ESPOCH Congresses: The Ecuadorian Journal of S.T.E.A.M.
Volume 2, Issue no. 3, DOI 10.18502/espoch.v2i3.11594
Production and Hosting by Knowledge E

Research Article

Implementation of Filters and Rules on a Gateway to Mitigate Cyberattacks Originated by Email

Implementación de Filtros y Reglas Sobre un Gateway para Mitigar Ciberataques Originados por Correo Electrónico

César Rochina Rochina[1]*, Joffre Monar Monar[2]

[1]Investigador Independiente, Quito, Ecuador
[2] Escuela Superior Politécnica de Chimborazo, Centro de Admisión y Nivelación Riobamba, Ecuador

ORCID
Joffre Monar:https://orcid.org/0000-0002-6534-183X

II INTERNATIONAL CONGRESS OF SCIENCE AND TECHNOLOGY MORONA SANTIAGO 2021 (II CICTMS 2021)

Corresponding Author: César Rochina Rochina; email: crochina@protonmail.com

Published: 9 August 2022

Production and Hosting by Knowledge E

Abstract

This work proposes a methodology for the implementation of a set of rules and filters applied on a Gateway to mitigate the main cyberattacks originated through emails, such as: malware, spam, phishing, and includes information leakage. Through a comparative analysis of the tools that face these cyberattacks, ”Proxmox Email Gateway” is selected to be implemented in two test scenarios, the first without applying the methodology, and the second with its application, in which several Controlled cyberattacks of each of those previously defined. According to data obtained from the test scenarios, it was found that the application of this set of rules reduces cyberattacks by 38.75%, and with the statistical chi-square test with a confidence level of 95% it is shown that the set of filters and elaborate rules applied on a Gateway if it reduces the percentage of the amount of cyberattacks originated through e-mail.

Keywords: *Cyber-attack, email, spam, phishing, malware, Proxmox Email Gateway.*

Resumen

El presente trabajo propone una metodología para la implementación de un conjunto de reglas y filtros aplicados sobre un Gateway para mitigar los principales ciberataques originados a través de correos electrónicos, como: malware, spam, phishing, e incluye a la fuga de información. Mediante un análisis comparativo de las herramientas que afrontan a estos ciberataques, se selecciona a “Proxmox Email Gateway” para ser implementado en dos escenarios de prueba, el primero sin aplicar la metodología, y el segundo con su aplicación, en los cuales se ejecutaron varios ciberataques controlados de cada uno de los definidos previamente. De acuerdo con datos obtenidos de los escenarios de prueba, se contrastó que la aplicación de este conjunto de reglas reduce los ciberataques en un 38.75%, y con la prueba estadística de chi cuadrado con un nivel de confianza del 95% se demuestra que el conjunto de filtros y reglas elaborados aplicados sobre un Gateway si reduce el porcentaje de la cantidad de ciberataques originados a través de correo electrónico.

Palabras Clave: *Ciberataque, correo electrónico, spam, phishing, malware, Proxmox Email Gateway.*

OPEN ACCESS

How to cite this article: Rochina CR, Monar JM (2022). Implementation of Filters and Rules on a Gateway to Mitigate Cyberattacks Originated by Email. *ESPOCH Congresses: The Ecuadorian Journal of S.T.E.A.M.*, 2(3), 967–983. DOI 10.18502/espoch.v2i3.11594

1. Introducción

En la actualidad uno de los principales servicios que poseen las empresas es el correo electrónico, siendo ésta, el servicio de red que permite la comunicación entre sus usuarios e incluso con sus clientes y terceros, por este medio, se intercambian información y archivos importantes, tales como: documentos, fotografías. [1, 3].

Las principales amenazas a través de los correos electrónicos son: la propagación de malware a través de enlaces y archivos adjuntos, y el phishing [3, 5].

Es común recibir o enviar archivos adjuntos y enlaces externos a través del correo electrónico, frecuentemente entre remitente y destinatarios conocidos, sin embargo, no tienen la certeza de saber si están o no libres de malware [4, 6].

Las amenazas cibernéticas realizan cambios constantes en sus perspectivas, sin embargo, el uso de correo electrónico malicioso y el correo no deseado persiste como una herramienta vital para propagar malware, a razón de que a través de éste medio se puede llegar directamente al usuario final. Al aplicar la combinación correcta de técnicas de ingeniería social, como phishing, enlaces maliciosos y archivos adjuntos, los atacantes solo tienen que esperar a que los usuarios desprevenidos activen sus códigos maliciosos [6, 8].

El correo electrónico se ha convertido en uno de los principales vectores de ciber-ataque contra empresas en la actualidad. Un 87% de los profesionales de seguridad TI admitieron que su compañía se ha enfrentado a una amenaza a través de email en el último año [9].

Acoplado al objetivo de la seguridad de la información, considerando el rol principal del correo electrónico y las constantes amenazas de seguridad asociados a éstas, son los aspectos fundamentales que motivan a realizar la presente investigación que consiste en implementar un conjunto de reglas y filtros aplicados sobre un Gateway con el fin reducir los ciberataques originados a través de correo electrónico.

