# SPAM-K: Uma Aplicação SDN para a Definição de Padrões visando a Redução de Falsos na Detecção de SPAMs em Serviços de Correio Eletrônico

**Wesley Silvério Guimarães**


Universidade Federal de Uberlândia
Faculdade de Computação
Programa de Pós-Graduação em Ciência da Computação

Uberlândia
2023

**Wesley Silvério Guimarães**

# SPAM-K: Uma Aplicação SDN para a Definição de Padrões visando a Redução de Falsos na Detecção de SPAMs em Serviços de Correio Eletrônico

Dissertação de mestrado apresentada ao Programa de Pós-graduação da Faculdade de Computação da Universidade Federal de Uberlândia como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação.

Área de concentração: Ciência da Computação

Orientador: Prof. Ph.D. Pedro Frosi Rosa

Uberlândia
2023

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

G963 Guimarães, Wesley Silvério, 1976-
2023 SPAM-K: Uma Aplicação SDN para a Definição de Padrões visando a Redução de Falsos na Detecção de SPAMs em Serviços de Correio Eletrônico [recurso eletrônico] / Wesley Silvério Guimarães. - 2023.

Orientador: Prof. Ph.D. Pedro Frosi Rosa.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Ciência da Computação.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2023.462
Inclui bibliografia.

1. Computação. I. Rosa, Prof. Ph.D. Pedro Frosi ,1959-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Ciência da Computação. III. Título.

CDU: 681.3

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:
Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

**UNIVERSIDADE FEDERAL DE UBERLÂNDIA**
Coordenação do Programa de Pós-Graduação em Ciência da Computação
Av. João Naves de Ávila, 2121, Bloco 1A, Sala 243 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4470 - www.ppgco.facom.ufu.br - cpgfacom@ufu.br

# ATA DE DEFESA - PÓS-GRADUAÇÃO

| | | | | | |
|---|---|---|---|---|---|
| Programa de Pós-Graduação em: | Ciência da Computação | | | | |
| Defesa de: | Dissertação de Mestrado 12/2023, PPGCO | | | | |
| Data: | 14 de julho de 2023 | Hora de início: | 15:08 | Hora de encerramento: | 17:18 |
| Matrícula do Discente: | 12012CCP012 | | | | |
| Nome do Discente: | Wesley Silvério Guimarães | | | | |
| Título do Trabalho: | SPAM-K: Uma Aplicação SDN para a Definição de Padrões visando a Redução de Falsos na Detecção de SPAMs em Serviços de Correio Eletrônico | | | | |
| Área de concentração: | Ciência da Computação | | | | |
| Linha de pesquisa: | Sistemas de Computação | | | | |
| Projeto de Pesquisa de vinculação: | - | | | | |

Reuniu-se na Sala 1B230, Bloco 1B, Campus Santa Mônica, da Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Ciência da Computação, assim composta: Professores Doutores: João Henrique de Souza Pereira - FACOM/UFU, Sérgio Takeo Kofuji - EP/USP e Pedro Frosi Rosa - FACOM/UFU, orientador do candidato.

Iniciando os trabalhos, o presidente da mesa, Prof. Dr. Pedro Frosi Rosa, apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao Discente a palavra para a exposição do seu trabalho. A duração da apresentação do Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

A seguir o senhor presidente concedeu a palavra, pela ordem sucessivamente, aos examinadores, que passaram a arguir o candidato. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o candidato:

**Aprovado**

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Pedro Frosi Rosa**, **Professor(a) do Magistério Superior**, em 17/07/2023, às 12:06, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **João Henrique de Souza Pereira**, **Professor(a) do Magistério Superior**, em 17/07/2023, às 20:48, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **SERGIO TAKEO KOFUJI**, **Usuário Externo**, em 24/07/2023, às 14:00, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4649907** e o código CRC **A82AA638**.

**Referência:** Processo nº 23117.049795/2023-47 SEI nº 4649907

*Este trabalho é dedicado às crianças adultas que,*
*quando pequenas, sonharam em se tornar cientistas.*

# Agradecimentos

Hoje é um dia de grande alegria e gratidão em minha jornada acadêmica, pois finalmente concluo minha dissertação de mestrado em Ciências da Computação. Gostaria de aproveitar este momento para expressar minha sincera gratidão a todas as pessoas que estiveram ao meu lado e contribuíram para o sucesso desta conquista.

Primeiramente, gostaria de agradecer a Deus por Sua orientação, força e bênçãos durante todo o percurso desta pesquisa. Sem Sua presença constante e Sua sabedoria divina, eu não teria conseguido enfrentar os desafios, superar obstáculos e chegar até aqui. Sou profundamente grato por Sua graça e amor incondicional.

Também quero prestar uma homenagem especial à memória de minha querida avó, que infelizmente não está mais fisicamente entre nós. Ela sempre foi uma fonte inesgotável de amor, sabedoria e apoio. Lembro-me com carinho dos momentos em que ela me incentivava a buscar meus sonhos e seguir meus estudos força e coragem. Tenho certeza de que ela estaria orgulhosa desta grande realização e sei que seu espírito continua a me inspirar e a me guiar em minha jornada acadêmica e além.

Gostaria de expressar minha profunda gratidão ao meu orientador, Pedro Frosi Rosa. Sua orientação, conhecimento e dedicação foram fundamentais para o sucesso desta dissertação. Você me guiou com paciência, ofereceu orientações valiosas, incentivou meu crescimento acadêmico dia a dia. Sua expertise e comprometimento foram essenciais para que eu alcançasse este marco em minha carreira, a você professor o meu profundo agradecimento, muito obrigado.

Além disso, gostaria de agradecer a todos os professores e colegas que contribuíram para minha formação acadêmica. Seus ensinamentos, apoio e inspiração moldaram minha jornada e ampliaram meus horizontes. Sou grato por ter tido a oportunidade de aprender com vocês e de compartilhar experiências enriquecedoras ao longo deste período.

