ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

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

CESAR GONZALO ROCHINA ROCHINA

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA – ECUADOR

Junio 2021

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado 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, de responsabilidad del señor CESAR GONZALO ROCHINA ROCHINA ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Ing. Oswaldo Geovanny Martínez Gaushima; M.Sc.
PRESIDENTE

OSWALDO GEOVANNY MARTINEZ GUASHIMA
Firmado digitalmente por OSWALDO GEOVANNY MARTINEZ GUASHIMA

Ing. Joffre Stalin Monar Monar, Mag.
DIRECTOR

JOFFRE STALIN MONAR MONAR

Ing. Paúl Xavier Paguay Soxo; Mag.
MIEMBRO

Firmado digitalmente por PAUL XAVIER PAGUAY SOXO
Fecha: 2021.04.29 10:23:42 -05'00'

Ing. Marco Vinicio Ramos Valencia; Mag.
MIEMBRO

Firmado electrónicamente por:
MARCO VINICIO RAMOS VALENCIA

Riobamba, junio 2021

DERECHOS INTELECTUALES

Yo: César Gonzalo Rochina Rochina, soy responsable de las ideas, doctrinas, resultados expuestos en este trabajo de Titulación y el patrimonio intelectual del mismo pertenece a la Escuela Superior Politécnica de Chimborazo.

Firmado electrónicamente por:
CESAR GONZALO ROCHINA ROCHINA

César Gonzalo Rochina Rochina

No. Cédula: 0201957206

DECLARACIÓN DE AUTENTICIDAD

Yo: César Gonzalo Rochina Rochina, declaro que el presente Trabajo de Titulación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados. Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Firmado electrónicamente por:
CESAR GONZALO ROCHINA ROCHINA

César Gonzalo Rochina Rochina

No. Cédula: 0201957206

DEDICATORIA

A mi esposa e hija quienes con su amor incondicional supieron motivarme moral y materialmente para seguir luchando y mejorando cada día, y culminar una etapa más de mi vida, a mis padres por su dedicación y ejemplo de vida, y a mis hermanos, quienes han estado conmigo siempre en todas las etapas de mi vida.

César

AGRADECIMIENTOS

Agradezco a Dios por darme salud y cuidar de mis seres queridos, a los maestros de mi formación de postgrado quienes compartieron sus valiosos conocimientos y guiaron la culminación de este trabajo de investigación. Agradezco infinitamente a mi esposa e hija, por comprender mi ausencia durante las largas jornadas de estudio, a mis padres y hermanos por todo el apoyo para cumplir mis metas.

César

CONTENIDO

Paginas

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

Se elaboró una metodología basada en reglas y filtros para detectar correos electrónicos maliciosos, para ello, mediante el estudio de arte de los diferentes ciberataques que se originan a través de correos electrónicos se determinaron los siguientes: ataque de malware, Spam, y phishing, así como también que el correo electrónico es un medio utilizado para la fuga de información, de la misma forma, se determinó las características principales que poseen las herramientas que afrontan a dichos ciberataques, siendo estas: Antimalware, Antispam, personalización de reglas, generación de Listas Negras y Blancas, seguimiento de eventos, autoaprendizaje, y la administración web. Mediante un análisis comparativo se seleccionó la herramienta "Proxmox Email Gateway" para ser implementado en los dos escenarios de pruebas, el primero sin aplicar la metodología elaborada y el segundo con su aplicación, para cada uno de los escenarios se ejecutaron cibertaques controlados. De acuerdo a lo datos obtenidos de los escenarios de pruebas se contrastó que la metodología elaborada reduce los ciberataques originados a través de correo electrónico en un 38,75 % y mediante la prueba estadística de chi-cuadrado con un nivel de confianza del 95% se demostró que la metodología elaborada mediante la aplicación de filtros y reglas sobre un Gateway si reduce el porcentaje de la cantidad de ciberataques originados a través de correo electrónico. Se recomienda monitorear el Gateway de correo electrónico de manera constante, con el fin de adicionar nuevos filtros y reglas que detecten los cibertaques más recientes, ya que cada día se descubren nuevas técnicas o malware que vulneran los sistemas de seguridad.

Palabras Claves: <CIBERATAQUE>, <CORREO ELECTRÓNICO>, <SPAM>, <PHISHING>, <MALWARE>, < ZIMBRA>, <PROXMOX MAIL GATEWAY>.

LUIS ALBERTO CAMINOS VARGAS

Firmado digitalmente por LUIS ALBERTO CAMINOS VARGAS
Nombre de reconocimiento (DN): c=EC, l=RIOBAMBA, serialNumber=0602766974, cn=LUIS ALBERTO CAMINOS VARGAS
Fecha: 2021.04.29 12:47:17 -05'00'

UNIDAD DE PROCESOS TÉCNICOS DBRA DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE ESPOCH

ABSTRACT

A methodology based on rules and filters was developed to detect malicious emails, for this, by studying the art of the different cyberattacks that originate through emails, the following were determined: malware attack, Spam, and phishing, as well as well as that email is a means used for information leakage, In the same way, the main characteristics of the tools that face these cyberattacks were determined, these being: Antimalware, Antispam, customization of rules, generation of Black and White Lists, event tracking, self-learning, and web administration. Through a comparative analysis, the "Proxmox Email Gateway" tool was selected to be implemented in the two test scenarios, the first without applying the developed methodology and the second with its application. For each of the scenarios, controlled cyber attacks were executed. According to the data obtained from the test scenarios, it was found that the methodology developed reduces cyberattacks originated through email by 38.75% and by means of the chi-square statistical test with a confidence level of 95%, demonstrated that the methodology developed by applying filters and rules on a Gateway does reduce the percentage of the number of cyberattacks originated through email. It is recommended to monitor the email gateway constantly, in order to add new filters and rules that detect the most recent cyber attacks, since new techniques or malware that violate security systems are discovered every day.

Keywords: < CYBER ATTACK>, <EMAIL>, <SPAM>, <PHISHING>, <MALWARE>, <ZIMBRA>, <PROXMOX MAIL GATEWAY>.

CAPÍTULO I

1. INTRODUCCIÓN

1.1 Planteamiento del problema

1.1.1 Situación problemática

La importancia de la seguridad de la información para las empresas u organizaciones, sean éstas públicas o privadas, radica en el hecho de que la información es el activo más preciado, por lo tanto, la protección ante el riesgo de pérdida o degradación de la confidencialidad, integridad y disponibilidad, se encamina en la capacidad de mitigar las amenazas que afecten a éste bien.

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 éste medio, se intercambian información y archivos importantes, tales como: documentos, fotografías, entre otros. (Fajardo, 2017)

El correo electrónico, también puede ser utilizado por ciberdelincuentes para consumar ciberataques. Las principales amenazas que se tiene a través de los correos electrónicos son: La propagación de malware a través de enlaces y archivos adjuntos, y el phishing. Es común recibir archivos adjuntos y enlaces externos por medios de correos electrónicos, el verdadero problema es que no se tiene la certeza de saber si son archivos o enlaces libres de malware, e incluso, muchas veces provienen de personas o entidades conocidas que ni siquiera el remitente sabe que está enviando archivos o enlaces infectados de malware. (Barracuda, 2018)

El phishing (robo de identidad), su principal característica es parecer a correos inofensivos de personas conocidas o entidades bancarias, que a través de ingeniería social incita al usuario a interactuar con ella o a través de un enlace externo, con la finalidad de obtener información confidencial. (Doig, 2019)

Las amenazas cibernéticas realizan cambios constantes en sus perspectivas, pero el uso de correo electrónico malicioso y el correo no deseado como medio de propagación siguen siendo una de las herramientas vitales para que los ciberdelincuentes distribuyan malware, a razón de que el correo electrónico lleva las amenazas 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. (Cisco, 2018)

El correo electrónico se ha convertido en uno de los principales vectores de ciberataque 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, de acuerdo con el reciente informe 2018 Email Security Trends de Barracuda. (Barracuda, 2018)

Talos, la división de ciberseguridad de Cisco, ha analizado en su informe "Email: Click with Caution" que el correo electrónico es el principal vector para la distribución de «malware» (92,45 %) y de «phishing» (96 %). Y protegerse es cada vez más difícil para el 70 por ciento de los consultados, debido al uso de técnicas de ingeniería social y archivos adjuntos menos sospechosos, además, según los últimos datos de Cisco, los ataques Business Email Compromise (BEC) y Email Account Compromise (EAC) supusieron en 2018 unas pérdidas mundiales de 1.300 millones de dólares. En comparación, el «ransomware» que aportó a los ciberdelincuentes 3,6 millones. (Talos Cisco, 2019)

En el intento de gestionar y mitigar incidentes de seguridad informática, se siguen desarrollando diferentes técnicas, métodos y herramientas tanto proactivas como reactivas que permiten hacerles frente a ciberdelincuentes, tales como: Firewalls, Sistemas de Prevención de Intrusos IPS, Sistemas de Detección de Intrusos IDS, Honeypots, antimalware, entre otros.

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

- "Diseño de un marco de trabajo para la gestión de riesgos de ingeniería social basado en los estándares ISO 27002 y NIST 800-50". (Fernández, 2019)
- "Análisis y diseño de una propuesta para mitigar ataques cibernéticos a correos electrónicos utilizando técnicas de hacking ético". (Díaz, 2019)
- "Diseñar e implementar el prototipo de una arquitectura de seguridad aplicada a una institución financiera para mitigar los Ataques de malware". (Alvear,2019)
- "Diseño de un proceso de hardening de servidores para una Institución financiera del sector público". (Caiza, 2019)

Estas investigaciones si bien son importantes para mejorar el nivel de seguridad en el uso de correos electrónicos, están principalmente enfocadas al usuario final y en la seguridad de servidores a nivel general y no definen métodos o técnicas puntuales que sirvan como base para asegurar el correo electrónico a nivel de servidor antes que las amenazas que se propagan a través de este servicio puedan llegar al buzón del usuario.

Persiguiendo el objetivo de la seguridad de la información, teniendo en cuenta el rol principal del correo electrónico y los problemas de seguridad asociados a éstas, son los aspectos fundamentales que motivan a realizar la presente investigación que consiste en elaborar una

metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway.

1.1.2 Formulación del problema

¿Es posible reducir los ciberataques originados a través de correos electrónicos mediante una metodología basado en la aplicación filtros y reglas sobre un Gateway?

1.1.3 Preguntas directrices o específicas de la investigación

¿Cuáles son los principales ciberataques que se originan a través del correo electrónico?

¿Cuáles son las metodologías existentes para reducir los ciberataques originados a través de correos electrónicos?

¿Cuáles son las características, reglas y filtros aplicados sobre la herramienta Gateway de correo electrónico?

¿Qué porcentaje de ciberataques originados a través de correos electrónicos se reducirán aplicando la metodología basada en filtros y reglas sobre un Gateway?

1.2 Justificación de la investigación

1.2.1 Justificación Teórica

En la actualidad, ante el nivel de complejidad y la cantidad de ataques a las que son sometidas las infraestructuras informáticas de las empresas, se han desarrollado diferentes tipos de protección que tratan de contener y mitigar las técnicas desarrolladas para atentar contra la confidencialidad, integridad y disponibilidad de la información, de la misma forma, los ciberataques se han incrementado perfeccionando sus técnicas para evadir éstas protecciones con el fin de conseguir su objetivo.

Una de las nuevas técnicas utilizadas por los atacantes en la actualidad es utilizar las cuentas de correos electrónicos logrando crear una copia casi exacta como si se tratara de una cuenta oficial y legítima, de esta manera, los atacantes logran engañar a la víctima para propagar y hacer llegar archivos adjuntos infectados con malware, siendo capaces de eludir los niveles de seguridad implementadas, convirtiéndose en una de las técnicas más directas, efectivas e incluso rápidas para lograr su cometido. (Cofense, 2017)

Según el Informe de investigaciones sobre la infiltración de datos de 2018 de Verizon, del que Cisco es un colaborador, el correo electrónico es el principal vector para la distribución de malware (92,4 %) y la suplantación de identidad (96 %), por lo tanto, es importante tomar medidas de protección ante este tipos de amenazas para mitigar ciberataques que afecten a la seguridad de la información de una organización. (Verizon, 2019)

Gateway para correo electrónico viene a ser una solución integrada de seguridad de correos, proporcionando monitoreo en tiempo real del tráfico de correo electrónico, desplegada frente al servidor, actúa como puerta de entrada y salida a la plataforma de correo electrónico para escanear, detectar y bloquear el spam y malware, además, permite el filtrado de contenido con el que se puede aminorar la fuga de información confidencial que se produce a través de este servicio.

Los servicios Gateway para el correo electrónico son contramedidas rentables que las empresas u organizaciones pueden adquirir e implementar contra los ciberataques que se presentan a través de los correos, trasladando a cuarentena los correos electrónicos sospechosos hasta que se puedan determinar si se trata de un correo legítimo y libre de amenazas para la organización.

En la presente investigación, se va a diseñar y evaluar una metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway, en base a las principales amenazas actuales que se propagan a través de éste servicio y ésta metodología permitirá reducir los ciberataques con la detección y aislamiento de los correos electrónicos de contenido malicioso, así como también, impedir o disminuir la fuga de información confidencial.

1.2.2 Justificación Metodológica

Basados en las metodologías existentes tales como: Filtros Bayesianos, Listas Negras, entre otras; se diseñará y evaluará una metodología basadas en reglas y filtros sobre un Gateway para la seguridad de correos electrónicos;

A continuación se describen brevemente dos (2) de las metodologías más importantes:

- Filtros Bayesianos.- Pueden agrupar diferentes análisis de vocabulario que permiten generar un conjunto de palabras a tomar en cuenta al momento de aplicar el filtro, se basan, principalmente, en la experiencia de correos electrónicos marcados manualmente por el usuario como spam, por lo tanto, se necesitan de la intervención de los usuarios para ser más efectivos.

- Listas Negras.- Son listas que contiene direcciones IP de servidores de correo, cuentas de correos electrónicos y comprueba la confiabilidad del remitente para aceptar o denegar los correos electrónicos, con la finalidad de reducir la recepción de correos no solicitados o de contenido maliciosos.

1.2.3 Justificación Práctica

Con la implementación del Gateway aplicando la metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway se procura reducir los ataques cibernéticos en las infraestructuras informáticas de una organización, principalmente en el servicio de correo electrónico, las pruebas se realizarán en un ambiente simulado que contenga dos (2) escenarios, el primero sin la aplicación de la metodología y en el segundo con su aplicación, y contrastar ambos escenarios para determinar el nivel de reducción de los ciberataques que se originan a través de éste servicio.

Existen varias herramientas Gateway de código abierto y propietario que permite implementar la seguridad del servidor de correo electrónico, en la presente investigación se utilizarán herramientas de código abierto que permitan utilizar sus caracterizas principales sin ningún tipo de limitación, al contrario de lo que ocurre con herramientas privativas que es necesario licenciamiento vigente.

Para la evaluación de la metodología, Proxmox Email Gateway será la herramienta que se utilizará en el escenario de pruebas, ésta solución de seguridad adaptable a cualquier tamaño de empresa, líder en su ámbito, ayuda a proteger el servidor de correo electrónico de manera eficiente hasta el 99.99% contra las amenazas, gracias a su arquitectura flexible combinada con la interfaz de administración basada en la Web que permite a usuarios autorizados controlar y administrar todos los correos electrónicos entrantes y salientes. (Proxmox y Yourconnect Co, 2019)

Zimbra Mail Server será implementado como servidor de correo electrónico en el escenario de pruebas, solución líder de código abierto para empresas, proveedores de servicios, instituciones académicas y gubernamentales, gracias a su flexibilidad, adaptabilidad, fiabilidad y bajo mantenimiento. (Zimbra y Redcetus cl, 2018)

Las herramientas descritas que se utilizarán para el escenario de pruebas principalmente se basa a su presupuesto menor en su implementación a razón de que éstos pertenecen al código abierto, mismo que no se comercializa por licencia sino por suscripción permitiendo a los usuarios puedan cambiar y mejorar el software de manera colaborativa, funciones que el software privativo no permitirían por derechos de autor.

El beneficio resultante de este trabajo de investigación es el de elaborar una metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway, que se pueda aplicar e implementar dentro de una infraestructura informática de una empresa u organización y mejorar la protección de la información.

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Diseñar y evaluar una metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway.

1.3.2 Objetivos específicos

- Estudiar los ciberataques que se originan a través de correos electrónicos mediante el análisis de la documentación bibliográfica existente para determinar los tipos de ciberataques a considerar en la elaboración de la metodología.
- Analizar las herramientas Gateway de seguridad de correo electrónico mediante el estudio del estado del arte para definir las características, filtros y reglas base de la metodología a elaborar.
- Elaborar la metodología en base a definiciones sustentadas en el estudio del estado del arte para reducir los ciberataques originados a través de correo electrónico.
- Evaluar la metodología mediante la implementación de un Gateway sobre un escenario de pruebas aplicando la metodología elaborada y otra sin su aplicación para contrastar el porcentaje de reducción de ciberataques originados a través de correos electrónicos.

1.4. Hipótesis

La metodología elaborada mediante la aplicación de filtros y reglas sobre un Gateway reducirá el porcentaje de la cantidad de ciberataques originados a través de correo electrónico.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Antecedentes del problema

La mayoría de las empresas u organizaciones desconocen la magnitud del problema con el que se enfrentan a los ciberataques, considerando a la seguridad como algo secundario en sus infraestructuras informáticas y generalmente no se invierte en el capital humano ni tecnológico necesario para prevenir el daño y/o pérdida de la información o servicios.

El correo electrónico es un servicio de comunicación imprescindible para el funcionamiento de una empresa, gracias a sus beneficios tales como: accesibilidad, rapidez y la posibilidad de enviar documentos adjuntos, es así que se ha convertido en una herramienta necesaria y útil para transmitir todo tipo de mensajes interna y externamente en las empresas, así como también entre clientes y proveedores. (INCIBE, 2017)

El uso y los beneficios evidentes que brinda el correo electrónico dentro de una organización han hecho que sea uno de los medios que utilizan los ciberdelincuentes para llevar a cabo sus ataques, por tal razón, como toda herramienta de comunicación corporativa es necesario precisar el uso correcto y seguro, ya que, además de abusos y errores no intencionados, pueden causar perjuicio en la empresa. (Faj.0ardo, 2017)

2.2 Bases teóricas

2.2.1 Correo electrónico

1. Introducción

El correo electrónico, también conocido como e-mail, es un servicio de red que permite enviar y recibir mensajes con múltiples destinatarios o receptores. Además de un texto escrito, puede incluir archivos como documentos, imágenes, música, archivos de video, sean éstas para usos laborales, educativos, comerciales o simplemente personales. (Ecured, 2016)

La facilidad de uso, rapidez y el bajo costo de la transmisión de información han hecho que la mayoría de las instituciones y particulares tengan el correo electrónico como principal medio de comunicación. Para su uso se necesita especificar una cuenta del usuario y la dirección del destinatario, y al remitir el email, el mensaje es enviado al buzón de correo de su proveedor, posterior a ello, este se almacena y reenvía hasta el buzón del destinatario. (Fajardo y Ecured, 2017)

2. Elementos del correo electrónico

El mensaje de correo electrónico contiene dos partes esenciales que son: Encabezado y Cuerpo.

Encabezado

También conocido como "header" es un registro de información técnica del remitente, destinatario, y servidores que llevan a cabo la transmisión hasta que el mensaje sea entregado.

```
Return-Path: <jorge@    .ec>
Received: from mail-sor-f65.google.com (mail-sor-f65.google.com. [209.85.220.65])
        by mx.google.com with SMTPS id n1sor6445028oij.96.2020.04.24.11.36.44
        for <c       21@gmail.com>
        (Google Transport Security);
        Fri, 24 Apr 2020 11:36:44 -0700 (PDT)
Received-SPF: neutral (google.com: 209.85.220.65 is neither permitted nor denied by best guess record for domain of
jorge@    .ec) client-ip=209.85.220.65;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@    -ec.20150623.gappssmtp.com header.s=20150623 header.b=G6YA1vwj;
       spf=neutral (google.com: 209.85.220.65 is neither permitted nor denied by best guess record for domain of jorge@    .ec)
smtp.mailfrom=jorge@    .ec
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=    :c.20150623.gappssmtp.com; s=20150623;
        h=mime-version:from:date:message-id:subject:to;
        bh=cNTq1ojs+f/O/9ZJ91ZthR4MH3PV/IRpUX9hST3aJ94=;
        b=G6YA1vwjQICQ+/LbNDRj2lg1kj1HGMYj4uzU4wGuhItO1YQXDeDu1R4G+IXEBx6z25
         ZcWInpFS+5rUii6XC1qmkR1TfTGinhl5j1Kq4oY0qn6Fr3K0v+lnpElhuD2viafDGgDG
         SvNJH9Zkybkhze2Cknq/iixD1Wpxg5rXBPyrFnB1iScBwF3CFgOc6ooekbWa4/orG9qb
         caHzQoieQlYD3Ru2yllI07VvcZGOvBY+UGLusbyxLXU/Z4YCz1ZP7KEPkL7MpNrbXV8a
         A99yQtP+id6HmgcYSKs+cJ2PPiVlG1ZwHAi4XltYV0E2c3V7RkKE/ASzDbvUPFDUc5xl
         TXPQ==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20161025;
        h=x-gm-message-state:mime-version:from:date:message-id:subject:to;
        bh=cNTq1ojs+f/O/9ZJ91ZthR4MH3PV/IRpUX9hST3aJ94=;
        b=RIBtFLgJnwuBbtW9pDzxe5S/vS9h+S+rh0hJMew0lzZd3+g/O8nDMkSJIWNjzXJrhj
         ycpMvlSdVWtcZPqmSftsY4MKDjgQO6XhSdXNwLniCFoXAuUWOD0JU3LcQMfHZdi46jGO
         HkFqYmZfiJ6NetxKTgI6U+V96tNrsnLkbHUuB7ZdO6XRa8HJu36YEz4SXbxxV/Wf+xvq
         lOnauXbXIA48RNpw8OlT3xgP6o0urBvWT+mU1Xwh+MkcJWjDFnr8/pCpnF57593KQore
         ziQZzwOuYjYUbLQM7ueLNE9sojabMrhwfNXXeF6X3OYsw4c7w5SbFhGhTjqOu/BSXj75
         xqag==
X-Gm-Message-State: AGi0Pub/Ay9oFTxELTDPguTVbvSxbzMBVTEWwymlUR2IWgOLdWEOmJzq 98odActFUHRqbo0M4h3e96+OklbL2yBbGVTkPrh4kQ==
X-Google-Smtp-Source: APiQypJOumuj0dYZsY45eNeti1DcVPwf/rDcxb2f6KrGCnaSo5cBY6R2KUenyhVL1kV9F7HlXE2fGu8oUmXKDEbe+3g=
X-Received: by 2002:a54:4708:: with SMTP id k8mr6154683oik.62.1587753404052; Fri, 24 Apr 2020 11:36:44 -0700 (PDT)
MIME-Version: 1.0
From: Jorge      <jorge@    .ec>
Date: Fri, 24 Apr 2020 13:36:33 -0500
Message-ID: <CAGchkgtEvTmSmVjtWVUWJvZ=RW2UAj9EWf2GM8pOhHcXmYb+TA@mail.gmail.com>
Subject: Webinar Burpsuite
```

Figura 1-2: Encabezado del correo electrónico
Realizado por: Rochina César, 2020.