2. MATERIALES Y MÉTODOS

Para lograr el propósito de esta investigación, se aplicó el presente procedimiento:

2.1. A. Determinación de los ciberataques originados a través de correo electrónico

De acuerdo al “2018 Data Breach Investigations Report” [10], el 92.4 % de malware y el 96% de phishing, se distribuyen a través del correo electrónico [10], los tipos

de archivos más utilizados para propagar malware son documentos: pdf, doc, xlsx; y archivos comprimidos: zip, rar. [8]

En el año 2019, la proporción de spam de correo electrónico fue de 56.51%, la tasa más baja se registró en septiembre 54.68% y la más alta en mayo 58.71%.[11]

Según Adam Kujawa, director de Malwarebytes Labs, "el phishing es la forma más sencilla de ciberataque y, al mismo tiempo, la más peligrosa y efectiva, eso se debe a que ataca el ordenador más vulnerable y potente del planeta: la mente humana" [12].

Otra de las constantes amenazas son las fugas o filtración de información confidencial ocasionados por usuarios internos de una organización, ya sea de forma inadvertida o deliberada, para el primer caso la falta de conocimiento y formación en el manejo de información podrían ser las principales causas, mientras que, para el segundo caso, las causas podrían ser: el descontento de un empleado y el beneficio económico personal [6, 8, 13].

A continuación, en la Tabla 1, se resume los principales ciberataques originados a través de correos electrónicos.

Table 1

Ciberataques a través de correo electrónico.

Tipos de ciberataques	Descripción
Malware	Mensajes de correos electrónicos de contenido malicioso en archivos adjunto o enlaces externos.
Phishing	Mensajes de correo electrónicos aparentemente de remitente legitimo con la finalidad conseguir que se revele información confidencial.
Spam	Mensajes de correo electrónico masivo, anónimo y no solicitado.
Fuga de información	Mensajes de correo electrónico no autorizado, con información confidencial.

2.2. B. Secure Email Gateway

Es una solución integrada de seguridad que permite escanear correos electrónicos entrantes y salientes, con el fin de encontrar contenido malicioso o vulneren políticas definidas dentro de la red de una organización. La solución sitúa entre el servidor de correos y el firewall de borde con un espacio aislado para detectar y proteger contra la intrusión de malware, el spam, phishing. Además, posee módulos configurables para neutralizar la fuga de información, proporcionando una capa adicional de seguridad de correos electrónicos en las infraestructuras informáticas. [14, 16].

La herramienta Gateway para los escenarios de pruebas fue seleccionada de acuerdo al cumplimiento de las características que posee cada una de ellas, y en base a su menor costo para su implementación a razón de que son soluciones de código abierto, mismo que no se comercializa por licencia sino por suscripción permitiendo a los usuarios cambiar y mejorar el software de manera colaborativa, funciones que el software privativo no permitiría por derechos de autor [15, 16].

Table 2

Valoración de cumplimiento de características.

Cumplimiento de las características	SI	NO
Valoración	1	0

Table 3

Valoración de la herramienta Gateway.

Características del Gateway	Proxmox	Hermes	Mail Scanner	Mai ICleaner	Orange Assasin
Sender policy framework (SPF)	1	1	1	1	1
Motor AntiMalware	1	1	1	1	1
Listas Negras, Blancas, Gris	1	1	1	1	1
Filtro Bayesiano	1	1	1	1	1
Búsqueda y Seguimiento de eventos	1	1	1	0	0
Reglas del sistema personalizada	1	1	1	1	1
Autoaprendizaje	1	1	1	1	0
Administración web	1	1	0	1	0
TOTAL	8	8	7	7	5

De acuerdo con la Tabla 3, tomando en cuenta la valoración total de las dos herramientas con mayor puntaje y la experiencia del investigador en la administración de la plataforma Proxmox, en el escenario de pruebas se implementó “Promox Email Gateway” como la herramienta del servidor Gateway de correo electrónico [17].

C. Escenarios de prueba

El escenario de prueba simula una infraestructura de servicio de correo electrónico, para ello, en la red DMZ se implementó el servidor “Promox Mail Gateway” [17] como solución de seguridad, y Zimbra como servidor de correo electrónico [18].

Para realizar las pruebas, se implementó dos escenarios: el primer escenario simulará una infraestructura sin aplicar el conjunto de filtros y reglas, y el segundo escenario con su aplicación.