Não posso deixar de agradecer minha família e amigos, cujo amor, compreensão e apoio incondicionais foram essenciais durante essa caminhada. Obrigado por acreditarem em mim, por me incentivarem quando eu mais precisava e por celebrarem cada pequena vitória ao meu lado. Sua presença fez toda a diferença em minha jornada e sou grato por

tê-los ao meu lado.

Por fim, agradeço a todos que, de alguma forma, contribuíram para minha jornada acadêmica e me ajudaram a chegar até aqui. Sei que esta conquista não seria possível sem o apoio, encorajamento e colaboração de cada um de vocês.

Que este momento de gratidão seja apenas o início de uma trajetória repleta de realizações, aprendizados e contribuições para a área da Ciência da Computação. Que eu possa utilizar o conhecimento adquirido para fazer a diferença em minha profissão, para ajudar a resolver desafios complexos e para.

*"Acredito que um dia Deus permitirá que vençamos a morte através da computação, onde será possível transplantarmos a nossa consiência para um corpo sintético."*

*(Wesley Silvério)*

# Resumo

Desde a década de 2010, as redes de computadores foram transformadas pela inserção do Plano de Controle definido pela filosofia SDN. Com a criação do ONF, fabricantes de elementos de rede passaram a utilizar o protocolo OpenFlow em seus equipamentos para interfacear com o plano de controle. Se a adoção foi massiva em equipamentos de infraestrutura, com NFV (*Network Functions Virtualization*), chegando elementos na borda da rede, tais como firewalls, o mesmo não aconteceu com as aplicações. Esta dissertação tem como objetivo desenvolver o SPAM-K, uma aplicação da camada de controle SDN/NFV, para controlar agentes de um sistema de correio eletrônico, para introduzir a capacidade de identificar com precisão mensagens indevidas, como SPAMs. A pesquisa envolveu a análise de filtros anti-spam de diferentes MTAs ao redor do mundo, considerando diversos fatores como eficiência, segurança e flexibilidade. A SPAM-K apresenta um plano de controle destinado a padronizar as implementações do protocolo de autenticação e configurações importantes para garantir a autenticidade do remetente. Os resultados mostram que a SPAM-K pode melhorar significativamente a eficiência e a segurança dos servidores de e-mail. Conclui-se que a aplicação desenvolvida pode atender a necessidades de usuários, incluindo empresas, governos e indivíduos, garantindo a entrega rápida e segura de mensagens autênticas nas caixas de entrada, evitando assim perdas de tempo e financeiras.

**Palavras-chave:** ONF, SDN, NFV, Control Plane, SMTP, SPAM, DMARC, SPF.

# Abstract

Since the 2010s, computer networks have been transformed by the insertion of the Control Plane defined by the SDN philosophy. With the creation of ONF, network element manufacturers started to use the OpenFlow protocol in their equipment to interface with the control plane. If adoption was massive in infrastructure equipment, with Network Functions Virtualization (NFV) reaching border elements, such as firewalls, the same did not happen with applications. This dissertation aims to develop SPAM-K, an application of the SDN/NFV control layer, to control agents of an MHS system, i.e. electronic mail, to introduce the ability to accurately identify undue messages, such as SPAMs. The research involved analyzing anti-spam filters from different MTAs around the world, considering various factors such as efficiency, security and flexibility. SPAM-K introduces a control plane aimed at standardizing authentication protocol implementations and important settings to ensure the sender is authentic. The results show that SPAM-K can significantly improve the efficiency and security of email servers. It is concluded that this project can meet the needs of users, including companies, governments and individuals, ensuring fast and secure delivery of authentic messages in inboxes, thus avoiding time and financial losses.

**Keywords:** ONF, SDN, NFV, Control Plane, SMTP, SPAM, DMARC, SPF.

# Lista de ilustrações

# Lista de tabelas

# Lista de siglas

**ANN** *Artificial Neural Networks*

**CNN** *Convolutional Neural Network*

**DKIM** *Domain Keys Identified Mail*

**DL** *Deep Learning*

**DMARC** *Domain-based Message Authentication, Reporting & Conformance*

**EBI** *East Bound Interface*

**EFOA** *Enriched Firefly Optimization Algorithm*

**ETSI** *European Telecommunications Standards Institute*

**FQDN** *Fully Qualified Domain Name*

**HTTP** *Hyper Text Transfer Protocol*

**IM** *Instant Message*

**ISP** *Internet Service Provider*

**ITU-T** *International Telecommunication Union - Telecommunication Sector*

**IMAP** *Internet Message Access Protocol*

**JMPR** *Junk Mail Program Report*

**K-MTA** *Kayrós* MTA - implementado para o projeto SPAM-K

**K-NN** *K-Nearest Neighbors*

**MANO** *Management and Orchestration*

**MCS** *Multiple Classifier Systems*

**MDA** *Message Delivery Agent*

**ML** *Machine Learning*

**MHS** *Message Handling System*

**MSA** *Message Submission Agent*

**MTA** *Message Transfer Agent*

**MUA** *Message User Agent*

**NFV** *Network Functions Virtualization*

**NFVI** *Network Function Virtualization Infrastructure*

**ONF** *Open Networking Foundation*

**PCA** *Principal Component Analysis*

**PKI** *Public Key Infrastructure*

**POP3** *Post Office Protocol Version 3*

**PV-DM** *Paragraph Vector & Distributed Memory*

**RBL** *Real-time Blackhole List*

**RF** *Random Forests*

**RNN** *Recurrent Neural Network*

**ROI** *Return on Investiment*

**SBI** *South Bound Interface*

**SDN** *Software Defined Networking*

**SMTP** *Simple Mail Transfer Protocol*

**SORBS** *Spam and Open Relay Blocking System*

**SPAM** *Sending and Posting Advertisement in Mass*

**SPAM-K** SPAM-*Killer Controller Application*

**SPF** *Sender Policy Framework*

**SVM** *Support Vector Machine*

**SSH** *Secure Shell*

**VNF** *Virtual Network Function*

**VPS** *Virtual Private Server*

# Sumário

# Capítulo 1

# Introdução

Comunicação é uma necessidade essencial dos seres, em particular dos humanos, que desde tempos imemoriais têm usado os mais diversos meios para se comunicar – fumaça, percussão etc. Com o advento das redes, uma das primeiras aplicações disponibilizadas, para comunicações pessoais e corporativas, se materializou com o correio eletrônico. Em maio de 1977, David H. Crocker (The Rand Corporation), John J. Vittal (Bolt Beranek and Newman Inc.), Kenneth T. Pogran (Massachusets Institute of Technology) e D. Austin Henderson Jr.(Bolt Beranek and Newman Inc.) foram responsáveis pela especificação da RFC 724 (CROCKER et al., 1977), que pode ser considerado o primeiro padrão de correio eletrônico da Internet. Em agosto de 1982, a RFC 822, revisada por Crocker, se tornaria o padrão da ARPA/Internet para mensagens de texto (CROCKER, 1982). Deste momento em diante, foram acrescidos outros formatos de mídias e incluídos aspectos de segurança.

