el FBI calcula que el ramsonware (Secuestro de información) origino $2300 millones de daños causados solo en los últimos tres años a nivel mundial.

Debemos destacar que el descuido humano es una de las principales causas de ataques cibernéticos. Podríamos pensar que aún hay gran parte de la población adulta que no está familiarizada con la tecnología y mucho menos con herramientas digitales de protección frente a los ciberataques, pero no solo preocupa la población adulta, se calcula que el 86% de la población mundial entre 25 y 34 años son usuarios de Smartphone, y 94% de estos usuarios utiliza la banca en línea. Es evidente que prefieren realizar sus actividades bancarias sin ir al banco. Solamente en Estados Unidos 44% de los usuarios y han sido víctimas del cibercrimen, un 31% comparte sus contraseñas y credenciales de acceso a su cuenta bancaria ,por ultimo un 84% pone en riesgo sus cuentas al conectarse desde redes wifi públicos. (carlos, 2018)

Aun se cree que quienes realizan estos ciberataques actúan solos, pero se sabe que actúan en grupos de 6 a más personas. Gente especializada en el cibercrimen, organizaciones del cibercrimen nacionales e internacionales, incluso existen jerarquías y ciberataques planeados estratégicamente en conjunto.

Diariamente ocurren millones de ataques a persona u organizaciones, empresas públicas o privadas. Solo una pequeña fracción de estos ataques tienen éxito. Se estima que solo en Latinoamérica se realiza un ataque cada 12 segundos, aproximadamente 1100000 ciberataques por día. Un estudio realizado por Intel Security calculo que en promedio se generan 20 incidentes de seguridad en una organización en tan solo un día.

El cibercrimen es uno de los delitos más rentables, triplicando al narcotráfico y va en aumento, es por ello el motivo de este trabajo de investigación para prevenir los ciberataques en las pymes del Perú y saber responder a estos de una manera efectiva.

# **CAPITULO I: EL PROBLEMA OBJETIVOS E HIPOTESIS**

## El problema de investigación:

### 1 .1.1 **Situación problemática**

Los ciberataques aprovechan las vulnerabilidades, asociadas a los dispositivos informáticos, al software o a las personas que lo utilizan y lo administran.

Las estadísticas muestran que el cibercrimen esta por encima de los robos físicos, hablamos de millones de dólares. Y no es un delito cometido por pocos sino mas bien por organizaciones criminales que están creciendo considerablemente.

Dentro del cibercrimen a escala global o nacional los más desfavorecidos son las PYMES, las pequeñas y medianas empresas, debido a que sus medidas de seguridad no son los suficientemente robustas o peor aun ni siquiera cuenta con sistemas de protección ante un eventual ataque cibernético y este es el principal problema.

Actualmente en el Perú se registra 500 robos diarios de información afectando un total de 70 millones de clientes y generando pérdidas de 135 millones de dólares en el 2017 teniendo un aumento del 18% en de ataques durante el 2018 elevando el monto a 160 millones, siendo estas cifras considerables que dejan a vista la falta de prevención ante ciberataques por parte de las pymes.

Se tiene que tomar en cuenta que un ciberataque genera perdidas económicas elevadas , los hackers realizan el robo de información de cuentas privadas de las empresas y documentos internos que detallan los movimientos financieros de la empresa.

### 1 .1.2 Formulación **del problema**

**PROBLEMA GENERAL:**

**P:G:**¿En que medida la seguridad de la información influye en la prevención de ataques cibernéticos en las pymes del Perú?

**PROBLEMAS ESPECIFICOS:**

¿En que medida la seguridad de la información influye a las empresas pymes del Perú la protección de información?

¿En que medida la prevención de ataques informáticos en las pymes del Perú influye a evaluar los riesgos y amenazas que presentan las empresas?

### 1 .1.3 Delimitación **del problema**

1. **Delimitación Espacial:**

Esta presente tesis de investigación para la obtención de bachiller profesional, va a contener una delimitación espacial que comprende la seguridad de la información y prevención de los ataques cibernéticos en las pymes del Perú 2018b.

1. **Delimitación Temporal:**

La delimitación temporal que abarcara esta presente tesis de investigación se desarrollara a partir del mes de abril en el cual se ha iniciado el proyecto de tesis y culmina a fines de junio.