D. Técnicas propuestas

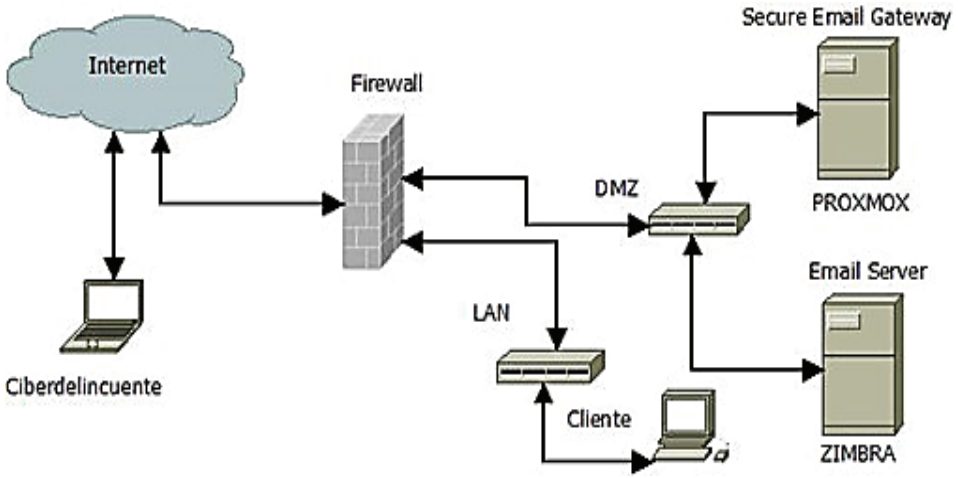

Figure 1

Diseño de la infraestructura de servicio de correo electrónico.

La metodología establece cinco fases a seguir para su implementación:

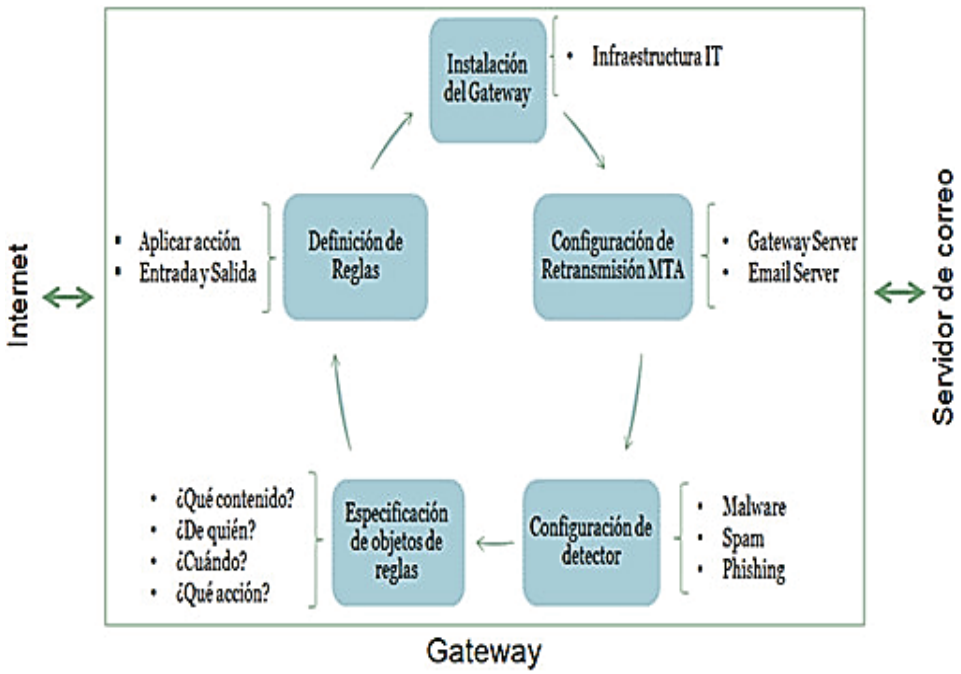

Figure 2

Esquema general de las fases de la metodología.

1. Instalación del Gateway de correo electrónico

El Gateway de correo electrónico deberá ser instalado entre el firewall de borde y el servidor de correo electrónico, el Gateway analizará todo el tráfico del protocolo SMTP entrante desde la red pública y el tráfico saliente desde el servidor de correo electrónico.

2. Configuración de Retransmisión MTA

En el servidor de correo electrónico se establece el nombre o la dirección IP del Gateway y el puerto como el host de retransmisión para entrega de correos electrónicos externos (gmail.com, espoch.edu.ec, etc.).

En el servidor Gateway se configura el nombre o la dirección IP del servidor de correo electrónico, el dominio interno de correos, y los puertos para dominio interno y externo.

Al utilizar el protocolo TLS en el Gateway, se asegura la transmisión de datos SMTP con un cifrado de extremo a extremo entre el Gateway y los servidores de SMTP en el internet, así como también con el SMTP Interno.

3. Configuración de detector de malware, Spam y Phishing

La configuración del motor de detección de malware dependerá del Gateway que se esté implementando, algunos Gateway de correo electrónico de código abierto utiliza CLAMV, mientras que las herramientas de código propietario incorporan su propio motor antimalware.

Los parámetros para el escaneo de archivos maliciosos que se deben tener en cuenta son los siguientes: tamaño de archivo, cantidad de recursión de escaneo y encriptación de archivos.

La configuración del motor de detección de spam y phishing dependerá del Gateway que se esté implementando, muchos Gateway de correo electrónico de código abierto utiliza Spamassassing, mientras que las herramientas de código propietario incorporan su propio motor *anti-Spam*.

La utilización automática de Filtros Bayesianos, Listas negras en tiempo real (RBL), Listas Blancas automáticas, Listas de Hash Razor, ayuda el autoaprendizaje del motor anti-Spam a nivel global, así como también, al seleccionar el lenguaje correcto de correos electrónicos entrantes según la necesidad de cada organización ayudan a reducir el número de correos a inspeccionar.

