ESPOCH Congresses: The Ecuadorian Journal of S.T.E.A.M.
Volume 3, Issue no. 4, DOI 10.18502/espoch.v3i4.17171
Production and Hosting by Knowledge E

Conference Paper

Computer Attacks and Their Impact on the Security of Servers with Linux Operating System of Local Government Entities

Los ataques informáticos y su incidencia en la seguridad de servidores con sistema operativo Linux de entidades de gobierno local

Francisco Javier Aguilar Feijóo[1], Diego Fernando Andaluz Espinosa[2]*

[1]Gobierno Autónomo Descentralizado de la Provincia de Orellana, Francisco de Orellana, Ecuador
[2]Universidad de las Fuerzas Armadas, Quito, Ecuador

ORCID
Francisco Javier Aguilar Feijóo: https://orcid.org/0009-0002-3857-5056
Diego Fernando Andaluz Espinosa: https://orcid.org/0000-0002-2033-2737

X CONGRESO INTERNACIONAL DE CIENCIA TECNOLOGÍA EMPRENDIMIENTO E INNOVACIÓN SECTEI 2023

Corresponding Author: Diego Fernando Andaluz Espinosa; email: Ecuadordfandaluz@espe.edu.ec

Published: 25 September 2024

Production and Hosting by Knowledge E

Abstract

This research aims to determine the incidence of computer attacks on servers with the Linux operating system of local government entities. The study is limited to the decentralized autonomous government (GAD) of the Ecuadorian Amazon. Initially, the most common computer attacks that have affected organizations in recent years were determined using statistical reports from important computer security companies positioned as leaders in Gartner's magic quadrant. Phishing and distributed denial of service (DDoS) attacks are established as computer attacks under study. Computer attacks are carried out before and after mitigation measures are established. With the help of the information systems risk analysis and management methodology (MAGERIT), the vulnerability, level of impact, and risk computer attacks cause on servers with the Linux operating system are determined. This research aims to serve as a guide to the information technology departments of local governments in implementing mechanisms that safeguard the most important asset of an organization, such as information.

Keywords: *computer attack, phishing, DDoS, MAGERIT, Linux.*

Resumen

La presente investigación tiene como finalidad determinar la incidencia de los ataques informáticos en los servidores con sistema operativo Linux de entidades de gobierno local. El estudio está delimitado a un gobierno autónomo descentralizado (GAD) de la Amazonía ecuatoriana. Inicialmente se determina los ataques informáticos más comunes que han afectado a las organizaciones en los últimos años haciendo uso de reportes estadísticos de importantes empresas de seguridad informática posicionadas como líderes en el cuadrante mágico de Gartner. Se establece como ataques informáticos objeto de estudio los ataques de phishing y de denegación de servicio distribuido (DDoS). Se realizan ataques informáticos antes y después de establecer las medidas de mitigación y con la ayuda de la metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT) se determina la vulnerabilidad, el nivel de impacto y el riesgo que los ataques informáticos provocaban en los servidores con sistema operativo Linux.

How to cite this article: Francisco Javier Aguilar Feijóo, Diego Fernando Andaluz Espinosa (2024). Computer Attacks and Their Impact on the Security of Servers with Linux Operating System of Local Government Entities. *ESPOCH Congresses: The Ecuadorian Journal of S.T.E.A.M.*, 3(4), 159–176. DOI 10.18502/espoch.v3i4.17171

El presente trabajo de investigación pretende ser de gran utilidad y servir de guía a los departamentos de tecnologías de la información de gobiernos locales en la implementación de mecanismos que salvaguarden el activo más importante de una organización como lo es la información.

Palabras Clave: *ataque informático, phishing, ddos, magerit, linux.*

1. Introduction

The growing and continuous use of information technologies has meant that organizations have to fight against countless computer attacks. Demonstrating the need to establish mechanisms that allow computer assets to be kept safe, especially the information they have [1].

On April 23, 2008, Executive Decree 1014 was published, which establishes as public policy the use of free software in computer systems and equipment in the public sector. Therefore, in Ecuador, free software becomes a technological policy, where the use of open standards and community work lead to digital inclusion, technological sovereignty, and local innovation [2].

The Decentralized Autonomous Government of the Province of Orellana (GADPO), as a public entity and as a case study of this research, maintains an infrastructure of servers, mostly with a Linux operating system, where the information it generates is stored. For this reason, the need arose to investigate the incidence that phishing, and DDoS computer attacks would cause in this type of infrastructure and, based on the results obtained, determine what measures could be taken to mitigate their effects [3].

As an alternative solution, this study proposes a procedure for securing Linux servers. This aims to serve as a guide for organizations to implement protection mechanisms against computer attacks that may put at risk the confidentiality, integrity, and availability of information, considered the most valuable asset that companies have today [5].