A continuación se describen los principales datos que contiene el encabezado del mensaje de correo electrónico:

From: Nombre y la dirección de correo del emisor.

To: Nombre y la dirección de correo del destinatario, puede contener varios destinatarios.

Date: Fecha de envío del correo que contiene día y la hora.

Subject: Asunto utilizado en el mensaje.

Return-Path: En el caso de que se encuentre un error durante el envío del mensaje o que, por lo que sea, este no pueda llegar a la bandeja de entrada, el correo será remitido a la dirección especificada en esta sección.

Received: Direcciones IP del servidor por los que ha pasado el mensaje, así como también los protocolos de autenticación.

Message-ID: Identificador único del correo electrónico concreto.

Envelope-To – Esta cabecera muestra que este correo fue enviado al buzón de correo del suscriptor del cual la cuenta de correo electrónico es destinatario@ejemplo2.com.

Delivery Date: Fecha y hora en la que el correo fue recibido por el servicio o cliente de correo.

X-Spam-Status: Puntuación de Spam generada por el servicio o cliente de correo.

Content-Type: Formato del mensaje, como por ejemplo, html o texto plano.

Message Body: Contenido del correo electrónico escrito por el remitente.

Cuerpo

El contenido o el cuerpo del mensaje es la parte más visible del correo electrónico, en esencia, el contenido mismo del mensaje escrito por el remitente que llega al buzón de entrada.

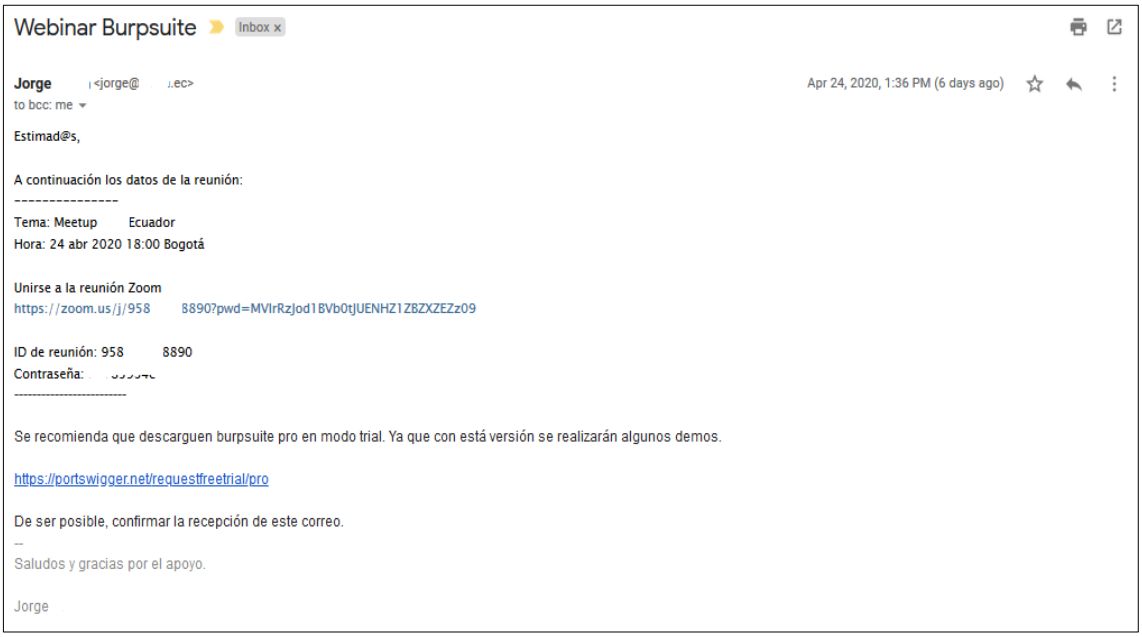


Figura 2-2: Cuerpo del correo electrónico

Realizado por: Rochina César, 2020.

Los datos más visibles que se observan conjuntamente con el cuerpo del mensaje son: el remitente y la fecha de envío.

2.2.2 Arquitectura del servicio de correo electrónico

1. Servidor de correo electrónico

Es una aplicación informática cuya función principal es permitir el intercambio de mensajes de correo electrónico entre distintos usuarios o dispositivos integrados en las redes de datos, así como también permite a los usuarios la gestión de los correos de forma privada.

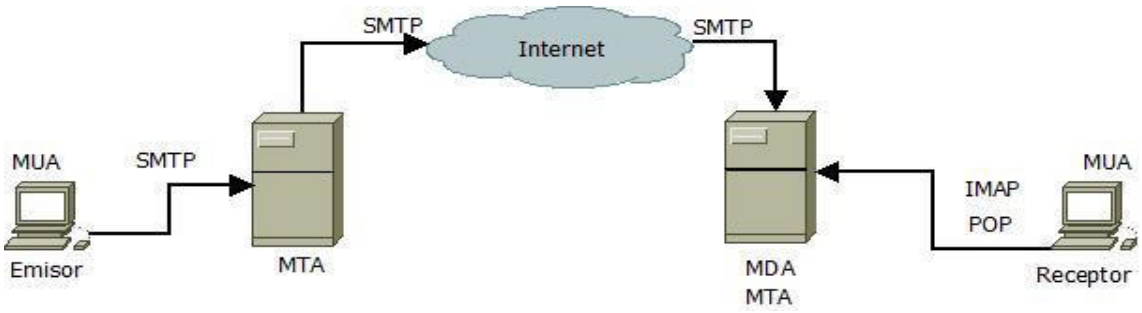


Figura 3-2: Arquitectura del servicio de correo electrónico

Realizado por: Rochina César, 2020.

2. Agente de Usuario de Correo

MUA (Mail User Agent) es el programa cliente que permite al usuario acceder a sus correos electrónicos mediante los protocolos POP e IMAP.

3. Agente de Transferencia de Correo

MTA (Mail Transfer Agent) es el programa que recibe los correos electrónicos desde los clientes y transfiere hacia el servidor de correo del destinatario usando el protocolo SMTP. Un mensaje de correo electrónico pasa por al menos un MTA hasta llegar al destino final.

4. Agente de Entrega de Correo

MDA (Mail Delivery Agent) es el programa encargado de permitir al usuario a través de un programa MUA acceder a sus correos electrónicos, los agentes MDA no transportan mensajes entre sistemas ni actúan como interfaz para el usuario final

2.2.3 Protocolos de correo electrónico

1. Protocolo para la Transferencia Simple de Correo

SMTP (Simple Mail Transfer Protocol) su función principal es transferir el correo electrónico desde un servidor origen hasta el servidor destino, de esta forma posibilitando al usuario enviar un correo a uno o más destinatarios (Aguirre, 2019)

2. Protocolo de Acceso a Mensajes de Internet

IMAP (Internet Message Access Protocol) tiene como finalidad acceder y administrar los mensajes de correo electrónico directamente en el servidor sin transferirlo al cliente como lo

hace POP. Cuando un servidor de correo IMAP es utilizado, los mensajes de correo se mantienen en el servidor a las que el usuario puede acceder y permite al cliente crear, renombrar o borrar directorios en el servidor para organizar y almacenar correo. (Aguirre, 2019)

3. Protocolo de Oficina Postal

POP (Post Office Protocol) este protocolo es utilizado para acceder y administrar los mensajes de correo electrónico almacenados en el servidor y transferir al dispositivo cliente del usuario a través de los programas MUA, tales como: Microsoft Outlook, Mozilla Thunderbird, Mail de Mac OS, o Evolution en distribuciones Linux. (Aguirre, 2019)

2.2.4 Herramientas de servidores de correo electrónico

Actualmente en el mercado existen varias herramientas tanto de código abierto como de código propietario que permite implementar un servidor de correo electrónico dentro de una organización:

1. Microsoft Exchange Server

Es una solución de software de sistema de mensajería y colaboración entre usuarios, desarrollado por Microsotf diseñado para ser utilizado dentro de un entorno comercial. Es parte de la línea de productos para servidores Microsoft Servers y es ampliamente utilizado por las grandes empresas, permite almacenar información, nombrar calendarios, contactos y tareas compartidas. Además, brinda a sus usuarios la posibilidad de compartir información, ya sea a través de Outlook en sus escritorios, o bien en Outlook Web Access a través de un navegador web. (BaeHost, 2016)

2. Zimbra Mail Server

Zimbra Mail Server es una solución de software de código abierto para ser implementada como servicio de correo electrónico y calendario, creado por Zimbra Inc. (San Mateo, California), dispone de socios estratégicos de prestigio cómo Red Hat, HP, Intel, Novell, Apple. Para la distribución en el mercado existen dos versiones: una versión Libre que sirve de base al producto y en la que colabora la Comunidad de Código Abierto, y una versión comercial que a partir de la versión libre añade servicios y funcionalidades con enfoque profesional en base a soporte y mantenimiento. (HostingNet, 2019)

2.2.5 Ciberataques a través de correos electrónico

1. Ciberataque

"Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen." (Doig, 2019)

Ciberataque es un conjunto de acciones ofensivas hecha por individuos u organizaciones contra sistemas de información dependientes de infraestructura y sistemas tecnológicos de instituciones, personas o empresas, con el fin de alterar o exponer información confidencial , denegar servicios e incluso el espionaje. (Muedas y Rojas, 2019)

2.2.6 Principales ciberataques

A continuación se describen los principales ataques que se propagan a través del correo electrónico:

1. Malware

Malware es la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso destinado a acceder a un dispositivo de forma inadvertida sin el conocimiento del usuario cuya función realizar alguna acción maligna. (Mendiola, 2019)

El malware puede llegar de muchas maneras para ser infectado a un dispositivo. Una de las más utilizadas por los ciberdelincuentes son los correos electrónicos, mismos que son propagados a través de archivos adjuntos enlaces externos.

A continuación se describen los tipos de malware más comunes

- Ransomware.- El ransomware es un tipo de malware que cifra el contenido de un sistema e impide a los usuarios el acceso a ella, para restablecer exige pago económico.
- Troyano.- Es un tipo de malware que se camufla como software legítimo y permite a los ciberdelincuentes espiar, robar datos confidenciales e incluso obtener control del sistema a través de una puerta trasera.
- Spyware.- Es un tipo de malware diseñado para recopilar información sobre la actividad del usuario. Está programado para pasar inadvertido, de manera que el usuario no perciba ni tenga conocimiento de ningún tipo de actividad anormal.
- Adware.- Es un programa malicioso diseñado para mostrar anuncios al usuario. Suelen instalarse junto a otros programas legítimos. Su objetivo es recopilar información sobre la actividad del usuario para, así, mostrar anuncios que sean específicos y dirigidos a la víctima.

Hoy en día es común que recibamos correos electrónicos con archivos adjuntos o enlaces externos, siendo ésta una manera rápida e interesante de enviar o recibir cualquier documento o información. Sin embargo, no se sabe si estos están libres de malware, mismos que pueden ser enviados de manera maliciosa por algún ciberdelincuente o incluso por parte de algún contacto legítimo de manera involuntaria.

Según el informe presentado por la "SERIE DE CIBERSEGURIDAD DE CISCO 2019", los ciberdelincuentes van mas más allá de utilizar adjuntos tradicionales como un archivo binario que fácilmente pueden ser analizados y colocados en cuarentena por los módulos de un servidor de correo electrónico, actualmente, es mucho más probable que el malware se envíe en forma indirecta, ya sea a través de adjuntos menos sospechosos tales como archivos de tipo office o archivos comprimidos, así como también documentos comerciales comúnmente usados por URL contenidas en el cuerpo del mensaje, de ésta forma el malware pasaría desapercibidos por los sistemas de seguridad.

A continuación se presenta los tipos de archivos más comunes que usan los Ciberdelincuentes para propagar malware a través de correo electrónico.

Tabla 1-2: Tipos de archivos maliciosos

Tipo de archivos adjuntos maliciosas	Porcentaje
.doc	41.8%
.zip	26.3%
.js	14.0%
.pdf	9.9%
.rar	3.9%
.exe	1.7%
.docx	0.8%
.ace	0.5%
.gz	0.5%
.xlsx	0.2

Fuente: (Cisco, 2019)

Como se puede observar en la Tabla 1-2: Tipos de archivos maliciosos, los tipos de archivos más utilizados para la propagación de malware a través de correo electrónico son documentos

tales como: pdf, doc, xlsx; así como también archivos de compresión tales como: zip, rar, gz, entre otras.

Según Verizon en su Informe de investigación de violación de datos del año 2017 indica que el 66 % del software malicioso analizado fueron instalados través de e-mail.

2. Spam

El spam es todo correo electrónico masivo, anónimo y no solicitado. (Kaspersky, 2018)

Correo masivo.- el spam se envía en grandes cantidades. Muchos de estos son utilizados con fines publicitarios y comerciales, por lo tanto, para que el spam sea rentable, el volumen de correos iniciales tiene que ser muy alto.

Sin embargo, muchos mensajes de correo electrónico Spam no son ni publicidad, ni ningún tipo de propuesta comercial, además de ofrecer bienes y servicios, los correos de spam pueden usarse para llegar a sus destinatarios con contenido de las siguientes categorías:

- Spam falso utilizado para distribuir malware
- Mensajes políticos
- Mensajes Cuasi-caritativos
- Estafas financieras
- Cadenas de mails

Correo Anónimo: generalmente el spam es enviado desde direcciones falsificadas con el objetivo de ocultar el remitente real.

Correo No solicitado: las listas de correo destinatarios, los boletines y otros materiales de publicidad que los usuarios finales han aceptado recibir pueden parecer spam, pero en realidad son correos legítimos. En otras palabras, la misma pieza de correo puede ser clasificado como spam o como correo legítimo, dependiendo de si el usuario dio o no su consentimiento en la recepción.

Durante el año 2019, la proporción de spam de correo electrónico fue de 56,61%.

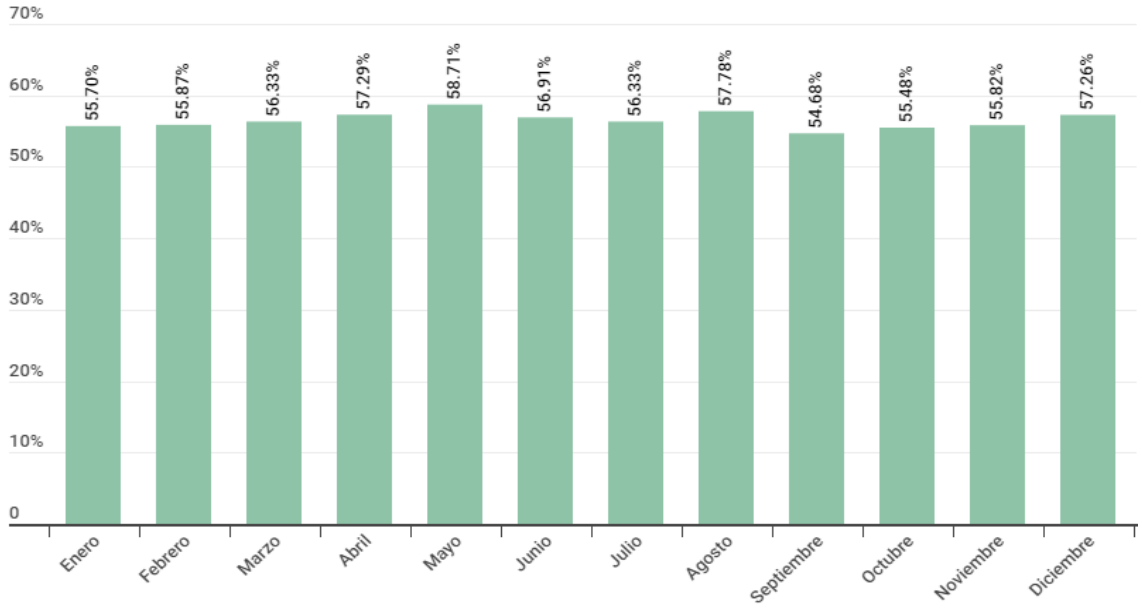


Figura 4-2: Proporción de spam de correo electrónico

Fuente: (Kaspersky, 2019)

La tasa más baja se registró en septiembre (54,68%) y la más alta en mayo (58,71).

3. Phishing

El phishing es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso. (Avast, 2019)

Generalmente de los ataques de phishing comienzan con la recepción de un correo electrónico o un mensaje directo en el que el remitente se hace pasar por un usuario legítimo tales como: un banco, una empresa u otra organización real con el fin de engañar al destinatario. Este correo electrónico incluye enlaces a un sitio web preparado por los ciberdelincuentes que imita al de la una empresa legítima y en el que se invita a la víctima a introducir sus datos personales.

A diferencia de otros tipos de ciberataques, el phishing no necesariamente se requiere de conocimientos técnicos especializados. 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”. (Malwarebytes Labs, 2019)

Spam, Phishing, e ingeniería social

La ingeniería social consiste en engañar al ser humano, de esta forma los ciberdelincuentes crean alarma en los receptores de los mensajes, con indicaciones de urgencia, y diferentes

llamadas a la acción con la finalidad de que el usuario actúe de inmediato ante el estímulo y no se detenga a analizar los riesgos de su acción, para que cedan su información personal como contraseñas o datos bancarios o para que permitan el acceso a un equipo con el fin de instalar software malicioso de forma inadvertida.

En la mayoría de los sistemas de información, su sistema de seguridad no recae en un fallo técnico o en el código informático, sino más bien una persona porque es más fácil engañar a alguien para que revele su contraseña que vulnerar su seguridad. De hecho, los atacantes a menudo recurren al phishing porque no pueden encontrar ninguna vulnerabilidad técnica. (Panda Security, 2019)

En este sentido existe una gran vinculación entre el spam y el phishing, ya que los correos electrónicos fraudulentos generalmente suelen enviarse de forma masiva, anónima y sin el consentimiento del destinatario, con el fin de multiplicar el número de víctimas potenciales de los ciberdelincuentes.

La clasificación mundial de ataques de phishing está encabezada por Venezuela, seguido de Brazil, según el informe "El spam y el phishing en 2019" publicado por Kaspersky Lab.

Tabla 2-2: Porcentaje de países víctimas de ataques de phishing

País	Porcentaje
Venezuela	31.16%
Brasil	30,26%
Grecia	25,96%
Portugal	25,63%
Australia	25,24%
Argelia	23,93%
Chile	23,84%
Reino Unido	23,82%
Ecuador	23,53%
Guayana Francesa	22,94%

Fuente: (Kaspersky, 2019)

Engaños por correo electrónico, descargas de software pirata y publicidad invasiva con códigos maliciosos son algunas de las principales modalidades de ataques cibernéticos que vivió

América Latina en el 2019, Según Roberto Martínez, analista de ciberseguridad en Kaspersky, "cree que la falta de cultura de ciberseguridad en las poblaciones hace que aumenten los riesgos. Entre más personas caigan en el falso correo del banco que le pide sus credenciales, más 'campañas' se van a seguir presentando." (Kaspersky, 2019)

A continuación en la tabla, se describen las principales ciberataques originados a través de correos electrónicos.

Tabla 3-2: Tipos de ciberataques por 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.

Realizado por: Rochina César, 2020

4. Fugas de información confidencial

Otra de las constantes amenazas que se tiene a través de los correos electrónicos 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 son muy variadas y podrían ser: el descontento de un empleado y el beneficio económico personal. (INCIBE, 2016)

2.2.7 Seguridad de Correos electrónico

Las empresas u organizaciones que hacen uso de cualquier herramienta de comunicación o informática corporativa y con el fin de mitigar los ciberataques que se originan a través de correo electrónico deberán contar con distintos niveles de seguridad tales como: políticas, normas y procedimientos para el uso correcto y seguro, así como también, contar con soluciones técnicas y tecnologías implementadas en sus infraestructuras de comunicación e informáticas. (INCIBE, 2019)

Persiguiendo los objetivos de la presente investigación se estudia las soluciones tecnológicas de seguridad a nivel de servidor de correo electrónico.

La mayoría de software de servidores de correo electrónico integran módulos de seguridad, mismas que deberán estar configuradas correctamente, tales como: la capa de sockets segura (Secure Sockets Layer) que permite crear una sesión de comunicación cifrada entre el servidor y los clientes de correo electrónico, cifrado de mensajes de correos, reglas Anti- Spam y Anti-Phishing, siendo estos los principales módulos básicos que ayudan a combatir los ciberataques asociados a este servicio. (IBM, 2018)

Sin embargo, para maximizar la mitigación de los cibertaques que se originan a través de correo electrónico es necesario contar con las medidas de seguridad adicional que permita el escaneo exhaustivo de los mensajes de correos electrónicos entrantes y salientes, para este fin, una de las principales soluciones son las puertas de enlace de correo seguro (Secure Email Gateway). (Eset, 2018)

1. Open Mail Relay

Se da cuando un servidor de correo electrónico se encuentra configurado de tal manera que permite la retransmisión de un correo electrónico sin autenticación en el servidor, siendo esta uno de las principales fuentes de transmisión de correos Spam. Para contener esta vulnerabilidad se debe cerrar esta opción, de esta forma, bloquea la retrasmisión abierta y exige a los usuarios que se autentiquen en su servidor.

2. Listas Negras

Son registros que contienen las direcciones de remitentes maliciosos, generalmente se las agrupa de la siguiente manera:

- RBL, Real Time Blackhole List, es una de las técnicas más antiguas y más utilizadas que contienen una base de datos de direcciones desde donde se genera el SPAM, y son altamente efectivas.
- DNSBL, DNS Black List, es un acuerdo entre servidores DNS para bloquear dominios que generan SPAM por medio de su IP que son almacenados dentro de una base de datos.
- DRBL, Distributed Realtime Block List, difiere de DNSBL en la naturaleza de la distribución ya que permite a cada red que establezca su base de datos.
- DNSWL, DNS White List, lista de direcciones que indica quien envía SPAM, puede ser rara vez, nunca etc.
- RHSBL, Right Hand Side Blacklist, es similar a DNSBL, pero a diferencia de este tiene en cuenta el nombre de los dominios más no la IP.

- URiBL, Uniform Resource Identifier Blacklist, utilizada para identificar objetos o direcciones URLs maliciosas integradas dentro del cuerpo del mensaje del correo electrónico.

3. Lista Gris

Es una técnica utilizada para protegerse contra el Spam, los remitentes que no se encuentran dentro de la lista blanca y no es conocido previamente, se registrará como lista gris y el mensaje será rechazado temporalmente. Si el correo es legítimo, el servidor de origen, después de un retraso, volverá a intentarlo y, si ha transcurrido el tiempo suficiente, se aceptará el correo electrónico, caso contrario será bloqueado como Spam.