4. **Especificación de objetos de las reglas**

Define objetos que permite crear reglas personalizadas según las necesidades de cada organización, para definir reglas que permita el filtro de las cuentas de correo electrónico, dominios, Direcciones IP, tipo de contenido y finalmente la acción resultante, se ha categorizado los objetos de la siguiente manera: Usuarios, Contenido, Acción, Tiempo.

2.3. Objeto Acción

Son las acciones que se deben tomar sobre un determinado correo electrónico al cumplirse una o un conjunto determinado de reglas, las principales acciones indispensables son los siguientes: Aceptar, Bloquear, Mover a cuarentena, Notificar al administrador.

Acción Aceptar

El Gateway transfiere el correo electrónico al destino sea esta interno o externo.

Acción Bloquear

El Gateway Bloquea el correo electrónico

Acción Mover a Cuarentena

El Gateway mueve el correo electrónico a cuarentena hasta una acción manual del administrador o hasta cumplir un determinado tiempo definido.

Además de estas acciones, se deberán definir acciones personalizadas tales como: Notificar al administrador, Excluir archivos adjuntos.

Acción Notificar al Administrador

El Gateway notifica al administrador sobre los correos electrónicos bloqueados y enviados a cuarentena.

Acción Excluir archivos adjuntos

Se deberán excluir archivos adjuntos en los siguientes casos:

El Gateway removerá el archivo adjunto malicioso del correo electrónico, y el correo será transmitido al destino. Además, se pueden incluir la notificación de la acción realizada al administrador y/o al remitente.

El Gateway excluirá el archivo adjunto del correo electrónico si el archivo es superior al tamaño permitido, y el correo será transmitido al destino. Además, se pueden incluir la notificación de la acción realizada al administrador y/o al remitente.

2.4. Objeto Usuario

El objeto usuario define la dirección de correo electrónico, dominio, o dirección IP de servidores SMTP del remitente o el destinatario del correo electrónico al cual se aplicará una determinada o un conjunto de acciones, para ello se ha utilizada la creación categorizada de las listas Negras y Listas Blancas.

La construcción de listas blancas y listas negras personalizas se deberá realizar por tipo de remitentes, esto puede ser dirección IP de servidores SMTP, dominios de correo electrónico, direcciones o cuentas de correos, y éstas a su vez clasificadas o agrupadas

por proveedores, instituciones gubernamentales, instituciones educativas, etc, según sea requerido o definidas por las políticas internas de cada organización.

La clasificación y agrupación de dominio, direcciones IP, o cuentas de correos electrónicos en una lista, permitirá un mejor uso de éstas a la hora de definir las reglas de filtrado.

2.5. Objeto Contenido

Representa el contenido del correo electrónico y los archivos adjuntos, son objetos que deberán ser analizados para ejercer una acción sobre el archivo o a su vez sobre el correo electrónico.

2.6. Objeto Tiempo

En el objeto tiempo se puede definir un rango de tiempo u horario personalizado en el cual las reglas estarán activas.

3. Definición de Reglas

Para definir las reglas, se deberá tener en cuenta el trayecto del correo electrónico (Entrada o Salida, desde el punto de vista del Gateway) y la prioridad de la regla, además, contar con mínimo dos objetos definidos, indispensable “Objeto Acción”.

Las reglas se ordenan por prioridad, las reglas con mayor prioridad se ejecutarán primero, en caso de que las prioridades de dos o más reglas sean iguales la ejecución, el primero en ejecutar serán las reglas de entrada, seguido por las reglas de salida, y finalmente las reglas aplicadas para los dos trayectos “Entradas y Salidas”.

La prioridad de la regla se definirá según el nivel de riesgo que representa a la organización, generalmente las reglas de filtro contra las amenazas de malware, spam, phishing son de alta prioridad, puede tomar valores desde cero hasta cien.

4. Resultados

A. Desarrollo de pruebas

El desarrollo de las pruebas consiste en la evaluación de dos escenarios, el primero sin aplicar la metodología, y el segundo escenario con su aplicación.

A continuación, se describen los dos escenarios de pruebas desarrollados en la presente investigación:

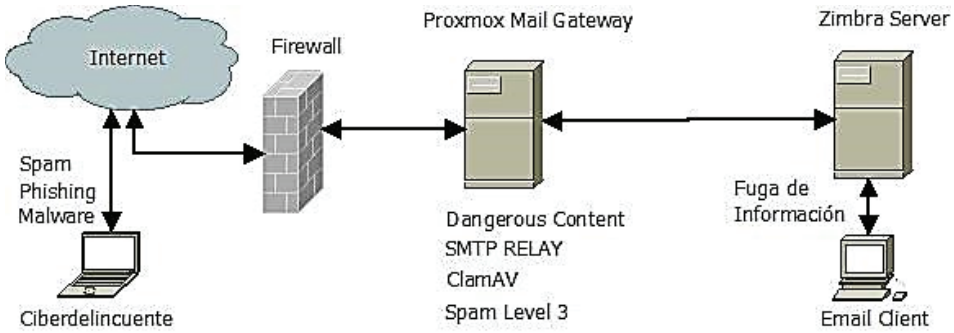

Figure 3

Diseño del primer escenario de pruebas.

