



MAESTRÍA EN SOFTWARE PROYECTO DE TITULACIÓN II

SEMANA III: EL MÉTODO CIENTÍFICO DISEÑO DE LA INVESTIGACIÓN.

Compilación: Walter Fuertes Díaz, PhD

Motivación

2

- **Este capítulo le permitirá:**
 - ▣ Conocer la importancia del Diseño de la Investigación;
 - ▣ Definir los enfoques cuantitativo y cualitativo de la investigación;
 - ▣ Definir cuál es el tipo de diseño más apropiado para la investigación: experimental, no experimental o múltiple;
 - ▣ Analizar cuáles son los tipos, métodos y estrategias de Investigación en Ingeniería de Software;
 - ▣ Ensamblar esta información en el diseño de investigación de su proyecto de titulación.



¿Si la investigación es un conjunto de procesos sistemáticos, críticos y empíricos que se aplican al estudio de un fenómeno o problema, entonces cuál es la importancia del **Diseño de la investigación?**

Contenido

3

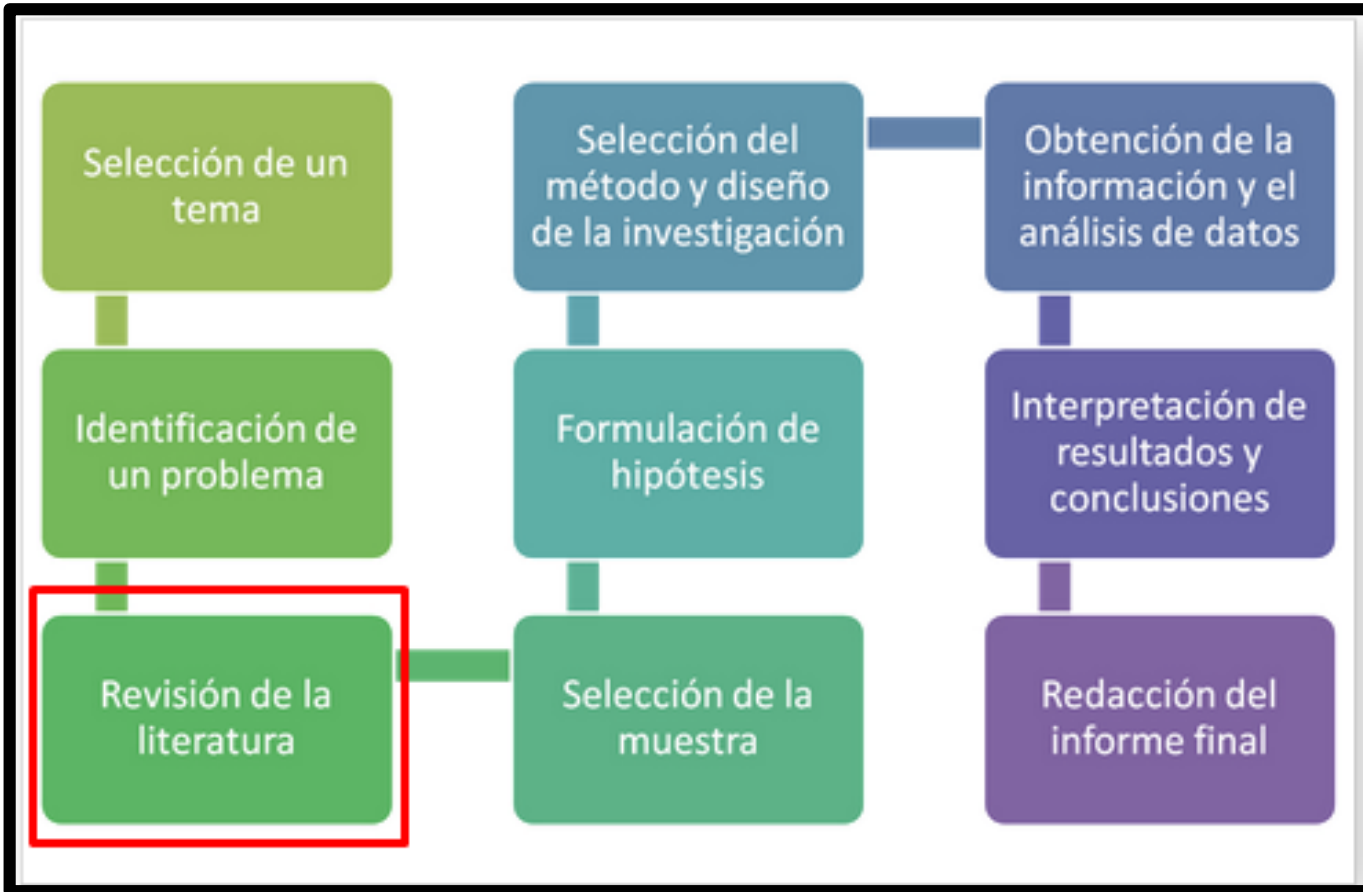
- Fundamentación
- El Método científico
 - ▣ Formulación del Problema
 - ▣ Análisis de la Literatura
 - ▣ Formulación de la Hipótesis
 - ▣ Diseño Experimental
 - ▣ Análisis de Resultados, verificación y validación
 - ▣ Elaboración del Reporte de Investigación
- Bibliografía

Diseño de la Investigación

- *El diseño de investigación se define como los métodos y técnicas elegidos por un investigador para combinarlos de una manera razonablemente lógica para que el problema de la investigación sea manejado de manera eficiente.
- **El diseño de la investigación representa el punto donde se conectan las etapas conceptuales del proceso de investigación como el planteamiento del problema, el desarrollo de la perspectiva teórica y las hipótesis con las fases subsecuentes cuyo carácter es más operativo.



Diseño de la Investigación



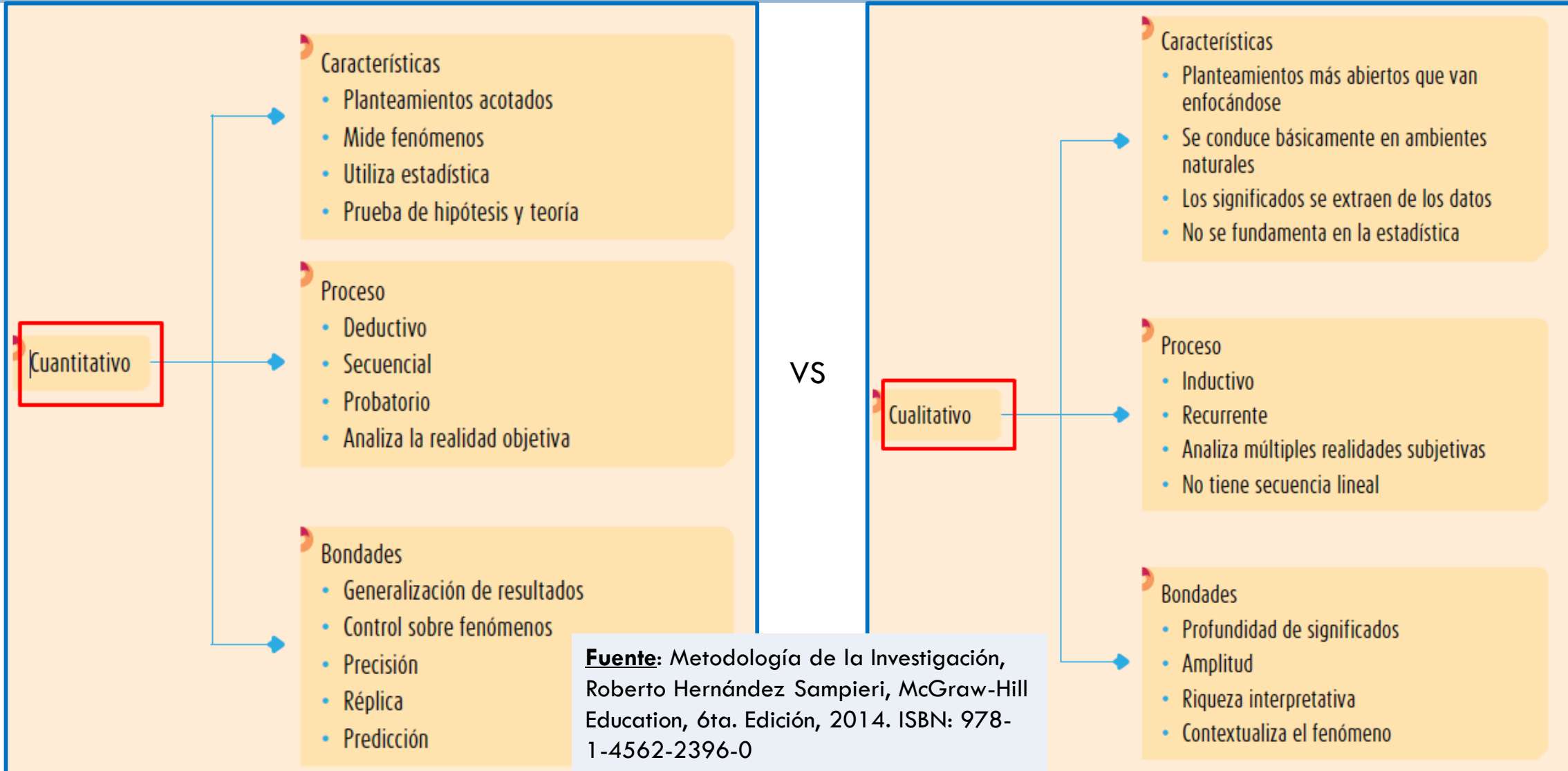
Fases de la Investigación e innovación educativa y su relación con el Método Científico

- **Etapas principales del diseño de investigación:**
 - ▣ Recolección;
 - ▣ Medición; y
 - ▣ Análisis de datos.
- **Diseño de Investigación cuantitativa:**

Utiliza la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico, con el fin establecer pautas de comportamiento y probar teorías.
- **Diseño de Investigación cualitativo:**

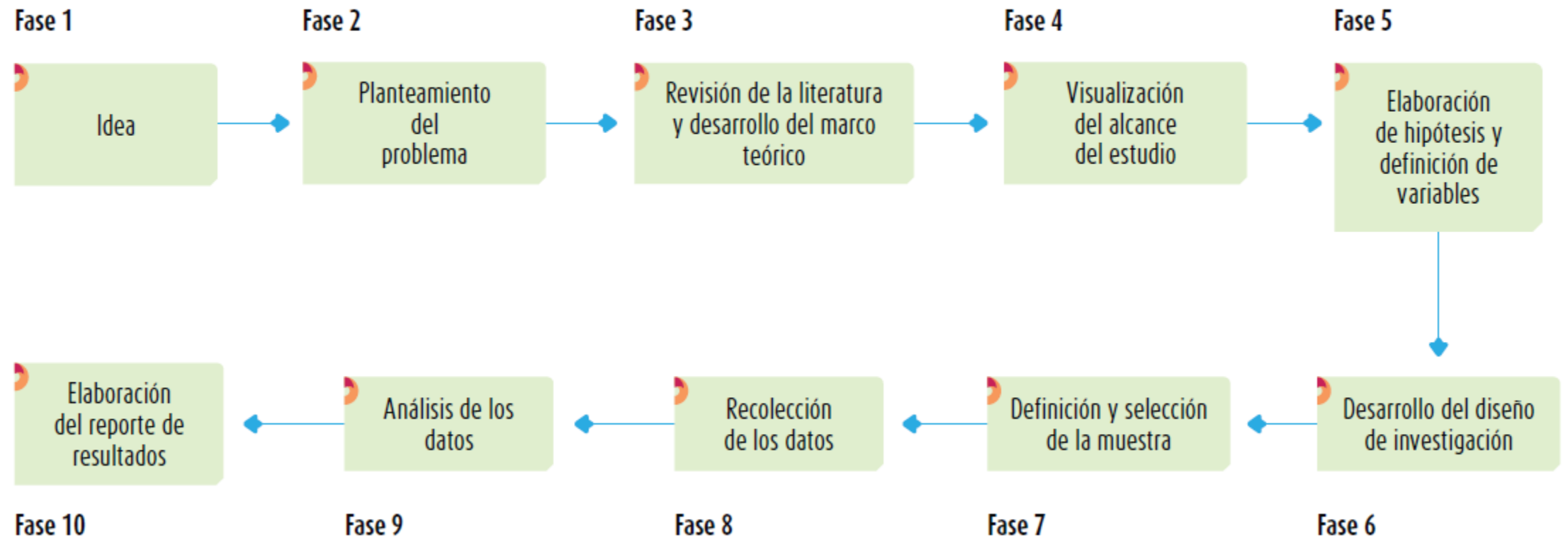
Propone evaluar, ponderar e interpretar información obtenida a través de recursos como entrevistas, conversaciones, registros, memorias, entre otros, con el propósito de indagar en su significado profundo..