2. Materials and Methods

This research has a qualitative-quantitative approach. Quantitative because it will seek to determine the incidence of computer attacks on the security of Linux servers based on numerical measurement and statistical analysis. It is also qualitative since value judgments will be made regarding the security of Linux servers in the GADPO.

The basic research modality will be bibliography, since we will use books and dissertations in the field of computer security, scientific articles, and existing laws. Also,

field modality because we will seek to obtain information about computer attacks on Linux servers.

This type of research is experimental because situations that affect the security of Linux servers are voluntarily caused. Descriptive since an analysis is carried out to determine the impact that computer attacks have on the security of servers with the Linux operating system. Also, explanatory because it can support the importance of knowing how computer attacks are carried out.

2.1. Population and sample

The population to be studied for this research will be computer attacks. To obtain the sample, we proceed to determine the endpoint protection companies positioned as leaders in Gartner's magic quadrant in the years 2016, 2017, and 2018.

Table I. Featured endpoint protection platforms.

1 Trend Micro

1. 2016 2 Intel Security

3 Kasperky Lab

1. (a) Trend Micro

2. 2017 2 Kaspersky Lab

3. Sophos

(a) Symantec

3 2018 2 Sophos

3 Trend Micro

The companies that have stood out as leaders the longest in the last three years are selected. Based on these statistical reports, the computer attacks that most affect organizations are sought.

Tabla 1

Endpoint protection platforms.

1	Trend Micro
2	Kaspersky Lab
3	Sophos

Based on research carried out in 2016, 2017, and 2018 by Trend Micro, Kasperky Lab, and Sophos, the most common computer attacks have been identified.

Tabla 2

Most common computer attacks.

No.		Computer attacks
	Endpoint platform	Computer attack
1	Trend Micro	Pishing Unpatched vulnerabilities DDoS SQL injection Cross site scripting
2	Kaspersky Lab	Viruses, worms and spyware Spam Phishing Network intrusions DDoS
3	Sophos	Ransomware

Since phishing and DDoS attacks are considered by both Trend Micro and Kaspersky Lab as computer attacks that have affected organizations in recent years, they are established as a sample for this research.

Table IV.

Tabla 3

Sample.

No.	Sample
	Computer attack
1	Phishing
2	DDoS

2.2. Information gathering

The techniques used were observation and simulation of phishing and DDoS computer attacks on the GADPO Linux servers. This made it possible to obtain data to later tabulate and analyze. (Table V) shows the details, the questions, and their purpose.

2.3. Processing and analysis stages

To process the collected information, the following was done:

1. Thorough review of information, purification of faulty and irrelevant information.
2. Re-collection in certain individual cases to correct errors.
3. Tabulation of information.
4. Information management (readjustment of tables with empty boxes or with quantitatively reduced data that does not influence the analysis).

Tabla 4

Information collection plan.

No.		Information gathering
	Questions	*Objective*
1	Why?	To achieve the research objectives and support the proposed hypothesis
2	what people or objects?	Servers with GADPO Linux operating system
3	On what aspects?	Computer attacks on Linux operating system servers
4	Where?	Decentralized Autonomous Government of the Province of Orellana
5	What collection techniques?	Observation, tests
6	With what?	Software Tools

5. Statistical study of data for presentation of results.

6. The statistical method used is Chi Square ($X2$), which allowed us to analyze and determine if there is a relationship between two categorical variables.

7. Values indicating absolute independence, which are called expected frequencies (fo), were calculated by comparing them with the experimental frequencies (ft).

$$X^2 = \frac{(fo - ft)^2}{2} (1)$$

8. Conclusions based on the analysis of information and technological tool.

2.4. Hypothesis

Do computer attacks affect the server security of the GADPO's Linux operating system?

Null hypothesis (Ho): Computer attacks do not affect the server security of the GADPO's Linux operating system.

Alternative hypothesis (Ha): Computer attacks do affect the server security of the GADPO's Linux operating system.

2.5. Procedure

The research process was carried out in two settings. First, to obtain data that allows verification of the proposed hypothesis, several computer attacks were carried out on the GADPO Linux servers.

Then, based on the results obtained, mitigation measures were established, and computer attacks were carried out again to perform a statistical comparison and validate the effectiveness of the security measures implemented.

2.5.1. Scenario I

Kali Linux was used as the operating system, which is a Linux distribution used for penetration testing and security audits [7].

The phishing attack was carried out with the help of the Social Engineering Toolkit (SET) tool. [8].

Figure **1** shows the network diagram used to carry out phishing attacks.