Según el estándar RFC 2505 (AntiSpam Recommendations for SMTP MTAs), el correo no deseado debe ser rechazado cuando se produce el diálogo entre servidores SMTP, lo que quiere decir que el correo no debería llegar al servidor de correo del receptor, y al emisor debería llegarle un mensaje de error temporal. (Graciani, 2016)

Códigos de error SMTP:

- 5xy, (Fatal error), quiere decir que la trasferencia ha finalizado y que el correo regresa al emisor del correo.
- 4xy, (Temporary error), quiere decir que la trasferencia se pone en cola hasta que pueda realizar en un periodo posterior.
- 2xy, quiere decir que el MTA es el encargado en dicho punto para que se cumpla el envío del correo

3. Gateway

Gateway es considerado como un dispositivo de comunicación que actúa como un punto de entrada de una red a otras redes permitiendo mediar entre dos equipos o sistemas informáticos, además, decide cómo encaminar paquetes y qué reglas aplicar, actúa como portal entre dos programas y como medio de comunicación entre los protocolos que les permite compartir datos en los mismos dispositivos informáticos o entre diferentes sistemas informáticos. (Gomez, 2019)

Funcionamiento de un Gateway

Un Gateway recibe y modifica el empaquetamiento de la información de la red de origen para apropiar a la sintaxis o formato de la red de destino y posteriormente reenviarlo, de ésta forma pueden comunicarse redes o servicios con arquitecturas completamente distintas.

Un Gateway puede incluir otras funciones opcionales, algunas de las más importantes pueden ser:

- Secure Email Gateway (SEG)

  La puerta de enlace de correo seguro (Secure Email Gateway) es un dispositivo o software que escanea correos electrónicos entrantes y salientes en busca de contenidos maliciosos o rompan alguna política de la organización, además permite analizar contenido fraudulento tales como: malware, phishing y correos no deseados, así como también evitar que los datos sensibles salgan de la organización. (Forcepoint, 2018)

- Firewall de aplicaciones web

  Un Gateway como firewall ayuda a proteger todas las aplicaciones web mediante el filtrado y la supervisión del tráfico HTTP, previniendo diferentes ataques, y con ello que no ingresen códigos nocivos en la red de destino. (Avanan, 2019)

- Servidor proxy

  El comportamiento del Gateway como servidor proxy facilita el acceso a documentos externos cuando dispositivos internos de una red lo solicitan. El Gateway obtiene el documento en cuestión, y a continuación se lo sirve al equipo que lo solicitó. (Avanan, 2019)

- Servidor de nombre de dominios

  Este comportamiento facilita la comunicación cuando un equipo de una red solicita información de una dirección lógica, que corresponde a un servidor externo a dicha red. El Gateway traducirá dicha dirección al valor físico correspondiente. (Avanan, 2019)

- VPN (Virtual Private Network)

  Gateway por medio de la técnica denominada "tunneling", realiza conexiones punto a punto en redes de amplia difusión. Esto permite obtener la apariencia y muchas de las ventajas de este tipo de conexiones, aunque se estén atravesando estructuras incompatibles. (Avanan, 2019)

2.2.8 Funcionalidades de Secure Email Gateway (SEG)

La puerta de enlace de correo electrónico seguro (Secure Email Gateway) es una solución integrada de seguridad, desplegada en frente al servidor de correos con un espacio aislado para detectar y proteger contra la intrusión de malware, el spam, phishing e incluso integra módulos

para evitar la fuga de información, proporcionando una capa adicional de seguridad correos electrónicos en las infraestructura informáticas de las empresas. (Fortinet, Cellopoint, 2019)

1. Anti –Malware

La seguridad contra malware constituye una capa de protección fundamental en el servicio de correo electrónico permitiendo un análisis exhaustivo de su contenido, con el fin de determinar que esté libre de malware, principalmente en sus archivos adjuntos o en sus enlaces externos, además, integra la funcionalidad de actualización permanente de firmas de malware para reconocer las amenazas más recientes. (Kaspersky, 2019)

2. Anti –Spam

Es una solución de software que permite restringir la entrada o salida de correo electrónico spam, utilizando varias tecnologías de filtros, basándose en la identidad del remitente y analizando automáticamente las cabeceras y el contenido de todos los correos electrónicos antes de ser entregados al buzón del usuario. (UNAM CERT, 2017)

3. Anti – Phishing

La protección anti-phishing permiten analizar cada uno de los correos electrónicos de forma automatizada con el fin de detectar y bloquear los mensajes entrantes o salientes que contengan enlaces fraudulentos o dominios falsificados, que tienen la intención de obtener datos confidenciales, protegiendo así a los usuarios de estos tipos de fraudes o estafas online. (Email Manager, 2019)

4. Prevención de fuga de información

La puerta de enlace de correo seguro (Secure Email Gateway) integra módulos de seguridad que permite filtrar contenidos específicos en documentos y evitar la fuga de información sensible o confidencial de forma intencional o involuntaria a través de correos electrónicos de parte de usuarios internos. (Proofpoint, 2020)

2.2.9 Características de Secure Email Gateway

1. Sender policy framework(SPF)

Denominado también “Convenio de Remitentes”, se trata de un estándar abierto de seguridad que se encarga de comprobar la identidad del remitente de un correo electrónico recurriendo directamente de los registros de dominios (DNS), y permitiendo que los servidores destinatarios puedan asegurar de que el mensaje de correo que están recibiendo proviene de una

IP autorizada por el remitente. Crear un registro SPF específico en el Sistema de nombres de dominio, es especificar que direcciones IP están autorizadas para enviar correos electrónicos.

2. Motor Anti-malware

Compatibilidad de un motor de escaneado inmediato de bajo nivel basado en firmas de malware, diseñado para detectar ransomware, troyanos, spyware y otras amenazas maliciosas, además la incorporación de utilidades de línea de comandos para el escaneado de archivos bajo demanda y una herramienta inteligente para actualizaciones de firmas automáticas.

3. Listas Negras

Una lista negra, también denominada "blacklist" puede ser una lista de direcciones de correo electrónico, direcciones IP o a su vez, direcciones de registros de dominios, que han sido identificados como remitentes maliciosos, e indica al sistema el bloqueo total o parcial del correo electrónico antes de llegar al servidor y ser entrego al buzón de los usuarios.

4. Listas Blancas

Una lista blanca, también denominada "whitelist" puede ser una lista de direcciones de correo electrónico, direcciones IP o a su vez, direcciones de registros de dominios, que el administrador ha identificado como fiables para indicar al sistema no ser analizados por el escáner anti-spam.

5. Filtro Bayesiano

Los filtros bayesianos reúnen diferentes tipos de análisis de vocabulario, que permiten generar una lista de frases o palabras identificándolas como buenas y malas para tener en cuenta a la hora de filtrar la información, se basan principalmente, en el conocimiento que van adquiriendo por la continuidad de aquellos mensajes que los propios usuarios marcan como spam.

6. Seguimiento de eventos

Permite realizar la búsqueda y seguimiento de eventos en tiempo real producidos sobre los correos electrónicos y cambiar las preferencias de las acciones a ejecutar sobre dicho evento así como también generar informes para su posterior análisis.

7. Autoaprendizaje

El algoritmo de autoaprendizaje permite al sistema recopilar información estadística de todos los correos analizado para luego ser aplicados de manera automática en el menor tiempo posible.

8. Reglas de sistema

El sistema de reglas orientado a objetos habilita reglas personalizadas de filtro por usuario, dominios, marco de tiempo, tipo de contenido, acción resultante, entre otros, permitiendo configurar su propio sistema personalizado.

9. Administración web

La administración a través de una interfaz web ofrece al administrador gestionar todas las funciones y características desde un solo panel principal.

2.2.10 Arquitectura lógica de despliegue de "Secure Email Gateway"

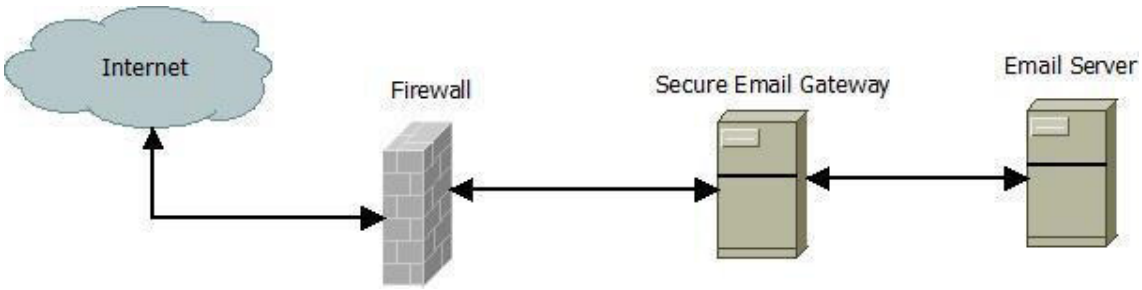


Figura 5-2: Despliegue del Gateway de correo electrónico

Realizado por: Rochina César, 2020.

La Figura 5-2, muestra una solución de seguridad desplegada entre el firewall de borde y el servidor de correo electrónico para proteger contra el ingreso y salida de mensajes de correo electrónicos maliciosos y evitar la fuga de información a través de este servicio. Algunas soluciones principalmente de licenciamiento propietario integran hardware y software, sin embargo, existen varias soluciones de código abierto que se puede implementar de acuerdo a las necesidades de cada organización utilizando varias tecnologías a través de filtros y reglas personalizadas.

2.2.11 Soluciones de Secure Email Gateway

Actualmente en el mercado, existen muchas soluciones o herramientas de puerta de enlace de correo electrónico seguro, se puede agrupar en dos grupos principales que son: código abierto y código propietario, a continuación de describen las principales de cada una de ellas:

2.2.12 Secure Email Gateway de código propietario

Según diagrama de cuadrante de gartner y en el artículo "The Top 11 Email Security Gateways" del sitio web "Expert Insights" especializado en ciberseguridad, se han identificado algunas de las principales plataformas de Secure Email Gateway, tales como: Proofpoint Essentials, Mimecast Secure Email Gateway, Barracuda Essentials, Cisco Cloud Email Security, Microsoft Advanced Threat Protection, Symantec Email Security. (Expert Insights, 2020)

Figura 6-2: Cuadrante de Gartner de las herramientas Gateway

Fuente: (Gartner, 2015)

1. Proofpoint Essentials

Proofpoint Essentials es una solución de seguridad de correo electrónico todo en uno, desarrollado por Proofpoint, un proveedor de seguridad cibernética. Ofrece protección de correo electrónico en la puerta de enlace y está dirigido a pequeñas, medianas y grandes organizaciones. (Proofpoint, 2019)

Características principales:

- Protección de correo electrónico mejorada con antivirus basado en firmas y protección contra phishing
- Protección contra amenazas con filtrado de contenido, filtrado saliente y defensa de archivos adjuntos
- El motor de reglas de filtro robusto que permite controlar la configuración de seguridad del correo electrónico personalizada.
- Crecimiento y continuidad, con archivado y cifrado disponibles como complementos adicionales
- Protección contra URL maliciosos dentro del contenido del correo electrónico.
- Generación de informes y registros completos para brindar a las empresas más control y conocimiento de la seguridad de su correo electrónico
- Administración con inicios de sesión de múltiples niveles, administración de dominio e integración de directorio activo.
- Implementación simple para las plataformas de correo Exchange, Office 365 y Google G Suite
- Se integra directamente con Azure proporcionando administración integrada para clientes de Office 365 y Exchange

2. Mimecast Secure Email Gateway

Mimecast Secure Email Gateway, es una plataforma de puerta de enlace seguro de correo electrónico, desarrollado por Mimecast, uno de los mayores proveedores mundiales de seguridad cibernética. Integra un gran conjunto de aplicaciones de seguridad basadas en la nube para proteger a las organizaciones contra el correo electrónico y las amenazas de seguridad basadas en la web, producto dirigido a clientes de nivel empresarial. (Mimecast, 2019)

Características principales:

- La protección contra la suplantación bloquea los intentos de phishing y el spam con servicios de autenticación de DNS.
- Funciones de protección contra amenazas de alto nivel que incluyen sandboxing de archivos adjuntos y protección de URL
- Base de datos de amenazas que controla miles de millones de correos electrónicos garantiza que la protección contra amenazas esté actualizada
- Filtro robusto personalizado de amenazas de correo electrónico
- Generación de informes completos en tiempo real
- Herramientas de autoservicio para usuarios finales, como permitirles bloquear remitentes
- Panel central de administración de funciones basado en la web.

- Continuidad de correo electrónico disponible si la red de correo electrónico deja de funcionar
- Incluye una opción de archivado de correo electrónico, así como mensajería segura y envío de archivos grandes

3. Cisco Cloud Email Security

La plataforma de seguridad de correo electrónico de Cisco, está basada en la nube con capacidades avanzadas de defensa contra amenazas actuales, tales como: el compromiso del correo electrónico empresarial, el phishing, el correo no deseado y la pérdida de datos, solución dirigida para todo tamaño de organizaciones.

Características:

- Actualización permanente de protección contra amenazas cibernéticas de correos electrónicos por red de inteligencia de amenazas líder en el mercado, Talos.
- Bloquea el correo no deseado con filtrado basado en reputación para URL
- Filtrado de spam de varias capas, con una baja tasa de falsos positivos
- Fuerte protección contra el compromiso del correo electrónico comercial
- Técnicas de aprendizaje automático para identificar y bloquear ataques de phishing dirigidos
- La autenticación de correo electrónico por DNS.
- Rastreo de correo electrónico por destinatario, remitente, asunto, archivos adjuntos y eventos del mensaje.
- Protección contra amenazas maliciosas disfrazadas de enlaces para darse de baja e interfaz uniforme para gestionar las suscripciones.
- Seguridad de datos para contenido confidencial en correos electrónicos salientes, con gestión centralizada e informes que simplifican la protección de datos.
- Escaneo de virus y detección de greymail para proteger contra amenazas maliciosas
- Seguimiento detallado de mensajes e informes a través de un panel de información general del sistema
- Módulos de capacitación con simuladores intuitivo que proporciona escenarios de phishing listos para usar que reflejan amenazas cibernéticas.
- Panel de control centralizado

4. Barracuda Email Security Gateway

Barracuda es un proveedor que proporciona soluciones de seguridad basadas en la nube. Email Security Gateway de Barracuda, es una solución de seguridad de correo electrónico "todo en uno", basado en puerta de enlace seguro, que bloquea las amenazas de correo electrónico antes

de que ingresen a la red de una organización, tiene como objetivo brindar a las pequeñas y medianas organizaciones una solución para la seguridad del correo electrónico y la protección de datos. (Barracuda, 2019)

Características:

- Protección de malware, spam y el análisis en tiempo real
- Protección avanzada contra amenazas y escaneo de URL
- Se integra con Office 365, lo que lo convierte en un buen "servicio complementario"
- Fuerte soporte técnico y funciones de gestión
- El filtrado de salida y el cifrado ayudan a proteger a las empresas contra la pérdida de datos
- Módulos adicionales Archivado y Continuidad de servicio de correo

5. Symantec Email Security

Symantec es un proveedor de productos de seguridad cibernética a nivel mundial. La plataforma de seguridad de correo electrónico es una puerta de enlace segura basada en la nube, para proteger las amenazas de correo electrónico, producto dirigido a todo tamaño de empresas. (Symantec, 2019)

Características:

- Funcionalidad de sandboxing y análisis de comportamiento para proteger como amenazas emergentes de malware.
- Capacidad de defensa contra phishing con aislamiento de amenazas y controles de suplantación
- Protección contra spam
- Symantec opera una red de inteligencia global líder en el mercado con información de más de 175 millones de puntos finales
- Integración con otros productos de Symantec, como la protección contra la pérdida de datos y el cifrado
- Generación de informes y análisis para una visión profunda de los ciberataques.
- Protección de enlace de tiempo de clic para detener las sofisticadas campañas de ciberataques
- Proporciona pruebas sandbox de archivos adjuntos para proteger contra malware.

6. Microsoft Advanced Threat Protection

Microsoft Advanced Threat Protection (ATP) es un servicio de filtrado de correo electrónico basado en la nube para proteger la organización contra las amenazas de malware, spam y phishing.

Características:

- Comprobación automática de archivos adjuntos de correo electrónico en busca de contenido malicioso
- Verificación de URL de tiempo de clic en mensajes de correo electrónico y archivos de Office
- Deteccion y bloqueo de archivos maliciosos en sitios de grupo y bibliotecas de documentos, como SharePoint, OneDrive y Microsoft Teams
- La protección contra phishing y suplantación a sus usuarios y dominios mediante el aprendizaje automático y algoritmos avanzados.
- Generación de informes en tiempo real que le permite identificar y analizar amenazas actuales.
- Simulator de ataques que permite ejecutar escenarios de ataque realistas con el fin de identificar vulnerabilidades y mantener las retroalimentaciones actualizadas.

2.2.13 Secure Email Gateway de código abierto

De acuerdo a la comunidad Linux Hint, se han identificado algunas de las principales plataformas de Secure Email Gateway de código abierto, tales como: Proxmox Email Gateway, Hermes Secure Email Gateway, Mail Scanner, Mail Cleaner y OrangeAssasin. (Linux Hint, 2020)

1. Proxmox Email Gateway

Proxmox Email Gateway es una solución de seguridad de correo electrónico de código abierto, con una arquitectura flexible combinada con interfaz web de administración, maximiza la protección del servidor de correo electrónico contra amenazas más recientes de malware, spam, phishing, fuga de información, entre otras, dirigida a cualquier tipo y tamaño de organización. (Proxmox Solutions, 2020)

Características:

- Escaneo exhaustivo de correos electrónicos con el fin de bloquear o eliminar malware incrustado, y actualización permanente de firmas de malware
- Sistema de reglas personalizadas orientado a objetos para definir reglas de filtro por usuario, dominio, marco de tiempo, tipo de contenido y acción resultante.
- Búsqueda y seguimiento en tiempo real de registros de eventos.

- Protección contra spam y phishing basada en la creación de registro de servicios de autenticación de DNS.
- Protección y control de acceso a través de listas negras y blancas mediante la aplicación de diferentes objetos como dominios, dirección de correo electrónico, expresión regular, red IP, grupo LDAP y otros.
- Generación de lista gris para el control de fallas temporales integradas según las especificaciones RFC para la entrega de correo.
- Protección contra correo de contenido "hosts de spam (Spam Uri Realtime BlockList)" que se mencionan en los cuerpos de mensajes.
- Generación personalizada de Filtro Bayesiano
- Panel de administración central de todas las funciones a través de interface web.

2. Hermes Secure Email Gateway

Hermes Secure Email Gateway es una solución de seguridad de puerta de enlace de correo electrónico, de código abierto basada en servidor Ubuntu, desarrollado por la empresa tecnología Deeztek, que proporciona protección contra correo no deseado, malware, archivado y cifrado de correo electrónico completo en tránsito y en reposo. (Deeztek, 2020)

Características:

- Protección contra spam y phishing basada en servicios de autenticación de DNS.
- Integración de usuarios a través de Directorio Activo
- Escaneo de correos para la protección contra malware
- Filtro robusto de acciones personalizada sobre los correos electrónicos
- Búsqueda de registros de eventos por palabras claves y rango de fechas
- Archivado y cifrado de correo electrónico
- Protección de correos electrónicos basados en la nube como Google Mail y Microsoft Office 365.
- Administración central de funciones basada en interface web.

3. Mail Cleaner

MailCleaner es una puerta de enlace de filtro de correo electrónico malicioso de código abierto, presente en dos ediciones: Comunidad (Libre) y Empresarial (Pago). (Mailcleaner, 2020)

Características:

- Integración a través de Directorio Activo y LDAP
- Escaneo de correos para la protección contra malware
- Filtro personalizada sobre los correos electrónicos

- Búsqueda de registros de eventos en tiempo real
- Integración con Google Mail y Microsoft Office 365.
- Administración central a través de interface web.

4. Mail Scanner

MailScanner es un diseño de sistema de seguridad epara puertas de enlace de correo electrónico de código abierto estable basadas en Linux, dirigidas a organizaciones gubernamentales, corporaciones comerciales e instituciones educativas, protege contra amenazas de malware, phishing, spam que son distribuidos a través de mensajes de correo. (MailScanner, 2020)

Características:

- Protección contra malware en base a firmas actuales.
- Protección contra el spam y phishing con reglas personalizadas.
- Soporte técnico colaborativo con la comunidad de MailScanner
- Filtrado de contenido de correos de salida para proteger a las empresas contra la pérdida de datos
- Integración de módulos adicionales para la gestión web

5. OrangeAssassin

OrangeAssassin es una versión mejorada de Apache SpamAssassin, un nuevo marco de filtrado de correo electrónico anti-spam de código abierto desarrollado en Python. (Apache Software Foundation, 2020)

Características

- Protección contra el spam y phishing con reglas personalizadas.
- Protección contra spam y phishing basada en servicios de autenticación de DNS.
- Generación personalizada de Filtro Bayesiano

2.2.14 Cuadro comparativo de soluciones de Secure Email Gateway

A continuación, se presenta un cuadro comparativo que resume las funciones y las características esenciales de las soluciones Gateway de código propietario y de código abierto.

Para el caso de soluciones propietarias se ha tomado las características de licenciamiento base, y para las soluciones de código abierto se ha tomado en cuenta la versión de comunidad (Community).

Tabla 4-2: Cuadro comparativo de herramientas Gateway

Solución SEG ---------- Características	**Proofpoint Essentials**	**Mimecast Secure Email Gateway**	**Barracuda Essentials**	**Cisco Cloud Email Security**	**Symantec Email Security**	**Proxmox Email Gateway**	**Hermes Secure Email Gateway**	**Mail Scanner**	**Mail Cleaner**	**Orange Assasin**
Tipo de Licencia	Propietario	Propietario	Propietario	Propietario	Propietario	Open Source	Open Source	Open Source	Open Source	Open Source
Sender policy framework(SPF)	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Motor AntiMalware	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Listas Negras, Blancas, Gris	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Filtro Bayesiano	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Búsqueda y Seguimiento de eventos	SI	SI	SI	SI	SI	SI	SI	SI	NO	NO
Reglas del sistema personalizada	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Autoaprendizaje	SI	SI	SI	SI	SI	SI	SI	SI	SI	NO
Administración web	SI	SI	SI	SI	SI	SI	SI	NO	SI	NO

Realizado por: Rochina César, 2020.

De acuerdo al cuadro comparativo presentado en la Tabla 4-2, se puede identificar que no todas las soluciones de código abierto cumplen con las características esenciales de una puerta de enlace de correo electrónico seguro, en el caso de código propietario todas cumplen. Las herramientas de código abierto tales como: Promox Email Gateway y Hermes Secure Email Gateway en sus versiones de comunidad (Community) conservan las mismas funcionalidades y características que las soluciones de código propietario, además, bajo suscripción comercial y de soporte se pueden integrar características adicionales.