Investigación Cuantitativa vs Cualitativa



Investigación Cuantitativa vs Cualitativa

Figura 1.1 Proceso cuantitativo.



Investigación Cuantitativa vs Cualitativa

- La definición de investigación es válida tanto para el enfoque **cuantitativo** como para el **cualitativo**;
- Ambos constituyen un proceso general que, a su vez, integra diversos procesos.
- El proceso cuantitativo es secuencial y probatorio. Cada etapa precede a la siguiente y no podemos “brincar” o eludir pasos, aunque desde luego, es factible redefinir alguna fase;
- El proceso cualitativo es “en espiral” o circular, en el sentido de que las etapas interactúan y no siguen una secuencia rigurosa.

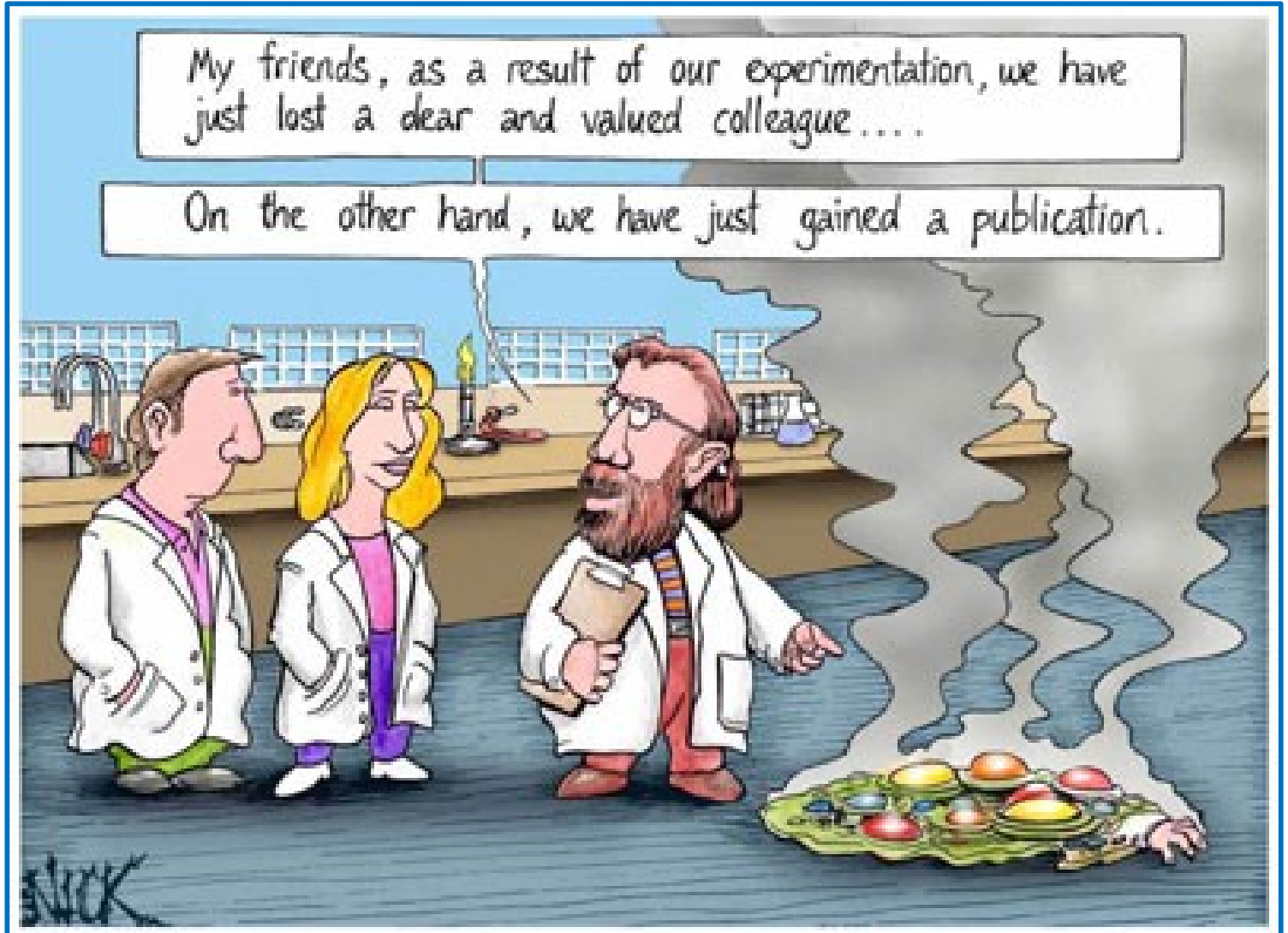


Diseño de la Investigación

10

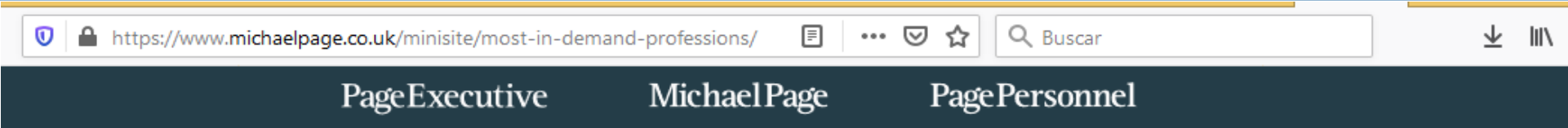
Ingeniería de software:

Es la aplicación de un enfoque sistemático, disciplinado y **cuantificable** para el diseño, desarrollo, operación y mantenimiento de software y el estudio de estos enfoques; es decir, la aplicación de la ingeniería al software



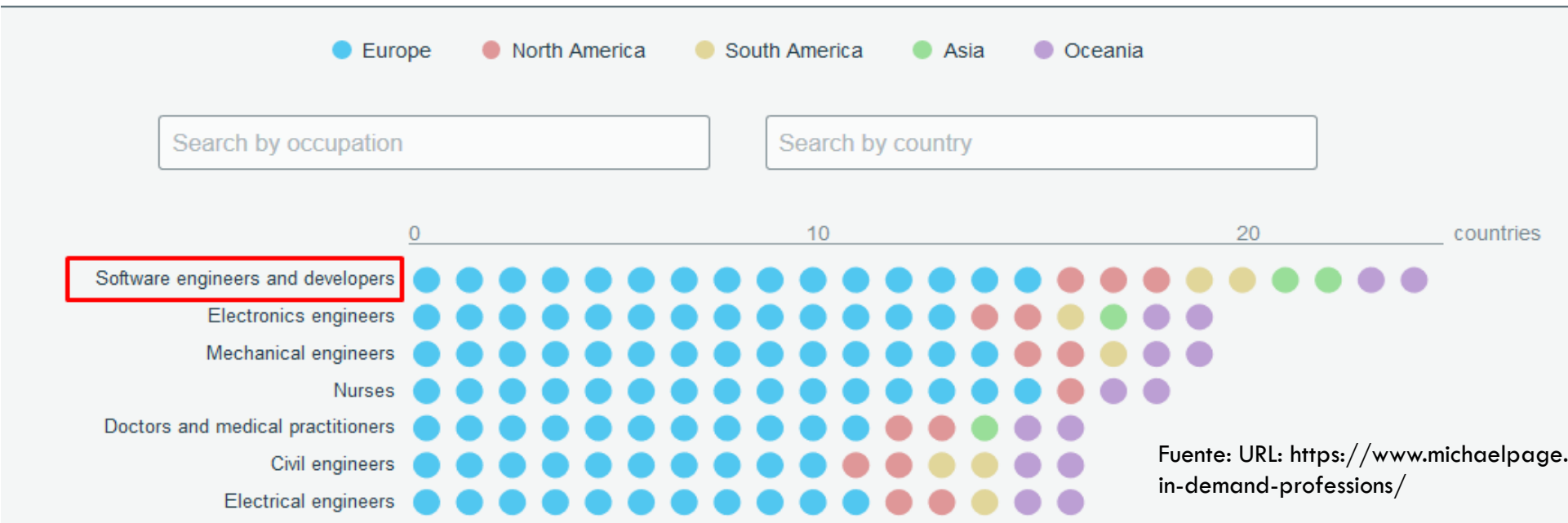
The World's Most In Demand Professions

11



THE WORLD'S MOST IN DEMAND PROFESSIONS

Across the developed countries of the world, skilled professionals are in high demand. Software engineers are needed in 24 countries, nurses are needed in 18, while 11 countries report a shortage of accountants. Explore the chart below to see which occupations are most in demand across the world and discover which skills are needed.



Actividad de Aprendizaje

¿Cómo se escriben los resultados de investigación en Ingeniería de Software?

Actividad de Aprendizaje:

Tema: Análisis de Artículos técnicos-científicos relacionados con investigación en Ingeniería de Software.

Writing Good Software Engineering Research Papers Minitutorial

Mary Shaw
Carnegie Mellon University
mary.shaw@cs.cmu.edu

Abstract

Software engineering researchers solve problems of several different kinds. To do so, they produce several different kinds of results, and they should develop appropriate evidence to validate these results. They often report their research in conference papers. I analyzed the abstracts of research papers submitted to ICSE 2002 in order to identify the types of research reported in the submitted and accepted papers, and I observed the program committee discussions about which papers to accept. This report presents the research paradigms of the papers, common concerns of the program committee, and statistics on success rates. This information should help researchers design better research projects and write papers that present their results to best advantage.

- What concrete evidence shows that your result satisfies your claim?

If you answer these questions clearly, you'll probably communicate your result well. If in addition your result represents an interesting, sound, and significant contribution to our knowledge of software engineering, you'll have a good chance of getting it accepted for publication in a conference or journal.

Other fields of science and engineering have well-established research paradigms. For example, the experimental model of physics and the double-blind studies of medicines are understood, at least in broad outline, not only by the research community but also by the public at large. In addition to providing guidance for the design of research in a discipline, these paradigms establish the norms of scientific disciplines through a

Se pide:

- ▣ Dividir el aula en 4 grupos de estudiantes.
- ▣ Designar un coordinador por equipo;
- ▣ Descargarse el artículo titulado:
 - Shaw, Mary. "Writing good software engineering research papers." *25th International Conference on Software Engineering, 2003. Proceedings.. IEEE, 2003.*
- ▣ Repartirse las secciones para su lectura comprensiva, análisis e interpretación, grupo a grupo.
- ▣ Cada grupo debe exponer durante el desarrollo de la clase mediante una presentación en Power-Point de máximo 5 slides (exceptuando carátula y referencia bibliográfica), el resumen, análisis y síntesis de su apartado. El maestrante que exponga, primero deberá presentar a su equipo.
- ▣ Al finalizar, un maestrante debe compilar y dar un único formato a la presentación con todas las exposiciones y luego remitir a todos los compañeros.

Diseño de la Investigación

13

- ❑ **Elementos básicos de una buena investigación:**
 - ❑ **Evidencia empírica:** observación y experimentos son repetibles, y puede ser experimentada por otros en la misma circunstancias experimentales.
 - ❑ **Razonamiento lógico:** una habilidad que permite la determinación de la verdad a través de una secuencia de pasos que están separados de emocional y de esperanza.
 - ❑ **Escepticismo:** una actitud que ayuda a evitar el autoengaño y el engaño con otros.