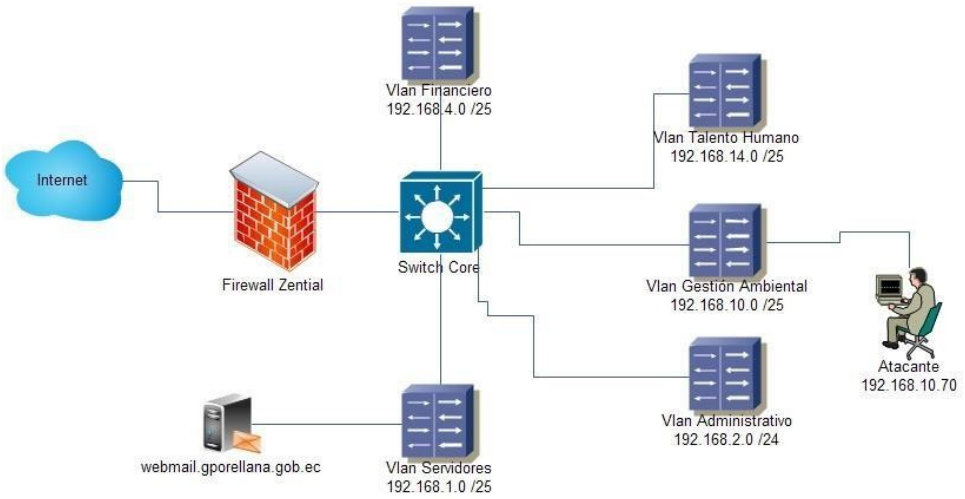

Figura 1

Network scheme used to carry out the phishing attack.

With the SET tool, the fake website was built, which made it possible to obtain the usernames and passwords of the users who accessed the hoax. One of the fake websites built is shown in Fig. 2.

Four phishing attacks were carried out on the institutional email server and the online procedures server, obtaining the following results:

The DDoS attacks were carried out on the firewall server of the GADPO data network because it was considered a critical service, which, if failed, would cause the collapse of the existing services on the network. Fig. 3 details the scheme used to carry out this type of attack.

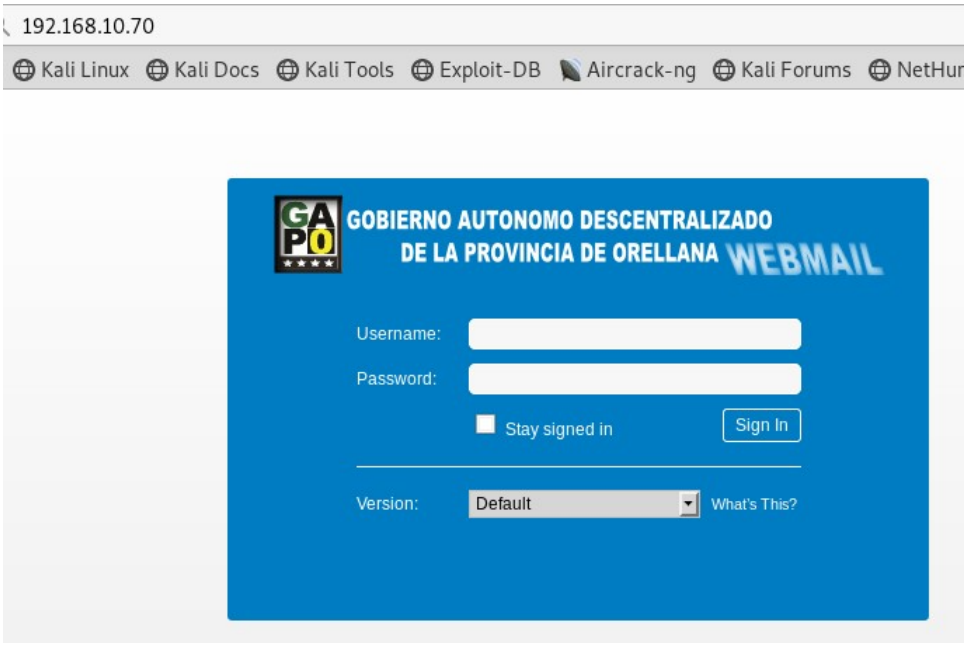

Figura 2

Fake website for phishing attack.

Tabla 5

Phishing attacks carried out on GADPO Linux servers.

Attack No.		Computer attacks	
	cloned website	Attacked users	Successful attacks
1	Institutional email server	73	52
2	Institutional email server	21	12
3	Online procedure server	21	15
4	Online procedure server	16	10
	TOTAL	131	89

A multi-router traffic graph (MRTG) was used to analyze network traffic and collect information about the bandwidth usage generated by the DDoS attack. software written in C that allows collecting information about the current load of hardware resources [9].