## 1.1 Motivação e Justificativa

O conceito de Redes Definidas por Software (*Software Defined Networking* (SDN)) (HALEPLIDIS et al., 2015), foi introduzido por volta de 2009 (CASADO; MCKEOWN; SHENKER, 2019), com a filosofia de separar aspectos de controle, dos aspectos de dados e, em 2011, foi criada a *Open Networking Foundation* (ONF), um consórcio sem fins lucrativos liderado por operadoras de telecomunicações que usam um modelo de negócios de código aberto projetado para avançar o paradigma SDN e padronizar o protocolo *OpenFlow* e tecnologias relacionadas[1].

A introdução de SDN e a criação da ONF provocaram movimentos significativos na indústria e na academia, sendo que, em outubro de 2012, um grupo de operadoras de telecomunicações europeias, membros da *European Telecommunications Standards Institute* (ETSI), e operadoras de outros continentes, publicaram um *white paper* em uma conferência em *Darmstadt* sobre SDN e *OpenFlow*.

[1] https://opennetworking.org/

Esse movimento levou a ETSI a padronizar a arquitetura denominada *Network Functions Virtualization* (NFV), que é composta por três camadas: *Network Function Virtualization Infrastructure* (NFVI); *Virtual Network Function* (VNF); e *Management and Orchestration* (MANO). A ETSI entende que NFV tem o papel de nortear empresas no processo de criação de suas próprias funções virtualizadas de rede.

Nesse sentido, muitos esforços foram envidados e muitos resultados foram alcançados, uma vez que uma série de funções que antes eram desempenhadas por "caixas" (*appliances*), passaram a ser disponibilizadas como funções da redes, tais como Roteadores, *Switches* virtuais, *Firewalls*, *Proxies*, entre outras funções.

Entretanto, é possível observar que todos esses esforços foram direcionados para a infraestrutura da rede, que passou a ser gerida pelo Plano de Controle introduzido pela arquitetura NFV, todavia, até onde nossas pesquisas nos mostraram, diversas aplicações transversais, continuam sendo disponibilizadas como antes, sem a gestão de um plano de controle, como é o caso de Correios Eletrônicos.

Embora Correios Eletrônicos[2] sejam um tipo de ferramenta, para troca de mensagens interpessoais ou corporativas, utilizado há décadas, levantamentos do Gartner Group mostram que essas ferramentas são, neste momento presente, muito utilizadas em diversos cenários, e Rahmad, Suryanto e Ramli (2020) reforçam a importância do correio eletrônico na atualidade.

A despeito de tecnologias de *Instant Message* (IM), tais como Discord, Telegram, Whatsapp e Signal, que são muito utililzadas atualmente, de acordo com o *Gartner Group*, sistemas de correios eletrônicos (denominado pela *International Telecommunication Union - Telecommunication Sector* (ITU-T) como *Message Handling System* (MHS)) são utilizados massivamente por corporações. Todavia, alguns problemas permanecem atuais, como é o caso de mensagens indevidas ou não autorizadas.

Os MHS são constituídos de agentes com funções bem definidas sendo: *Message User Agent* (MUA) - agente que desempenha o papel do cliente, oferecendo a interface para usuários finais; *Message Transfer Agent* (MTA) - agente que desempenha o papel de encaminhamento de mensagens[3]; *Message Delivery Agent* (MDA) - agente especializado em entrega de mensagens[4]; e *Message Submission Agent* (MSA) - agente especializado em submissão de mensagens com requisitos de segurança[5].

Um MTA (ou MSA) é a parte de um MHS que oferece a função de receber e transferir mensagens de correio eletrônico (Envelope[6]) para outros MTAs, até que o envelope chegue

[2] Correios eletrônicos tais como: Internet Mail (*Simple Mail Transfer Protocol* (SMTP)), Microsoft Outlook, IBM Domino, IBM Mailtoo, entre outros.

[3] MTA também é referido como servidor de e-mail no universo do Internet Mail (SMTP)

[4] No contexto Internet Mail, MDA é comumente referenciado como Servidor *Post Office Protocol Version 3* (POP3) (ROSE; MYERS, 1996) ou *Internet Message Access Protocol* (IMAP) (CRISPIN, 2003)

[5] Introduzido para submissão de mensagens pela RFC 2476 (GELLENS; KLENSIN, 1998) para suportar novos requisitos de segurança usando a porta 587

[6] Envelope é o nome da primitiva de correios eletrônicos

ao MDA relativo ao MUA de destino. Em função da larga adoção na Internet, o Protocolo SMTP (KLENSIN, 2008), foi escolhido no escopo desta dissertação (KUROSE; ROSS, 2020), (PETERSON; DAVIE, 2021), (TANENBAUM; WETHERALL, 2019), (FOROUZAN, 2018), (STALLINGS, 2019).

Um dos maiores problemas envolvendo correios eletrônicos são mensagens recebidas, mas que foram enviadas sem a solicitação ou anuência do destinatário, comumente denominadas *Sending and Posting Advertisement in Mass* (SPAM). Embora haja vários protocolos, presentes em diversas tecnologias, temos que o SMTP, se tornou o padrão de fato, mesmo no universo corporativo, em função de sua adoção na Internet.