Research
Design
Qualitative
&
Quantitative
Approaches
John W. Creswell

Diseño de la Investigación

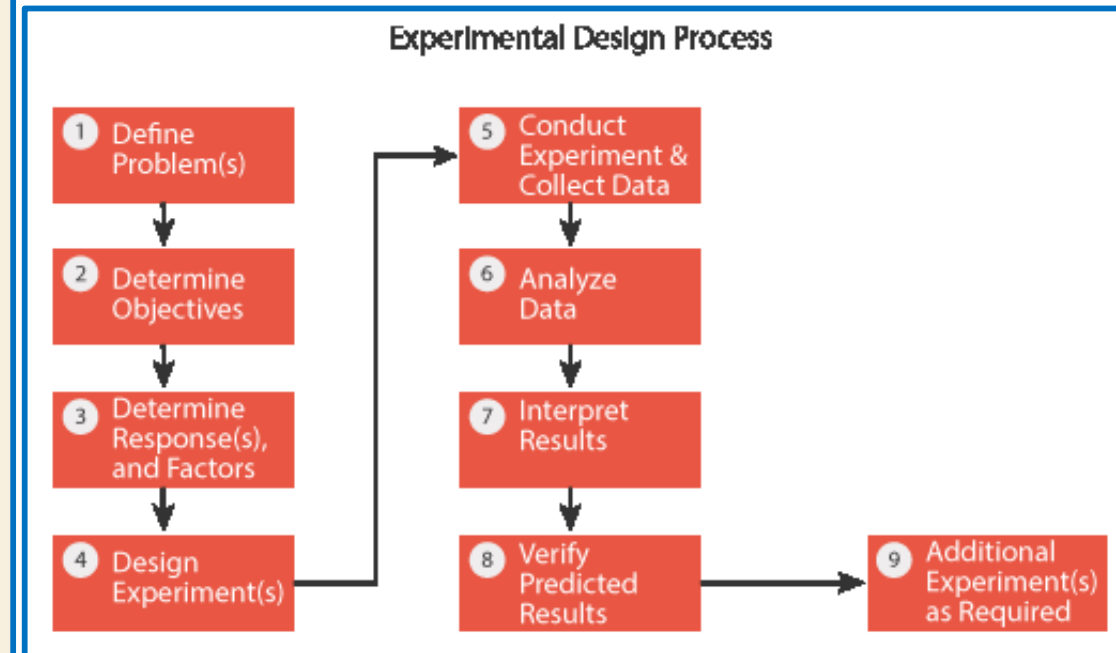
- Una vez realizada la parte conceptual de la investigación (Formulación del Problema, Análisis de la Literatura, y Formulación de la Hipótesis) el investigador debe visualizar la manera práctica y concreta de contestar las preguntas de investigación, que significa cumplir con los objetivos fijados;
- Esto implica seleccionar o desarrollar uno o más diseños de investigación y aplicarlos al contexto particular de su estudio;
- El término **diseño** se refiere al plan o estrategia concebida para obtener la información que se desea con el fin de responder al planteamiento del problema;
- En el enfoque cuantitativo, el investigador utiliza sus diseños para analizar la certeza de las hipótesis formuladas en un contexto en particular o para aportar evidencias respecto de los lineamientos de la investigación;
- En el enfoque cuantitativo, la calidad de una investigación se relaciona con el grado en que apliquemos el diseño tal como fue concebido;
- En el enfoque cuantitativo puede aplicar la investigación experimental e investigación no experimental.

Diseño de la Investigación

15

□ Diseño Experimental

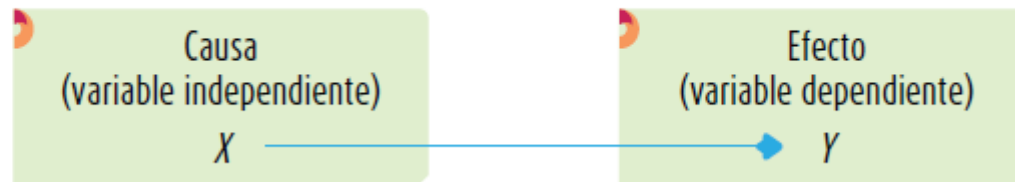
- Un experimento tiene como propósito evaluar o examinar los efectos que se manifiestan en la variable dependiente cuando se introduce la variable independiente, es decir, se trata de probar una relación causal.
- Montgomery (1993) define literalmente el experimento como “... una prueba o ensayo,” en la que es posible manipular deliberadamente una o más variables independientes para observar los cambios en la variable dependiente en una situación o contexto estrictamente controlado por el investigador.
- El diseño de investigación se puede entender como el desarrollo de un plan o estrategia que especifica las acciones y medios de control que se efectuarán para alcanzar los objetivos del experimento, responder a las preguntas de investigación y someter a contrastación las hipótesis



Diseño Experimental

- “En un sentido científico, se refiere a un estudio en el que se manipulan intencionalmente una o más variables independientes (supuestas causas antecedentes), para analizar las consecuencias que la manipulación tiene sobre una o más variables dependientes (supuestos efectos consecuentes), dentro de una situación de control para el investigador (Fleiss, 2013; O’Brien, 2009 y Green, 2003).
- Es decir, los diseños experimentales se utilizan cuando el investigador pretende establecer el posible efecto de una causa que se manipula.”

Figura 7.1 Esquema de experimento y variables.



Diseño Experimental

- El primer requisito es la manipulación intencional de una o más variables independientes. La variable independiente es la que se considera como supuesta causa en una relación entre variables, es la condición antecedente, y al efecto provocado por dicha causa se le denomina variable dependiente (consecuente).
- Cabe destacar que el investigador puede incluir en su estudio dos o más variables independientes o dependientes.
- Cuando en realidad existe una relación causal entre una variable independiente y una dependiente, al variar intencionalmente la primera, la segunda también variará.
- Ejemplo, si la **motivación** es causa de la **productividad**, al variar la motivación deberá variar la productividad.

La variable dependiente se mide

La variable dependiente no se manipula, sino que se mide para ver el efecto que la manipulación de la variable independiente tiene en ella.

Diseño Experimental



**Empirical Research:
Definition,
Methods, Types
and Examples**



Content Index

1. Empirical research: Definition
2. Empirical research: Origin
3. Types and methodologies of empirical research
 - 3.1 . Quantitative research methods
 - 3.2 . Qualitative research methods
6. Steps for conducting empirical research
7. Empirical research methodology cycle
8. Advantages of Empirical research
9. Disadvantages of Empirical research
10. Why is there a need for empirical research?

Diseño Experimental

- **“Pasos de un experimento:** A continuación mencionamos los principales pasos que se dan en el desarrollo de un experimento:
 - ▣ **Paso 1:** Decidir cuántas variables independientes y dependientes deberán incluirse. Deben incluirse las variables que sean necesarias para probar las hipótesis, alcanzar los objetivos y responder las preguntas de investigación.
 - ▣ **Paso 2:** Elegir los niveles o modalidades de manipulación de las variables independientes y traducirlos en tratamientos experimentales.
 - ▣ **Paso 3:** Desarrollar el instrumento o instrumentos para medir las variables dependientes.
 - ▣ **Paso 4:** Seleccionar una muestra de casos o personas del tipo o perfil que nos interesa.
 - ▣ **Paso 6:** Seleccionar el diseño experimental o cuasi-experimental apropiado para nuestras hipótesis, objetivos y preguntas de investigación.
 - ▣ **Paso 7:** Planear cómo vamos a manejar los casos o a los participantes. Con personas, elaborar una ruta crítica sobre qué van a hacer desde que llegan al lugar del experimento hasta que se retiran.
 - ▣ **Paso 8:** En el caso de experimentos “puros”, dividirlos al azar o emparejarlos; y en el caso de cuasi-experimentos, analizar cuidadosamente las propiedades de los grupos intactos.
 - ▣ **Paso 9:** Aplicar las pre-pruebas (cuando las haya), los tratamientos y las pos-pruebas.”

Diseños no experimentales

- “Podría definirse como la investigación que se realiza sin manipular deliberadamente variables.
- Es decir, se trata de estudios en los que **no** hacemos variar en forma intencional las variables independientes para ver su efecto sobre otras variables.
- Lo que se hace en la **investigación no experimental** es observar fenómenos tal como se dan en su contexto natural, para analizarlos (The SAGE Glossary of the Social and Behavioral Sciences, 2009b).
- En la investigación no experimental las variables independientes ocurren y no es posible manipularlas, no se tiene control directo sobre dichas variables ni se puede influir en ellas, porque ya sucedieron, al igual que sus efectos.
- La investigación no experimental es un paraguas de varios estudios cuantitativos, como las encuestas de opinión, los estudios ex post-facto retrospectivos y prospectivos, etc”

Investigación Bibliográfica

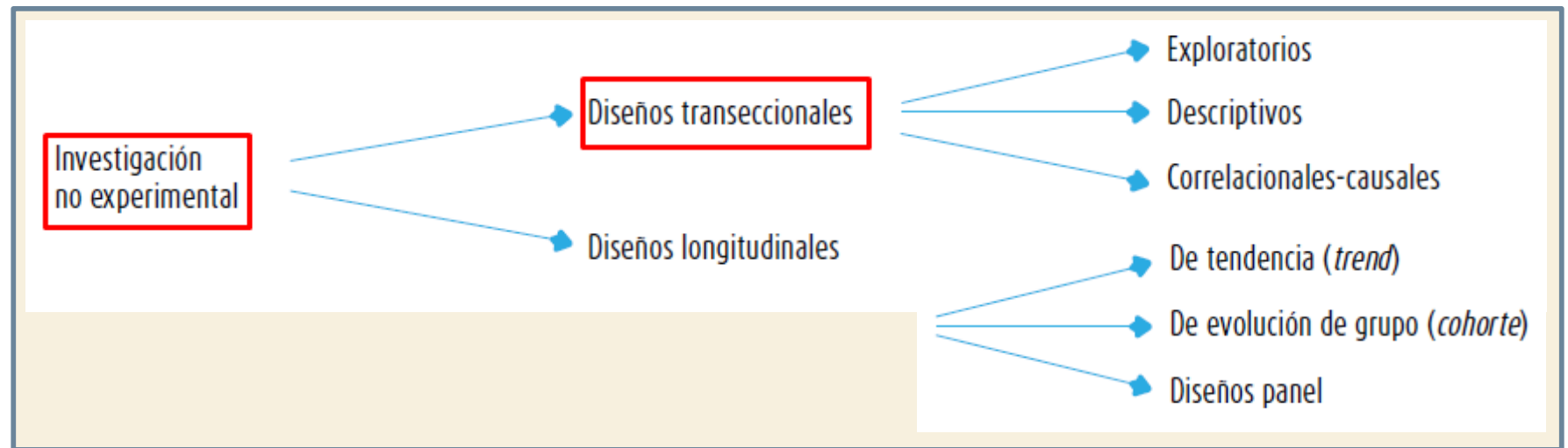
Básico de las investigaciones documentales, ya que a través de la revisión del material documental de manera sistemática, rigurosa y profunda se elija el análisis de diferentes fenómenos o a la determinación de la relación entre variables.

Diseños no experimentales

□ Ejemplo no científico

Experimento	Hacer enojar intencionalmente a una persona y ver sus reacciones.
No experimento	Ver las reacciones de esa persona cuando llega enojada.