The DDoS SYN Flood attack was carried out by executing the hping3 command, the same one that allowed the generation of a large number of network packets and caused the data network to be flooded. The command used was as follows:

hping3 -V -c 1000 -d 100 -S -p 8443 –flood –rand-source 192.168.10.55

Thirteen DDoS attacks were carried out on the GADPO firewall server, obtaining the following results:

The MAGERIT methodology allows an organization that works with digital information to know its value and know how to protect it [10]. With the help of this methodology, after

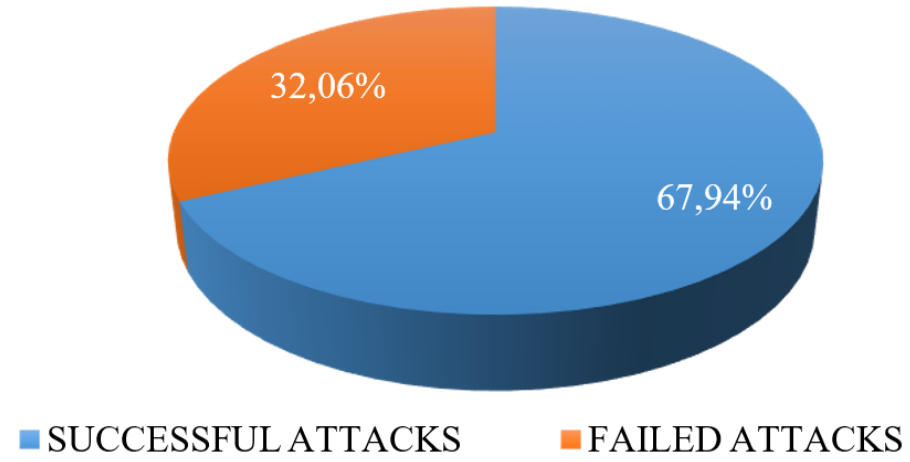

Figura 3

Final results of phishing attacks.

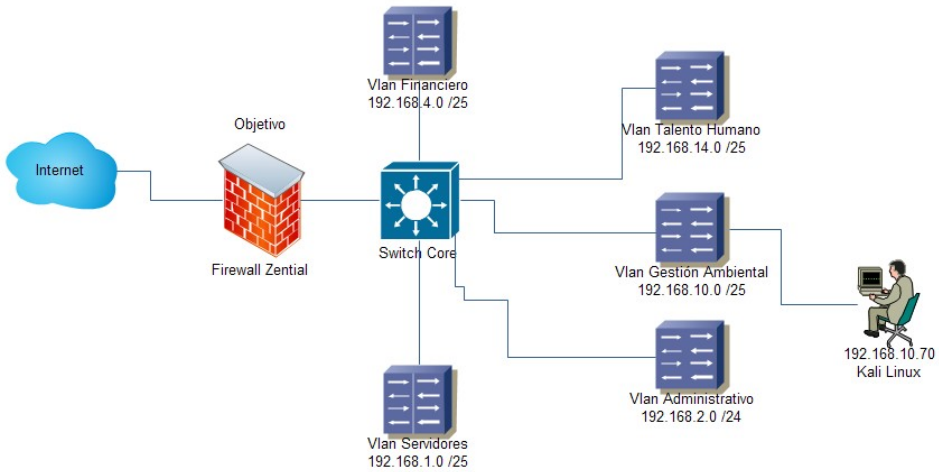

Figura 4

Network scheme used to carry out DDoS attack.

carrying out the computer attacks, the identification and determination of the impact of the risks to which Linux servers are exposed were carried out.

The scale used to measure the impact that a specific threat can produce on an information asset is the following [11]:

Vulnerabilities are the weaknesses that assets present and that make it easier for a specific threat to materialize [12].

The risk calculation is carried out using the scale suggested by MAGERIT [11], using the following formula:

Risk = *Threats* × *Vulnerability* (2)

Tabla 6

HPING3 command parameter description.

Parameter No.		DDoS attack command
	Parameter	Description
1	-c 2500	Number of packages to send
2	-d 100	Size in bytes of each packet
3	-S	Specifies that the SYN flag must be enabled
4	-p 8443	Specifies the port to which the attack will be directed
5	–flood	Send packages as quickly as possible
6	–rand-source	Generates spoofed IP addresses to disguise the real source, while stopping SYN-ACK response packets from the victim to the attacker

Tabla 7

DDoS attack result with 3 PCs.

Number of PCs	Attack number	Number of packages	Packet length (bytes)	
3	1	1000	100	12
3	2	1500	200	27
3	3	2000	300	31.5
3	4	2500	400	22.8
3	5	3000	500	22.8
3	6	3500	600	29.4
3	7	4000	700	29.4
3	8	4500	800	29.7
3	9	5000	900	30
3	10	5500	1000	29.1
3	11	6000	1500	30.3
3	12	6500	2000	24.6
3	13	7000	2500	27.6
	AVERAGE BANDWIDTH USE			26.63

Tabla 8

Magerit methodology impact scale.