Quando um usuário envia uma nova mensagem, ao chegar ao MTA de destino, responsável pelas mensagens do usuário destinatário, a mensagem poderá seguir um de dois caminhos: (i) Caixa de Entrada; ou (ii) Lixo Eletrônico (se for caracterizada como SPAM), sendo (i) o esperado para mensagens desejáveis e (ii) para SPAMs.

Todavia, é notório o problema de mensagens (ii) que vão parar na caixa de entrada (denominado de 'Falso Negativo de SPAM'). Isto por si só é um problema, uma vez que a caixa de entrada fica poluída com mensagens não solicitadas ou indesejáveis. O problema é ainda mais grave, podendo causar prejuízos importantes, quando mensagens (i) são classificadas como (ii). Este último problema recebe a denominação de 'Falso Positivo de SPAM'.

Existe uma indústria de fornecedores de ferramentas anti-SPAM, sendo que a eficácia de tais ferramentas têm sido cada vez menores, em função do aumento e da estratégia de envio de produtores de SPAMs, sabedores das deficiências das plataformas de correios eletrônicos disponíveis atualmente. O fato é que tais ferramentas são cada vez mais caras e menos eficientes.

## 1.2 Objetivos e Desafios da Pesquisa

O projeto tem como objetivo desenvolver uma especificação para ser utilizada na implementação de servidores de e-mail eficientes, que possam endereçar com mais precisão mensagens para as caixas de entrada relacionadas aos mais variados MTAs em todo o mundo. Esses servidores devem ser capazes de diferenciar mensagens autênticas de mensagens SPAMs, minimizando assim os Falsos Positivos.

Com a grande quantidade de MTAs espalhados pelo mundo, cada um com seus próprios filtros antispam, essa pesquisa científica se torna ainda mais complexa, visto que é necessário analisar os filtros antispam individualmente e desenvolver um padrão que possa ser aplicado a todos eles.

Uma das principais preocupações do projeto é evitar os Falsos Positivos, ou seja, mensagens legítimas que são erroneamente marcadas como SPAMs e, portanto, não são entregues às caixas de entrada dos destinatários. Isso pode causar muitos problemas,

como a perda de comunicações importantes e até mesmo a perda de negócios, como já mencionado.

Para resolver esse problema, é preciso desenvolver um padrão que permita que os servidores de e-mail identifiquem com precisão as mensagens autênticas e as separem das mensagens de SPAM. Isso envolve a análise de diversos fatores, tais como o remetente da mensagem, o conteúdo, a linguagem utilizada, entre outros.

Além disso, é importante garantir que servidores de e-mail sejam eficientes na entrega de mensagens, para que elas cheguem rapidamente às caixas de entrada dos destinatários. Para isso, é necessário considerar vários fatores, como a capacidade de processamento do servidor, a largura de banda da conexão à Internet e a velocidade de resposta do MTA.

Outro aspecto importante a ser considerado é a segurança das mensagens. Os servidores de e-mail devem ser capazes de detectar e bloquear mensagens maliciosas, como vírus e *phishing*, para garantir a proteção de usuários.

Ao desenvolver um padrão para a implementação de servidores de e-mail eficientes, é importante considerar as necessidades de todos os usuários, incluindo empresas, governos e indivíduos. O padrão deve ser flexível e adaptável às diferentes necessidades e requisitos de cada um desses grupos.

Em resumo, o objetivo do projeto é desenvolver um padrão que permita a implementação de servidores de e-mail eficientes e seguros, capazes de identificar com precisão mensagens autênticas e separá-las das mensagens de SPAM, minimizando os Falsos Positivos. Para isso, é necessário analisar os filtros antispam de diferentes MTAs em todo o mundo, considerar vários fatores, como eficiência, segurança e flexibilidade, e desenvolver um padrão que atenda às necessidades de todos os usuários.

### 1.2.1 Objetivo Geral

O objetivo geral desta dissertação é desenvolver uma aplicação do plano de controle, numa filosofia baseada em SDN, capaz de se comunicar com agentes de MHSs, para envio de mensagens de gestão de especificações antiSPAMs.

### 1.2.2 Objetivos Específicos

O estudo envolve uma série de objetivos específicos, delineados de forma sistemática, com o propósito de abordar questões críticas no cenário atual da comunicação entre os agentes de MHS. Estes objetivos são:

- **Analisar Comportamento de Agentes MHS:** O primeiro passo desta pesquisa é realizar uma análise detalhada do comportamento dos Agentes MHS, a fim de compreender seu funcionamento, suas vulnerabilidades e sua eficácia na prevenção de mensagens indesejadas (SPAM).

- ❑ **Analisar Parâmetros Relativos a SPAMs:** É crucial examinar os parâmetros e as métricas relacionadas ao fenômeno do SPAM, identificando padrões e tendências que possam servir como base para estratégias de mitigação.

- ❑ **Desenvolver um Padrão de Representação de Parâmetros Anti-SPAM:** Com base na análise anterior, será proposto o desenvolvimento de um padrão de representação de parâmetros anti-SPAM, visando facilitar a identificação e o combate a mensagens indesejadas.

- ❑ **Desenvolver uma Aplicação SDN para Comunicação com Agentes MHS:** A utilização de Redes Definidas por Software (SDN) será explorada para a criação de uma aplicação que permita uma comunicação eficiente e segura com os Agentes MHS.

- ❑ **Fazer Levantamento de MHS Representativos na Internet:** Um levantamento minucioso será conduzido para identificar e selecionar Agentes MHS representativos na Internet, que servirão como alvo das análises e dos testes subsequentes.

- ❑ **Elaborar Planos de Testes de Envio de Mensagens:** Serão desenvolvidos planos de testes que abrangem diferentes cenários e estratégias de envio de mensagens, com o intuito de avaliar a capacidade de resposta e a eficácia dos Agentes MHS.

- ❑ **Executar Planos de Testes nos MHS:** Os planos de testes elaborados serão implementados nos Agentes MHS selecionados, permitindo a coleta de dados empíricos que servirão como base para a análise subsequente.

- ❑ **Analisar os Dados Obtidos:** Os dados obtidos a partir dos testes serão submetidos a análises estatísticas e técnicas, visando identificar tendências, vulnerabilidades e oportunidades de melhoria nos Agentes MHS.