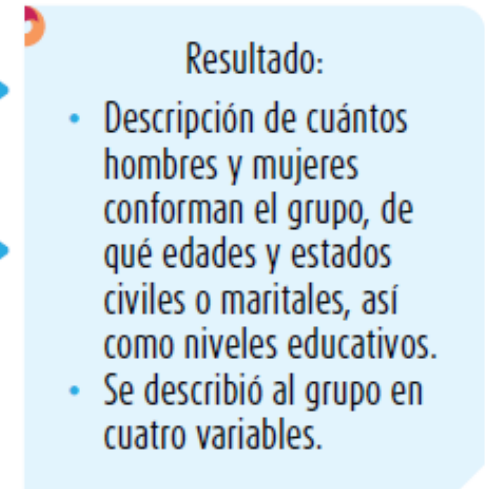
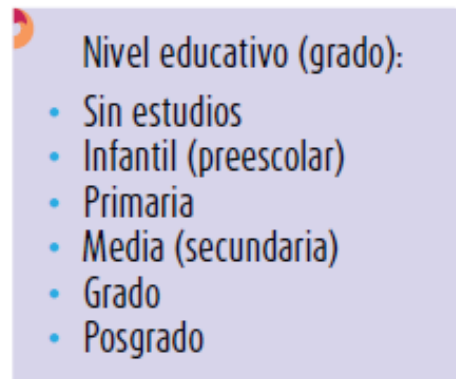
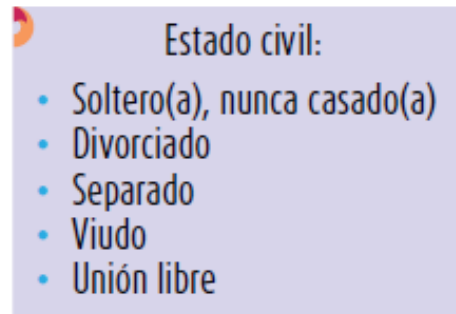
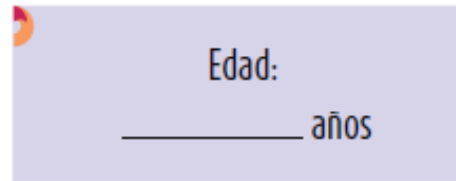
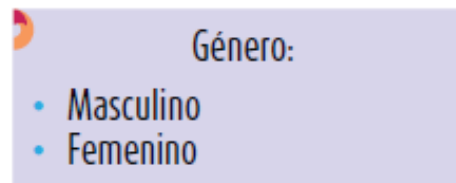
□ Clasificación



Diseños transeccionales descriptivos: Indagan la incidencia de las modalidades, categorías o niveles de una o más variables en una población, son estudios puramente descriptivos.

Diseños longitudinales: Recaban datos en diferentes puntos del tiempo, para realizar inferencias acerca de la evolución del problema de investigación o fenómeno, sus causas y sus efectos.

Ejemplo de variables en diseños transeccionales o descriptivos



Diseño Experimental

□ Basado en la experiencia:

- Diseño, implementación, y configuración de la plataforma de experimentación;
- Análisis, diseño, implementación y pruebas del programa de software;
- Diseño y construcción del artefacto (i.e., IoT);
- Diseño de los instrumentos de medición;
- Aplicación de los instrumentos de medición;
- Recopilación de datos;
- Procesamiento de datos (ETL);
- Procesamiento estadístico de datos;
- Análisis e interpretación de datos;
- Elaboración del reporte;
- Difusión de resultados





PROYECTO DE TITULACIÓN II

SEMANA I: EL MÉTODO CIENTÍFICO

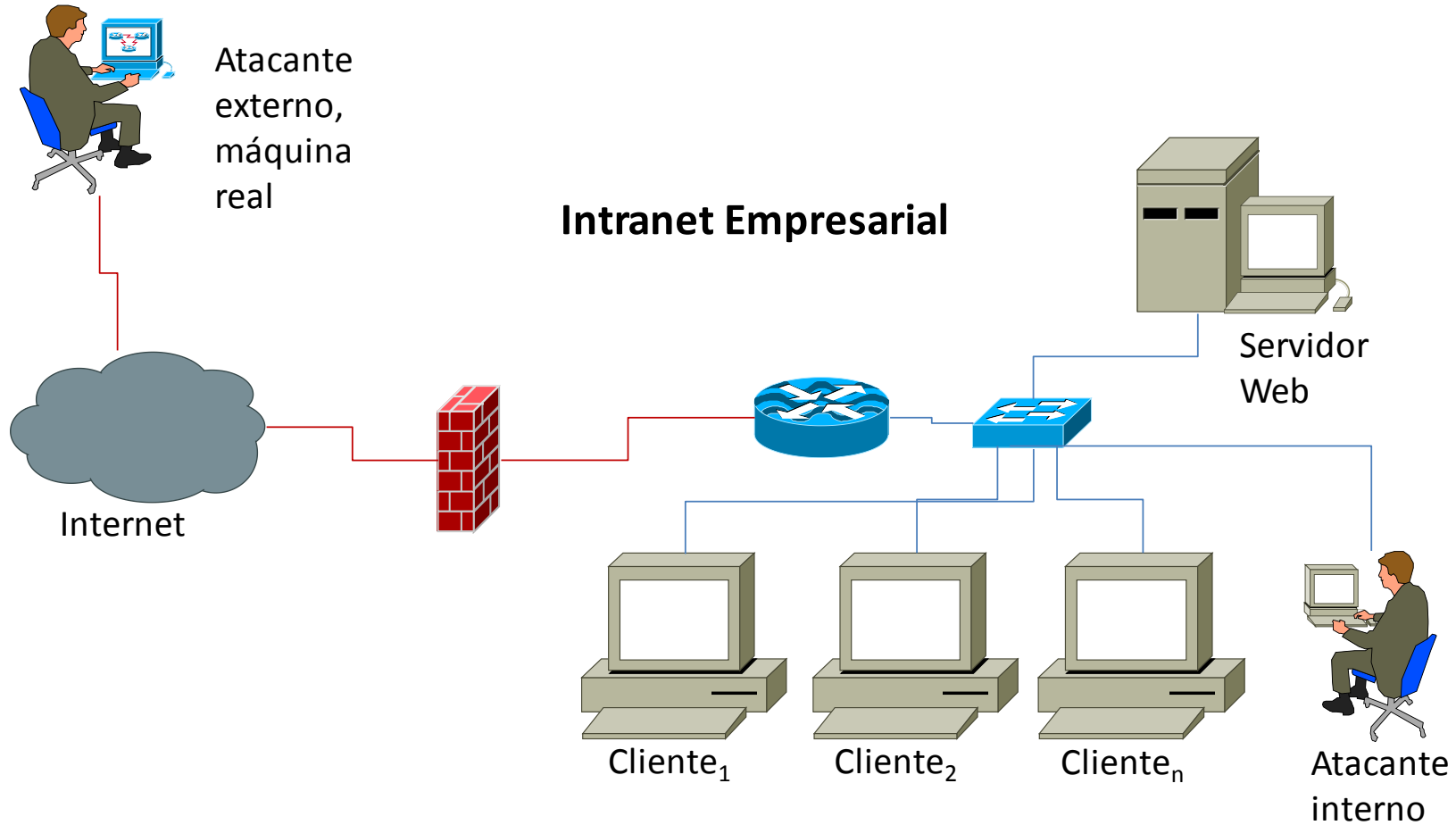
TALLER 3:
Matriz de consistencia metodológica

Compilación: Walter Fuertes Díaz, PhD

Diseño de la Investigación

25

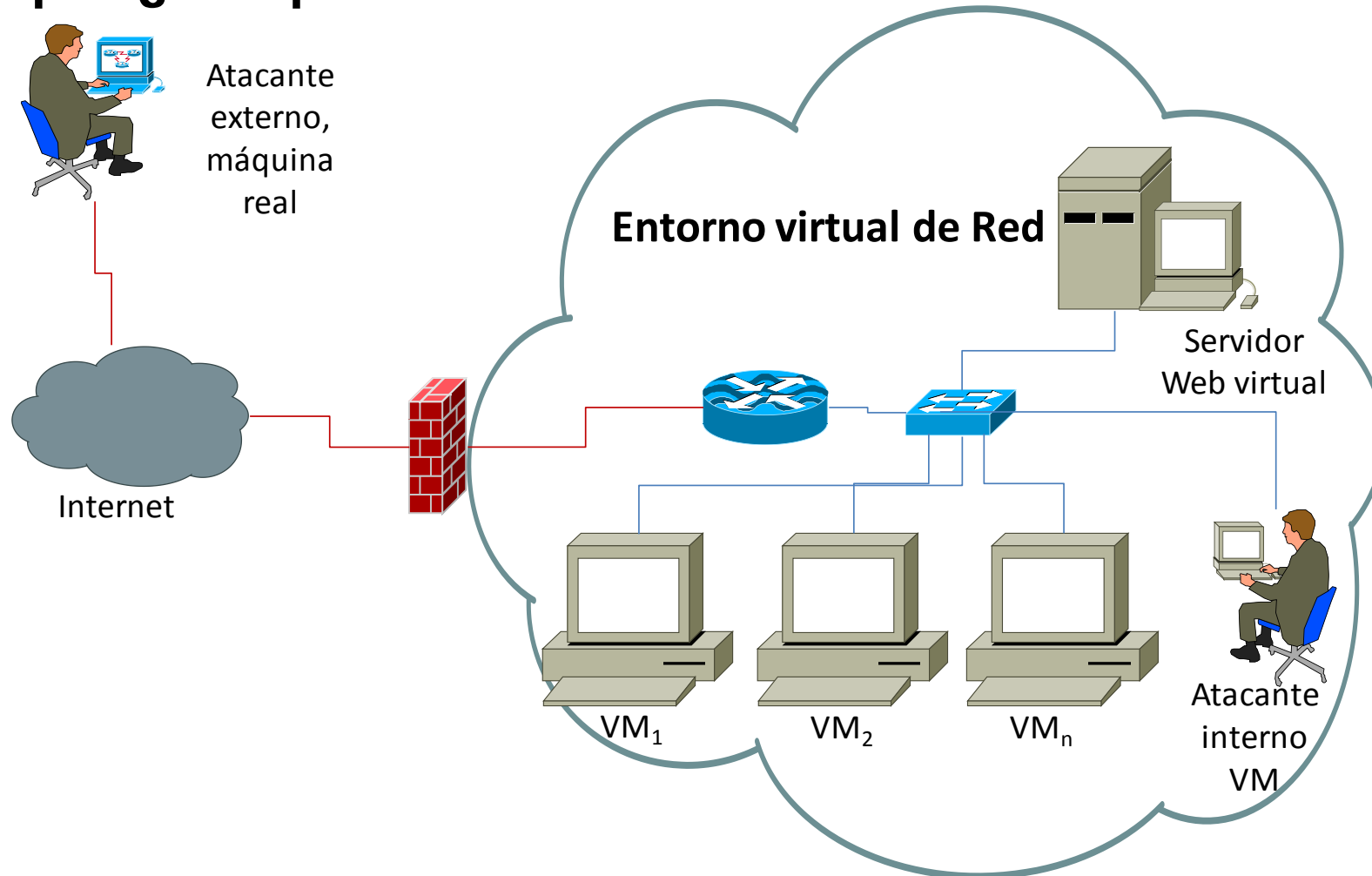
□ Topología Real



Diseño de la Investigación

26

□ Topología Experimental



Diseño de la Investigación

27

□ Tipos de investigación

▣ Documental

- Se ocupa del estudio de problemas planteados a nivel teórico, la información requerida para abordarla se encuentra básicamente en materiales impresos, audiovisuales y/o electrónicos.

▣ De campo

- Se caracteriza porque los problemas surgen de la realidad y la información requerida debe obtenerse directamente en ella.

▣ Proyecto Factible

- Consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas o necesidades de organizaciones o grupos sociales.

▣ Proyecto Especial

- Consiste en la elaboración de un libro, una novela, un documental, una película, un software educativo.

Diseño de la Investigación

28

□ **Recolección de datos**

- ▣ Definir la forma idónea de recolectar los datos de acuerdo al contexto de la investigación;
- ▣ Elaborar el instrumento de medición;
- ▣ Aplicar el instrumento de medición;
- ▣ Obtener los datos;
- ▣ Codificar los datos;
- ▣ Archivar los datos y prepararlos para el análisis.