Impact Level	Percentage
Low	0% - 25%
Intermediate	26% - 50%
High	51% - 75%
Very high	>76%

Information security dimensions affected by phishing and DDoS attacks are determined.

Tabla 9

Phishing attack vulnerability calculation.

No.		Phishing attack vulnerability	
	Attack	% Affected users	Vulnerability
1	Phishing	67.94%	67.94%

Tabla 10

DDoS attack vulnerability calculation.

No.		DDoS attack vulnerability	
	Attack	% Bandwidth usage	Vulnerability
1	DDoS	26.63%	26.63%

Tabla 11

Magerit Cyber Threat Scale.

No.	MAGERIT scale Threat	Percentage
1	View Information	0.33
2	Information Gathering	0.66
3	Disable Services	0.99

The dimensions affected in the case of phishing and DDoS attacks are:

Tabla 12

Impact on information security dimensions.

No.	Attack	Affect to dimensions. Dimensions Integrity Confidentiality	Availability
1	Phishing	x x	x
2	DDoS		x

Tabla 13

Risk calculation.

No.	Threat	Threat scale	Risk calculation Vulnerability	Impact	Risk
1	Phishing	View Information (0.33)	67.94%	High	22.42 %
2	Phishing	Information Gathering (0.66)	67.94%	High	44.84 %
3	Phishing	Disable Services (0.99)	67.94%	High	67.26 %
4	DDoS	Disable Services (0.99)	26.63%	Intermediate	26.36 %

2.5.2. Scenery II

Based on the results obtained in the first stage, measures were established to mitigate the effects caused by phishing and DDoS computer attacks.

To mitigate the risk that GADPO employees could be victims of a phishing attack, a training plan was designed. It was based on NIST SP 800-50 of the National Institute of Standards and Technology (NIST) of the United States Department of Commerce [14].

The structure of the designed training plan can be seen in Fig. 5 [15].