Figura 3

El primer escenario de pruebas simula una infraestructura de servicio de correo electrónico protegido por un Gateway con una implementación básica basado en reglas, para filtrar el contenido malicioso, protección contra spam y protección contra malware.

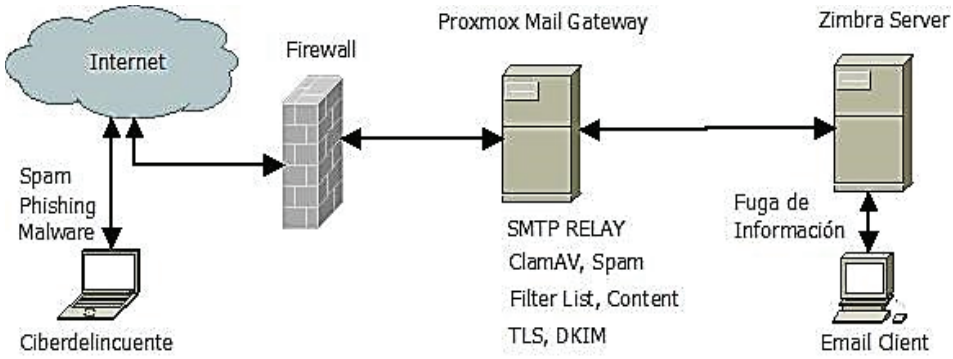

Figure 4

Diseño del segundo escenario de pruebas.

El segundo escenario de pruebas simula una implementación de acuerdo a la metodología de filtros y reglas aplicados sobre el Gateway, para proteger el servicio de correo electrónico, que consiste en: reglas de filtrado de contenidos y adjuntos maliciosos, implementación de listas blancas, listas negras, protección contra spam por niveles, protección contra malware, así como también, la transmisión segura desde y hacia entre el servidor de correo y el Gateway.

B. Ataques controlados

Sobre los dos escenarios se ejecutó ataques controlados de Spam, Phishing y Malware desde el internet, mientras que para el caso de fugas de información se ejecutó desde el cliente interno del correo corporativo.

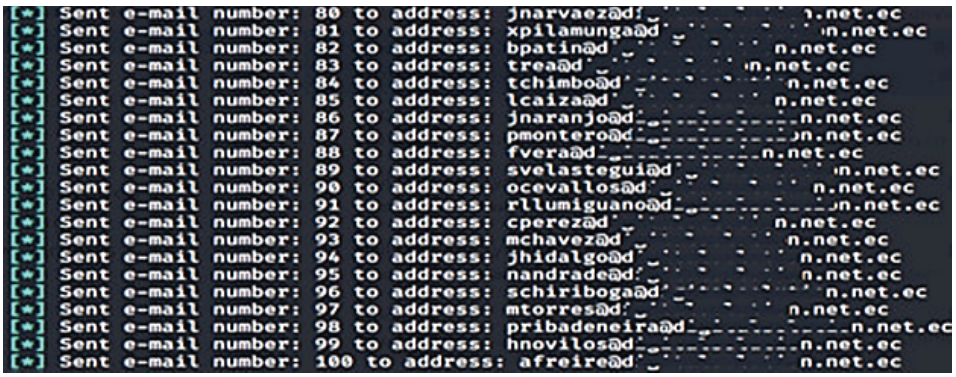

Figure 5

Ataques controlados sobre el escenario de prueba.

En la Figura 5, se puede observar un extracto de ataque realizado hacia un grupo de direcciones de correo, con la herramienta Social-Engineer Toolkit incorporado en Kali Linux [19, 20], en los escenarios de pruebas.

C. Análisis e interpretación de resultados

Se han ejecutado 400 ciberataques, lo que representa el 100% de ataques realizados para cada uno de los escenarios, en el primer escenario se obtuvo 228 ciberataques bloqueados, mientras que en el segundo escenario se obtuvo 383 ciberataques bloqueados.

Table 4

Resumen de ciberataques bloqueados.

	Total	Antes	Después
Cantidad	400	228	383
Porcentaje	100 %	57%	95,75%

A continuación, se describen los porcentajes de ciberataques bloqueados, obtenidos en los escenarios de pruebas realizadas en la presente investigación:

Como se puede apreciar la Figura 6, se tiene un total de 57 % de ciberataques bloqueados en el escenario antes de aplicar la metodología, y un total de 95.75 % de ciberataques bloqueados después de aplicar la metodología, representando un incremento del 38.75% en relación con el primer escenario.