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Diseño de la investigación

El diseño de la presente investigación corresponde con un estudio cuasi experimental (ya que no se seleccionan los grupos experimentales de forma aleatoria, sino que se escogen grupos ya formados), en este caso los datos de prueba son generados por el autor de esta investigación, con el que se pretende diseñar y evaluar una metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un gateway.

3.2 Tipo de investigación

Por la naturaleza de la presente investigación se utilizará un compendio de diferentes métodos y técnicas a través de las cuales se conseguirán tanto las bases teóricas de fundamento, así como las métricas de resultados.

Exploratorio

En la presente investigación se estudiará las principales amenazas y ciberataques que se originan a través de correo electrónico, así como también, las características, reglas y filtros que se puedan aplicar sobre el Gateway de correo electrónico.

Experimental

Se basa en pruebas realizadas en escenarios de laboratorio, en las que se observa los elementos más importantes del objeto de estudio que se investiga para obtener una captación de los fenómenos a primera vista.

Descriptiva

Luego de haber realizado la exploración e interpretación de resultados de la información, de manera sintética se describirá la metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway.

3.3 Métodos y técnicas de la investigación

3.3.1 Métodos

Para el desarrollo de la presente investigación se utilizará el método Científico–Deductivo.

Método científico

Se escogerá este método porque es verificable y explicativo, en la presente investigación se contrastará los resultados del antes y después de aplicar la metodología para reducir los ciberataques originados a través de correo electrónico mediante establecimiento de filtros y reglas sobre un Gateway.

Método Deductivo

Se utilizará este método ya que en la presente investigación se pretende demostrar que se puede reducir los porcentajes de los ciberataques originados a través correo electrónico con la aplicación de la metodología, que se originarán de un estudio previo, basados en filtros y reglas sobre un Gateway.

3.3.2 Técnicas

Las técnicas utilizadas en el presente trabajo de investigación son:

- Revisión de documentación.- Se utilizará esta técnica para la exploración de información necesaria durante la investigación.
- Pruebas.- Se realizará un escenario de pruebas con la finalidad de contrastar el porcentaje de reducción con y sin la aplicación de la metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway.
- Observación.- Mediante esta técnica se podrá observar la cantidad real, así como también a través de registros y log las formas de cibertaques efectuados en el escenario de pruebas.
- Análisis.- Se utilizará para analizar los resultados del porcentaje de reducción de ciberataques con la aplicación de la metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway.

Para la comprobación de la hipótesis se utilizará la estadística descriptiva.

3.4 Fuentes de información

3.4.1 Primarias

- Pruebas
- Observación de Resultados

3.4.2 Secundarias

- Artículos científicos referentes al tema de estudio.
- Trabajos de investigaciones nacionales e internacionales
- Conferencias académicas, congresos y seminarios
- Sitios web, revistas electrónicas y blogs oficiales relacionadas al tema de investigación

3.5 Planteamiento de Hipótesis

3.5.1 Hipótesis General

La metodología elaborada mediante la aplicación de filtros y reglas sobre un Gateway reducirá el porcentaje de ciberataques originados a través de correo electrónico.

3.5.2 Identificación de variables

Variable Independiente

- Metodología para reducir ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway.

Variable Dependiente

- Porcentaje de reducción de ciberataques

3.5.3 Operacionalización de variables

Tabla 1-3: Operacionalización conceptual de variables

VARIABLE	TIPO	CONCEPTO
Metodología para reducir ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway.	Independiente	Conjunto lineamientos base para reducir ciberataques originados a través de correos electrónicos mediante la aplicación de filtros y reglas sobre un Gateway.
Porcentaje de reducción de ciberataques	Dependiente	Nivel de reducción de ciberataques originados a través de correo electrónico

Realizado por: Rochina César, 2020.

Tabla 2-3: Operacionalización Metodológica de variables

VARIABLES	INDICADORES	TÉCNICAS	INSTRUMENTOS
V.I. Metodología para reducir ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway	Porcentaje de ciberataques bloqueados	Observación	Escenario de pruebas
V.D. Porcentaje de reducción de ciberataques	Porcentaje de bloqueo de malware. Porcentaje de bloqueo de spam. Porcentaje bloqueo phishing. Porcentaje de bloqueo de fuga de información	Observación	Matriz resultante de ciberataques al servicio de correo electrónico sobre los escenarios de pruebas.

Realizado por: Rochina César, 2020.

3.6 Población y muestra

3.6.1 Población de estudio

La gran cantidad de correos electrónicos no deseados (spam), phishing y principalmente el crecimiento constante de nuevas variantes de malware que se propagan a través del correo electrónico hace que la población de estudio sea desconocida o infinita.

3.6.2 Selección de la muestra

Toda la población establecida

3.6.3 Tamaño de muestra

En la presente investigación se tiene una población desconocida, por lo tanto, para determinar el tamaño de muestra se utilizará la siguiente formula estadística: (Pino, 2016)

n = (Z α ^2 * p * q) / (e^2)

Dónde:

Z, valor correspondiente a la distribución de Gauss zα = 0.5 = 1.96 con un nivel de confianza del 95 %

e, error de aceptación del 5%

p, porcentaje de población con atributo deseado y q, porcentaje de población con atributo no deseado con un valor de 50%

n = 384,16

De acuerdo a la fórmula el tamaño de muestra debe ser igual o mayor a 384,16, para la presente investigación se define un tamaño de muestra de 400 correos electrónicos.

3.7 Instrumentos de recolección de Datos

Para la recolección de los datos se realizará la implementación de los escenarios de pruebas, las herramientas utilizadas son de código abierto debido a su menor presupuesto para su implementación y además permiten utilizar sus características principales sin ningún tipo de limitación, al contrario de lo que sucede con herramientas privativas que es necesario algún tipo de licenciamiento vigente.

De acuerdo al contexto señalado anteriormente, entre las herramientas de software de servidor de correo electrónico descritas en el Marco Teórico de la presente investigación, para el escenario de pruebas se implementó Zimbra como el servidor de correo electrónico.

Para implementar el servidor Gateway de correo electrónico en el escenario de pruebas, además de ser software libre, se valoró de acuerdo al cumplimiento de las características que posee cada una de ellas, descritas en el Marco Teórico de la presente investigación.

Tabla 3-3: Valores asignados por cumplimiento de características

Cumplimiento de la características	**SI**	**NO**
Valoración	1	0

Realizado por: Rochina César, 2020.

Tabla 4-3: Valoración de la herramienta Gateway según sus características

Gateway ---------- Características	**Proxmox Email Gateway**	**Hermes Secure Email Gateway**	**Mail Scanner**	**Mail Cleaner**	**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**

Realizado por: Rochina César, 2020.

De acuerdo a la Tabla 4-3, las herramientas "Promox Email Gateway" y "Hermes Secure Email Gateway" en sus versiones de comunidad (Community) cumplen con todas las características, con un valor total de 8 puntos, siendo el puntaje máximo y el mayor valor con respecto a otras herramientas.

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.

A continuación se describe brevemente las herramientas utilizadas en el escenario de pruebas:

1. Proxmox Mail Gateway

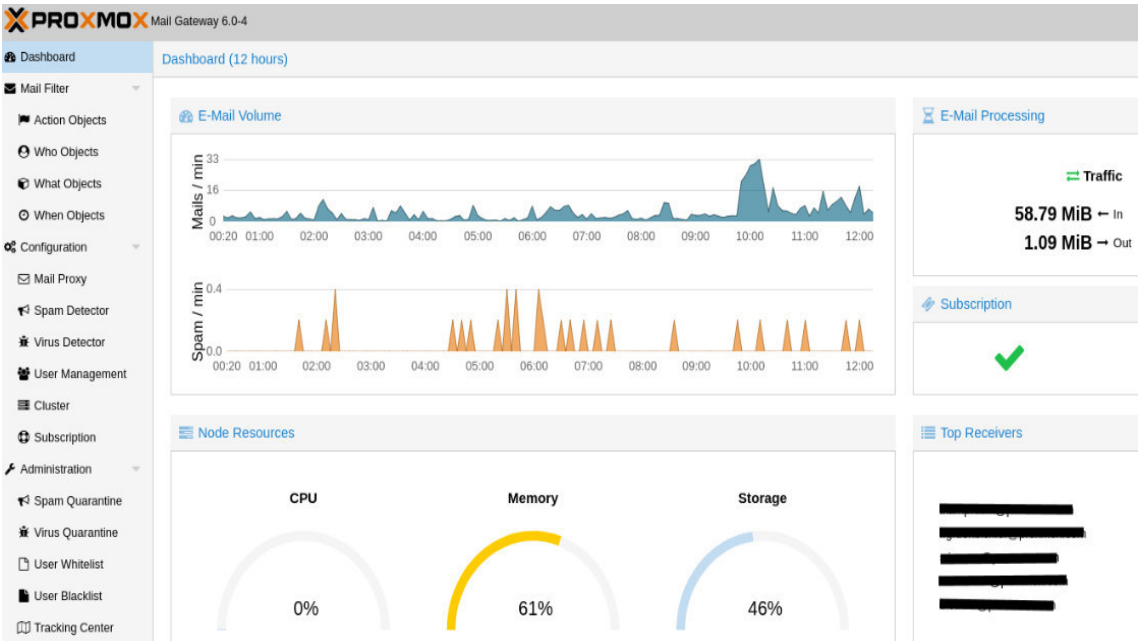


Figura 1-3: Dashboard Proxmox Mail Gateway

Fuente: (Proxmox Mail Gateway, 2020)

Es una herramienta integral de seguridad de correo electrónico de código abierto que ayuda a proteger un servidor de correo de los ciberataques que se originan y propagan a través del correo electrónico. Permite gestionar todos los flujos de correspondencia de correo entrante y saliente, ya que actúa como una puerta de enlace entre la red externa y el servidor de correo interno de una empresa u organización. (Proxmox, 2018)

2. Servidor Zimbra

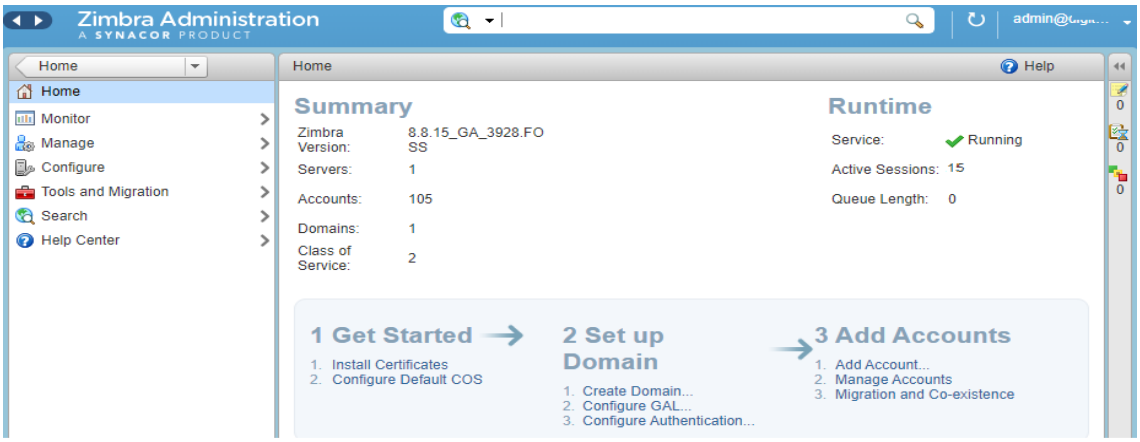


Figura 2-3: Zimbra Server Administration

Fuente: (Zimbra, 2020)

Zimbra es un servidor de mensajería de colaboración que permite compartir, almacenar y organizar mensajes de correo electrónico, citas, contactos, tareas, documentos, entre otros, construido sobre una arquitectura estable y escalable con los protocolos estándar abiertos como: SMTP, LMTP, SOAP, XML, IMAP, POP, así como también, sobre una base sólida de otras aplicaciones de código abierto que disponen de un reconocido prestigio por su seguridad y velocidad tales como: Linux, Apache, Postfix, MySQL, OpenLDAP, Lucene. (Zimbra, 2018)

Zimbra puede ser implementado en las principales distribuciones Linux del mercado tales como: Red Hat Enterprise, Fedora, Ubuntu, Debian, SUSE Linux, Mac OS X y VMware (Zimbra Appliance), para su administración posee una completa consola Web, y una gran suite de aplicaciones clientes para su uso, además, características tales como copia de seguridad y restauración en tiempo real. (Zimbra, 2018).

3. Kali Linux

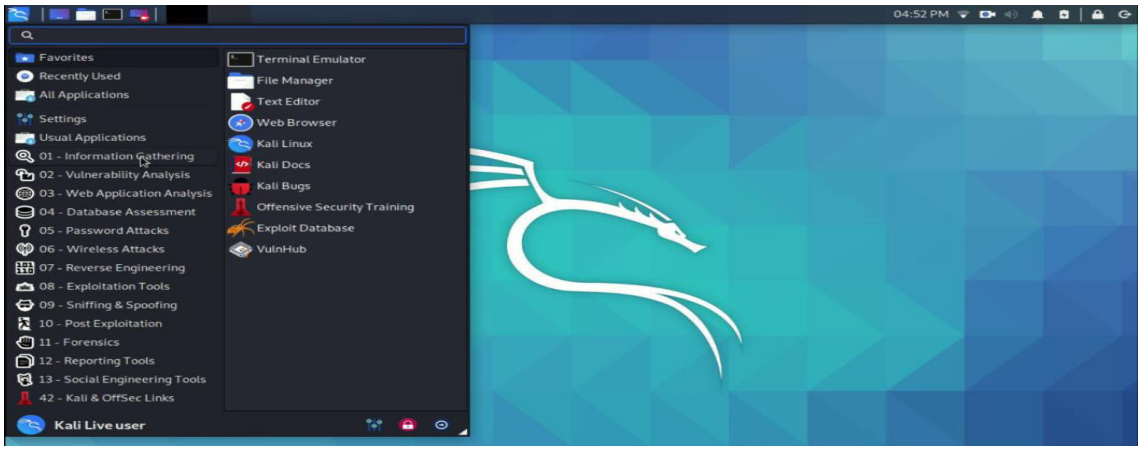


Figura 3-3: Kali Linux

Fuente: (Kali org, 2020)

Es un sistema operativo basada en Debían GNU/Linux que permite realizar pruebas avanzadas de penetración y auditorias de seguridad, posee muchas aplicaciones relacionadas a la seguridad informática como por ejemplo: setoolkit que permite realizar ataques de ingeniería social, nmap un scanner de puertos, wireshark un snifer, Jhon de Ripper un crackeador de puertos, aircrack software para realizar pruebas de seguridad en redes inalámbricas, metasploit para la explotación de vulnerabilidades. (Kali Org, 2019).

3.8 Escenario de pruebas

3.8.1 Descripción del escenario

El escenario de prueba consiste en la simulación de un escenario real de infraestructura de servicio de correo electrónico, para ello, en la red DMZ se implementó el servidor “Promox

Mail Gateway" como puerta de enlace (Gateway) de correo del servidor de correo electrónico Zimbra.

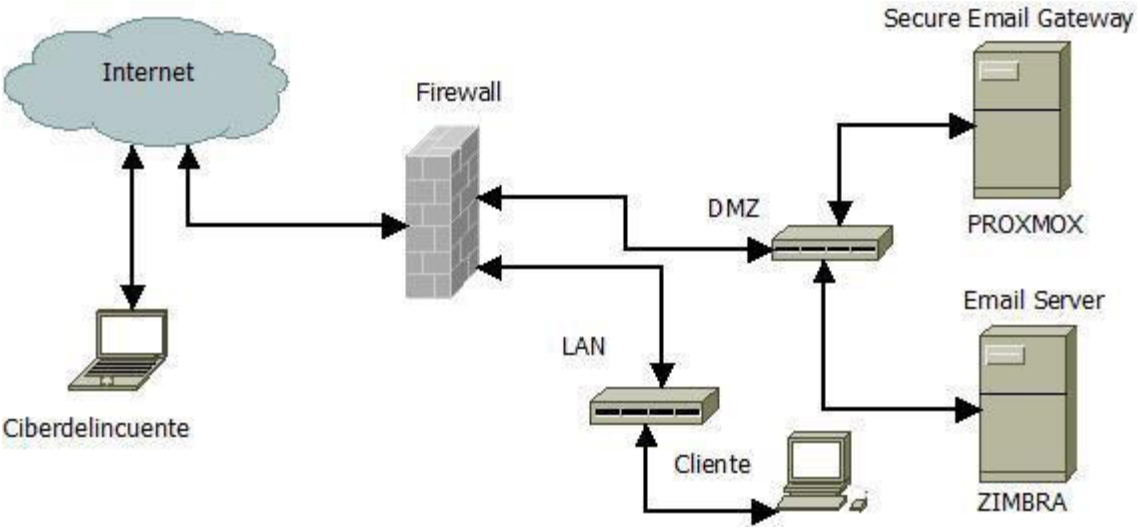


Figura 4-3: Diseño de la infraestructura de servicio de correo electrónico

Realizado por: Rochina César, 2020.

Para la presente investigación se desarrolló (2) dos escenarios: el primer escenario simulará una infraestructura sin aplicar la metodología, mientras que el segundo escenario simulará una infraestructura aplicando la metodología basada en filtros y reglas sobre un Gateway elaborada en la presente investigación.

3.8.1 Hardware y software del escenario

Para la implementación del escenario de pruebas se contó con el siguiente hardware y software:

Tabla 5-3: Hardware utilizado en el escenario de pruebas

Nombre	**Especificaciones**	**Descripción**
SERVIDOR FÍSICO DE PRUEBAS	HUAWEI / INTEL XEON E5-26580 3.20GHz / 16 GB DE RAM	Servidor de máquinas virtuales (VM), en el cual se asignó el servidor Gateway y de correo electrónico
SERVIDOR GATEWAY	VM / 2 GB DE RAM	Servidor de Gateway de correo electrónico
SERVIDOR DE CORREO	VM / 2 GB DE RAM	Servidor de correo electrónico
1 EQUIPO PORTÁTIL	ASUS / INTEL CORE I3 2,1 GHz / 8 GB RAM	Equipo personal para la ejecución de ciberataques y desarrollo del proyecto de tesis.

Realizado por: Rochina César, 2020.

Tabla 6-3: Software utilizado en el escenario de pruebas

Software	Descripción
CentOS 7 x64	Sistema operativo Linux
Zimbra Collaboration Open Source	Servidor de correo electrónico
Proxmox Email Gateway 6.2-3 x64	Servidor de Gateway de correo electrónico
Kali Linux 2020 1b.	Herramienta utilizada para ejecutar ataques controlados sobre el escenario de pruebas.

Realizado por: Rochina César, 2020.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

En el presente Capítulo, se analizarán los datos obtenidos en los escenarios de pruebas elaboradas y se contrastarán sus resultados, además se realizará la comprobación de la hipótesis definida para la presente investigación.

4.1 Desarrollo de pruebas

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

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

4.1.1 Escenario de prueba sin la metodología propuesta

El primer escenario de prueba consiste en la implementación del servicio de correo electrónico con un servidor Gateway de configuración estándar, a continuación se presenta el diagrama lógico:

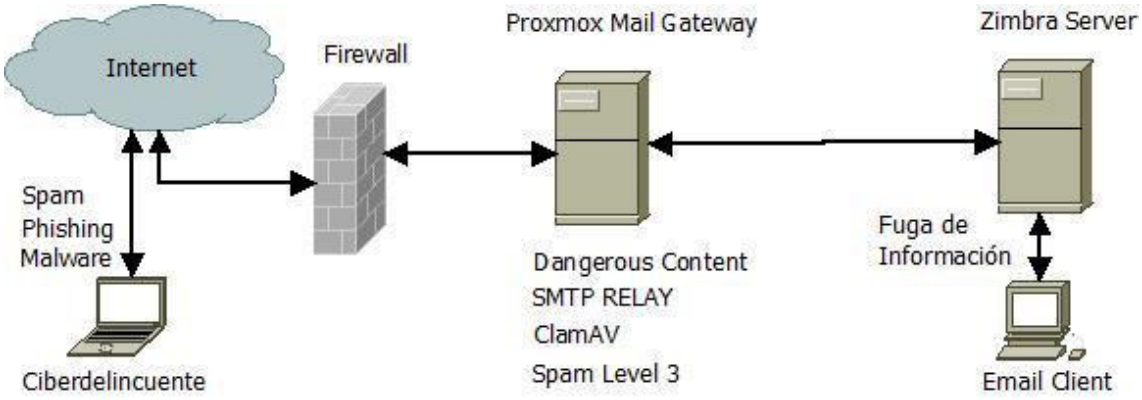


Figura 1-4: Diseño del primer escenario de pruebas

Realizado por: Rochina César, 2020.

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

4.1.2 Escenario de prueba con la metodología propuesta

El segundo escenario de prueba consiste en la implementación del servicio de correo electrónico con un servidor Gateway configurada de acuerdo a la metodología elaborada.

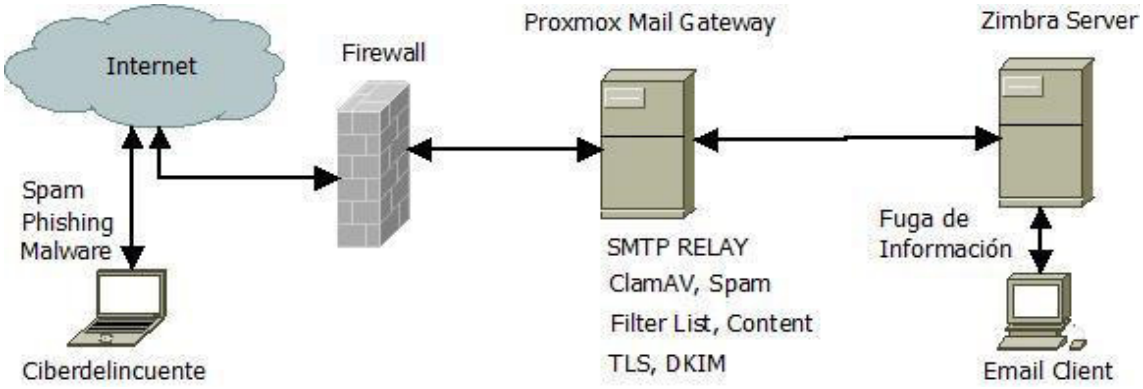


Figura 2-4: Diseño del segundo escenario de pruebas

Realizado por: Rochina César, 2020.

El segundo escenario de pruebas simula una implementación personalizada de filtros y reglas sobre el Gateway de acuerdo a la metodología elaborada, 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.