En el cual abarca todos los aspectos y los puntos mencionados por nuestro asesor de tesis y el plan de estudios.

1. **Delimitación Social:**

En la presente tesis de investigación se encuentran involucrados los siguientes participantes:

-Asesor: Ing. Edgar Peña Casas.

-Los autores de la presente tesis: Aguilar Oyolo Yordi

Mandujano Bendezu mireya

1. **Delimitación Conceptual:**

En la presente tesis de investigación comprende dos variables: La seguridad de la información y prevención ataques cibernéticos en las pymes 2018.

## **1.2 JUSTIFICACIÓN E IMPORTANCIA**

Justificación:

Con la presenta investigación se buscar lograr la prevención de ataques cibernético mediante la identificación de riesgos o agujeros de seguridad de los sistemas informáticos usados por las pymes.

Importancia:

El siguiente proyecto es importante porque permite detectar las vulnerabilidades en las empresas antes el desarrollo evolutivo de los ataques cibernéticos. Además de proporcionar las medidas a tomar en cuenta frente a un ataque cibernético, puesto que ninguna empresa por mas sistemas de protección que tenga está 100% seguro frente a los delitos informáticos realizados por cibercriminales.

## **1.3 OBJETIVO**

**OBJETIVO GENERAL:**

**O.G:**¿En que medida la seguridad de la información permite la prevención de ataques cibernéticos en las pymes del Perú ?

**OBJETIVOS ESPECIFICOS:**

¿En que medida la seguridad de la información permite a las empresas pymes del Perú la protección de información?

¿En que medida la prevención de ataques informáticos en las pymes del Perú permite evaluar los riesgos y amenazas que presentan las empresas?

# **CAPITULO II: MARCO TEORICO**

## **2.1. Antecedentes**

### **2.1.1 Antecedentes Nacionales**

**ANTONIO INOGUCHI ROJAS ,ERIKA LIZET MACHA MORENO.**

**“GESTIÓN DE LA CIBERSEGURIDAD Y PREVENCIÓN DE LOS ATAQUES CIBERNÉTICOS EN LAS PYMES DEL PERÚ, 2016”. Lima – Perú (2017)**

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.

**DANIEL IVÁN TAIPE DOMÍNGUEZ**

**“LA AUDITORÍA DE SEGURIDAD INFORMÁTICA Y SU RELACIÓN EN LA**

**CIBERSEGURIDAD DE LA FUERZA AÉREA DEL PERÚ AÑO 2017.”**

El desarrollo de la presente investigación tuvo como objetivo analizar cómo el realizar una Auditoria de Seguridad Informática tiene implicancia en la Ciberseguridad en la Fuerza Aérea del Perú; desde luego el estudio lo que pretende es generar aportes que contribuyan a la solución de la problemática que se presenta en este sector; En cuanto a la metodología utilizada, se puede señalar que ha sido de tipo descriptiva según Bernal y otros (2000), diseño no experimental descriptiva correlacional, según Hernández y otros (2014); para la recogida de datos se aplicó dos cuestionarios, uno sobre Auditoria de seguridad informática y el otro sobre la implicancia en la Ciberseguridad de la Fuerza Aérea del Perú año 2017., que fue desarrollado por el Personal Militar de la Fuerza Aérea del Perú. En lo que refiere a los resultados se puede señalar que los encuestados manifiestan que el realizar una Auditoria de seguridad informática no tiene implicancia en la Ciberseguridad de la Fuerza Aérea del Perú año 2017. Lo que demuestra que el nivel de conocimiento del personal de Informática, las normas y políticas no tiene un buen nivel de Ciberseguridad.

**BARRANTES PORRAS CARLOS EDUARDO, HUGO HERRERA JAVIER ROBERTO LIMA-PERÚ “DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN DE PROCESOS TECNOLÓGICOS” (2012)**

El propósito del trabajo se centro en la implementación de un sistema de gestión de seguridad de información (SGSI), bajo una metodología de análisis y evaluación de riesgos desarrollada y diseñada por autores de este trabajo, también se usaron como referencias las NORMAS ISO 27001:2005 E ISO17799:2005

El la implementación permitió un aumento de seguridad de los activos de la información de la empresa CARD PERU S.A, que garantiza que los riesgos de seguridad de información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistematiza, estructurada, repetible, eficiente y adaptables ante los cambios que produzcan en los riesgos, el entorno y las tecnologías.