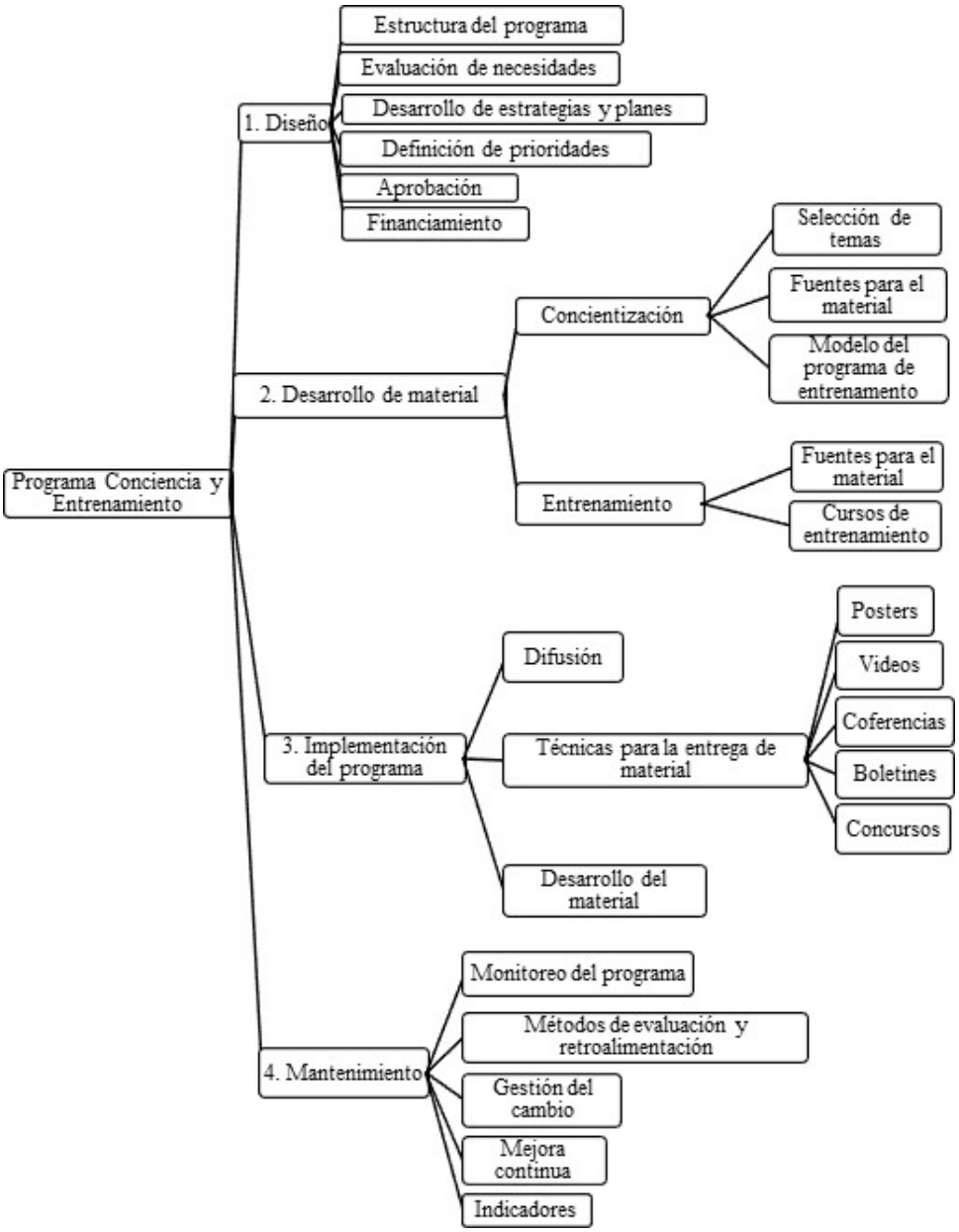

Figura 5

Structure of a training plan according to NIST SP 800-50.

It is considered as alternatives to mitigate DDoS type computer attacks [16, 17, 18]:

Table XV.

Tabla 14

Alternatives to mitigate DDoS attacks.

	Alternatives to mitigate DDoS		
No.	Alternative	Parameters	
		License	Cost
1	Using iptables (SYN Cookies, SYN Cache, SYN Proxy)	No	No cost
2	Appliances	Yes	Very High
3	Cloud solution	Yes	Mid

The alternative used to mitigate DDoS computer attacks was iptables, as it is a free tool, does not require licensing, and is also recommended by [16]. The iptables rules were configured on the firewall server of the GADPO data network.

Once the mitigation measures were implemented, computer attacks were conducted again under the same conditions described in stage I of this research, obtaining the following results:

After having trained GADPO users, successful phishing attacks reached 6.43%.

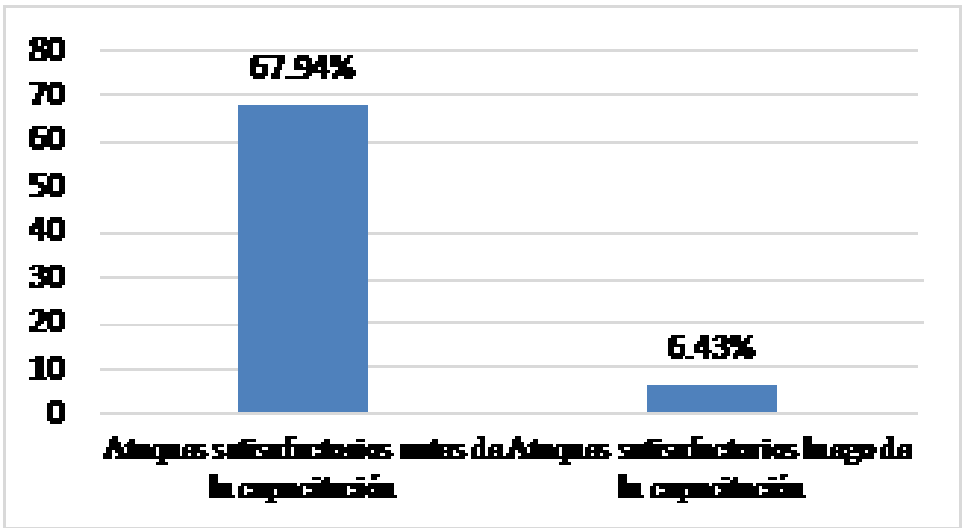

Figura 6

Final result of phishing attacks after training.

DDoS computer attacks reached 12.58% bandwidth usage after having implemented iptables rules on the firewall server.