Diseño de la Investigación

29

□ Instrumento de medición

- ▣ Toda medición o instrumento de recolección de los datos debe reunir dos requisitos esenciales: confiabilidad y validez.
 - La **confiabilidad** de un instrumento de medición se refiere al grado en que su aplicación repetida al mismo sujeto u objeto, produce iguales resultados
 - La **validez**, en términos generales, se refiere al grado en que un instrumento realmente mide la variable que pretende medir

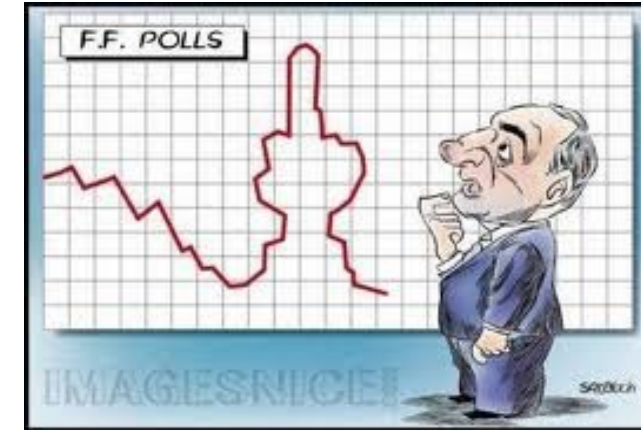


Análisis de Resultados

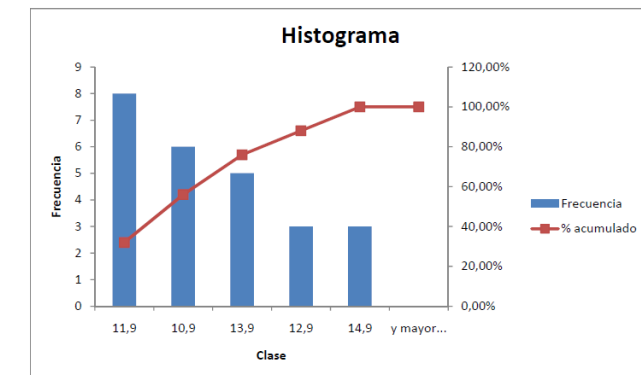
30

■ Procesamiento Estadístico

- Decidir qué pruebas estadísticas son apropiadas para analizar los datos, dependiendo de las hipótesis formuladas y los niveles de medición de las variables.
- Elaborar el programa de computadora para analizar los datos: utilizando un paquete estadístico o generando un programa propio.
- Correr el programa.
- Obtener los análisis requeridos.
- Interpretar los análisis.



Clase	Frecuencia	% acumulado	Clase	Frecuencia	% acumulado
10,9	6	24,00%	11,9	8	32,00%
11,9	8	56,00%	10,9	6	56,00%
12,9	3	68,00%	13,9	5	76,00%
13,9	5	88,00%	12,9	3	88,00%
14,9	3	100,00%	14,9	3	100,00%
y mayor...	0	100,00%	y mayor...	0	100,00%



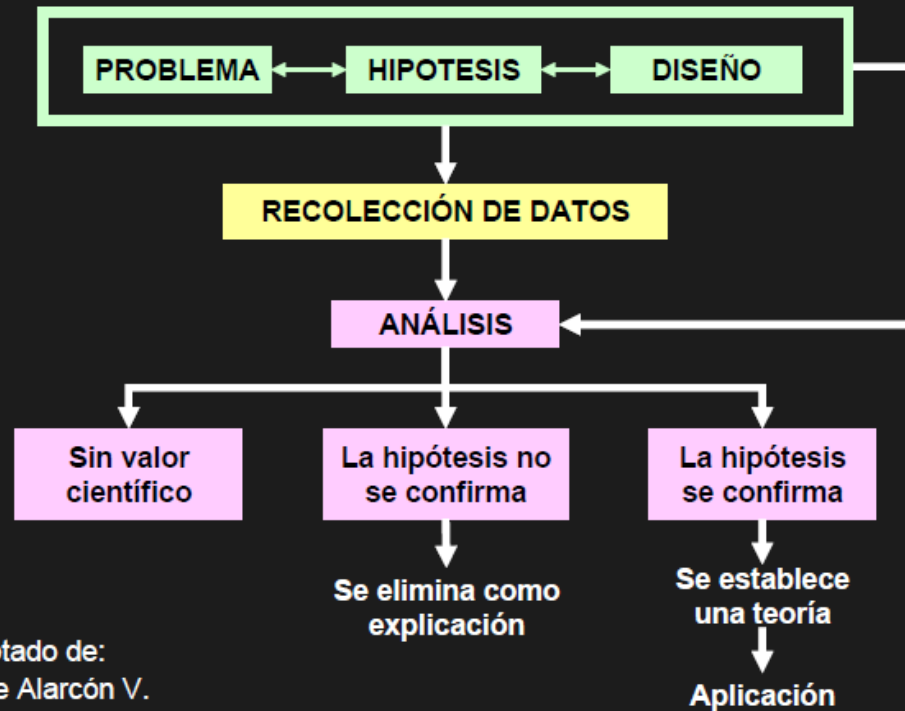
Fuente: Roberto Hernández Sampieri, Carlos Fernández Collado, Pilar Baptista Lucio, Metodología de la Investigación Científica, Mc Graw Hill, México, ISBN 968-422-931-3.

Análisis de Resultados

31

El análisis y la interpretación de los datos permitirán establecer la relación, entre el problema científico, el marco teórico, la hipótesis planteada y el objetivo.

PROCESO DE LA INVESTIGACIÓN CIENTÍFICA



Adaptado de:
Dr. Jorge Alarcón V.

Verificación y validación de la investigación

32

- Existen algunas técnicas para validar los proyectos de investigación.
 - ▣ Modelos Matemáticos
 - ▣ Simulación
 - ▣ Emulación
 - ▣ Desarrollo de Software
 - ▣ Procesamiento estadístico

Etapa III. Validación de la estrategia por parte de los expertos.

- Selección de los expertos.
- Aplicación de los instrumentos de validación.

Elaboración del Reporte de Investigación

33

Elaborar el reporte de resultados:

- Definición del usuario.
- Selección del tipo de reporte a presentar: académico o no académico,
- Escribir el reporte y elaborar las gráficas correspondientes.
- Presentación del reporte.

ICSNS International Journal of Computer Science and Network Security, VOL.11 No.11, November 2011

Alternative Engine to Detect and Block Port Scan Attacks using Virtual Network Environments

Walter Fuertes, Patricio Zambrano, Marco Sánchez and Patricio Gamboa

wfuertes@espe.edu.ec, patricio.zambrano@ice.gob.ec, marco176@hotmail.com, pzambo26@yahoo.com

Post Graduate Program, Escuela Politécnica del Ejército, Sangolquí - Ecuador

Summary

Currently, IP networks are constantly harmed by several attack techniques such as port scans, denial of service, brute force attacks, etc., which can collapse the continuity of business services. To address this problem, this paper focuses on an alternative solution for detection, block, and prevention of port scanning attacks. Particularly, this implementation is an alternative engine to automatically block specialized tool scans, namely PSAD (Port Scan Attack Detector), but it is conceptualized differently from the features that the program offers. To carry out this work, we have designed and implemented a virtual network environment that is to be configured as an experimenting platform with port scan attacks. To neutralize such attacks, we performed a security mechanism that takes the data reported by the PSAD and using parameterized variables (block time and level of category) automatic locks become viable, including custom records and notifications via e-mail. To validate our solution, several tests of port scan attacks have been run on public and private networks. Then we have compared the performance of our alternative engine with ClearOS (specialized security tool for Linux) and the PSAD. The results show that our alternative engine is faster and more reliable than the tools previously mentioned.

Keywords:

Network attacks, port scan attack, security, virtual network environments.

1. Introduction

Some of the biggest threats to the security network are the presence of bugs, viruses, Trojans, port scan, phishing and denial of service. These can cause your Web server or client to crash, corrupt your information, or, worst of all, allow outsiders unauthorized access [1]. These intrusions may render its resources inoperative and produce a loss of productivity, causing economic losses and compromising the business continuity. This paper centers its attention on port scan attacks since these attacks in actuality represent a considerable part of Internet traffic [2][3]. Thus, this research focuses on an alternative solution for the detection and blocking of port scan attacks performed on a virtual network environment (VNE) [4].

Within this context, the scientific community has demonstrated an ever growing interest in the

Manuscript received November 23, 2011.

Manuscript revised November 31, 2011.

implementation of solutions, for diminishing network security attacks making use of the virtualization technologies. Under this precept the work proposed by Keller & Naoos [5], formulates the implementation of a collaborative security lab using virtual machines. Other works [6][7][8] propose virtual technology integration, with the purpose of securing a network through the implementation of a remote laboratory intrusion detection system. Other researchers [9][10][11] have used virtual machines based on the *Honey net* concept, as a security tool. Within the same scope researchers have used virtualization platforms for disaster recuperation and mitigation of real IP attacks [12][13][14]. Regarding mitigation mechanisms of Denial of Service attacks (DoS), Fuentes et al. [15] exposes a research where IP real attacks were evaluated in order to detect and block DoS attacks using VNE. Within this scope Yaur & Song [16] details Internet filter rules (called SIFF). Lastly, Markovic & Reither [17] proposes D-WARD which is a Distributed Denial-of-Service defense system, the goal of which is the autonomous detection of these attacks using new traffic profile techniques.

To address the problem mentioned above, this work proposes the design and implementation of an alternate engine for automatic blocking to the already existing system inside the Port Scan Attack Detector (PSAD) [18] that will be more efficient as well as customizable. In essence, the alternative engine is an implemented routine which captures PSAD output data reducing the necessary time to analyze its register files and detect these attacks.

In order to carry out this work, all test infrastructures were conducted in a VNE using Virtual Box, a virtualization tool using virtualization software to be deployed on virtual machines destined for desktop computers and enterprise servers, which also implements full virtualization [19][20][21].

To validate our mechanism and as the main contribution, this paper proposes: *i)* to improve the system's response time when detecting port scans; and, *ii)* to configure a customizable algorithm that acquires PSAD data and notify the system administrator via e-mail.

The remainder of this paper is organized as follows: Section 2 presents the theoretical framework. Section 3 describes



ISSN 1390 - 5236

DECC - Report

Tendencias
revista
2
versión
en Computación



ESPE
ESCUELA POLITÉCNICA DEL EJÉRCITO
CAMINO A LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS
DE LA COMPUTACIÓN

Vol. 1, No. 2 - 2010

CONISOFT'2017

Ingeniería del Software

Definición IEEE¹. Aplicación de un enfoque cuantificable, disciplinado y sistemático para el desarrollo, operación y mantenimiento del software, y el estudio de estos enfoques; esto es, **la aplicación de la ingeniería al software**



¹ISO/IEC/IEEE Systems and software engineering -- Vocabulary ISO/IEC/IEEE 24765:2010(E), 2010, 1-418

Imagen de: [https://www.intracomdefense.com/ImageHandler.ashx?image=/content/SW_Engineering\(5\).jpg](https://www.intracomdefense.com/ImageHandler.ashx?image=/content/SW_Engineering(5).jpg)

CONISOFT'2017

La ingeniería en la Ingeniería de Software

Problemáticas en la IS

- Productos software de baja calidad
- Entregados fuera de plazo
- Con un costo mayor al estimado



You are a lucky bug. I'm seeing that you'll be shipped with the next five releases.

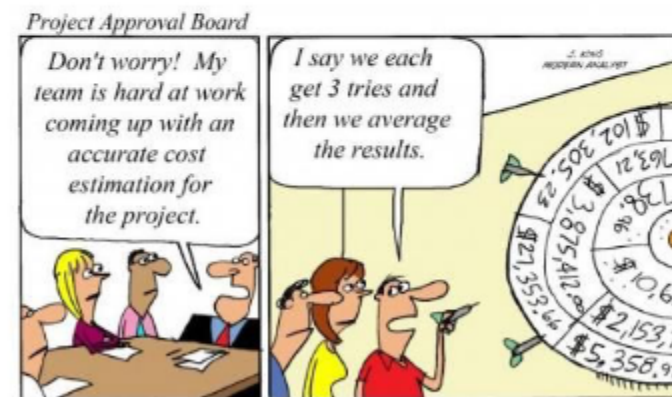


Imagem de: <https://blog.janeirodigital.com/2016/02/11/software-self-defense-101-improving-your-technical-estimates/>

Experimentación en Ingeniería de Software

La **investigación en ingeniería de software** tiene como fin continuar con la generación y codificación de conocimiento científico para incorporarlo en la práctica del desarrollo de software

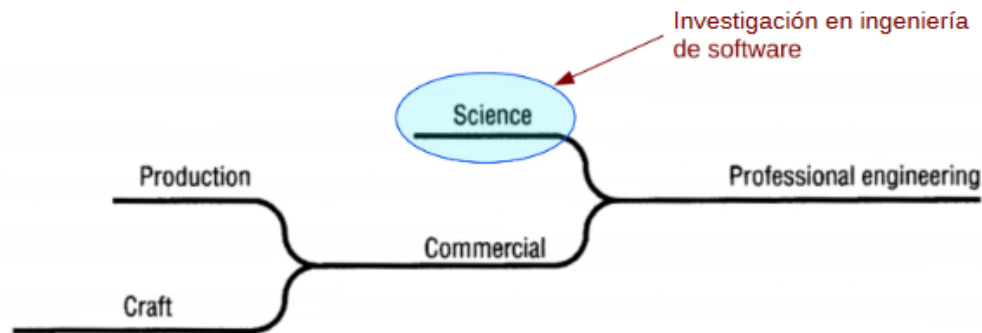


Imagen de: Shaw, M. Prospects for an Engineering Discipline of Software IEEE Softw., IEEE Comp. Soc. Press, 1990, 7, 15-24