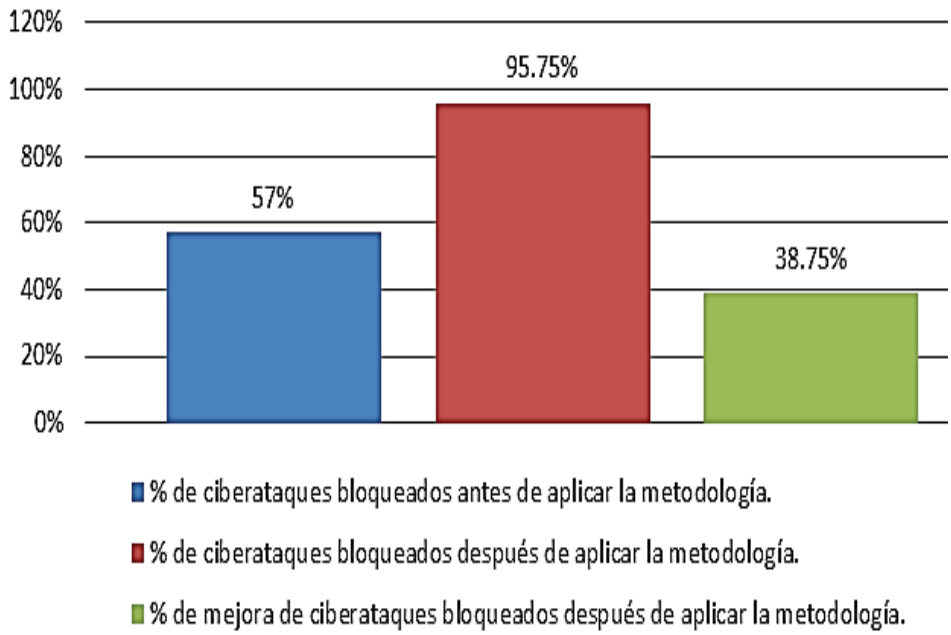

Figure 6

Porcentaje de ciberataques bloqueados antes y después de aplicar la metodología.

Table 5

Comparativa de ciberataques bloqueados para cada indicador

Ciberataque	Total	Antes	Después
Malware	100	89	98
Spam	100	45	97
Phishing	100	56	95
Fuga de información	100	38	93

Como se puede observar en la Tabla 5, para contrastar el porcentaje de reducción de ciberataques, se han ejecutado 100 ciberataques a través de correo electrónico por cada uno de los indicadores, sobre los dos escenarios de pruebas.

A continuación, se describen los porcentajes de mejora de ciberataques obtenidos durante las pruebas realizadas en base a cada uno de los escenarios:

Previa a la aplicación del conjunto reglas y filtros de la metodología se obtuvieron los siguientes porcentajes de ciberataques bloqueados: 89 % de ataques de malware, 45 % de ataques de Spam, 56% de ataques de Phishing, y el 38% de fuga de información, posterior a ello se bloquearon: 98% de ataque de malware, 97 % de ataque de Spam, 95 % de ataques Phishing, 93 % de correos electrónicos de fuga de información, y se contrasta que el nivel de porcentaje de bloqueos de ciberataques se ha incrementado,

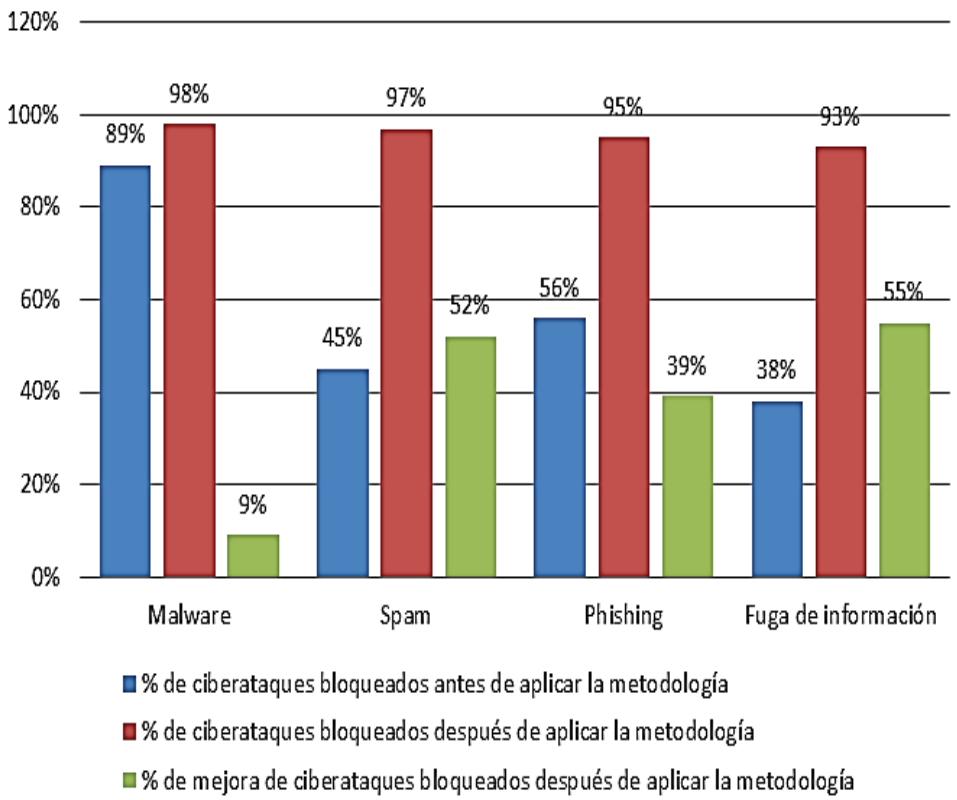

Figure 7

Porcentaje de mejora de ciberataques bloqueados después de aplicar la metodología.

para Malware en un 9%, para Spam en un 52%, para Phishing en un 39%, y para la fuga de información en un 55%.