- ❑ **Realizar Implementação de Provisionamento em Laboratório:** Será desenvolvida uma implementação em ambiente laboratorial, visando a simulação e a validação das estratégias de provisionamento anti-SPAM.

- ❑ **Criar uma Aplicação Capaz de Orquestrar os Pré-Requisitos Autenticativos Anti-SPAM em MHS:** Uma aplicação será criada para orquestrar e gerenciar os pré-requisitos autenticativos necessários para o combate ao SPAM nos Agentes MHS.

- ❑ **Mitigar a Existência de Falsos Positivos nos Agentes MHS:** Finalmente, o objetivo é aprimorar a eficácia dos Agentes MHS na identificação de SPAM, reduzindo ao máximo a ocorrência de falsos positivos.

Ao abordar esses objetivos específicos, esta dissertação almeja efetuar uma contribuição substancial no sentido de mitigar a existência dos falsos, além de desempenhar um papel edificante na comunidade acadêmica, fomentando um estímulo para que esta prossiga com suas investigações de maneira contínua e persistente.

## 1.3 Hipótese

A compreensão do comportamento dos filtros antispam dos principais MTAs do mundo, como Microsoft, Google e Yahoo, é de extrema importância para definir padrões de configuração dentro de servidores de envio de e-mail. Esses padrões são necessários para atender às exigências dos receptores e garantir que as mensagens autênticas não sejam marcadas como SPAMs.

A hipótese deste trabalho é que a especificação de um padrão para a implementação de servidores eficazes de e-mail é fundamental para minimizar os prejuízos devidos a mensagens legítimas serem identificadas como SPAMs. Esse padrão seria gerido por uma aplicação do plano de controle logicamente centralizado.

Com a especificação de um padrão, os receptores poderão entender que não se trata de uma mensagem indevida, mas sim de uma mensagem autêntica, minimizando a identificação equivocada de mensagens como SPAMs. É importante ressaltar que a implementação desses padrões deve ser realizada de forma cuidadosa e responsável, levando-se em consideração a segurança e a privacidade dos usuários.

## 1.4 Contribuições

A comunicação por meio de ferramentas de e-mail é uma das formas mais utilizadas e importantes de comunicação corporativa, conforme o relatório do Gartner Group. Diante disso, a contribuição principal deste trabalho é oferecer um padrão para usuários de ferramentas de e-mail trocarem mensagens mais eficazmente e com menor probabilidade de perda de mensagens autênticas.

O padrão proposto visa diminuir prejuízos causados pela identificação equivocada de mensagens como SPAMs e, além disso, o padrão pode incluir a troca de anexos de forma segura e eficiente, garantindo que esses anexos sejam entregues corretamente e sem perda de informações.

A implementação do padrão proposto pode ser benéfica não apenas para empresas, mas também para governos e indivíduos que dependam do e-mail como ferramenta de comunicação. Com a SPAM-*Killer Controller Application* (SPAM-K), os usuários podem se comunicar de forma mais eficaz e segura, aumentando a produtividade e minimizando os riscos de perda de informações importantes.

## 1.5 Estrutura da Dissertação

O Capítulo 2 apresenta o estado da arte em termos de planos de controle baseados na filosofia SDN/NFV e, também, as pesquisas e trabalhos correlatos em torno de anti-SPAM para sistemas MHS. O Capítulo 3 apresenta a proposta de arquitetura de uma aplicação, a SPAM-K, para a camada de aplicação do plano de controle. O Capítulo 4 apresenta o ambiente requerido para implantação, bem como a implementação de um agente MTA de referência para o ambiente de testes. O Capítulo 5 apresenta os resultados obtidos bem como uma análise comparativa. O Capítulo 6 apresenta as conclusões finais, bem como possibilidades de trabalhos futuros. O Anexo A apresenta listas de endereços de emails criados em diversos provedores de email de âmbito mundial.

Capítulo 2

# MHS e anti-SPAM: Estado da Arte

Centros de pesquisas e organizações têm feito grandes investimentos no desenvolvimento de soluções anti-SPAM, bem como, há um esforço significativo para a implantação de tais soluções nos diversos segmentos de negócios. Este capítulo tem o objetivo de apresentar o estado da arte em iniciativas para eliminar ou mitigar mensagens do tipo SPAM e com esta finalidade, a Seção 2.1 apresenta a fundamentação teórica, a Seção 2.2 analisa os principais trabalhos correlatos e a Seção 2.3 apresenta boas práticas na configuração de ambientes MHSs.

## 2.1 Fundamentação Teórica

Como exposto na Seção 1.1 (Motivação e Justificativa), tem-se envidado muitos esforços para o desacoplamento do Plano de Controle da infraestrutura da rede (CASADO; MCKEOWN; SHENKER, 2019) e isto se materializou com a especificação da arquitetura NFV pela ETSI, em particular, com a camada NFV/MANO (**??**). Para plataformas de Correio Eletrônico, não foi possível encontrar iniciativas, até onde nossas pesquisas nos levaram, sendo deste modo o fulcro desta seção.

Zhang e Hu (2020) discorrem sobre um método de controle inteligente para sistemas de filtragem de e-mails, propondo um modelo que utiliza técnicas de aprendizado de máquina (*Machine Learning* (ML)) e mineração de dados (*data mining*) para aprimorar a eficiência da filtragem de e-mails. O método proposto consiste em um sistema de controle inteligente que utiliza técnicas de aprendizado profundo para identificar SPAM com maior precisão.

Os autores também apresentam uma análise comparativa entre sua proposta e outras abordagens existentes na literatura. Eles avaliam a eficácia do modelo aplicado a um conjunto de dados de e-mails de SPAM e mostram que seu método supera outras técnicas em termos de eficiência e precisão na identificação de SPAM.

Além disso, o artigo discute os desafios e tendências futuras na pesquisa de sistemas de filtragem de e-mails. Os autores destacam a importância de abordagens de controle

inteligente para sistemas de filtragem de e-mails e suas implicações na mitigação dos problemas de falsos positivos e falsos negativos na identificação de e-mails de SPAM.