Enfoques de investigación usados en la Ingeniería de Software

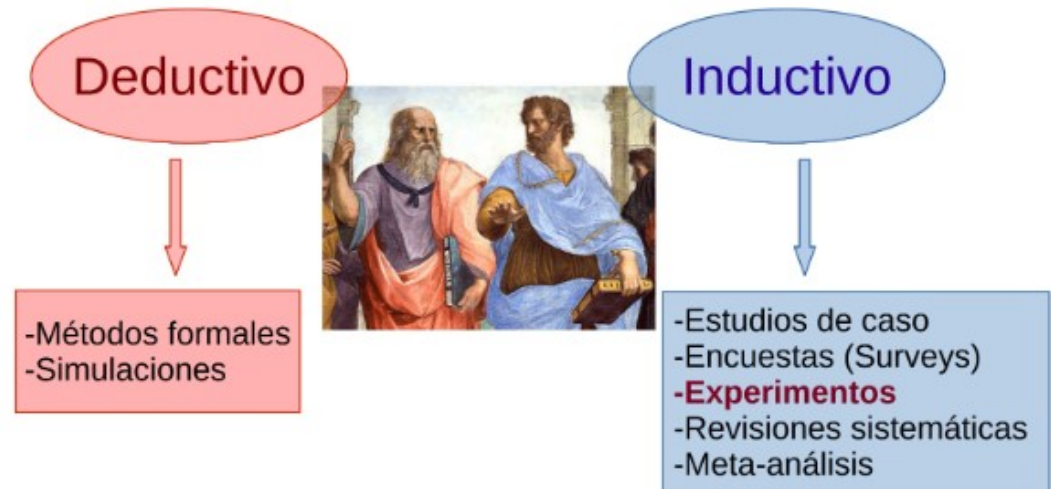


Imagen de: <https://www.biografiasyvidas.com/monografia/aristoteles/>

Experimentación en Ingeniería de Software

Experimentos

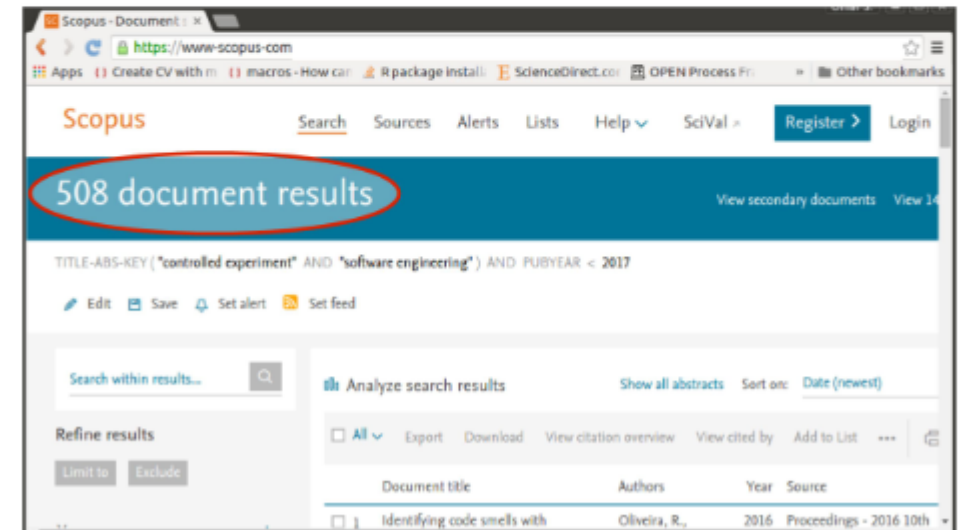
Son útiles para:

- Confirmar teorías i.e. probar teorías existentes
- Confirmar juicios convencionales i.e. probar las creencias, intuiciones de las personas, en este caso prácticas en IS
- Explorar relaciones i.e. probar que cierta relación se mantiene
- Evaluar la exactitud de un modelo i.e. probar que la exactitud de ciertos modelos es como se esperaba
- Validar mediciones i.e. asegurar que una medida realmente mide lo que se supone debe medir

Experimentos reportados en IS

- cadena de búsqueda:

```
TITLE-ABS-KEY ( "controlled experiment" AND  
"software engineering" ) AND PUBYEAR < 2017
```



Experimentación en Ingeniería de Software

CONISOFT'2017

Experimentación en Ingeniería de Software

Experimentación

El **objetivo** de la experimentación es identificar las **causas** por las que se producen determinados resultados (**efecto**)



Imagen de: <http://www.writeawriting.com/essay/cause-and-effect-essay/>

A partir de una **base teórica** de conocimientos es posible codificar estos conocimientos para aplicarlos a la resolución de problemas afines al desarrollo y mantenimiento del software

CONISOFT'2017

Experimentación en Ingeniería de Software

Experimentación en IS

Puede servir como un mecanismo fiable para validar empíricamente (con hechos) las prácticas en IS.

Ayuda a construir una **base teórica** a partir de hechos recabados.

La experimentación en IS hace posible la **identificación y comprensión de las variables** que entran en juego en la construcción de software, así como las conexiones que existen entre ellas

Experimentación en Ingeniería de Software

CONISOFT'2017

Experimentación en Ingeniería de Software

Experimentación en IS

- La formalización de la experimentación surge en la década de los 80s



36.pdf

77.39%

IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. SE-2, NO. 3, JULY 1981

Experimentation in Software Engineering

VICTOR R. BASILI, SENIOR MEMBER, IEEE, RICHARD W. SELBY, MEMBER, IEEE, AND
DAVID H. HUTCHENS, MEMBER, IEEE

Abstract—Experimentation in software engineering supports the advancement of the field through an iterative learning process. In this paper we present a framework for analyzing most of the experimental work performed in software engineering over the past several years. We describe a variety of experiments in the framework and discuss their contribution to the software engineering discipline. Some useful recommendations for the application of the experimental process in software engineering are included.

Index Terms—Controlled experiment, data collection and analysis, empirical study, experimental design, software metrics, software technology measurement and evaluation.

I. INTRODUCTION

As any area matures, there is the need to understand its components and their relationships. An experimental process provides a basis for the needed advance-

ware engineering over the past several years. We then discuss a variety of these experiments, their results, and the impact they have had on our knowledge of the software engineering discipline.

II. OBJECTIVES

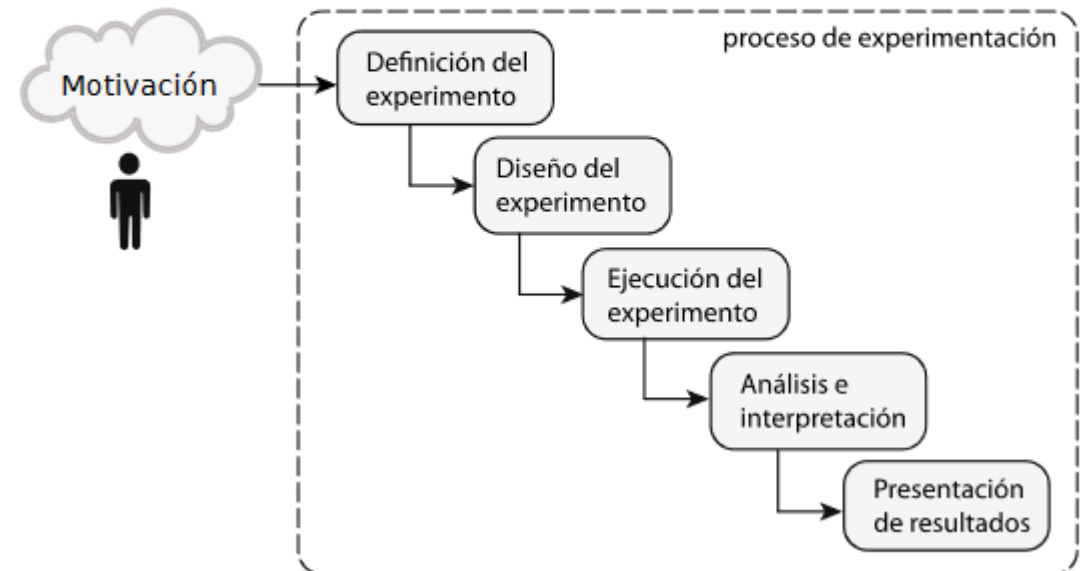
There are three overall goals for this work. The first objective is to describe a framework for experimentation in software engineering. The framework for experimentation is intended to help structure the experimental process and to provide a classification scheme for understanding and evaluating experimental studies. The second objective is to classify and discuss a variety of experiments from the literature according to the framework. The description of several software engineering studies is intended to provide an overview of the knowledge resulting

imagen de: <https://alchetron.com/Harrison-Rhodes-361036-W>

CONISOFT'2017

Proceso de experimentación en Ingeniería de Software

Proceso de experimentación



Experimentación en Ingeniería de software

□ Tipos

- Procedimientos;
- Modelos descriptivos;
- Modelos analíticos;
- Modelos empíricos;
- Herramientas;
- Prototipos;
- Modelos predictivos;
- Etc.

□ Métodos

- Método o medio de desarrollo;
- Método de análisis o evaluación;
- Diseño, evaluación o análisis de una instancia particular;
- Generalización o caracterización;
- Estudio o exploración de viabilidad

□ Estrategias

- Repotenciar modelos, métodos o herramientas;
- Mejorar los resultados o aplicación de los métodos o herramientas;
- Desarrollar modelos formales;
- Empírica;
- Observacional;
- Correlacional;
- Experimental,
- Cuasi-Experimental;
- No experimental