**JORGE LUIS ABANTO GARNIQUE**

**“LA DESPROTECCIÓN DE LOS DATOS PERSONALES DE LOS CIBERNAUTAS PERUANOS, EXPUESTOS A CÓDIGO MALICIOSO Y SU INCIDENCIA EN LA VULNERACIÓN AL DERECHO A LA INTIMIDAD”CHINCHA(2012)**

La investigación gira en torno a uno de los derechos constitucionales, más relevantes como es el derecho a la intimidad, que está integrado por dos . aspectos: el primero correspondería al derecho que tiene todo ser humano a disponer de momentos de soledad, recogimiento y quietud que le permitan replegarse sobre sí mismo, meditar, orar, abrirse a la contemplación tanto exterior como interior; el segundo aspecto se traduciría en el derecho de mantener fuera del conocimiento ajeno hechos o actos que pertenecen a lo privado de una persona.

Al analizar los elementos que integran el concepto del derecho a la vida privada, encontramos que no solo se trata del control de la información de hechos reservados de nuestra vida, sino también de los derechos a la tranquilidad, a la paz, a la soledad, a que ninguna persona se inmiscuya o fisgonee, respecto a los actos de la vida privada.

En este contexto, es conveniente destacar, la presencia en estos últimos años de un accionar ilícito a través, en el mundo informático, donde los cibernautas se ven expuestos a un conjunto de amenazas informáticas, que pueden atentar contra su información, en este caso datos de alta relevancia y trascendencia como son los que pertenecen a la vida privada.

### **2.1.2 Antecedentes Internacionales**

**ENRIQUE JAVIER SANTIAGO, JESÚS SÁNCHEZ ALLENDE**

**“RIESGOS DE CIBERSEGURIDAD EN LAS EMPRESAS EN LAS EMPRESAS” MADRID(2017)**

En este artículo se abordan los principales riesgos de seguridad al que están expuestas las empresas del siglo XXI con enfoque descriptivo. Se afronta el riesgo a partir de la relevancia que tienen los activos de información para las organizaciones, se describen los efectos de la tecno dependencia si no se salvaguardan los recursos, el concepto de riesgo y el rol que tienen las vulnerabilidades y las amenazas en la probabilidad de materialización de los incidentes de seguridad como también el impacto que tiene en las organizaciones el compromiso de los activos de información.

Se relacionan también las principales amenazas que afectan el riesgo en las empresas de diferentes sectores. Y se recopilarán una relación de técnicas de ataque empleadas por hackers de sombrero negro para comprometer los activos de información digital de las organizaciones. Se hace una reseña de las amenazas actuales que hoy en día afectan a la seguridad de la información, la recopilación del estado del arte del riesgo al que se exponen las empresas y las tendencias a las que apunta el mercado que pudieron ser identificadas a partir de las fuentes de referencia.

## **2.2 Bases Teóricas**

**Ataques Cibernéticos de Países:** 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.

**Ataques Cibernéticos de Empresas Privadas:** 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.

**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 internetmasivas, 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 deinternet conocida como el under-ground, que básicamente es una red donde no se puede rastrear con facilidad de que país o localidad estas conectado.

**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 seles pude señalar como espía infiltrado por un Estado enemigo de otro, tambiénhay casos de empleados de la organización que son cautivados y contratados por bandas de terroristas o cibercriminales.

## **2.3 Marco Conceptual**

**Procesos Estratégicos:** son aquellos que involucran la toma de decisiones, se definen metas, se asignan recursos, precisan presupuestos y detallan la programación.

**Procesos de soporte o administrativos:** son los que soportan el resto de procesos a través de la gestión de recursos humanos, materiales y financierosentre los cuales se encuentran: facturación, contabilidad general, cuentas por cobrar y pagar, rotación de inventarios, entre otros.

**Procesos productivos o misionales:** son aquellos que permiten la investigación desarrollo de productos, transformación de los bienes o servicios, orientados a la satisfacer una necesidad, dentro de los cuales encontramos información de alta importancia para la organización como lo son las bases de datos de clientes, catálogos de productos, políticas de precios, campañas de marketing (estrategia comercial), información de proveedores, escalas de negociación (términos descuentos), acuerdos de prestación de servicios.