Gupta e Gupta (2019) fazem uma revisão abrangente das técnicas utilizadas para filtragem de e-mails de SPAM. Os autores abordam diversos aspectos relevantes nesse contexto, tais como a definição do problema de filtragem de e-mails de SPAM, suas implicações e desafios, e as principais técnicas utilizadas para sua solução.

Os autores discutem os métodos baseados em listas negras - em que e-mails são filtrados com base em listas de remetentes conhecidos de SPAM, e os métodos baseados em listas brancas - em que apenas e-mails de remetentes conhecidos são permitidos. Além disso, são discutidos também métodos mais sofisticados, como a utilização de técnicas de aprendizado de máquina, análise de conteúdo e de características de e-mails.

O artigo destaca ainda a importância da utilização de técnicas de filtragem de e-mails de SPAM para a proteção de usuários de serviços de e-mail e para a prevenção de ameaças cibernéticas. Os autores também destacam a necessidade de desenvolver técnicas cada vez mais sofisticadas e eficazes de filtragem de e-mails de SPAM, dada a crescente sofisticação das técnicas utilizadas por *spammers* para contornar as técnicas de filtragem existentes.

Vannucci e Prosperi (2018) apresentam uma análise detalhada da eficácia do sistema anti-SPAM de código aberto disponível no âmbito do ***Apache SpamAssassin Project***. A análise aponta que SPAM é uma prática indesejável, prejudicial à produtividade, que pode ter implicações na segurança do usuário. Os autores conduziram testes experimentais para avaliar a precisão e a eficiência do sistema, em comparação com outras soluções comerciais de mercado.

Os resultados indicaram que o *SpamAssassin* apresentou desempenho satisfatório na detecção e filtragem de mensagens de SPAM, com uma precisão média superior a 95%. Além disso, o estudo apontou para a importância da configuração adequada do sistema e da atualização frequente das regras de detecção, para manter a eficácia e a relevância do *SpamAssassin*.

Hameed e Khan (2019) analisam várias técnicas de filtragem de SPAM utilizadas por sistemas de e-mail, investigando a eficácia de diferentes métodos, incluindo a filtragem baseada em regras, filtragem bayesiana, filtragem de listas negras e filtragem baseada em aprendizado de máquina. A análise conclui que a combinação de várias técnicas de filtragens é essencial para melhorar a precisão na detecção de SPAM e que a escolha da técnica a ser utilizada deve ser baseada nas necessidades específicas da organização. O artigo oferece *insights* valiosos para pesquisadores e profissionais que buscam melhorar a eficácia de seus sistemas de filtragem de SPAM em e-mails.

Salamon, Vida e Duda (2020) analisam a aplicação de técnicas de aprendizado de máquina para classificação de e-mails de SPAM, em um ambiente de *big data*, e apresentam os desafios envolvidos na identificação de e-mails de SPAM em grandes volumes de dados, bem como uma revisão das técnicas de aprendizado de máquina utilizadas para lidar com

esse problema.

É apresentado um experimento envolvendo as técnicas propostas em um conjunto de dados de e-mails reais e compara os resultados com outras abordagens da literatura. Os resultados obtidos mostram a eficácia das técnicas de aprendizado de máquina propostas na classificação de e-mails de SPAM em um ambiente de *big data*.

Niazi e Bhatti (2019) apresentam o modelo *Support Vector Machine* (SVM) de detecção de SPAM de e-mails baseado em um conjunto de métodos de aprendizado supervisionado usados para classificação, regressão e detecção de *outliers*. A abordagem multiclasse permite classificar e-mails mais precisamente, considerando as diversas categorias de SPAM existentes. O modelo é comparado a outros métodos de filtragem de SPAM, demonstrando desempenho superior em termos de precisão e taxa de falsos positivos.

Wang e Li (2019) apresentam um modelo aprimorado para a detecção de SPAM de e-mails, utilizando uma abordagem baseada no Algoritmo *Naive Bayes*. O modelo proposto é capaz de lidar com diferentes tipos de SPAM, incluindo e-mails com conteúdo malicioso e *phishing*. Além disso, o modelo aprimorado é comparado a outros métodos de filtragem de SPAM, demonstrando desempenho superior em termos de precisão e taxa de falsos positivos.

Oliveira, Santos e Souza (2019) analisam a eficácia de um filtro de SPAM baseado em técnicas de aprendizado de máquina. O estudo comparou diferentes algoritmos de classificação de SPAM, incluindo *Naive Bayes*, SVM e *K-Nearest Neighbors* (K-NN). Os resultados mostram que o algoritmo *Naive Bayes* apresentou melhor desempenho em termos de precisão e sensibilidade, enquanto o K-NN apresentou pior desempenho. O estudo também mostrou que a utilização de técnicas de pré-processamento, como a remoção de *stop words*[1] e a aplicação de *stemming*[2], contribuiu para melhorar a eficácia dos filtros de SPAM.

Brito, Costa e Silva (2021) analisam a eficácia do *SpamAssassin*, baseado em um conjunto de emails classificados como SPAM e não-SPAM. A eficácia da ferramenta é avaliada em termos de sensibilidade, especificidade e acurácia. Os resultados mostram que *SpamAssassin* é eficaz na detecção de SPAM, alcançando altas taxas de sensibilidade e especificidade. No entanto, os autores apontam que ainda existem desafios a serem superados na detecção de SPAM, como o uso de técnicas de *phishing* e engenharia social por *spammers*.

Maia, Santos e Azevedo (2021) realizaram uma análise do desempenho do software Postfix como servidor de email, objetivando avaliar o tempo de resposta do servidor para diferentes cargas de trabalho, bem como identificar os fatores que mais impactam no desempenho. A análise usou uma ferramenta de teste de carga, que enviava mensagens

[1] Em computação, uma palavra vazia (*stop word*) é uma palavra que é removida antes ou após o processamento de um texto em linguagem natural.