Investigación - Acción

Investigación - Aplicada

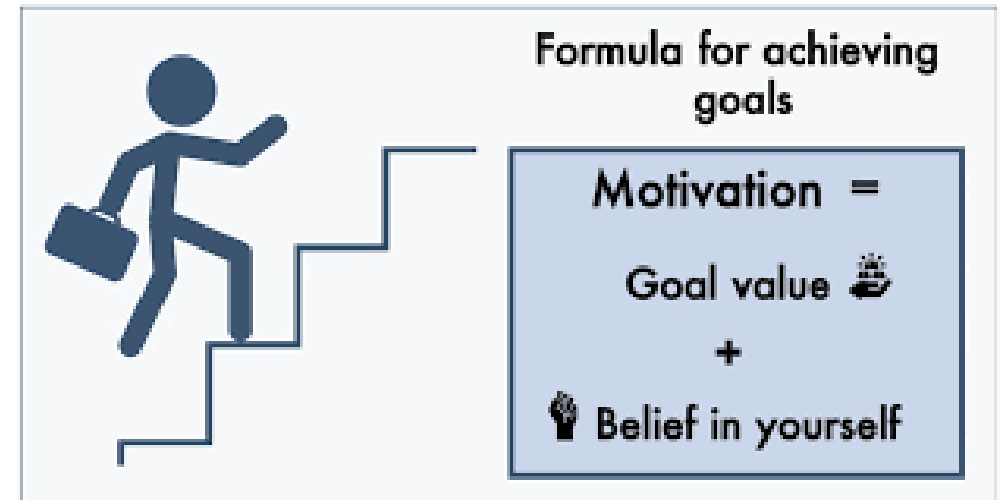
Revisión de la Literatura

Construcción de Artefactos

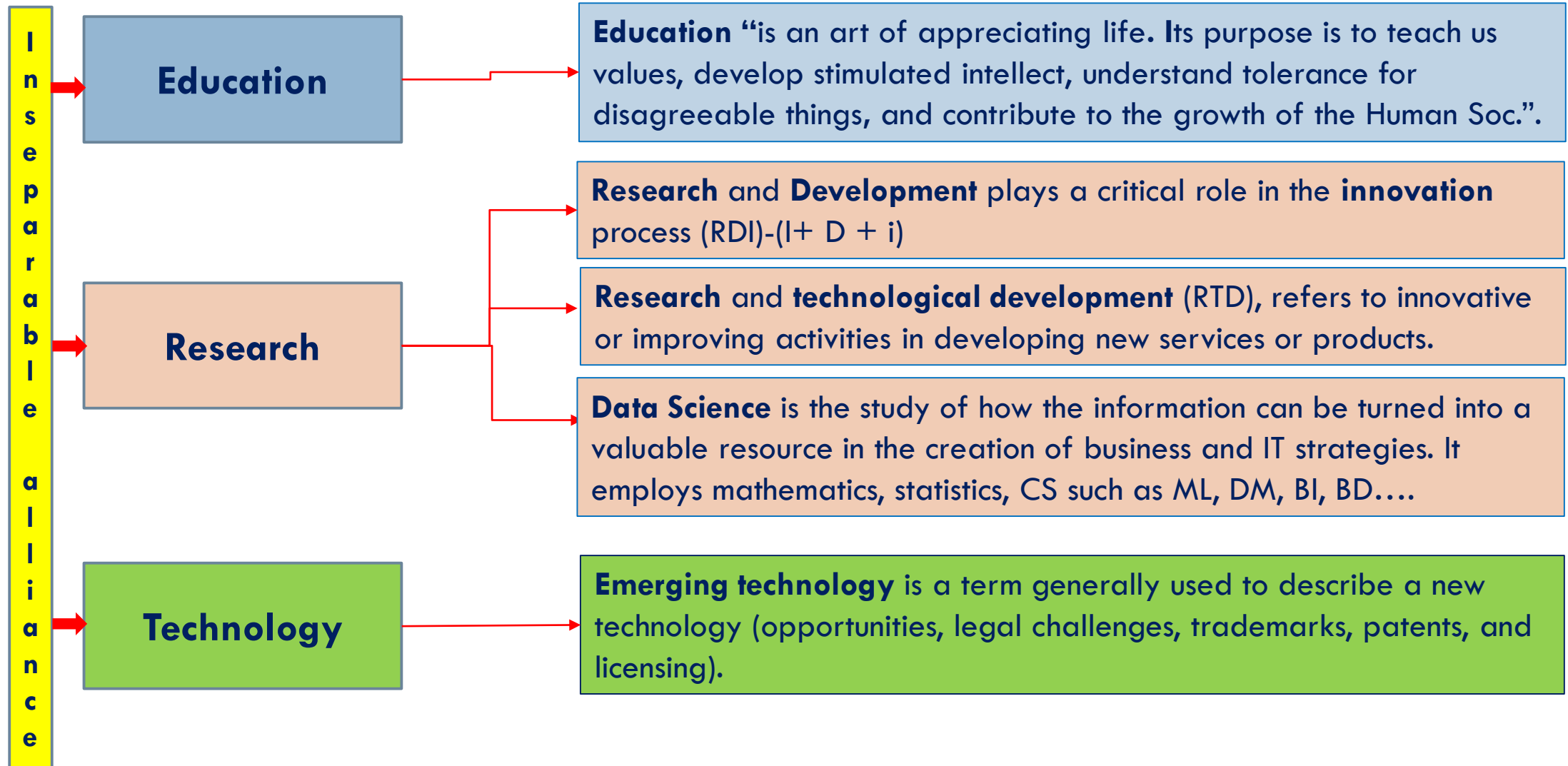
Case Studies

□ Goals

- To report some research experiences related to Emerging technologies such as IoT and data sciences;
- To motivate the graduate professional and students to keep being fascinated by the research process, and the results obtained.



Case Studies - Goals and Motivation



Case Study No. 1

Software-based Platform for Education and Training of DDoS Attacks using Virtual Network

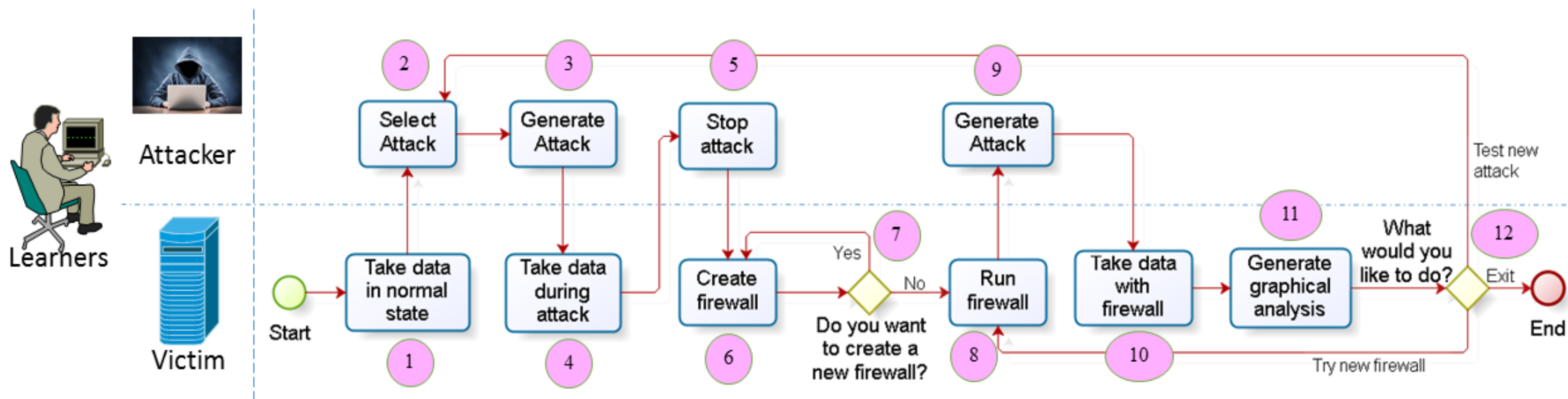
“Los seres excelentes son aquellos que están intentando hacer las cosas siempre en forma superior, y luchan incansablemente por lograrlos”

Miguel Ángel Cornejo, “El ser Excelente”



Software-based Platform for Education and Training of DDoS Attacks using Virtual Networks

Research Design: Training platform execution



Research Design: Software Implementation and Architecture

44



Client tier



Interface based
Shell Script to
select type of
DDoS attacks

Attacker

Presentation tier



System services
to display
statistical graphs

Analytical approach

Business tier



Logic of the
application to
configure
firewalls in Linux
written in Java

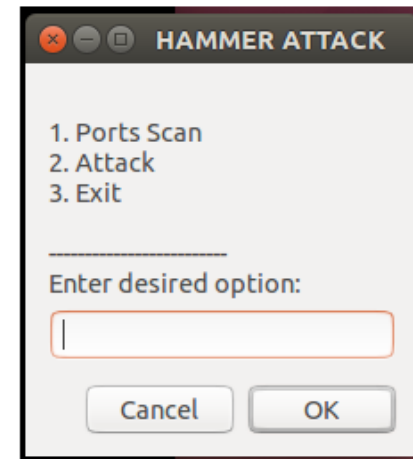
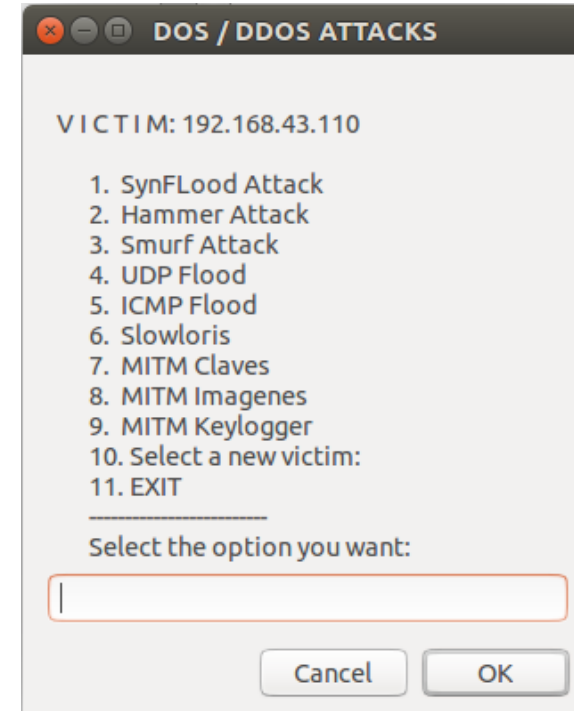
Detect and mitigate

Data tier



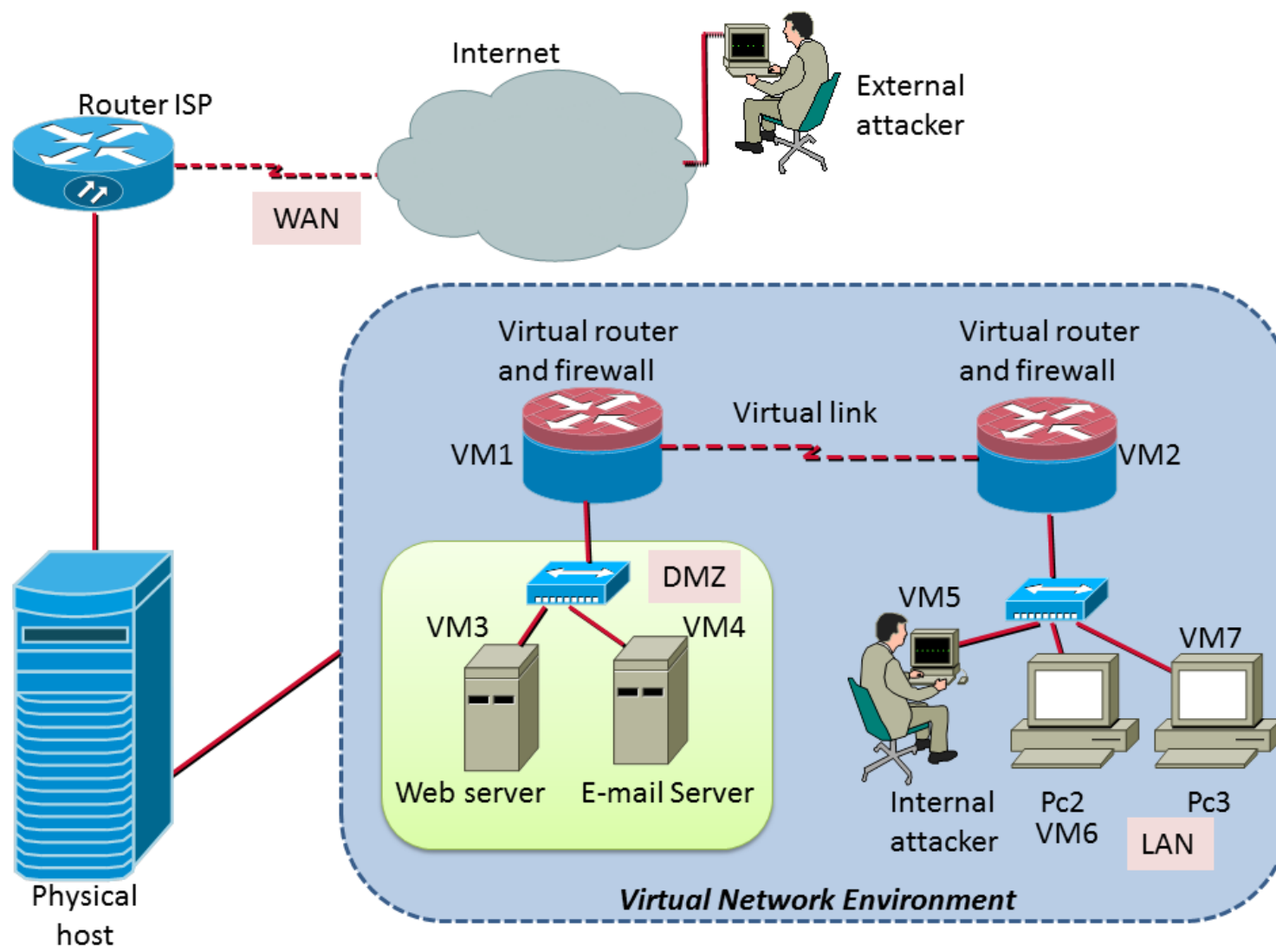
Store and register
logs and the
servers states

Victim



Software-based Platform for Education and Training of DDoS Attacks using Virtual Networks