4.1.3 Ataques controlados sobre el escenario de prueba

Sobre los (2) dos escenarios se ejecutó ataques controlados de Spam, Phishing y Malware desde la internet, mientras que para el caso de fugas de información se ejecutó desde el cliente interno del correo corporativo.

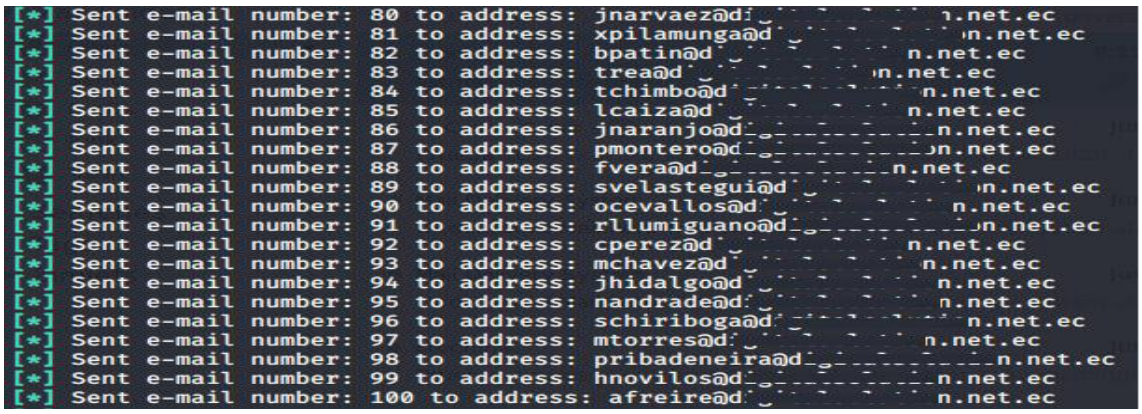


Figura 3-4: Ataques controlados sobre el escenario de prueba

Realizado por: Rochina César, 2020.

En la Figura 3-4, se puede observar un extracto de ataque desde la herramienta Social-Engineer Toolkit incorporado en Kali Linux, ejecutado de forma controlada hacia un grupo de cuentas de correo electrónico corporativo implementado sobre los dos escenarios de pruebas.

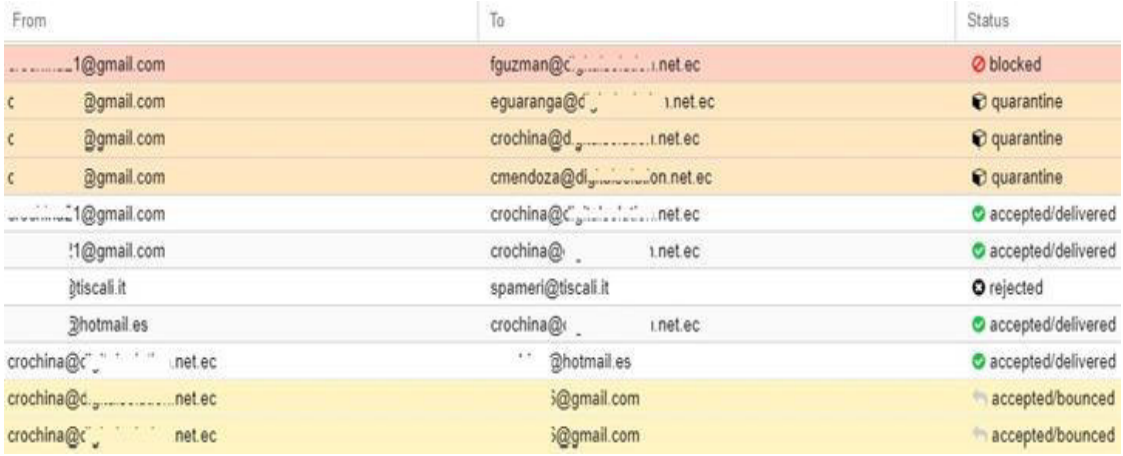


Figura 4-4: Panel de seguimiento de correo de Proxmox Mail Gateway

Realizado por: Rochina César, 2020.

En la Figura 4-4, se muestra el panel de seguimiento de la herramienta Proxmox Mail Gateway, en el cual se puede observar el tráfico y el estado de todos los correos electrónicos entrantes y salientes, el estado indica la acción establecida por el Gateway sobre cada correo electrónico de acuerdo al cumplimiento de filtros y reglas aplicados en los escenarios de pruebas.

4.2 Análisis e interpretación de resultados

4.2.1 Análisis e interpretación de resultados de la variable independiente

Variable independiente:

- Metodología para reducir ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway.

Indicador:

- Porcentaje de ciberataques bloqueados.

Tabla 1-4: Resumen de ciberataques bloqueados antes y después de aplicar la metodología

	Ataques ejecutados para cada escenario	**Ataques bloqueados antes de aplicar la metodología**	**Ataques bloqueados después de aplicarla metodología**
Cantidad	400	228	383
Porcentaje	100 %	57%	95,75%

Realizado por: Rochina César, 2020.

Se han ejecutado 400 ciberataques, lo que representa el 100% de ataques realizados para cada uno de los escenarios, en el escenario antes de aplicar la metodología se obtuvo 228 ciberataques bloqueados, mientras que, en el escenario después de aplicarla metodología se obtuvo 383 ciberataques bloqueados.

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

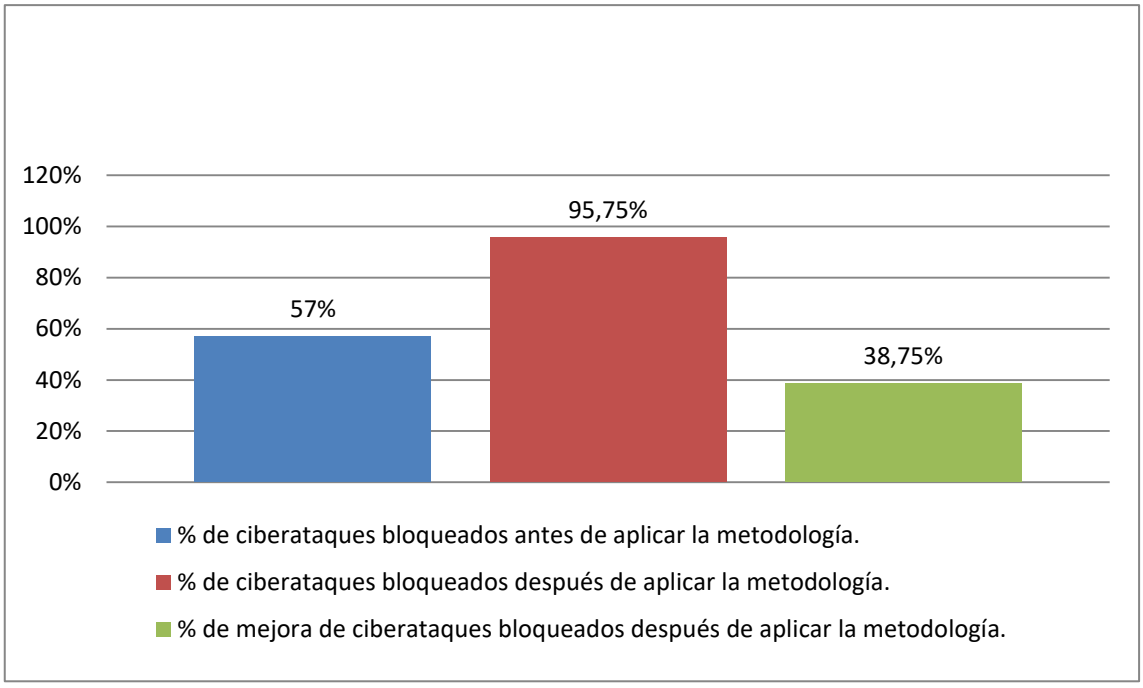


Figura 5-4: Porcentaje de ciberataques bloqueados antes y después de aplicar la metodología.

Realizado por: Rochina César, 2020.

Como se puede apreciar en la figura 5-4, 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 en el escenario después de aplicar la metodología, representando un incremento del 38,75% en relación al primer escenario.

4.2.2 Análisis e interpretación de resultados de la variable dependiente

Variable dependiente:

- Porcentaje de reducción de ciberataques

Indicadores:

- Porcentaje de bloqueo de malware.
- Porcentaje de bloqueo de spam.
- Porcentaje bloqueo phishing.
- Porcentaje de bloqueo de fuga de información.

Tabla 2-4: Comparativa de ciberataques ejecutados antes y después de aplicar la metodología.

Ciberataque originado a través de correo electrónico	**Cantidad de Ciberataques ejecutados**	**Ciberataques bloqueados antes de aplicar la metodología**	**Ciberataques bloqueados después de aplicar la metodología**
Malware	100	89	98
Spam	100	45	97
Phishing	100	56	95
Fuga de información	100	38	93

Realizado por: Rochina César, 2020.

Como se puede observar en la Tabla 2-4, para contrastar el porcentaje de reducción de ciberataques por cada uno de los indicadores de la variable dependiente, se han ejecutado 100 ciberataques a través de correo electrónico, por cada uno de los indicadores, en los dos escenarios de pruebas implementados.

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

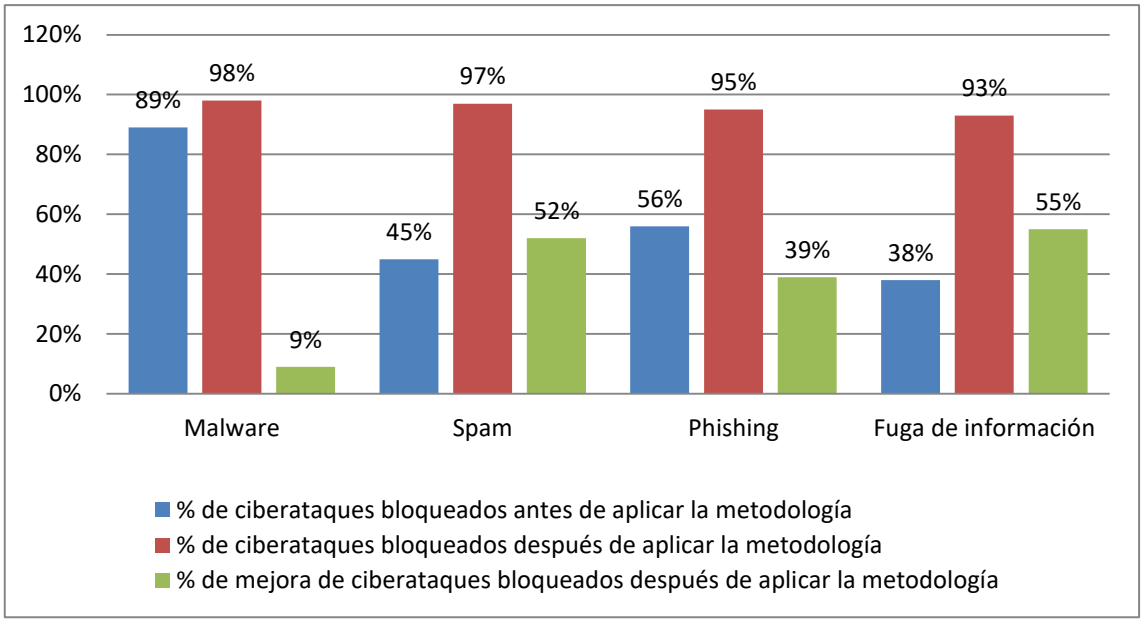


Figura 6-4: Porcentaje de mejora de ciberataques bloqueados después de aplicar la metodología.

Realizado por: Rochina César, 2020.

Antes de aplicar 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, mientras que, después de aplicar la metodología se bloquearon el 98% de ataque de malware, 97 % de ataque de spam, 95 % de ataques phishig, 93 % de correos electrónicos de fuga o filtración de información y finalmente se puede contrastar que el nivel de porcentaje de bloqueos de ciberataques se ha incrementado, para malware en un 9%, para Spam en un 52%, para phishing en un 39%, y para la fuga de información en un 55%.

4.3 Validación de hipótesis

Para la comprobación de la Hipótesis General: "La metodología elaborada mediante la aplicación de filtros y reglas sobre un Gateway reducirá el porcentaje de la cantidad de ciberataques originados a través de correo electrónico", se utilizó estadística inferencial aplicando Chi-Cuadrado (X^2), y se determinó las siguientes hipótesis: nula H0 y Alternativa H1:

- Hipótesis Nula H0: "La metodología elaborada mediante la aplicación de filtros y reglas sobre un Gateway no reducirá el porcentaje de la cantidad de ciberataques originados a través de correo electrónico"
- Hipótesis Alternativa H1: "La metodología elaborada mediante la aplicación de filtros y reglas sobre un Gateway si reducirá el porcentaje de la cantidad de ciberataques originados a través de correo electrónico"

Valores Observados

Tabla 3-4: Frecuencias de Valores observados

Valores Observados			
	ANTES	**DESPUÉS**	**TOTAL**
Cantidad de ciberataques bloqueados	228	383	611
Cantidad de ciberataques no bloqueados	172	17	189
TOTAL	400	400	800

Realizado por: Rochina César, 2020.

Valores Esperados

La tabla de frecuencias esperadas se obtiene de la siguiente manera:

$$Eij = \frac{(Total\ Columna) * (Total\ Fila)}{Suma\ Total}$$

Tabla 4-4: Frecuencia de valores esperados

Valores esperados			
	ANTES	**DESPUÉS**	**TOTAL**
Cantidad de ciberataques bloqueados	305,5	305,5	611
Cantidad de ciberataques no bloqueados	94,5	94,5	189
TOTAL	400	400	800

Realizado por: Rochina César, 2020.

Se determina el valor calculado del Chi-cuadrado (X^2), de acuerdo a la siguiente formula:

$$x^2 calc = \sum \frac{(Oij - Eij)^2}{Eij}$$

Dónde:

Oij: son las frecuencias observadas, es el número de casos observados clasificados en la fila i columna j

Eij: son las frecuencias esperadas, es el número de casos esperados correspondiente a cada fila y columna

$X^2calc = (228 – 305,5)^2 / 305,5 + (383 - 305,5)^2/305,5 + (172 - 94,5)^2/94,5 + (17-94,5)^2/94,5$

$X^2calc = 166,44$

Se determina los grados de Libertad, para lo cual se utiliza la siguiente fórmula:

$$gl= (f-1)*(c-1)$$

Dónde:

f = Número de filas

c = Número de columnas

$$gl= (2-1)*(2-1)$$

gl= 1

Nivel de confianza de 95 % = 0.95 y Nivel de significancia del 5% = 0.05

El nivel de significancia es el error que se puede cometer al rechazar la Hipótesis Nula Ho siendo verdadera, generalmente se trabaja con un 5%, es decir 0,05, que indica que hay una probabilidad (p) del 0,95 de que la Hipótesis Nula Ho sea verdadera.

Por lo tanto, el valor crítico según la tabla de distribución (Anexo C) con los valores de 1 grado de libertad y 0,95 de nivel de confianza se tiene:

X^2 Critico = 3,84

Criterio de decisión

Se acepta la H0: si X^2 calc ≤ X^2 Critico, caso contrario se rechaza la H0 y se acepta la H1.

Resultados de la investigación:

Se tiene los siguientes valores:

$X^2calc = 166,44$

X^2 Critico = 3,84

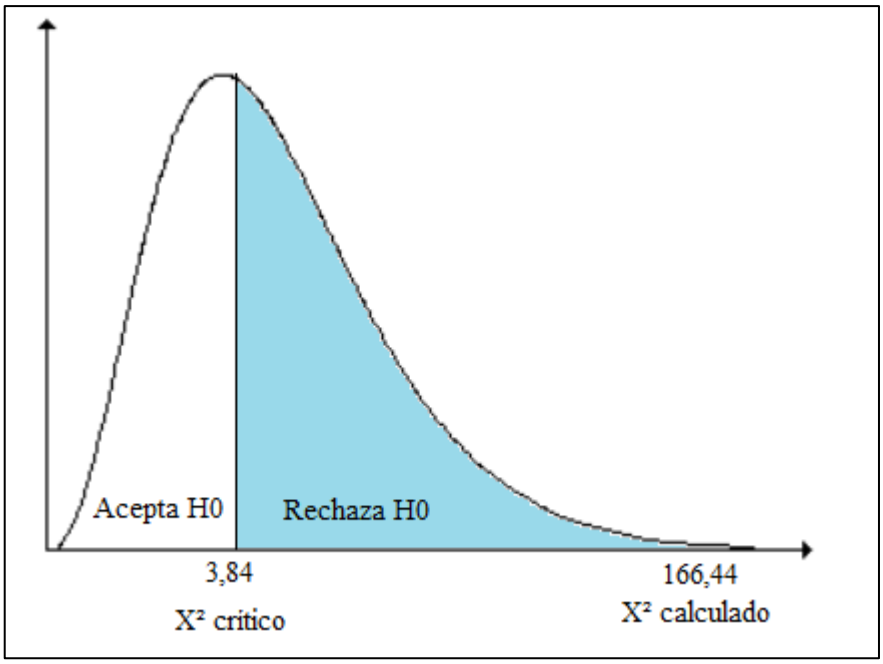


Figura 7-4: Distribución de chi cuadrado

Realizado por: Rochina César, 2020.

Interpretación

Se puede observar en la Figura 6-4 que X^2 calc es mayor que X^2 Critico, es decir 166,44 > 3,84, lo cual no cumple con el criterio de decisión.

Por lo tanto, se rechaza la hipótesis nula (H0) y se acepta la hipótesis alternativa (H1), con un nivel de confianza de 95 %.

Quedando demostrado que:

H1: "La metodología elaborada mediante la aplicación de filtros y reglas sobre un Gateway si reducirá el porcentaje de la cantidad de ciberataques originados a través de correo electrónico"

CAPÍTULO V

5. PROPUESTA

En el presente Capítulo, se describe la metodología propuesta para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway

5.1 Descripción de la metodología

La metodología basada en reglas y filtros ayudará a detectar correos electrónicos maliciosos, tales como: malware, Spam, y phishing, así como también la prevención de fuga de información, por lo tanto, se reducirán los ciberataques originados a través de correo electrónico. La metodología deberá ser aplicada sobre el servicio de correo electrónico con un Gateway de las siguientes características principales: Antimalware, Antispam, personalización de reglas, generación de Listas Negras y Blancas, seguimiento de eventos, autoaprendizaje, y la administración web.

5.2 Fases de la metodología

La metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway presenta el siguiente esquema general.

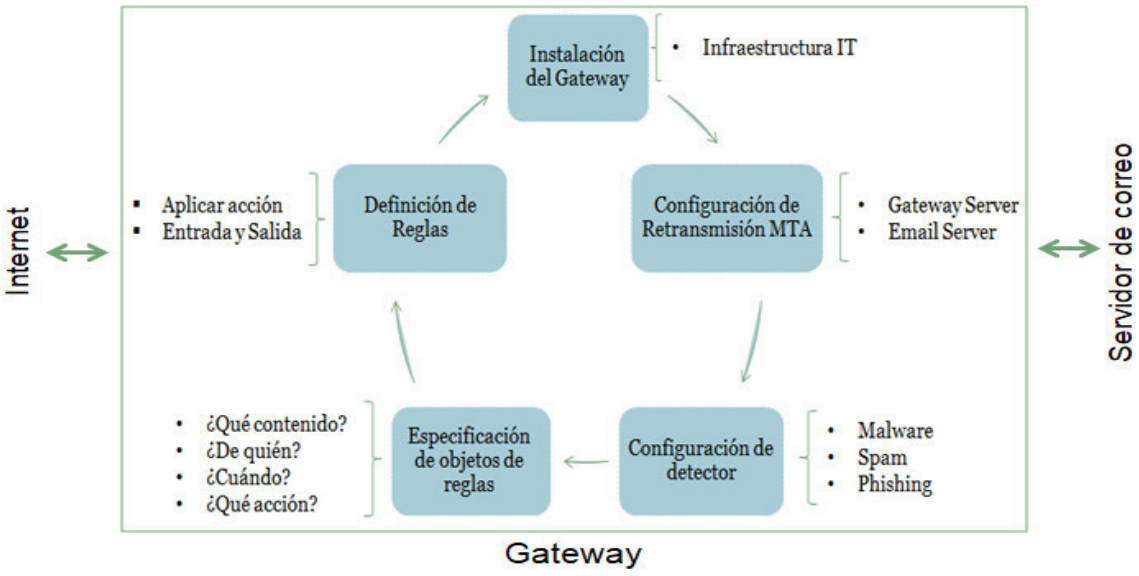


Figura 1-5: Esquema general de la metodología

Realizado por: Rochina César, 2020.

Como se puede apreciar en la Figura 1 -5 el esquema general, la metodología propuesta establece cinco (5) fases a seguir para su implementación:

1. Instalación del Gateway de correo electrónico.
2. Configuración de Retransmisión MTA.
3. Configuración de detector de malware, Spam y Phishing.
4. Especificación de objetos de las reglas.
5. Definición de Reglas.

A continuación, se detallan cada una ellas:

5.2.1 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.

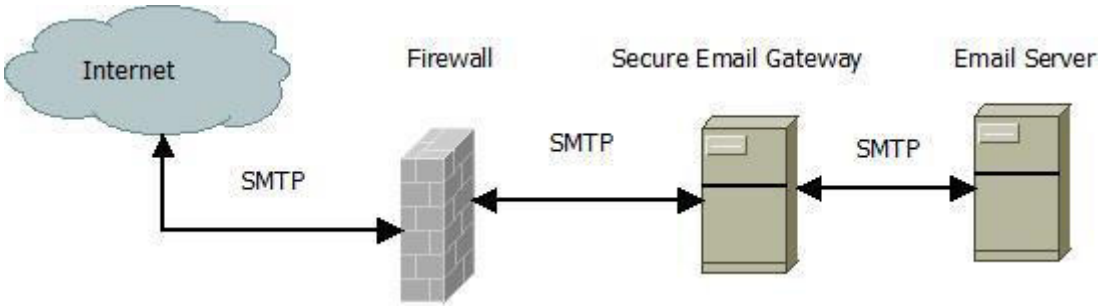


Figura 2-5: Diagrama de instalación del Gateway de correo

Realizado por: Rochina César, 2020.

De esta forma el servidor Gateway hará frente como servidor de correo electrónico hacia el internet.

5.2.2 Configuración de Retransmisión MTA

La configuración se deberá realizar tanto en el servidor de correo electrónico como en el servidor de Gateway.

1. Servidor de correo electrónico

En el servidor de correo electrónico se deberá indicar el nombre o la dirección IP del Gateway con su respectivo puerto, como el host de Retransmisión para entrega de correos electrónicos externos.

