

# **Universidad de las Fuerzas Armadas ESPE**

*Departamento de Ciencias Humanas y Sociales.*

*Metodología de la investigación.*

*Tema: Sistemas de Protección de Información*

*Título: Seguridad En Los Sistemas De Información  
con las tecnologías disponibles en 2019 y de alcance  
público.*

**AUTOR:**

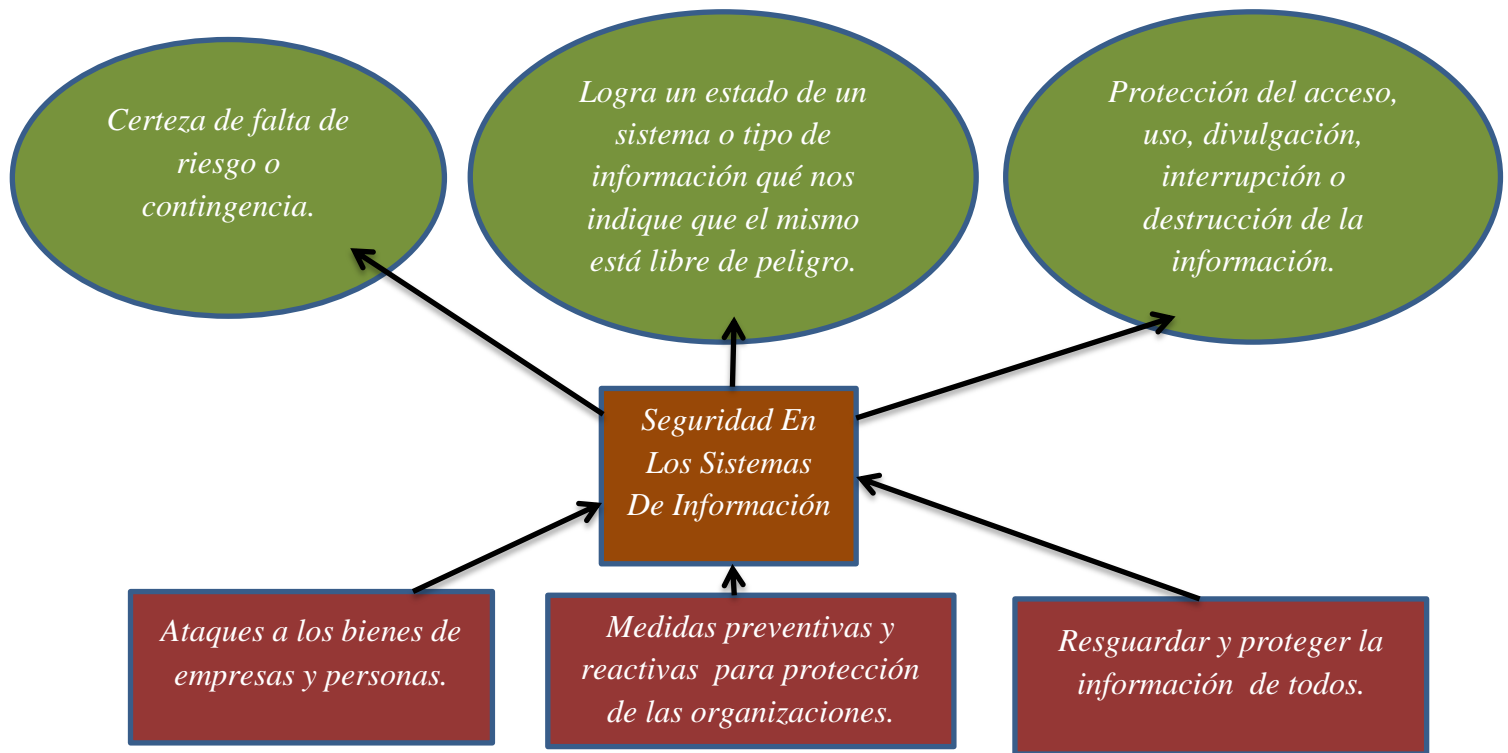
*Brandon Dillan Osejo Cuesta*

**QUITO –ECUADOR 2019**

**NRC: 2509**

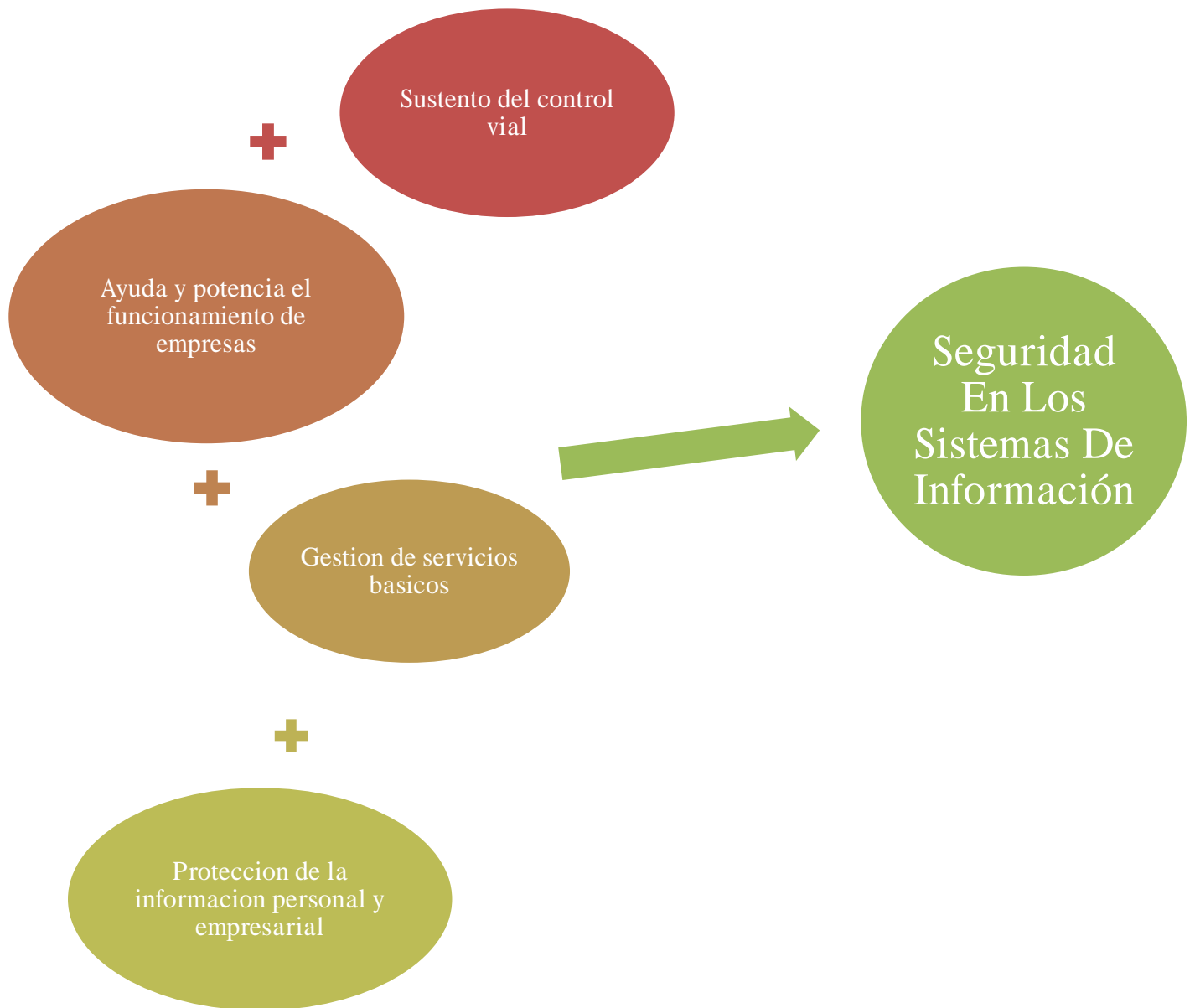
## Capítulo 1

### 1.1 Planteamiento del problema (árbol de problemas)



### 1.2 Formulación del problema de investigación

*¿Cómo funciona la seguridad en los sistemas de información? (Método holográfico)*



### **1.2.1 Sub Preguntas y Sub Problemas**

*¿Quién tiene acceso a la información?*

*¿Por qué es importante proteger la información?*

*¿La seguridad puede modificar la información?*

*¿Qué tan asequible es la información?*

*--¿Cuáles son los dispositivos más vulnerables en su seguridad?*

### **1.3.1 Objetivo General**

*Mantener un ambiente razonablemente seguro, que permita determinar la importancia de un sistema de seguridad, proteger los activos de información, así como el uso adecuado de los recursos y gestión del riesgo, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información y el aseguramiento de la continuidad de cualquier ente.*

### **1.3.2 Objetivos Específicos**

- *Proteger los activos de información, con base en los criterios de confidencialidad, integridad y disponibilidad.*
- *Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.*
- *Monitorear el cumplimiento de los requisitos de seguridad de la información.*
- *Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información*

## **1.4 Justificación e Importancia**

*Que la información que se encuentre, esté resguardada bajo unas buenas medidas de seguridad. En la Seguridad de la Información el objetivo de la protección son los datos mismos y trata de evitar su pérdida y modificación non-autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos. En el caso de la Protección de Datos, el objetivo de la protección no son los datos en si mismo, sino el contenido de la información sobre personas, para evitar el abuso de esta.*