[2] Em Morfologia Linguística e Recuperação de Informação, a *stemização* é o processo de reduzir palavras flexionadas ao seu tronco, base ou raiz, geralmente uma forma da palavra escrita.

de email para o servidor em diferentes taxas. Os resultados mostraram que o tempo de resposta aumenta significativamente à medida que a carga de trabalho aumenta, mas que o Postfix apresenta um desempenho satisfatório mesmo para cargas altas. Os autores identificaram que o tamanho das mensagens e o número de destinatários são os principais fatores que influenciam no desempenho do servidor. A pesquisa é relevante para administradores de sistemas e usuários que desejam avaliar o desempenho do Postfix como servidor de email em diferentes cenários.

Campos e Soares (2018) analisam a aplicação de técnicas de aprendizagem de máquina para a classificação de SPAM. Foi utilizado um conjunto de dados de e-mails, previamente classificados como SPAM ou não-SPAM, para treinar um modelo de classificação. Foi avaliada a eficácia do modelo utilizando medidas de precisão, revocação e F1-*score*. O modelo proposto apresentou uma alta taxa de acerto na classificação dos e-mails como SPAM ou não-SPAM.

Ribeiro e Silva (2021) analisam servidores de e-mail hospedados em nuvem, onde é discutida a segurança de servidores de e-mail e como a migração para a nuvem pode afetar essa segurança. Os resultados mostram que, embora haja preocupações de segurança na migração para a nuvem, a maioria dos servidores analisados apresentou níveis satisfatórios de segurança.

Santos, Azevedo e Araújo (2018) apresentam estudo comparativo entre dois servidores de email (Postfix e Sendmail) em termos de desempenho e segurança. Os resultados mostraram que o Postfix apresentou melhor desempenho em termos de taxa de transferência e tempo de resposta, além de apresentar maior segurança em relação a vulnerabilidades conhecidas, concluindo que o Postfix é uma opção mais adequada para ambientes de alta disponibilidade e segurança.

Sousa, Souza e Tavares (2018) analisam o desempenho do Postfix e, para isso, foram realizados testes de carga em um ambiente de laboratório e os resultados foram analisados com base em métricas como tempo de resposta e taxa de transferência. O artigo apresenta uma análise detalhada dos resultados obtidos, sendo um dos motivos para a adoção neste projeto.

Bukhari, Jameel e Naz (2019) apresentam uma abordagem para a detecção de emails de SPAM por meio do uso de técnicas de aprendizado de máquina e mineração de dados. Usando técnicas de mineração de dados, os autores coletaram e pré-processaram um grande conjunto de dados de e-mails e, em seguida, aplicaram uma variedade de algoritmos de aprendizado de máquina para identificar os emails de SPAM, com uma taxa de acerto superior a 90%. Esses resultados indicam que a abordagem proposta pelos autores é promissora para a detecção de SPAM em larga escala.

Hossain, Karim e Rahman (2021) apresentam uma abordagem inovadora para a detecção de emails de SPAM por meio do uso de técnicas de aprendizado de máquina. Os autores propõem uma abordagem híbrida de aprendizado de máquina, que combina téc-

nicas de processamento de linguagem natural e aprendizado de máquina para identificar emails de SPAM com alta precisão. Foi utilizado um conjunto de dados de emails de SPAM e emails legítimos para treinar e testar o modelo de aprendizado de máquina proposto. Os resultados apresentados no artigo indicam que a abordagem híbrida proposta pelos autores supera outras técnicas de detecção de SPAM em termos de precisão e taxa de falsos positivos.

É possível perceber que há muitos esforços, recentes, para mitigar SPAM, e é possível perceber também que várias dessas iniciativas, desempenhadas pelo próprio servidor de email, ou em equipamentos *on premise*, poderiam ser desempenhadas por um plano de controle, como é o caso daquele proposto pela SPAM-K.

## 2.2 Trabalhos Relacionados

Nesta seção são relacionados trabalhos (e até produtos) desenvolvidos com o objetivo de prover a sociedade e a indústria com soluções anti-SPAM. Pode-se observar que universidades, organismos de padronização, indústria e outros entes da sociedade envidaram esforços para a evolução de plataformas de MHS (BIBI et al., 2020). Com esse foco, houve uma evolução importante na redução de 'Falsos Negativos', isto é, diminuiu significativamente a ocorrência de SPAMs em caixas de entradas.

Todavia, há um efeito colateral nesta abordagem, pois 'mensagens esperadas', também passam eventualmente a ser classificadas como SPAMs, e são colocadas em anti-SPAMs ou lixeiras. É comum usuários serem arguidos se verificaram em suas pastas de anti-SPAMs ou lixeiras. Ao invés de selecionar características para criar padrões que validem e-mails autênticos, e os depositem nas caixas de entradas, o foco em regras restritivas fazem o contrário. Posto de outra forma, esta abordagem diminui 'Falsos Negativos', mas aumenta 'Falsos Positivos'.

Dalkılıç e Sipahi (2017) demostram preocupações com falsos positivos, uma vez que frequentemente mensagens legítimas são consideradas SPAMs. Nossas pesquisas demonstram que este fenômeno tem sido pouco explorado, no entanto, muitos trabalhos têm se utilizado de técnicas de autenticação tais como *Sender Policy Framework* (SPF), *Domain-based Message Authentication, Reporting & Conformance* (DMARC), *Domain Keys Identified Mail* (DKIM), DNS Reverso, entre outras. Embora, tais técnicas sejam vistas como obrigatórias, apenas seus empregos não são suficientes e mensagens legítimas continuam sendo consideradas como SPAMs pelos principais provedores de serviço.

Douzi et al. (2020) propõem duas representações baseadas em *Paragraph Vector & Distributed Memory* (PV-DM), que fazem a extração de informações em dois contextos, locais e global, para a captura e compreensão de palavras, realizando assim uma filtragem mais inteligente, envolvendo aprendizado de máquina. Entretanto, o problema não está somente no conteúdo da mensagem e, sim, na má configuração de estruturas presentes

nos MTAs. Por este motivo, por mais que se empregue técnicas de inteligência artificial, elas não são suficientes para dirimir o problema de SPAMs.