Experimental topology based on VNE



Research Design: Software Implementation and Architecture

46

- Deploying Linux firewall rules in a natural language, easy-to-understand such as the simple selection of one or more rules

RULES IPTABLES

State	Number	Nombre	Descripcion
<input type="checkbox"/>	8	Local masking and DMZS	Masking to go to the internet
<input type="checkbox"/>	9	Access DMZ - LAN	Access from DMZ to LAN
<input type="checkbox"/>	10	Close ports	Close ports range
<input type="checkbox"/>	11	Webmin Port	Close Webmin port
<input checked="" type="checkbox"/>	12	Synflood Defense	Protection of synflood attacks
<input type="checkbox"/>	13	Torshammer Defense	Protection of synflood attacks
<input type="checkbox"/>	14	UDP Defense	Protection of synflood attacks

Rules Selected: 1

Export

Apply changes

Show Rules

EXIT

Software-based Platform for Education and Training of DDoS Attacks using Virtual Networks

Walter Fuentes, Anabel Tunala, Ronnie Moncayo, Fausto Meneses, and Theofilos Toulkeridis
Computer Sciences Department, Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador
{wffuentes, rmoncayo, mtunala, fmeneses, ttoulkeridis}@espe.edu.ec

Abstract—The education and training of security networks is an essential challenge for the academy, due to the vertiginous increase of threats and vulnerabilities. This study aims to implement a software-based experimental platform over virtual network environments, in order to stimulate teaching in Distributed Denial of Service (DDoS) attacks. We have used the theories of learning oriented to the experience, reflexive observation, and active experimentation of the students. This allowed to evaluate the learning objectives based on Bloom's Digital Taxonomy. From the software point of view, the experimental paradigm of Software Engineering has been applied, using SCRUM as an agile methodology. During the development of the application, we implemented different roles including attackers, learners as well as victims in order to reconstruct and understand real attacks on IP networks. Hereby, for the role of attackers, we have used an interface to select the type of attack, while for the role of learners, we designed an intuitive interface that presents through natural language, to select possible firewall rules. This helped to learn, detect and mitigate potential attacks. Finally, for the role of victims, we included an analytical approach, which allowed to recognize online the impact of attacks on the performance of the computer system. The results demonstrate the functionality of the platform confirming that the introduced software meets the Usability criteria. Finally, our results present a network security learning, determined in terms of Bloom's Digital Taxonomy.

Keywords—DDoS attacks; virtual networks; Usability; learning theories; Bloom's Digital Taxonomy; Security education and training.

I. INTRODUCTION

Nowadays, network security issues have become gradually important in the education of engineers [1]. However, the training in this topic has been relatively complicated by its nature since many years [2]. Besides, and given its inadequate application it may be penalized by internal legislation as well as by international laws. Nonetheless, network attacks continue to grow in frequency, volume, and severity [3]. One of the well-known assault are the so-called Distributed Denial of Services attacks (DDoS) [4]. Based on these issues, a solution has been proposed by the UNESCO, which raises a technological debate from a pedagogical definition, aiming at teaching prevention standards and computer security to students, having a direct curricular implication [5]. Furthermore, ITU submitted an ITU-T X.1205 recommendation [6], in which it emphasizes the value of training and education in protecting the network as an institutional Cybersecurity strategy. Within this motivation, this research has been addressed on implementing an

experimental platform for learning and teaching DDoS attacks, for engineering students.

There have been selected studies focused on learning the problem of protecting information on computers. Since the year 2000 authors analyzed the implications of integrating computer security [2][7][8]. More recently, authors presented personalized learning platform with Moodle [9][10] or intelligent tutoring systems [11][12]. With respect to teach DDoS, in [13][14] presented an approach to detect DDoS attacks. Concerning the application of Virtual Network Environments (VNE) as explained before in [15][16], a few researchers [17][18][19][20][21][22] have proposed it as an experimental topology for teaching DDoS or for network security, which has been useful in training of a variety of network attacks and defense.

Our study aims to design and implement a software platform for training and education of DDoS attacks security using VNE, in order to improve the teaching-learning process in network protection. The following research questions have been considered: How to implement an educational platform for training DDoS attacks? How to measure Usability? How to determine student learning?

To fulfill these goals, a software application oriented to training and education in DDoS attacks has been designed and implemented, allowing us to visualize the attack's life cycle (i.e. inject various types of DDoS attacks, detect, analyze, and mitigate them). This application contemplates learning from the point of view of those actors who are involved in the process. It also considers at the cognitive dimension of Bloom's Digital Taxonomy to determine learning [23][24]. For the proof of concept, hybrid experimental topology has been used, that is based on real equipment and VNE, using open-source software to reduce hardware and software investment costs. In order to measure the quality of the experience that a user has had when interacting with the software application, we have used Usability measures in Software Engineering [25].

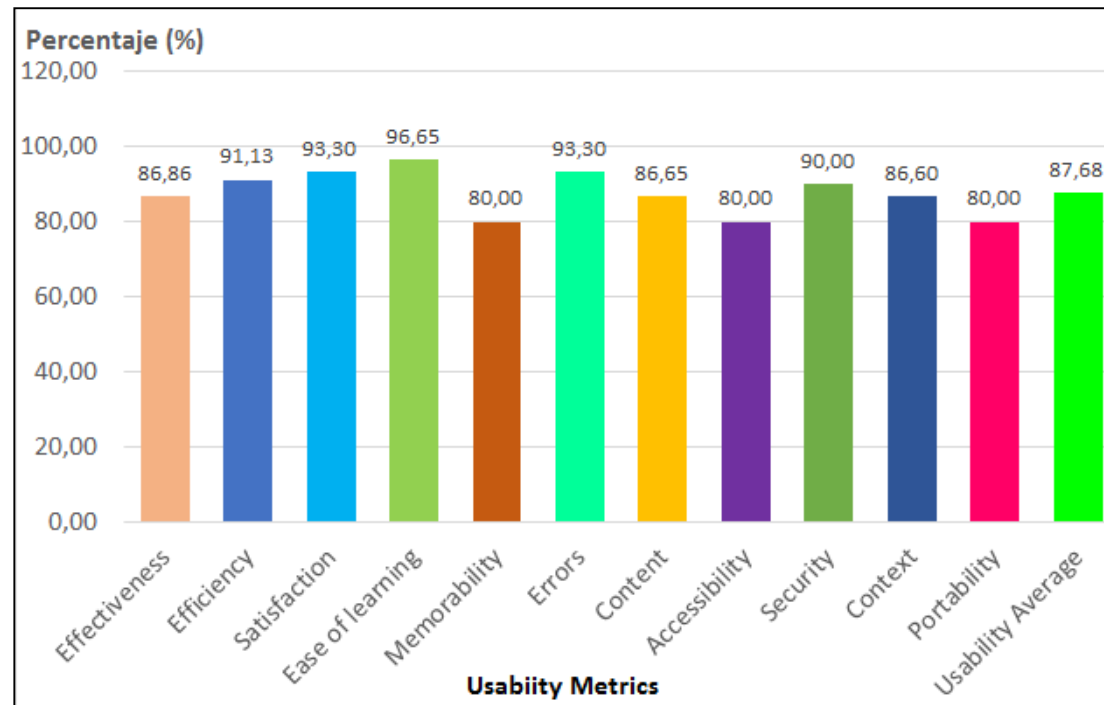
The main contributions of this research include: (1) Development of an interface that allows the generation and injection of various types of DDoS attacks, each of which has been setup within the application. (2) Development of a parameterizable GUI that allows the user to select different natural language rules with different network parameters. These rules will be automatically generated by the firewall.

The remainder of this article has the following organization: In section II, we are presenting the research design. Later, in Section III, we provide the experimental results and finally, we conclude including future work lines with Section IV.

Evaluation Results: Analytical approach of the application

47

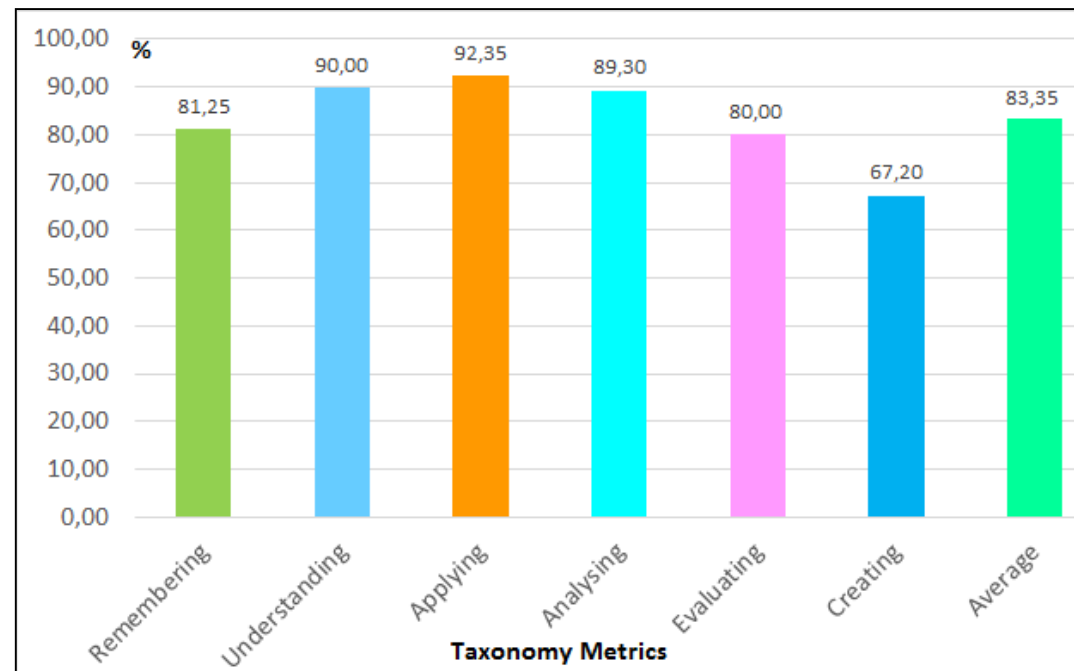
Measurement of Usability metrics of the software application



Evaluation Results: Analytical approach of the application

48

Results of learning objectives based on the Bloom's Digital Taxonomy



Referencias Bibliográficas

- Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering—a systematic literature review. *Information and software technology*, 51(1), 7-15.
- Roberto Hernández Sampieri et al.(2014), Carlos Fernández Collado, Pilar Baptista Lucio, Metodología de la Investigación Científica, Mc Graw Hill, México, ISBN: 978-1-4562-2396-0.
- Omar S. Gómez, Hoja de ruta para realizar experimentos en Ingeniería de Software, ESPOCH. URL: https://www.researchgate.net/profile/Omar_S_Gomez/publication/320696284_Hoja_de_ruta_para_realizar_experimentos_en_Ingenieria_de_Software/links/59f8b0b8458515547c26a15c/Hoja-de-ruta-para-realizar-experimentos-en-Ingenieria-de-Software.pdf
- Callejas Mauro, Alarcón Andrea y Álvarez Ana. (2017). Modelos de Calidad del Software, un estado del Arte. Tunja – Colombia. Recuperado de: <http://www.scielo.org.co/pdf/entra/v13n1/1900-3803-entra-13-01-00236.pdf>.
- **Question Pro, Empirical Research: Definition, Methods, Types and Examples.** <https://www.questionpro.com/blog/empirical-research/>
- Héctor Luis Ávila Baray (2006) Introducción a la Metodología de la Investigación, Cd. Cuauhtémoc, Chihuahua, México.
- Francisco Bijarro Hernández, Desarrollo Estratégico para la Investigación Científica, Universidad Autónoma de Tamaulipas, ISBN-13: 978-84-690-8111-2, N° REGISTRO: 07/76456.
- Jan Feyen , ¿Cómo elaborar propuestas de investigación?, ESPE-2010.
- Fuertes, Walter, et al. "Software-based computing platform as an experimental topology assembled to detect and mitigate DDoS attacks using virtual environments." *2016 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*. IEEE, 2016.
- Fuertes, Walter, et al. "Software-based Platform for Education and Training of DDoS Attacks using Virtual Networks." *2017 International Conference on Software Security and Assurance (ICSSA)*. IEEE, 2017.