Implementación:

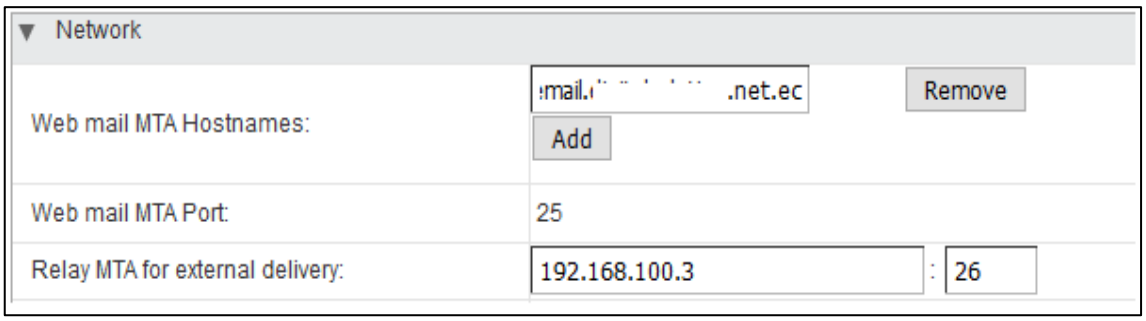


Figura 3-5: Configuración de Relay MTA en el servidor de correo electrónico

Realizado por: Rochina César, 2020.

Como se puede apreciar en el Figura 3-5, en el "Relay MTA" se ha ingresado la dirección IP del Gateway que es 192.168.100.3 y el puerto 26, con esto se garantiza que todos los correos electrónicos a dominios externos (gmail.com, espoch.edu.ec, etc.) serán retransmitidos a través Gateway.

2. Gateway de correo electrónico

En el servidor Gateway se deberá indicar el nombre o la dirección IP del servidor de correo electrónico, el dominio interno de correos, así como también habilitar los puerto para correos de dominio interno y dominio externo.

Implementación:

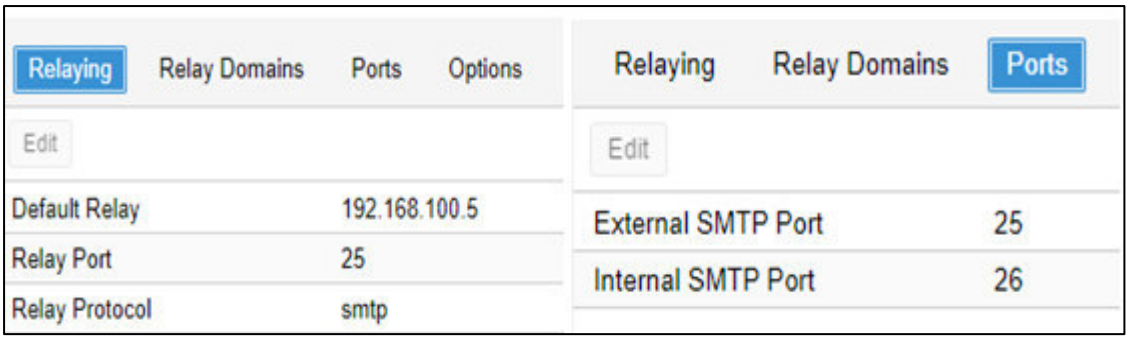


Figura 4-5: Configuración de Relay en el Gateway de correo electrónico

Realizado por: Rochina César, 2020.

Como se puede apreciar en la Figura 4-5, en el host de retransmisión se ha ingresado la dirección IP del servidor de correo electrónicos "192.168.100.5", en el dominio retransmisión "example.net.ec", para correos de dominios externos (gmail.com, espoch.edu.ec, etc.) se ha habilitado el puerto 25, y para el interno (example.net.ec) el puerto 26.

De esta manera se indica al Gateway que los correos electrónicos desde el internet (dominios externos) dirigidos hacia el dominio interno (example.net.ec) serán retransmitidos al servidor de correo interno especificado.

3. Transmisión Segura a través del protocolo TLS

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 la transmisión de datos con el SMTP Interno.

Implementación:

Figura 5-5: Protocolo TLS

Realizado por: Rochina César, 2020.

5.2.3 Configuración de detector de malware, Spam y Phishing

La configuración se deberá realizar en el servidor de Gateway.

1. Configuración de detector de malware

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

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.

El tamaño máximo de un archivo para que el motor anti malware del Gateway proceda con el escaneo debe ser igual al tamaño máximo del archivo adjunto permitido en el servidor de correo electrónico, si el tamaño del archivo permitido en el servidor de correo electrónico es superior, el Gateway no escaneará y el riesgo de que un archivo malicioso sea transmitido será alto.

La cantidad máxima de recursión representa, la profundidad o niveles el escaneo de archivos anidados, mientras que, activar el bloqueo de archivos encriptados no es recomendado ya que un archivo legítimo libre de malware puede ser bloqueado generando un falso positivo en el Gateway.

Implementación:

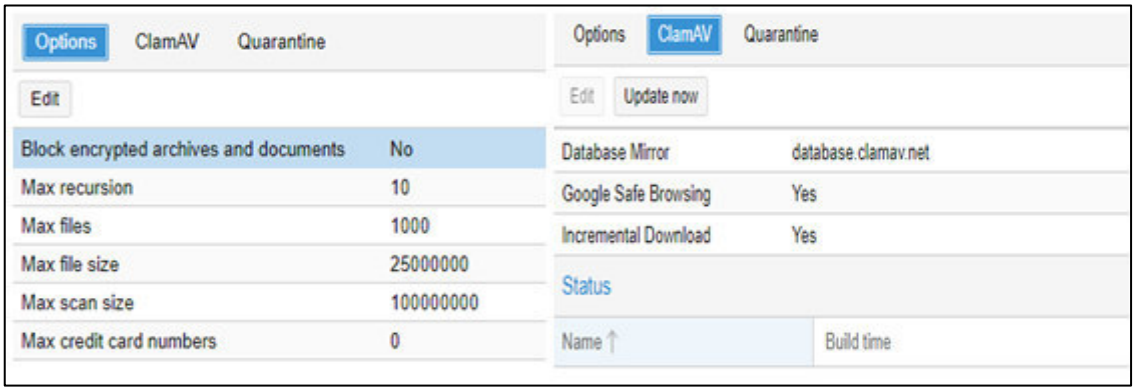


Figura 6-5: Configuración de detector de malware

Realizado por: Rochina César, 2020.

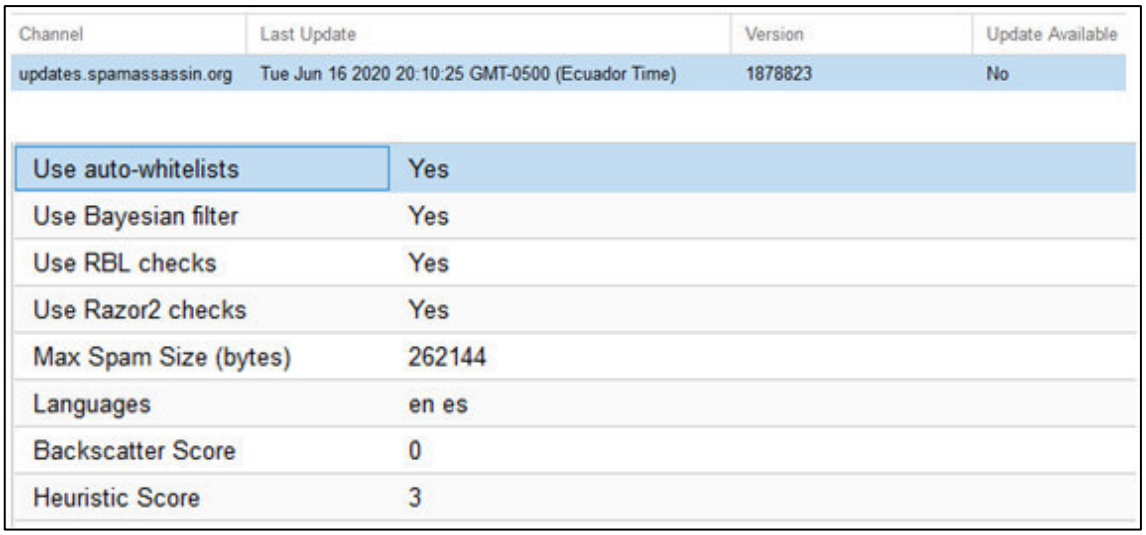
Proxmox Mail Gateway en su versión sin suscripción incorpora el motor de CLAMAV, se ha configurado 25 MB como tamaña máximo de archivo permitido para el escaneo, con una profundidad máxima de 10 niveles para archivo anidados.

2. Configuración de detector de Spam y Phishing

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.

Implementación:



Channel	Last Update	Version	Update Available
updates.spamassassin.org	Tue Jun 16 2020 20:10:25 GMT-0500 (Ecuador Time)	1878823	No

Use auto-whitelists	Yes
Use Bayesian filter	Yes
Use RBL checks	Yes
Use Razor2 checks	Yes
Max Spam Size (bytes)	262144
Languages	en es
Backscatter Score	0
Heuristic Score	3

Figura 7-5: Configuración de detector de spam

Realizado por: Rochina César, 2020.

Para la puntuación heurística cuanto menor sea la puntuación, más restrictivo será el filtro, en este caso se ha asignado el valor de 3, lo que significa que los correos catalogados con una puntuación superior serán catalogados como Spam, caso contrario serán entregados como correos legítimos libre de Spam.

5.2.4 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.

1. 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.

Implementación:

Name ↑	Description	Comment
Accept	accept message	Accept mail for Delivery
Notify Admin	notify __ADMIN__	Enviar notificación al Administrador
Notify Sender	notify __SENDER__	Enviar notificación al remitente
Block	block message	Block mail
Quarantine	Move to quarantine.	Move mail to quarantine
Excluir Adjuntos	remove all attachments	Excluir todos los archivos > Tamaño

Figura 8-5: Objetos de Acción

Realizado por: Rochina César, 2020.

Como se puede observar en la Figura 8-5, se ha creado tres objetos de acción mínimas que se requieren, adicionalmente se han creado los objetos de acción de notificación y exclusión de archivos adjuntos, mismos que serán aplicados posteriormente cuando se definan las reglas.

2. 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 categorizadas de las listas Negras y Listas Blancas.

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.

Implementación:

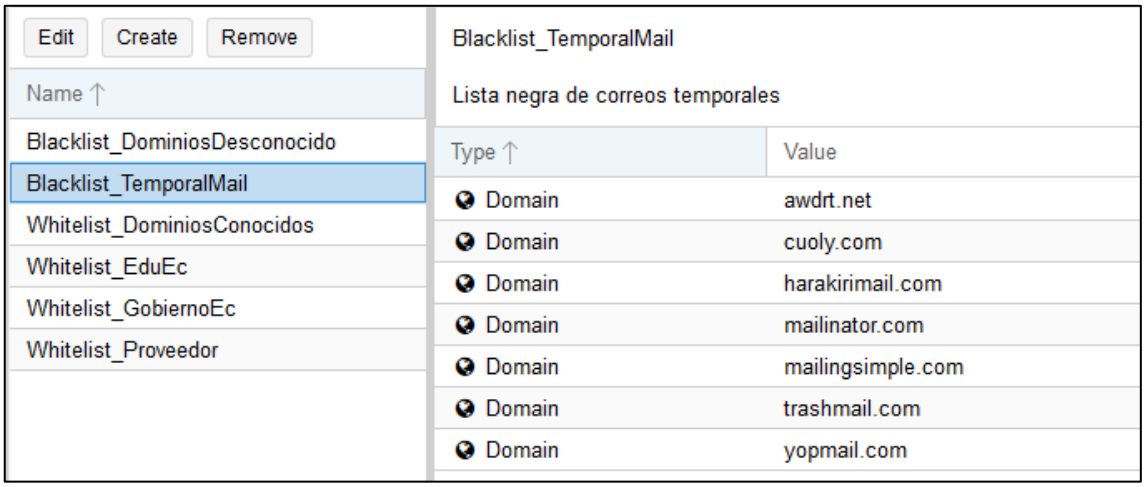


Figura 9-5: Listas Negras

Realizado por: Rochina César, 2020.

Como se puede observar en la Figura 9-5, se ha construido una lista negra por dominios de los correos temporales.

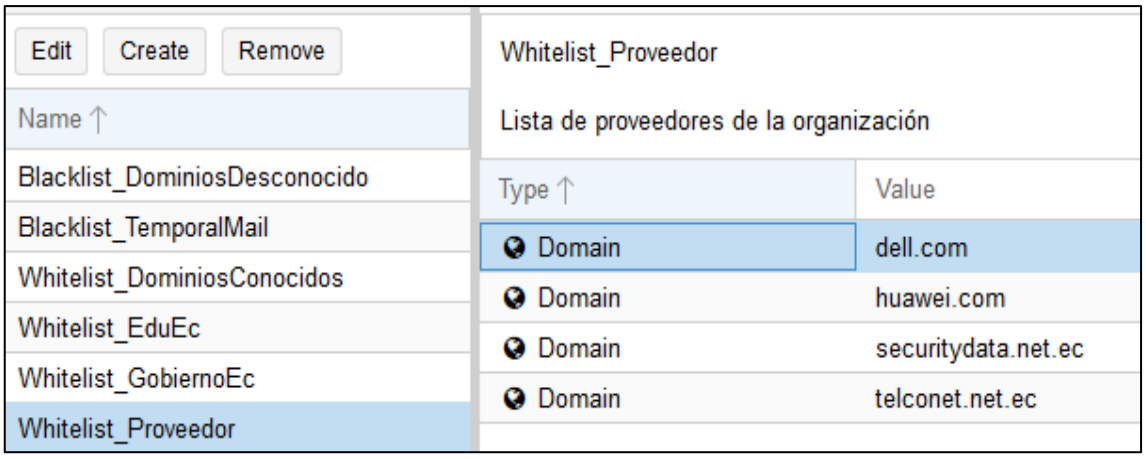


Figura 10-5: Listas Blancas

Realizado por: Rochina César, 2020.

Como se puede observar en la Figura 10-5, se ha construido una lista blanca agrupada por dominios de los proveedores de la empresa.

La clasificación y agrupación 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.

3. 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.

Implementación:

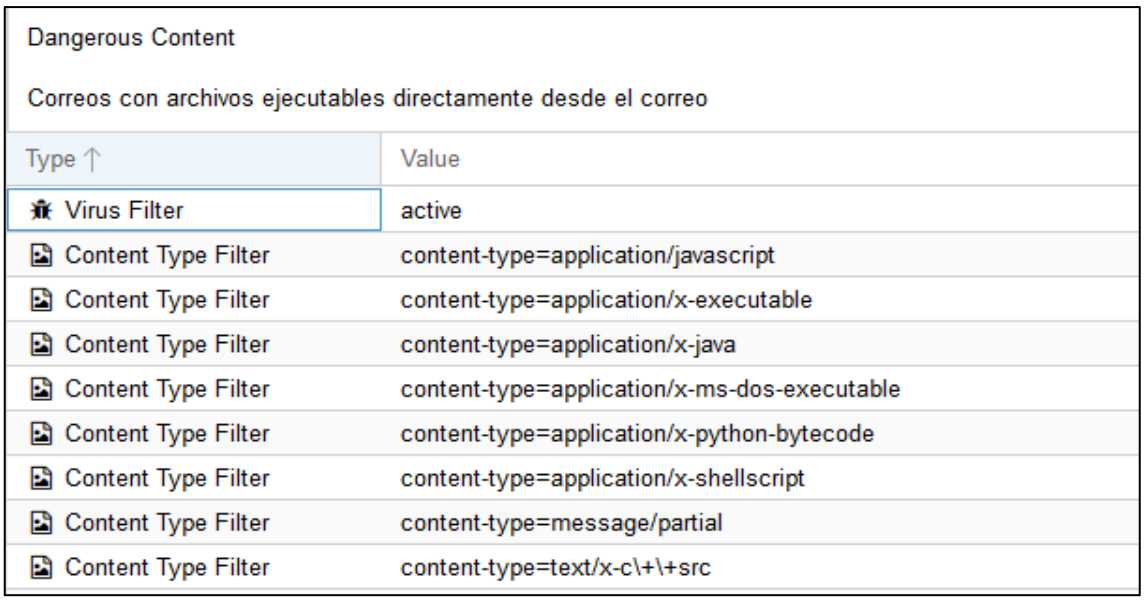


Figura 11-5: Objeto contenido de aplicaciones maliciosas

Realizado por: Rochina César, 2020.

Como se puede observar en la Figura 11-5, se ha creado un objeto de contenido y se le ha agrupado un listado de contenido malicioso que se puedan detectar dentro de un correo electrónico

Documentos

Archivos comunes utilizados en officina

Type	Value
Content Type Filter	content-type=application/msword
Content Type Filter	content-type=application/vnd\.ms-excel
Content Type Filter	content-type=application/vnd\.ms-powerpoint
Content Type Filter	content-type=application/vnd\.oasis\.opendocument\..*
Content Type Filter	content-type=application/vnd\.openxmlformats-officedocument\..*
Content Type Filter	content-type=application/vnd\.stardivision\..*
Content Type Filter	content-type=application/vnd\.sun\.xml\..*

Figura 12-5: Objeto de contenido de documentos

Realizado por: Rochina César, 2020.

Como se puede observar en la Figura 12-5, se ha creado un objeto de contenido y se le ha agrupado un listado de posibles documentos que se puedan detectar dentro de un correo electrónico, que posteriormente será utilizado por para la definición de las reglas.

4. Objeto Tiempo

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

Implementación:

Edit Create Remove

Name
All time
Office Hours

Office Hours

Usual office hours

Type	Value
TimeFrame	08:00-17:00

Figura 13-5: Objeto Tiempo

Realizado por: Rochina César, 2020.

En la Figura 13-5, se muestra una definición de un horario de oficina de 8H00 a 17h00 que puede ser aplicada en una regla.

5.2.5 Definición de Reglas

Para definir las reglas, primeramente 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, posteriormente, se tendrá en cuenta mínimo dos objetos definidos, siendo indispensable el "Objeto Acción".

Las reglas se ordenan por prioridad, por lo que las reglas con mayor prioridad se ejecutarán primero, en caso de que las prioridades de dos o más reglas sean iguales la ejecución se determinará de acuerdo al trayecto del correo electrónico, el primero en ejecutar serán las reglas de entrada, seguido por las reglas de salida, y finalmente las reglas aplicada para los dos trayectos "Entradas y Salida".

La prioridad de la regla deberá ser definida según el nivel de riesgo que represente a cada organización, generalmente las reglas de filtro contra las amenazas de malware, spam, phishing son de alta prioridad, la prioridad puede tomar valores desde cero (0) hasta cien (100).

Implementación:

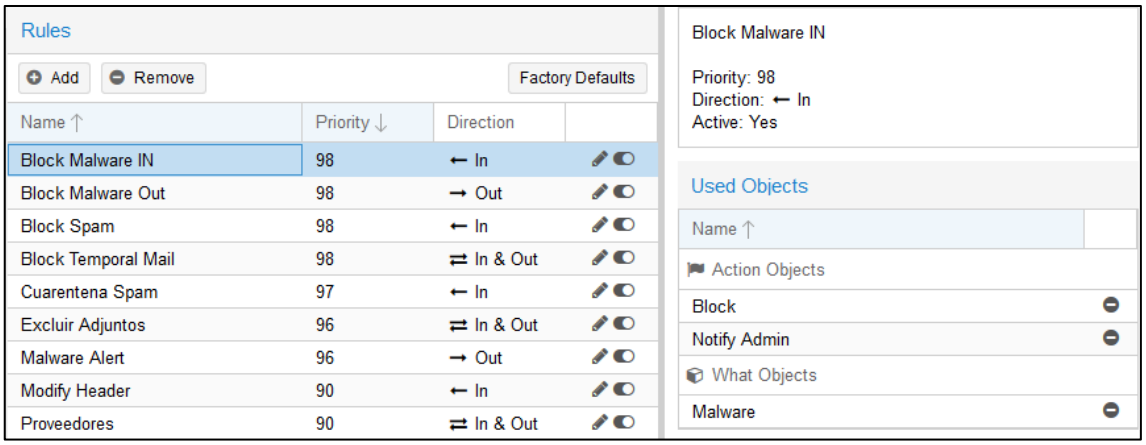


Figura 14-5: Reglas de Entrada

Realizado por: Rochina César, 2020.

Como se puede observar en la Figura 14-5, se ha definido una regla de entrada de alta prioridad (98) para bloquear correos electrónicos con malware, además se ha agregado el objeto de notificación respectiva al administrador.

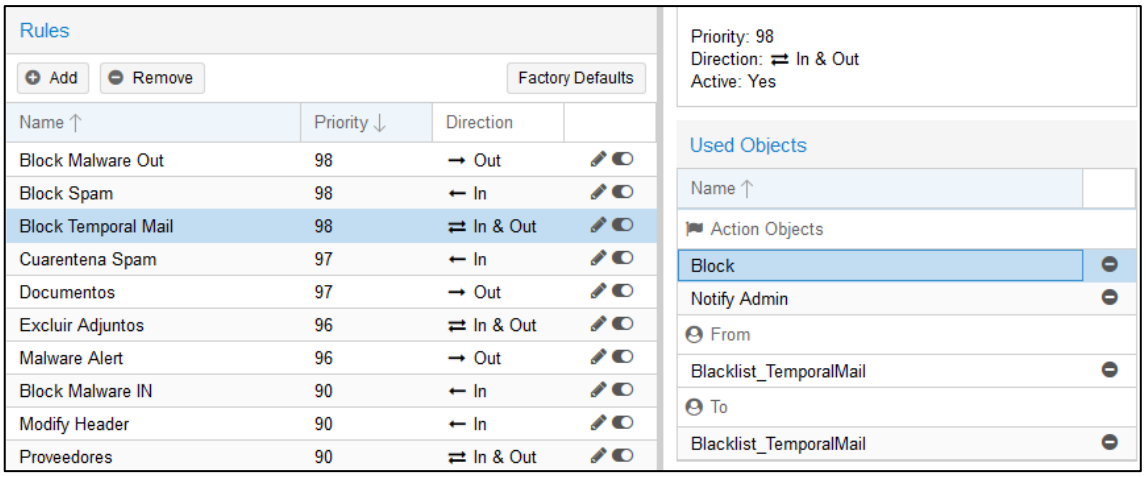


Figura 15-5: Regla conjunta a las dos trayectorias

Realizado por: Rochina César, 2020.

Como se puede observar en la Figura 15-5, se ha definido una regla aplicada para los dos trayectos (entrada y salida) de alta prioridad (97) para bloquear correos electrónicos de una lista negra personalizada por el usuario, la regla bloqueará todos los correos entrantes que provengan y correos electrónicos salientes dirigidos hacia las direcciones definidas en la lista negra, además ésta será notificado al administrador.