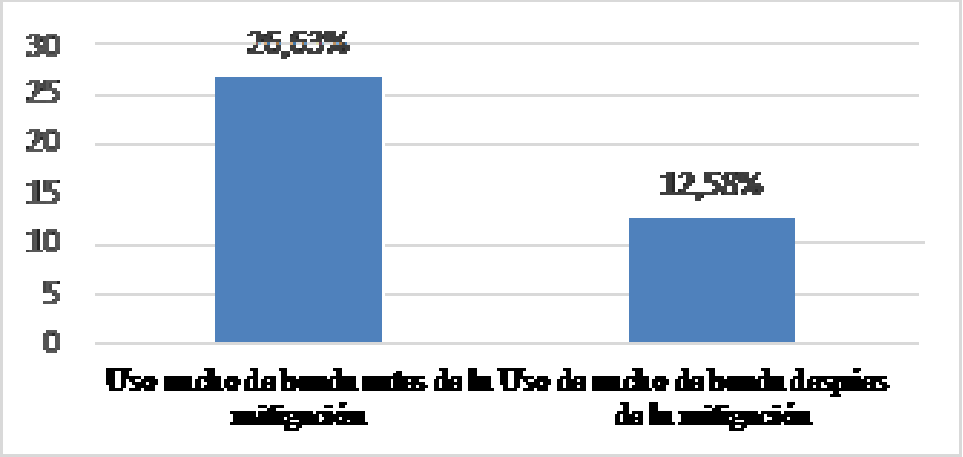

Figura 7

Bandwidth usage due to DDoS attacks.

3. Results and discussion

3.1. Hypothesis validation

To determine the level of impact of each of the computer attacks carried out on the GADPO Linux servers, the Likert scale proposed by Arellano in [13] was used.

Tabla 15

Likert scale.

No.		Likert scale	
	Affectation	Value	Percentage
0	Does not apply	0	—-
1	Very Low	1	0 – 20
2	Low	2	21 – 40
3	Medium	3	41 – 60
4	High	4	61 – 80
5	Very high	5	81 - 100

According to the degree of impact that each computer attack managed to cause on the information security dimensions, the following table is constructed, which is necessary to generate the contingency table of the Chi Square test [17].

The Chi-square test allows us to determine, as a result, whether two variables are related [19].

The contingency table is constructed from Table XVII.

The result of the Chi Square test is detailed in Table XIX.

Table XIX. Chi Square test calculation

Tabla 16

Attack test results.

		Computer attack results			
Test	Attack		Indicators		Total
		Confidentiality	Integrity	Availability	
Test 1	Phishing	4	4	4	12
Test 2	Phishing	3	3	3	9
Test 3	Phishing	4	4	4	12
Test 4	Phishing	4	4	4	12
Test 5	DDoS	0	0	1	1
Test 6	DDoS	0	0	2	2
Test 7	DDoS	0	0	2	2
Test 8	DDoS	0	0	2	2
Test 9	DDoS	0	0	2	2
Test 10	DDoS	0	0	2	2
Test 11	DDoS	0	0	2	2
Test 12	DDoS	0	0	2	2
Test 13	DDoS	0	0	2	2
Test 14	DDoS	0	0	2	2
Test 15	DDoS	0	0	2	2
Test 16	DDoS	0	0	2	2
Test 17	DDoS	0	0	2	2
Total		15	15	40	70
Likert		3.75	3.75	3.08	

Tabla 17

Chi Square test contingencies.

	Contingency table			
Affectation	Confidentiality	Integrity	Availability	Total
Low	0	0	1	1
Medium	0	0	12	12
High	1	1	1	3
Very high	3	3	3	9
Total	4	4	17	25

Calculated X^2 value = 14.201

The value found from the Chi Square test was 14.201, which is greater than the reference value of 12.596. Therefore, the null hypothesis (Ho) is rejected and the alternative hypothesis (Ha) is accepted, verifying that computer attacks do affect the security of servers with the GADPO Linux operating system[18].

Tabla 18

Ft	fo-ft	(fo-ft)∧2	x2
0.16	-0.16	0.026	0.16
1.92	-1.92	3.686	1.92
0.48	0.52	0.27	0.563
1.44	1.56	2.434	1.69
0.16	-0.16	0.026	0.16
1.92	-1.92	3.686	1.92
0.48	0.52	0.27	0.563
1.44	1.56	2.434	1.69
0.68	0.32	0.102	0.151
8.16	-5.16	26.626	3.263
2.04	-1.04	1.082	0.53
6.12	-3.12	9.734	1.591
TOTAL			14.201

Figura 8

Chi Square test graphical representation.

3.2. Discussion

To conduct the penetration tests, two scenarios were established. In the first scenario, computer attacks are carried out on the GADPO Linux servers. Then, in the second scenario, computer attacks are carried out once the protection measures have been implemented in order to be able to evaluate the effectiveness of the proposed solution [4].

In the first scenario, based on the results obtained from computer attacks carried out and with the help of the MAGERIT methodology, the following was determined:

Phishing computer attacks reached a vulnerability of 67.94%, which implies a high impact on information security; the risk of affecting confidentiality was 22.42%; the risk of availability was 67.26%; and the risk of the integrity of the information was 44.84%.

The DDoS attacks reached a vulnerability of 26.63%, an impact on information security of intermediate and a risk of information availability of 26.36%.