E. Prueba de hipótesis

Se pretende analizar los resultados obtenidos para poder demostrar la incidencia positiva de la utilización de un conjunto de reglas y filtros sobre un Gateway con el fin de reducir los ciberataques originados por correo electrónico, las mismas son:

Ha: La utilización de un conjunto de filtros y reglas sobre un Gateway se relaciona significativamente con la cantidad de ciberataques encontrados a través de correo electrónico

H0: La utilización de un conjunto de filtros y reglas sobre un Gateway no se relaciona significativamente con la cantidad de ciberataques encontrados a través de correo electrónico

De las Tablas 6 y 7 se obtiene el valor de Chi-cuadrado que es de 166.44 con un grado de libertad y un nivel de significancia del 0.05, el valor crítico según la tabla es de 3.84; por lo que X^2 calc es mayor que X^2 Critico, por lo tanto, se rechaza la H0 y se acepta la Ha, es decir que la utilización de un conjunto de filtros y reglas sobre un

Table 6

Frecuencias de valores observados.

Valores Observados	Antes	Después	Total
Cantidad Bloqueados	228	383	611
Cantidad no Bloqueados	172	17	189
TOTAL	400	400	800

Table 7

Frecuencia de valores esperados.

Valores Esperados	Antes	Después	Total
Cantidad Bloqueados	305,5	305,5	611
Cantidad no Bloqueados	94,5	94,5	189
TOTAL	400	400	800

Gateway se relaciona significativamente con la cantidad de ciberataques encontrados a través de correo electrónico y por lo tanto mejora el nivel de seguridad.

5. DISCUSIÓN

Se han realizado varias investigaciones previas con el fin de mejorar la seguridad en los correos electrónicos, entre las que destacamos: [21]

"Diseño de un marco de trabajo para la gestión de riesgos de ingeniería social basado en los estándares ISO 27002 y NIST 800-50". [22]

Establece una propuesta para la mitigación de riesgos que involucra el componente humano, únicamente establece ciertas reglas en el Firewall para controlar ataques tipo DDos SYN Flood, pero no aborda configuraciones para otro tipo de ataques que involucran a correos electrónicos.

"Análisis y diseño de una propuesta para mitigar ataques cibernéticos a correos electrónicos utilizando técnicas de hacking ético". [23]

Analiza ataques de tipo spoofing, phishing, mailing y bomba, y establece propuestas de solución para usuario final y no en prevenir estos ataques a nivel de soluciones en el servidor de correo electrónico.

"Diseñar e implementar el prototipo de una arquitectura de seguridad aplicada a una institución financiera para mitigar los Ataques de malware". [24]

Establece el uso de una herramienta para la detección de ataques tipo malware y los compara con controles de seguridad estándar como antivirus y firewall perimetral, pero no incluye configuraciones a nivel de software para evitarlas.

“Diseño de un proceso de hardening de servidores para una Institución financiera del sector público”. [25]

Establece configuraciones de Firewall a nivel de sistema operativo, pero no incluye otro tipo de firewall especializado, ni configuraciones personalizadas, para prevenir amenazas en correos electrónicos.

Estas investigaciones si bien son importantes para mejorar el nivel de seguridad en el uso de correos electrónicos, principalmente están enfocadas al usuario final y en la seguridad de servidores a nivel general.

La presente investigación define una metodología de filtros y reglas sobre un Gateway que servirá como base para asegurar el servicio de correo electrónico a nivel de servidor, como una solución adicional e específica de seguridad para mitigar ataques de tipo: Malware, Spam, Phishing y Fuga de información, y pueda ser aplicada e implementada dentro de una infraestructura informática de cualquier organización para mejorar la protección de la información.

6. Conclusiones

Mediante el estudio de los diferentes ciberataques que se originan a través de correos electrónicos se logró identificar los ciberataques más frecuentes acontecidos durante el año 2019, tales como: el malware con un 92.4 % y phishing 96 % son distribuidos a través de correo electrónico y el 56.51% de correos electrónicos son Spam, así como también, que el correo electrónico es un medio utilizado para la fuga de información.

Existen numerosas herramientas Gateway de correo electrónico de código abierto, así como también de código propietario que permiten mitigar los diferentes tipos de ciberataques que se originan a través del correo electrónico, mismas que comparten las siguientes características principales: Antimalware, Antispam, personalización de reglas, generación de Listas Negras y Blancas, seguimiento de eventos, autoaprendizaje, y la administración web.

Se implementó dos escenarios de pruebas, la primera sin aplicar el conjunto de filtros y reglas propuestos, y la segunda con su aplicación, sobre cada una de ellas se ejecutaron 400 ciberataques que consistió en correos electrónicos de contenido malicioso, dando como resultado lo siguiente: en el primer escenario se detectaron el 57 % de ciberataques, mientras que en el segundo escenario se detectaron el 95.75

% de ciberataques y de esta manera se contrastó que el conjunto de reglas y filtros propuesto si reduce los ciberataques originados a través de correo electrónico en un 38.75 %.