ÇCONCLUSIONES

- 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 56,61% de correos electrónicos son Spam o correos no solicitados, así como también se logró determinar que el correo electrónico es un medio o canal utilizado para la fuga de información.
- Existen una gran cantidad de 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, el primero sin aplicar la metodología y el segundo con su aplicación, sobre cada escenario 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 la metodología elaborado reduce los ciberataques originados a través de correo electrónico en un 38,75 %.
- Mediante la prueba estadística de chi-cuadrado con nivel de nivel de significancia del 5% y con un grado de libertad se tiene los siguientes valores: X^2 Critico = 3,84 de acuerdo a la tabla de distribución y para el X^2 calculado = 166,44, por lo tanto se rechaza la Hipótesis Nula y se acepta la Hipótesis Alternativa “La metodología elaborada mediante la aplicación de filtros y reglas sobre un Gateway si reducirá el porcentaje de la cantidad de ciberataques originados a través de correo electrónico”
- Se elaboró una metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway, que permite detectar correos electrónico de contenido malicioso, la metodología 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.

RECOMENDACIONES

- Monitorear de manera contante el Gateway de correo electrónico, con el fin de adicionar nuevos filtros y reglas que detecten los ciberataques más recientes considerando las fases descritas en la metodología, ya que cada día se descubren nuevas técnicas o malware que vulneran los sistemas de seguridad.
- Mantener actualizado los servidores de la herramienta Gateway y sus componentes tales como: detectores de malware, spam, phishing, así como también los servidores de correo electrónico internos y sus aplicaciones clientes.
- Realizar capacitación y concientización constante a todo el personal de la organización en las medidas de seguridad que se deben tomar ante los ciberataques basadas en ingeniería social.
- Como trabajo futuro con el fin de seguir mejorando el filtrado y la capacidad de detectar correos electrónicos maliciosos se recomienda ampliar el presente trabajo de investigación basándose en la nube e incluyendo tecnologías emergentes como el aprendizaje automático basados en la inteligencia artificial (IA) y la integración con los sistemas de monitoreo de seguridad centralizada.

GLOSARIO

Archivo adjunto: Son archivos que se insertan junto a un mensaje de correo electrónico desde el remitente y es enviado al destinatario.

Ciberataque: Un ciberataque es cualquier tipo de maniobra ofensiva hecha por individuos u organizaciones en contra de los sistemas o infraestructuras informáticas, usualmente originados de fuentes anónimas con el fin de alterar la integridad, disponibilidad o la confidencialidad de un servicio o información.

Ciberdelincuentes: Son personas que realizan actividades delictivas a través de una red de datos o internet como ataques a sistemas informáticos y piratería, fraude o falsificación, publicación de contenidos ilegales.

Confidencialidad: Es propiedad de la información que permite únicamente a los usuarios autorizados a acceder a dicha información.

Disponibilidad: Es propiedad de la información que garantiza a los usuarios autorizados a acceder a dicha información, toda vez que lo requieran

DNS: Son las iniciales de Domain Name System (sistema de nombres de dominio) y es una tecnología basada en una base de datos que sirve para resolver nombres en las redes, es decir, para conocer la dirección IP de la máquina donde está alojado el dominio.

Ingeniería social: Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.

Integridad: Es propiedad de la información que garantiza que los datos reflejen la realidad y que correspondan con lo que debe ser y no haya sido modificado por usuarios no autorizados.

Malware: Malware es un acrónimo del inglés de “malicious software”, que traduce como código malicioso. Son programas diseñados con el fin de infiltrase de manera desapercibida y anónima en un sistema y posteriormente cumplir con las funciones para la cual fue creado.

Mitigar: Conjunto de acciones para reducir la probabilidad de que un riesgo se materialice, estos pueden incluir remover una vulnerabilidad, implementar sistemas de seguridad para que una vulnerabilidad sea más difícil de explotar.

Social-Enginer Toolkit: Es un herramienta de código abierto especialmente diseñadas para realizar ataques de Ingeniería Social en procesos de auditorías en seguridad.

BIBLIOGRAFÍA

[1]. **Aguirre, B.** (2019).*Implementación de medidas de seguridad en un servidor de correos que minimicen el impacto de vulnerabilidades basadas en email*. UNIVERSIDAD TÉCNICA DE MACHALA. http://repositorio.utmachala.edu.ec/bitstream/48000/13592/1/ ECUAIC- 2019-SIS-DE00002.pdf

[2]. **AVANAN.** (2019). *What Is a Secure Email Gateway and Are They Still Viable in 2020?*. https://www.avanan.com/blog/what-is-a-secure-email-gateway

[3]. **Avast Security.** (2019). *Spam*. https://www.avast.com/es-es/c-spam

[4]. **Barracuda.** (2018). *Email Security Trends*. https://www.barracuda.com/campaign/emailsecurityreport

[5]. **Cisco.** (2019). *Seguridad de Correo Electrónico. CISCO CYBERSECURITY SERIES*. https://www.cisco.com/c/dam/global/es_es/products/security/pdfs/es_email_sec_report.pdf

[6]. **CISCO.** (2018), *Informe anual de Ciberseguridad*, https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

[7]. **COFENSE.** (2018). *Threat Intelligence*. https://cofense.com/sigma-operators-craft-new-techniques-deliver-phish-inbox/

[8]. **Doig, D. Diaz, J. Mendoza, J. Yanez, D.** (2019). *Escenarios de aprendizaje competitivo a través de uso de elementos lúdicos para entrenamiento en Ciberseguridad*. Universidad ESAN. https://repositorio.esan.edu.pe/bitstream/handle/ESAN/1686/2019_MADTI_17-1_04_T.pdf?sequence=1&isAllowed=y

[9]. **Ecured.** (2017). *Correo Electrónico*. https://www.ecured.cu/Correo_electr%C3%B3nico

[10]. **Fajardo, A.** (2017). *La importancia de contar con correo electrónico empresarial.* https://www.migesamicrosoft.com/la-importancia-contar-correo-electronico-empresarial/

[11]. **FORCEPOINT.** (2018). *Secure Email Gateway Defined and Explored*. https://www.forcepoint.com/cyber-edu/secure-email-gateway

[11]. **INCIBE.** (2017). *Uso de Correo Electrónico.* https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-correo-electronico.pdf

[12]. **Iso Tools.** (2018). *Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad.* https://www.pmg-ssi.com/2018/02/ confidencialidad-integridad-y-disponibilidad/

[13]. **Kali Org. (2019)**. *Most Advanced Penetration Testing Distribution.* https://www.kali.org/

[14]. **López, C.** (2019). *Gobierno de TI basado en el esquema gubernamental de seguridad de la información (EGSI) en el hospital San Luis de otavalo.* UNIVERSIDAD TÉCNICA DEL NORTE. http://repositorio.utn.edu.ec/bitstream/123456789/9573/2/04%20RED%20233%20TRABAJO%20GRADO%20.pdf

[15]. **Mendiola, S.** (2019). *Herramientas para la detección de malware en dispositivos Android utilizando técnicas de Machine Learning*. UNIVERSIDAD DE CASTILLA – LA MANCHA. https://pdfs.semanticscholar.org/c842/b428408c03ea367f50b26e3e2e5ff8d06e23.pdf

[16]. **Muedas, A. Rojas, R.** (2019). *Modelo de madurez de seguridad de aplicaciones web ante ciberataques para clínicas de nivel 2*. UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS. https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/628108/Muedas_HA.pdf?sequence=3&isAllowed=y

[17]. **Panda Security.** (2018), *Exploit*, https://www.pandasecurity.com/es/security-info/exploit

[18]. **Pino, A.** (2016). *Tamaño de la muestra población infinita.* https://prezi.com/c5lvkcpokdxu/tamano-de-la-muestra-poblacion-infinita/

[19]. **Pinto, D.** (Febrero 2019). *Análisis e implementación de controladores software para la integración y monitorización de sensores en plataforma de internet of things*. UNIVERSIDAD POLITECNICA DE MADRID. http://oa.upm.es/54273/1/TFG_DAVID_GARCIA_GOMEZ_PINTO.pdf

[20]. **Proofpoint.** (2018). *Email Gateway*. https://www.proofpoint.com/us/ glossary/email-gateway

[21]. **Proxmox.** (2018). *Proxmox Mail Gateway*. https://www.proxmox.com/en/proxmox-mail-gateway

[22]. Expert Insights**.** (2020), The Top 11 Email Security Gateways. https://expertinsights. com /insights/top-11- email-security-gateways/

[23]. **Rodriguez, E.** (2012). *Muestra y Muestreo.* https://www.uaeh.edu.mx/docencia/P_Presentaciones/tizayuca/gestion_tecnologica/muestraMuestreo.pdf

[24]. **Solarte, F. Enriques, E. Benavides, M.** (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001*. Revista Tecnológica ESPOL. http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

[25]. **Universidad Nacional de Luján.** (2017). *Amenazas a la Seguridad de la Información.* http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

[26]. **Yourconnect.** (2018). *Mail Gateway*. https://www.yourconnect.com/en/mail-gateway/

[27]. **Zimbra.** (2018). *Bring Together Email, Calendaring and Enterprise Applications.* https://www.zimbra.com/

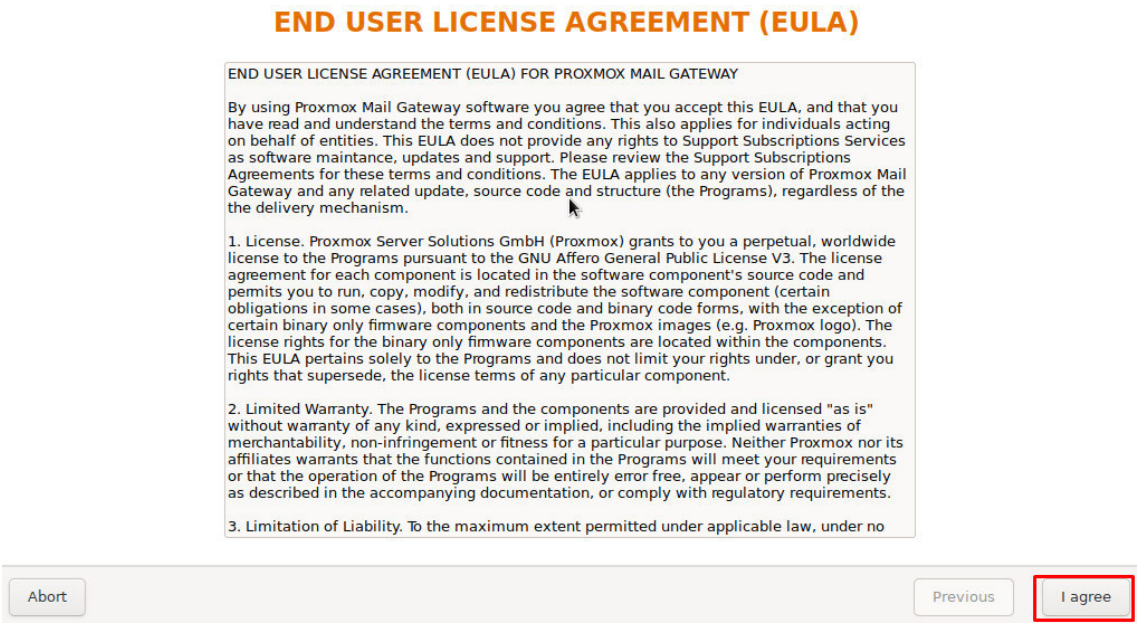
ANEXOS

ANEXO A. PROXMOX MAIL GATEWAY

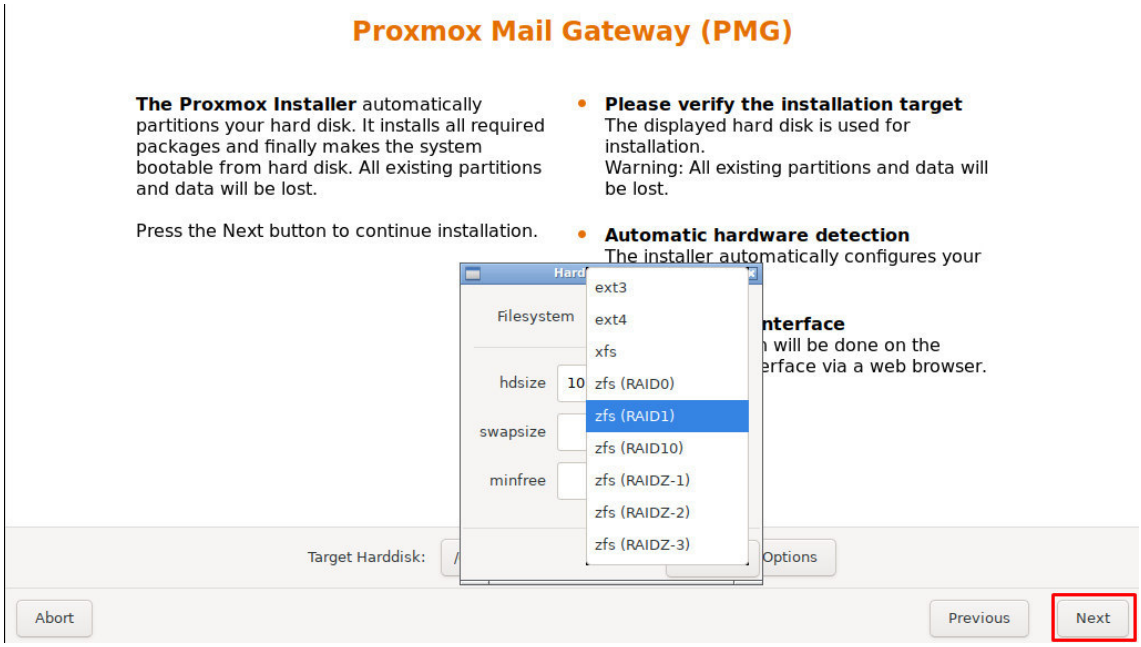
Instalación

1.- Seleccionar “Install Proxmox Mail Gateway”

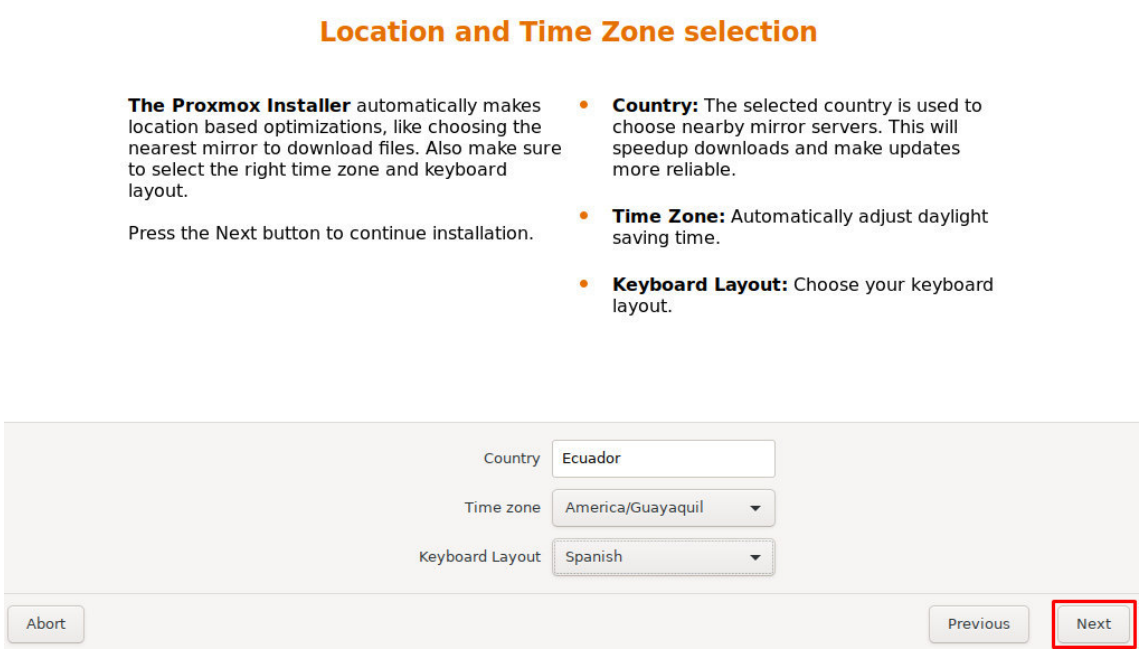
2.- Aceptar los términos de licencia



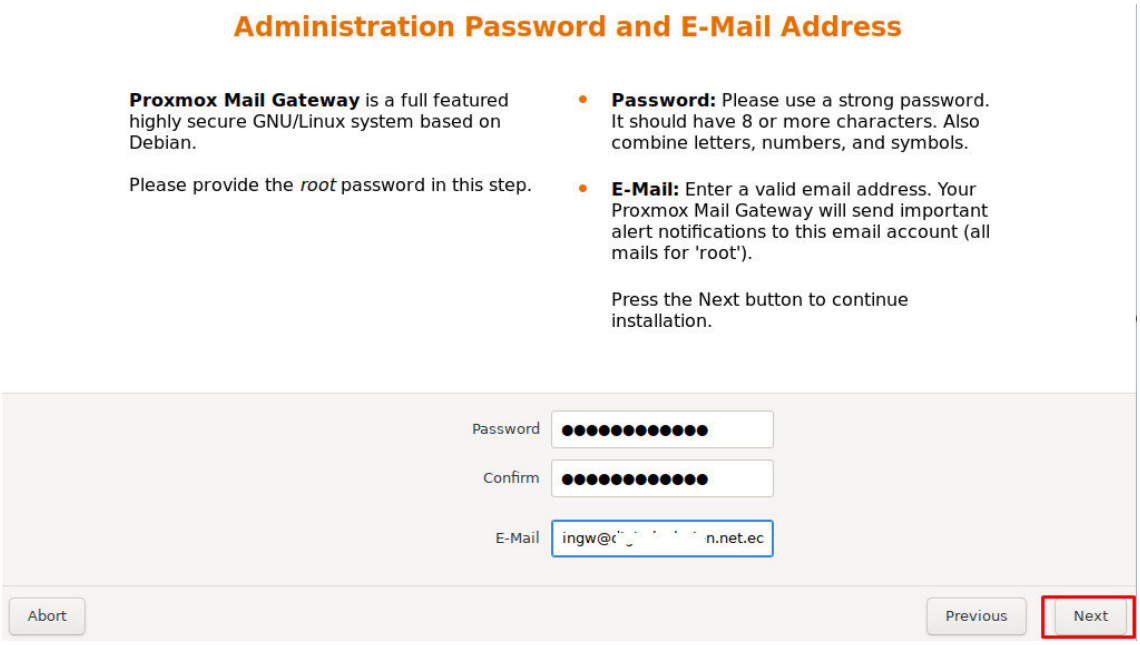
3.- Realizar las particiones de almacenamiento correspondientes.



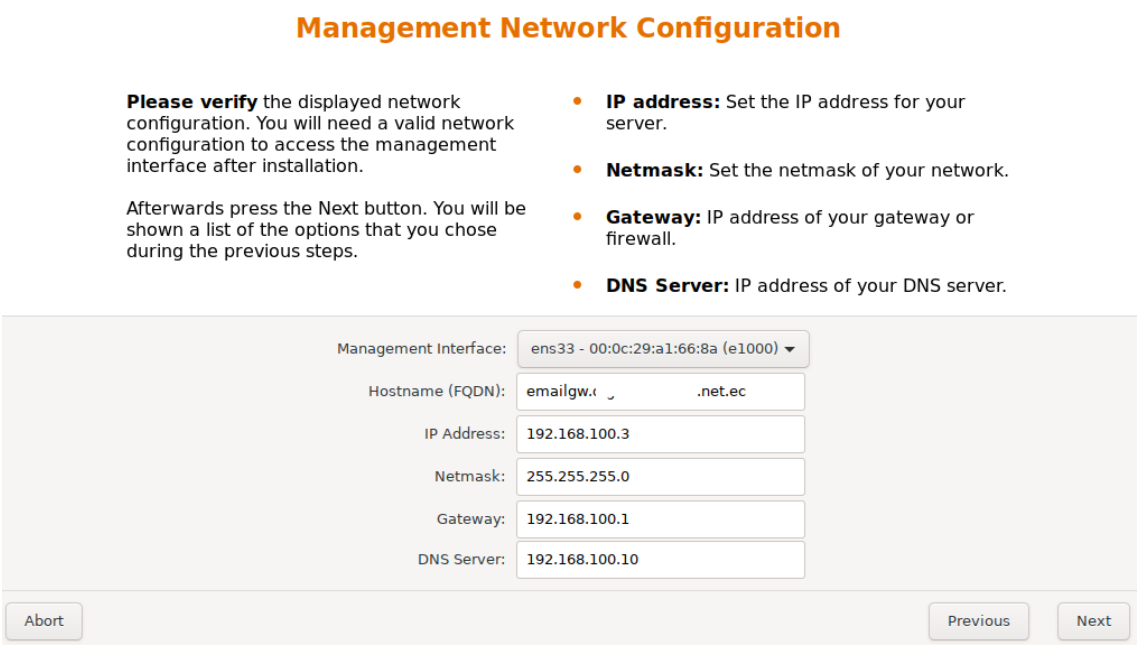
4.- Seleccionar la localización y la zona horaria



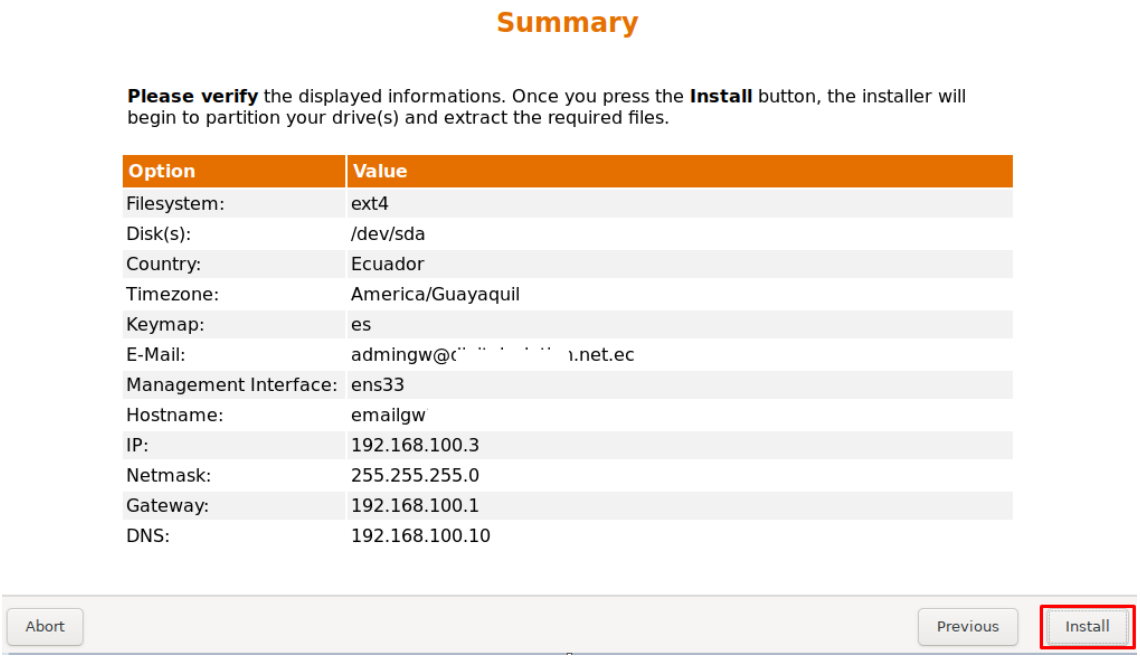
5.- Asignar una contraseña para el usuario administrador (root) y su correo electrónico.