Once the mitigation measures were established, which in the case of the phishing attack was a training plan for GADPO officials based on the guide prepared by [15] and NIST SP 800-50, For the DDoS attack, the iptables rules were configured on the firewall server following the recommendations of [16, 17, 18].

The vulnerability caused by the phishing attack was reduced to 6.43%; the impact of the attack was low; the confidentiality risk was 2.12%; the integrity risk was 4.24%; and the information availability risk was 6.37%.

The vulnerability to DDoS computer attacks reached 12.58%, with a minimal impact level and a risk to information availability of 12.45% [20].

With the validation of the proposed hypothesis, it was possible to verify that phishing and DDoS computer attacks do affect the security of GADPO's Linux operating system servers. Therefore, as [6] mentions, information security management is something that must already be included in the organizational culture. In addition, it is vitally important to establish security mechanisms at the level of guides, procedures, and good security practices.

4. Conclusions

1. The bibliographic research allowed us to obtain information related to best practices on establishing mitigation measures against phishing and DDoS computer attacks.

2. The MAGERIT risk management methodology served as a guide to determine the vulnerability, impact, and risk caused by phishing and DDoS computer attacks on the GADPO Linux servers.

3. The effects of phishing computer attacks were mitigated by applying a training plan based on NIST SP 800-50 to GADPO officials.

4. DDoS attacks were controlled using iptables, Syn Cookies, Syn Cache and Syn Proxy

5. A procedure for securing servers with the Linux operating system was established, consisting of four phases. These were identification of computer attacks, evaluation of impact, establishment of mitigation measures, and finally verification tests of effectiveness for implemented measures.

References

[1] Aguilar M. "Plan de seguridad informática basado en estándar ISO- IEC 27001 para proteger la información y activos del Gad cantonal de Pastaza," 2017.

[2] Electrónico SG. Estrategia Para La Implantación De Software Libre En La Administración Pública Central. 2009. pp. 1–28.

[3] L. E. P. de C. Rico Ávila, "Defensa en profundidad basada en servidores." pp. 1–7, 2013.

[4] Jorge M. "Aseguramiento de infraestructuras de red y de servidores," pp. 1–5.

[5] H. U. C. del P. Aguinaga. "Análisis y dise no de un sistema de gestión de seguridad de información basado en la norma ISO / IEC 27001: 2005 para una empresa de producción y comercialización de productos de consumo masivo," 2013.

[6] Garzón DS, Ratkovich JC, Vergara A. Metodología de Análisis de Vulnerabilidades para Empresas de Media y Peque na Escala. 2013. pp. 1–10.

[7] Avilés R, Silva M. "Implementación de un modelo de seguridad para control de accesos a la red de datos, evaluando herramientas de hacking ético, en la empresa Blenastor," 2017.

[8] Esquerra L. "Pruebas de penetración con la herramienta Kali Linux en la Universidad Central Marta Abreu de las Villas." 2014.

[9] Torres G. "Desarrollo de una guía práctica para la medición del tráfico de red IP y monitoreo de dispositivos en tiempo real mediante herramientas MRTG y PRTG," 2010.

[10] Joya J, Sacristán C. Desarrollo de una Propuesta de Mitigación de Riesgos y Vulnerabilidades en Activos Lógicos. 2017. pp. 1–124.

[11] Hurtado LF. "Mecanismos para mitigar riesgos generados por la intrusión en routers de frontera basados en resultados de un honeypot virtual," 2017.

[12] INCIBE. "Gestión de riesgos. Una guía de aproximación para el empresario," 2015.

[13] Arellano J. " Modelo de seguridad contra ataques de denegación de servicio (DoS) de tráfico SIP en Servicios VoIP para redes LAN corporativas" 2017.

[14] Vega C. Concienciación en seguridad de la información. 2015. pp. 1–10.

[15] Álvarez D. “Guía para la Elaboración de un Plan de Concientización y Entrenamiento, sobre Seguridad de la Información,” 2017.

[16] RedHat. “Mitigate TCP SYN flood attacks with red hat enterprise Linux 7 Beta,” 2014. [Online]. Disponible: https://www.redhat.com/en/blog/mitigate-tcp-syn-flood-attacks-red- hat-enterpriselinux-7-beta. [Accessed: 25-Nov-2020].

[17] Shah D, Kumar V. Tcp syn cookie vulnerability. 2018. pp. 3–5.

[18] Malina L, Dzurenda P, Hajny J. “Testing of DDoS protection solutions.” 2015.

[19] Luna A. “Modelo conceptual para el uso de componentes electrónicos en el proceso de identificación de un sistema de información,” 2018.

[20] Qasim B, Musawi A. “Mitigating DoS / DDoS attacks using iptables.” 2012 June; pp. 101–111.