### **Referencias webgrafia**

<https://www.obs-edu.com/int/blog-investigacion/sistemas/>

<https://www.youtube.com/watch?v=m7bnF7XkqnU>

<https://protejete.wordpress.com/gdr>

## Capítulo 2

### 2.1 Antecedentes (Estado del Arte)

Nº	Título/Tema	Autor/es	Conclusiones
1	SEGURIDAD EN INFORMÁTICA (AUDITORÍA DE SISTEMAS)	LUIS DANIEL ALVAREZ BASALDÚA	Actualmente, las organizaciones modernas que operan o centran gran parte de su actividad en el negocio a través de Internet necesitan dotar sus sistemas e infraestructuras informáticas de las políticas y medidas de protección más adecuadas que garanticen el continuo desarrollo y sostenibilidad de sus actividades; en este sentido, cobra especial importancia el hecho de que puedan contar con profesionales especializados en las nuevas tecnologías de seguridad que implementen y gestionen de manera eficaz sus sistemas.
2	ANÁLISIS Y EVALUACIÓN DE PARÁMETROS DE CALIDAD EN SERVICIOS CLOUD COMPUTING EN EL ECUADOR	YESSENIA PAULINA RELICA RELICA	Se concluye que el proveedor debe garantizar la seguridad y la integridad de la información, para prevenir futuras pérdidas de datos de los clientes, y asegurar que el proveedor que brinde este servicio tenga la certificación iso/cei 27001

### 2.2 Fundamentación teórica (Epistemología)

#### Tema 1. Seguridad Informática

##### 1.1 Privacidad y Operatividad

##### 1.2 Herramientas básicas utilizadas en seguridad informática

###### 1.2.1 Antivirus

###### 1.2.2 Backup

###### 1.2.3 Control de acceso

###### 1.2.4 Otros

##### 1.3 Sugerencias que pueden ayudar

##### 1.4 Privacidad de la Información

### 2.4 Variables de Investigación

Calidad de seguridad

Tipo de información

Vulnerabilidad de dispositivos

## 2.5 Operacionalización de las Variables

Variables	Definición conceptual	Dimensiones o categorías	Indicadores	Instrumentos
<b>Calidad de seguridad</b>	<i>La calidad y la seguridad de los datos son dos cualidades esenciales en la estrategia de gestión de datos de cualquier compañía. Por lo que es fundamental dotar los datos de estas dos propiedades desde incluso la fase preliminar de implantación de un sistema de gestión de datos.</i>	<i>Calidad funcional en el campo.</i>  <i>Calidad funcional en la base</i>  <i>Calidad de salida en la base</i>	<i>Estabilidad del servicio.</i>  <i>Resultado del servicios adquirido</i>  <i>Protección de los bienes informáticos</i>	<i>Encuestas</i>  <i>Entrevistas</i>  <i>pruebas</i>
<b>Tipo de información</b>	<p><i>Los sistemas de información manejan el flujo y mantienen la información que utiliza la empresa en su día a día para sus diferentes operaciones y están formados por varios componentes: personas, hardware, software, redes, procedimientos y datos.</i></p> <p><i>Los tipos de sistemas de la información más populares pueden clasificarse de la siguiente forma:</i></p> <ul style="list-style-type: none"> <li>• <b>Sistemas de procesamiento de transacciones</b></li> <li>• <b>Sistemas de control de procesos de negocio</b></li> <li>• <b>Sistemas de colaboración empresarial</b></li> <li>• <b>Sistemas de Información de Gestión</b></li> <li>• <b>Sistemas de apoyo a la toma de decisiones</b></li> <li>• <b>Sistemas de Información Ejecutiva</b></li> </ul>	<i>Clasificación de datos</i>  <i>Filtros de información</i>  <i>Calidad del servicio</i>	<i>Hay mejoría en el majeo de información</i>  <i>Se clasifica eficazmente los procesos</i>  <i>rapidez en los trabajos</i>	<i>Validación de información</i>  <i>Filtración de datos</i>  <i>Cuestionarios</i>

<b>Vulnerabilidad de dispositivos</b>	<i>La vulnerabilidad del dispositivo hace referencia al hardware y software del equipo al que se aplique un sistema y sus debilidades para proteger la información de agentes externos.</i>	<i>Plataforma de trabajo</i>	<i>Conservación de datos.</i>	<i>Pruebas</i>
		<i>Sistema operativo</i>	<i>Incidencia de fallos.</i>	<i>Testeo</i>
		<i>Seguridad actual</i>	<i>Aumento de la seguridad</i>	<i>Revisión</i>

## 2.6 Definiciones Conceptuales

*Informática: Conjunto de conocimientos técnicos que se ocupan del tratamiento automático de la información por medio de computadoras.*

*Antivirus: [programa] Que detecta la presencia de un virus informático en un disquete o en una computadora y lo elimina.*

*Backup: 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.*

*Vulnerable: Que puede ser vulnerado o dañado física o moralmente*

*Los verbos testar y **testear** son adecuados para la acción de 'someter algo a una prueba o control'*