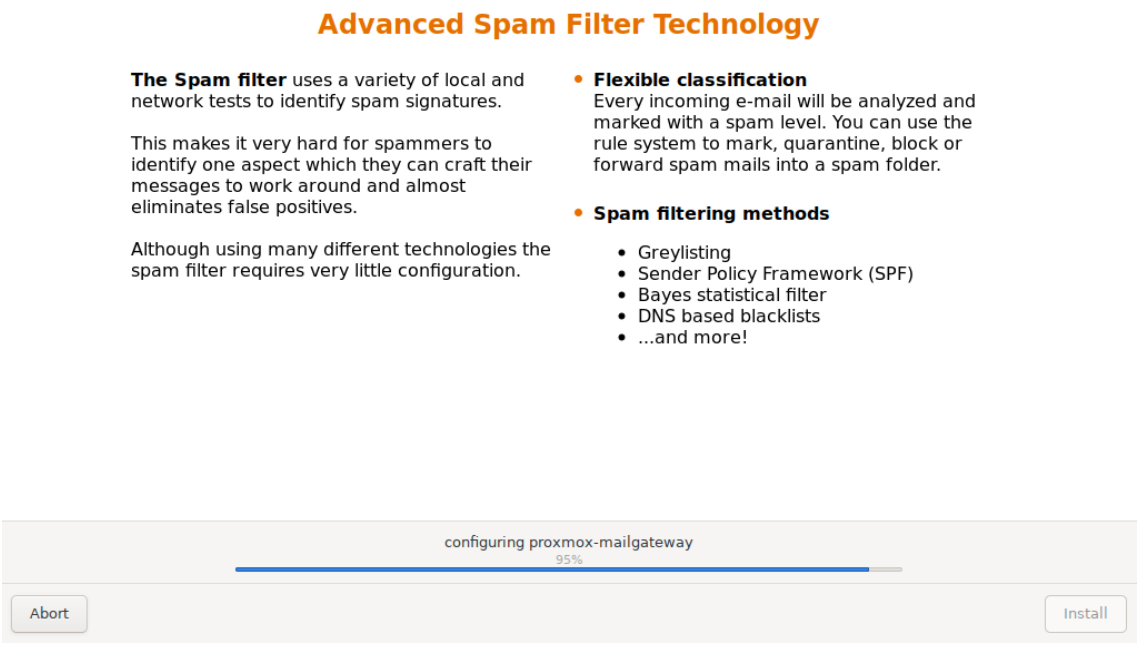
6.- Realizar la configuración de red



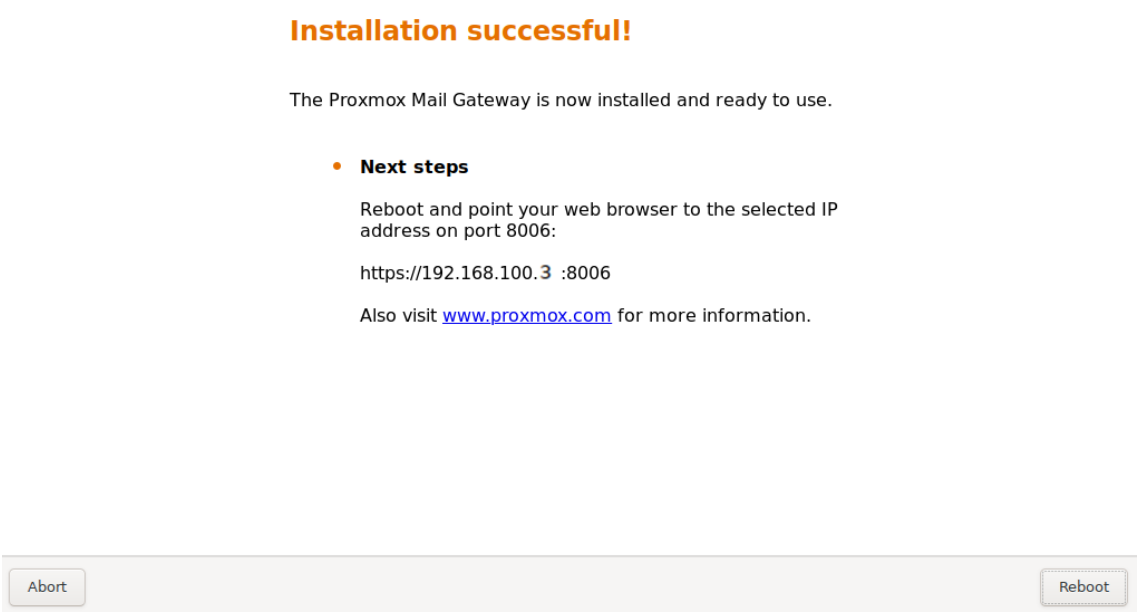
7.- Finalmente muestra un resumen con la configuración realizada.



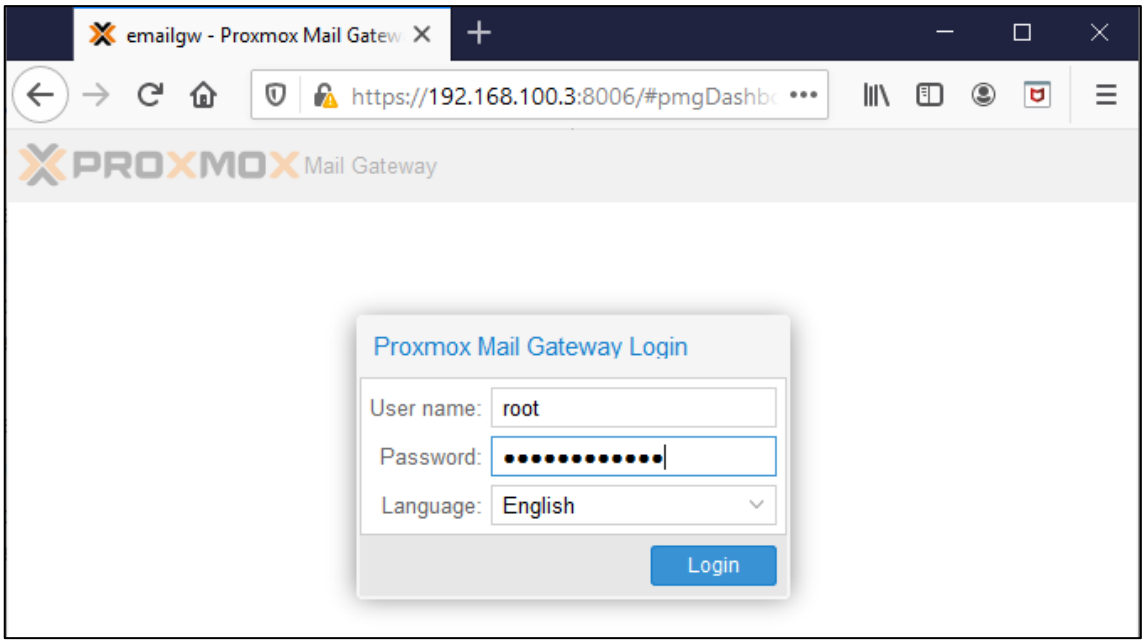
8.- Iniciar el proceso de instalación

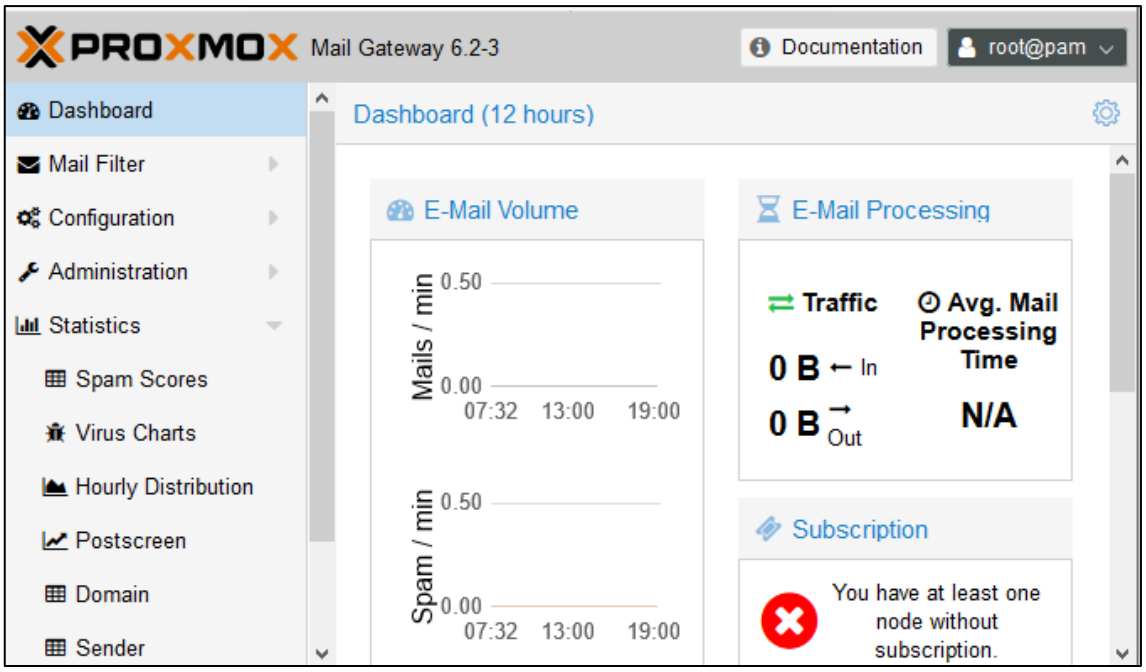


9.- Finalizada la instalación, reiniciar el equipo



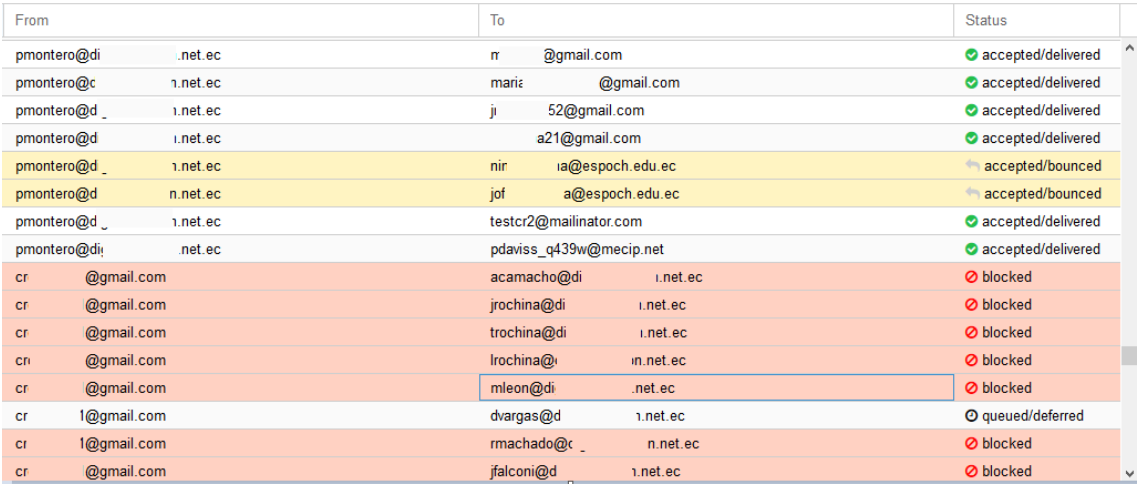
10.- Ingresar mediante navegador web a la consola de administración




PROXMOX Mail Gateway 6.2-3
Documentation
root@pam
Dashboard
Mail Filter
Configuration
Administration
Statistics
Spam Scores
Virus Charts
Hourly Distribution
Postscreen
Domain
Sender
Dashboard (12 hours)
E-Mail Volume
Mails / min
0.50
0.00
07:32
13:00
19:00
Spam / min
0.50
0.00
07:32
13:00
19:00
E-Mail Processing
Traffic
0 B ← In
0 B → Out
Avg. Mail Processing Time
N/A
Subscription
You have at least one node without subscription.

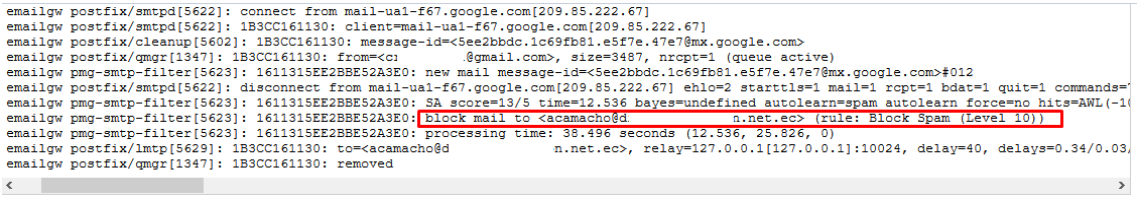
ANEXO B. SEGUIMIENTO DE DETECCIÓN DE CORREOS MALICIOSO EN EL GATEWAY DEL ESCENARIO DE PRUEBAS

A continuación se puede observar el seguimiento de mensajes bloqueados, exportados a cuarenta o aceptados (Retransmitidos a su destino) por el Gateway.



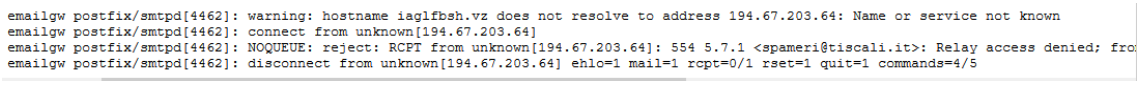
From	To	Status
pmontero@di .net.ec	n @gmail.com	accepted/delivered
pmontero@c n.net.ec	maria @gmail.com	accepted/delivered
pmontero@d n.net.ec	j 52@gmail.com	accepted/delivered
pmontero@d n.net.ec	a21@gmail.com	accepted/delivered
pmontero@d n.net.ec	nir ia@espoch.edu.ec	accepted/bounced
pmontero@d n.net.ec	jof a@espoch.edu.ec	accepted/bounced
pmontero@d n.net.ec	testcr2@mailinator.com	accepted/delivered
pmontero@di .net.ec	pdaviss_q439w@mecip.net	accepted/delivered
cr @gmail.com	acamacho@di n.net.ec	blocked
cr @gmail.com	jrochina@di n.net.ec	blocked
cr @gmail.com	trochina@di n.net.ec	blocked
cr @gmail.com	lrochina@ n.net.ec	blocked
cr @gmail.com	mleon@di .net.ec	blocked
cr 1@gmail.com	dvargas@d n.net.ec	queued/deferred
cr 1@gmail.com	rmachado@ n.net.ec	blocked
cr @gmail.com	jfalconi@d n.net.ec	blocked

En la siguiente grafica se puede observar la regla que bloqueó un determinado correo electrónico.

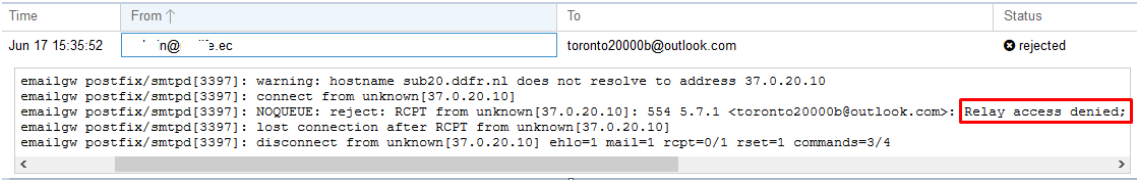


```
emailgw postfix/smtpd[5622]: connect from mail-ua1-f67.google.com[209.85.222.67]
emailgw postfix/smtpd[5622]: 1B3CC161130: client=mail-ua1-f67.google.com[209.85.222.67]
emailgw postfix/cleanup[5602]: 1B3CC161130: message-id=<5ee2bbdc.1c69fb81.e5f7e.47e7@mx.google.com>
emailgw postfix/qmgr[1347]: 1B3CC161130: from=<cr @gmail.com>, size=3487, nrcpt=1 (queue active)
emailgw pmg-smtp-filter[5623]: 1611315EE2BBE52A3E0: new mail message-id=<5ee2bbdc.1c69fb81.e5f7e.47e7@mx.google.com>#012
emailgw postfix/smtpd[5622]: disconnect from mail-ua1-f67.google.com[209.85.222.67] ehlo=2 starttls=1 mail=1 rcpt=1 bdat=1 quit=1 commands=
emailgw pmg-smtp-filter[5623]: 1611315EE2BBE52A3E0: SA score=13/5 time=12.536 bayes=undefined autolearn=spam autolearn_force=no hits=AWL(-1
emailgw pmg-smtp-filter[5623]: 1611315EE2BBE52A3E0: block mail to <acamacho@d n.net.ec> (rule: Block Spam (Level 10))
emailgw pmg-smtp-filter[5623]: 1611315EE2BBE52A3E0: processing time: 38.496 seconds (12.536, 25.826, 0)
emailgw postfix/lmtp[5629]: 1B3CC161130: to=<acamacho@d n.net.ec>, relay=127.0.0.1[127.0.0.1]:10024, delay=40, delays=0.34/0.03
emailgw postfix/qmgr[1347]: 1B3CC161130: removed
```

En las siguientes graficas se puede observar que el Gateway Deniega la retransmisión de correo electrónico suplantado.



```
emailgw postfix/smtpd[4462]: warning: hostname iaglfbsh.vz does not resolve to address 194.67.203.64: Name or service not known
emailgw postfix/smtpd[4462]: connect from unknown[194.67.203.64]
emailgw postfix/smtpd[4462]: NOQUEUE: reject: RCPT from unknown[194.67.203.64]: 554 5.7.1 <spameri@tiscali.it>: Relay access denied; fro
emailgw postfix/smtpd[4462]: disconnect from unknown[194.67.203.64] ehlo=1 mail=1 rcpt=0/1 rset=1 quit=1 commands=4/5
```



Time	From	To	Status
Jun 17 15:35:52	n@ e.ec	toronto20000b@outlook.com	rejected

```
emailgw postfix/smtpd[3397]: warning: hostname sub20.ddfr.nl does not resolve to address 37.0.20.10
emailgw postfix/smtpd[3397]: connect from unknown[37.0.20.10]
emailgw postfix/smtpd[3397]: NOQUEUE: reject: RCPT from unknown[37.0.20.10]: 554 5.7.1 <toronto20000b@outlook.com>: Relay access denied;
emailgw postfix/smtpd[3397]: lost connection after RCPT from unknown[37.0.20.10]
emailgw postfix/smtpd[3397]: disconnect from unknown[37.0.20.10] ehlo=1 mail=1 rcpt=0/1 rset=1 commands=3/4
```

Todas las peticiones SMTP al servidor de correo electrónico, quedaran registradas en el Gateway, ya que el Gateway afrontando hacia el internet.

Registro MX del dominio.

```
root@emailgw:~# dig mx d[redacted].net.ec

; <<>> DiG 9.11.5-P4-5.1+deb10u1-Debian <<>> mx d[redacted].net.ec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62720
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;[redacted].net.ec.                IN      MX

;; ANSWER SECTION:
d[redacted].net.ec. 14325   IN      MX      10 email.[redacted].net.ec.

;; Query time: 33 msec
;; SERVER: 192.168.100.1#53(192.168.100.1)
;; WHEN: Thu Jun 18 20:37:05 -05 2020
;; MSG SIZE  rcvd: 73

root@emailgw:~# dig email.d[redacted].net.ec

; <<>> DiG 9.11.5-P4-5.1+deb10u1-Debian <<>> email.[redacted].net.ec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 138
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;email.[redacted].net.ec.  IN      A

;; ANSWER SECTION:
email.d[redacted].net.ec. 7847 IN   A       186.[redacted]32

;; Query time: 20 msec
;; SERVER: 192.168.100.1#53(192.168.100.1)
```

ANEXO C. TABLA DE DISTRIBUCIÓN DE CHI CUADRADO UTILIZADO PARA LA DEMOSTRACIÓN DE LA HIPÓTESIS

n	*0,995*	*0,99*	*0,975*	*0,95*	*0,9*	*0,75*	*0,5*	*0,25*	*0,05*	*0,025*	*0,01*	*0,005*
1	7,879	6,635	5,024	3,841	2,706	1,323	0,455	0,102	0,004	0,001	0,000	0,000
2	10,597	9,210	7,378	5,991	4,605	2,773	1,386	0,575	0,103	0,051	0,020	0,010
3	12,838	11,345	9,348	7,815	6,251	4,108	2,366	1,213	0,352	0,216	0,115	0,072
4	14,860	13,277	11,143	9,488	7,779	5,385	3,357	1,923	0,711	0,484	0,297	0,207
5	16,750	15,086	12,833	11,070	9,236	6,626	4,351	2,675	1,145	0,831	0,554	0,412
6	18,548	16,812	14,449	12,592	10,645	7,841	5,348	3,455	1,635	1,237	0,872	0,676
7	20,278	18,475	16,013	14,067	12,017	9,037	6,346	4,255	2,167	1,690	1,239	0,989
8	21,955	20,090	17,535	15,507	13,362	10,219	7,344	5,071	2,733	2,180	1,646	1,344
9	23,589	21,666	19,023	16,919	14,684	11,389	8,343	5,899	3,325	2,700	2,088	1,735
10	25,188	23,209	20,483	18,307	15,987	12,549	9,342	6,737	3,940	3,247	2,558	2,156
11	26,757	24,725	21,920	19,675	17,275	13,701	10,341	7,584	4,575	3,816	3,053	2,603
12	28,300	26,217	23,337	21,026	18,549	14,845	11,340	8,438	5,226	4,404	3,571	3,074

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE

UNIDAD DE PROCESOS TÉCNICOS Y ANÁLISIS BIBLIOGRÁFICO Y DOCUMENTAL

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: *06/05/2021*

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: César Gonzalo Rochina Rochina
INFORMACIÓN INSTITUCIONAL
Instituto de Posgrado y Educación Continua
Título a optar: Magíster en Seguridad Telemática
f. Analista de Biblioteca responsable: Lic. Luis Caminos Vargas Mgs.

LUIS ALBERTO CAMINOS VARGAS

Firmado digitalmente por LUIS ALBERTO CAMINOS VARGAS
Nombre de reconocimiento (DN): c=EC, l=RIOBAMBA, serialNumber=0602766974, cn=LUIS ALBERTO CAMINOS VARGAS
Fecha: 2021.05.06 15:32:06 -05'00'