La implementación de filtros y reglas sobre un gateway para mitigar ciberataques originados por correo electrónico describe cinco (5) fases a seguir: Instalación del Gateway de correo electrónico, Configuración de Retransmisión MTA, Configuración de detector de malware, Spam y Phishing, Especificación de objetos de las reglas, y finalmente la Definición de Reglas

7. CONFLICTO DE INTERESES

No existe ningún conflicto de intereses en el desarrollo de esta investigación, los resultados obtenidos son auténticos y son el producto del análisis de los datos obtenidos en los dos escenarios de prueba.

References

[1] EcuRed. Correo Electrónico. [Online].; 2017 [cited 2020 abril 15]. Available from: https://www.ecured.cu/Correo_electr%C3%B3nico.

[2] Avast. Qué es el spam: guía esencial para detectar y prevenir el spam. [Online].; 2019 [cited 2020 marzo 13]. Available from: https://www.avast.com/es-es/c-spam.

[3] Cofense. Threat Intelligence. [Online].; 2018 [cited 2020 abril 15]. Available from: https://cofense.com/sigma-operators-craft-new-techniques-deliver-phish-inbox/.

[4] CISCO. Reporte Anual de Ciberseguridad. [Online].; 2018 [cited 2020 abril 20]. Available from: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf.

[5] Instituto Nacional de Ciberseguridad. Uso del correo electrónico. [Online].; 2017 [cited 2020 abril 15]. Available from: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-correo-electronico.pdf.

[6] Universidad Nacional de Luján. Amenazas a la Seguridad de la Información. [Online].; 2017 [cited 2020 marzo 13]. Available from: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12.

[7] Antonio Hernandez SS. Sistema para la detección de ataques phishing utilizando correo electrónico. TELEMÁTICA. 2018 agosto; 17(2).

[8] CISCO. Seguridad del correo electrónico. [Online].; 2019 [cited 2020 abril 15]. Available from: https://www.cisco.com/c/dam/global/es_es/products/security/pdfs/es_email_sec_report.pdf.

[9] Barracuda Networks Inc. Email Security Trends. [Online].; 2018 [cited 2020 abril 20]. Available from: https://blog.barracuda.com/wp-content/uploads/2018/06/EmailSecurityTrends_Global.pdf.

[10] Verizon. 2018 Data Breach Investigations Report. [Online].; 2019 [cited 2020 abril 20]. Available from: https://www.verizon.com/business/resources/reports/DBIR_2018_Report_execsummary.pdf

[11] Securelist by Kaspersky. El spam y el phishing en 2019. [Online].; 2019 [cited 2020 abril 20]. Available from: https://securelist.lat/spam-report-2019/90176/

[12] Malwarebytes. Suplantación de identidad (phishing). [Online].; 2019 [cited 2020 abril 20]. Available from: https://es.malwarebytes.com/phishing/

[13] Vaca M. Solución de control de fuga de información confidencial saliente (data lost prevention) a través de navegación web, correo electrónico y estaciones móviles [Tesis] , editor. [Guayaquil]: ESPOL; 2016.

[14] AVANAN. What Is a Secure Email Gateway and Are They Still Viable? [Online].; 2019 [cited 2020 abril 20. Available from: https://www.avanan.com/blog/what-is-a-secure-email-gateway.

[15] FORCEPOINT. What is a Secure Email Gateway? [Online].; 2018 [cited 2020 marzo 13]. Available from: https://www.forcepoint.com/cyber-edu/secure-email-gateway.

[16] Proofpoint. Email Gateway. [Online].; 2018 [cited 2020 marzo 13. Available from: https://www.proofpoint.com/us/threat-reference/email-gateway.

[17] Proxmox Server Solutions. Proxmox Mail Gateway. [Online].; 2018 [cited 2020 abril 23. Available from: https://www.proxmox.com/en/proxmox-mail-gateway.

[18] Ahmad Yannuri MIWAI. Design and Build Mail Server Systems Using Zimbra 8.8.15 and Antispam on Proxmox Mail Gateway 5.2. INSTITUTE OF COMPUTER SCIENCE (IOCSCIENCE). 2020 mayo; 4(1).

[19] Kali Linux. Kali Tools - SET Package Description. [Online].; 2020 [cited 2020 febrero 21]. Available from: https://tools.kali.org/information-gathering/set.

[20] GITHUB. Social-Engineer Toolkit. [Online].; 2020 [cited 2020 febrero 25. Available from: https://github.com/trustedsec/social-engineer-toolkit/.

[21] Rochina C. Diseño y evaluación de una metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway [Tesis] , editor. Riobamba: ESPOCH; 2021.

[22] Fernandez M. Diseño de un marco de trabajo para la gestión de riesgos de ingeniería social basado en los estándares ISO 27002 y NIST 800-50 [Tesis] , editor. Quito: UISEK; 2019.

[23] Alvear F. Análisis y diseño de una propuesta para mitigar ataques cibernéticos a correos electrónicos utilizando técnicas de hacking ético [Tesis] , editor. Quito: PUSE; 2019.

[24] García L. Diseñar e implementar el prototipo de una arquitectura de seguridad aplicada a una institución financiera para mitigar los ataques de malware [Tesis] , editor. Guayaquil: ESPOL; 2018.

[25] Caiza A. Diseño de un proceso de Hardening de servidores para una institución financiera del sector público [Tesis] , editor. Quito: UISEK; 2019.