**Las amenazas no tradicionales:** son las que involucran tanto actores estatales, como no estatales; son de carácter asimétrico; no requieren obligatoriamente de una acción militar; sin embargo, exponen al estado, sus instituciones y la infraestructura pública y privada; en este punto se ubican las Pymes.

**CAPITULO III: METODOLOGIA DE INVESTIGACION**

## **3.1) Tipo nivel y diseño de la investigación**

### **Tipo de investigación:**

Según el tipo de investigación tradicional la presente investigación es de tipo aplicada, porque esta centrada en encontrar mecanismos o estrategias que permitan lograr un objetivo concreto. A través de la presente investigación se buscó explicar la relación de la Seguridad de información con la prevención de ataques cibernéticos.

### **Nivel de investigación:**

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 la investigación es identificar los sistemas de información que brinden apoyo en la prevención de ataques cibernéticos.

### **Diseño de investigación:**

Para el diseño de la presente tesis de investigación, implementaremos una Investigación pre-Experimental. El cual se ocupa de la orientación dirigida a los procesos y desarrollos de las Pymes en el Perú para mejorar los sistemas de y protocolos de seguridad a través de herramientas tecnológicas para la ciberseguridad.

## **3.2) POBLACION Y MUESTRA**

### **Población:**

La población está conformada por las Pymes del Perú, que a 2018 suman 2 millones 332 mil 218 pymes a nivel nacional. Superando en un 7,1% al año anterior.Las empresas que mayor actividad económica registraron fueron el comercio al pormenor (10661), seguidos de los servicios de comida y bebidas (4521), continua el comercio al por mayor (2 mil 920) otros servicios (2 mil 916), servicios prestados a empresas (2 mil 546) y transporte y almacenamiento (1 mil 855).

### **Muestra:**

Tomaremos como muestra el último estudio realizado por Optical Network (Compañía peruana de Telecomunicaciones) quien mediante un estudio un total de 265 empresas peruanas, revelo que el 70% de las empresas no realizan un diagnostico adecuado sobre vulnerabilidad de sus sistemas informáticos, dedican solo entre 10 y 20% de su presupuesto en tecnologías de información para protegerse del cibercrimen, creando un alto riesgo de convertirse en victimas de ciberataque.

**BIBLIOGRAFIA**

Cavsi. (2019). *http://www.cavsi.com/preguntasrespuestas/que-es-pyme/*.

Concepto.de. (2019). *https://concepto.de/entrevista/#ixzz5os3KJ9lg*.

CONCEPTODEDEFINICION.DE. (2019). *https://conceptodefinicion.de/pymes/*.

Definicion. (2019). *https://definicion.mx/pymes/*.

HUAMANI, E. N. (2017). *DISEÑO E IMPLEMENTACION DE UN SISTEMA DE GESTION DOCUMENTAL DIGITAL PARA UNA INSTITUCION FINANCIERA.* UNIVERSIDAD NACIONAL SAN LUIS GONSAGA DE ICA, TESIS PARA OPTAR EL GRADO DE INGENIERO DE SISTEMAS, ICA -PERU.

InformaticaMilenium. (2019). *https://www.informaticamilenium.com.mx/es/temas/que-es-internet.html*.

Kyocera. (2019). *https://smarterworkspaces.kyocera.es/blog/la-gestion-documental-definicion-conceptos-clave-e-importancia-en-la-actualidad/*.

MasAdelante. (2019). *https://www.masadelante.com/faqs/intranet*.

Monografias. (2019). *https://www.monografias.com/trabajos87/analisis-contenido-como-herramienta-investigacion/analisis-contenido-como-herramienta-investigacion.shtml*.

MPIUA. (2019). *http://mpiua.invid.udl.cat/observacion-de-campo/*.

Oberta, U. (2019). *https://www.uoc.edu/portal/es/arxiu/gestio-documental/que-es/index.html*.

Tecnologías-Información. (2019). *https://www.tecnologias-informacion.com/modeladodatos.html*.

TicPortal. (2019). *https://www.ticportal.es/temas/sistema-gestion-documental/que-es-sistema-gestion-documental*.

Wikipedia. (2019). *https://es.wikipedia.org/wiki/Documento*.