Poonkodi et al. (2021) propõem um método de detecção de SPAM baseado em *Enriched Firefly Optimization Algorithm* (EFOA), em cujo método, a classificação de SPAM é realizada por meio de *Artificial Neural Networks* (ANN). EFOA trabalha em função do espaço/tempo e faz uma mineração de dados textuais contidos em mensagens, analisando somente o importante, e desta forma conseguiram distinguir e-mails legítimos de SPAM, tendo sido observados bons resultados em relação à diminuição dos Falsos Positivos. Todavia, esta técnica analisa o conteúdo, sendo que muitas mensagens, oriundas de MTAs com estruturas mal configuradas, tendem a ser consideradas Lixo Eletrônico.

Ramprasad et al. (2019) utilizam a filtragem baseada em conteúdo, como na citação anterior (POONKODI et al., 2021), em que os dados são pré-processados, removendo os conteúdos não importantes para filtragem, mantendo o conteúdo a ser analisado, sendo utilizado SVM, que é eficiente em se tratando do MTA Receptor, mas é preciso configurar padrões em MTA Emissores.

Sahni (2021) faz uma analise baseada no algoritmo *Naıve Bayes*, que utiliza filtro baseado em análise de palavras no MTA Receptor, mas se MTAs Emissores não estiverem com suas configurações adequadas, seus e-mails poderão ser considerados como SPAMs.

Deng et al. (2018) propõem um método híbrido, que combina uma rede neural profunda e um algoritmo de Florestas Aleatórias (*Random Forests* (RF)), para classificação de e-mails de SPAM. O método é avaliado em um conjunto de dados de e-mails de SPAM e obteve resultados promissores.

Li e Zhu (2019) apresentam um filtro de SPAM adaptativo baseado em Múltiplos Classificadores (*Multiple Classifier Systems* (MCS)) ponderados. O filtro é capaz de adaptar seu comportamento em resposta às mudanças na natureza do SPAM. Isto é particularmente interessante quando se considera que *spammers* têm evoluído rapidamente.

Liu, Xu e Liu (2019) reportam o uso de Rede Neural Convolucional (*Convolutional Neural Network* (CNN)) para filtragem de e-mails e propõem um modelo que usa convoluções bidimensionais para extrair recursos de texto e cabeçalho de e-mails. Eles avaliam o modelo em um conjunto de dados de SPAM e mostram que ele supera outras abordagens de aprendizado de máquina em termos de precisão e eficiência.

Bukhari, Jameel e Naz (2019) apresentam um método de detecção de SPAMs, por meio de técnicas de aprendizado de máquina e mineração de dados. O autor propõem um modelo que usa recursos de texto e cabeçalho de e-mails para identificar SPAMs. A avaliação de um modelo em um conjunto de dados de SPAM e mostram que ele tem uma taxa de precisão elevada.

Hossain, Karim e Rahman (2021) usam um método híbrido de aprendizado de máquina para detecção de SPAMs, que combina várias técnicas de aprendizado de máquina, incluindo ANN, Árvores de Decisão (*Decision Tree*) e Regras de Associação (*Association*

*Rule Learning*). Os autores aplicam o método em um conjunto de dados de SPAM e mostram que ele supera outras abordagens em termos de precisão e eficiência.

Zhang e Hu (2021) fazem utilização de um sistema de filtragem de e-mails baseado em técnicas de Aprendizado de Máquina (ML) e Aprendizado Profundo (*Deep Learning* (DL)). Sistemas de filtragem tradicionais geralmente usam regras baseadas em palavras-chave e outras heurísticas para classificar e-mails, como SPAM ou não SPAM. No entanto, essas abordagens têm limitações em sua eficácia, já que *spammers* facilmente alteram o conteúdo de seus e-mails. O sistema proposto aprende automaticamente a distinguir entre e-mails legítimos de SPAMs, sem a necessidade de regras explícitas. Foram usadas uma variedade de técnicas de processamento de linguagem natural, como extração de recursos, redução de dimensionalidade e classificação, para construir um modelo de classificação de e-mails. Além disso, exploraram DL, como Redes Neurais Convolucionais (CNN) e Redes Neurais Recorrentes (*Recurrent Neural Network* (RNN)), para melhorar a eficácia do modelo. Além de superar abordagens tradicionais, o sistema também foi capaz de lidar com variações no conteúdo do e-mail e adaptar-se a novos tipos de SPAMs.

Gao et al. (2019) apresentam um algoritmo baseado em Máquinas de Vetores de Suporte (SVM), usando ponderação por confiança. O algoritmo visa melhorar a precisão e eficiência da detecção de SPAM, ao incorporar informações de confiança na classificação dos e-mails. Segundo os autores, o método é lida com o desequilíbrio entre a quantidade de e-mails SPAM e não SPAM, desequilíbrio que é comum em sistemas de filtragem. Comparado a outros métodos, o método demonstra superioridade em termos de precisão e taxa de falsos positivos.

Jia et al. (2020) propõem um modelo de rede *Bayesiana* para detecção de SPAM, empregando técnicas estatísticas avançadas na construção de um modelo probabilístico, capaz de identificar e-mails indesejados com alta precisão. O modelo proposto é capaz de lidar com diferentes tipos de SPAM, incluindo *phishing*, publicidade e conteúdo malicioso. Os resultados experimentais demonstram que o modelo apresenta desempenho superior em comparação a outros métodos de filtragem de SPAM.

Cai, Wu e Zhang (2021) apresentam um modelo de detecção de SPAM baseado em uma versão melhorada do algoritmo *Naive Bayes*, aplicando técnicas de pré-processamento e seleção de recursos para melhorar o desempenho do algoritmo, no reconhecimento de padrões de SPAM em e-mails. O modelo proposto apresenta um desempenho superior em comparação com outros métodos de detecção de SPAM, incluindo modelos de Regressão Logística e Árvore de Decisão. Os resultados experimentais mostram que o modelo é capaz de detectar SPAM com alta precisão, além de apresentar uma baixa taxa de falsos positivos.

Silva, Lima e Filho (2019) reportam estudo sobre a aplicação de técnicas de aprendizado de máquina na classificação de e-mails, como SPAM ou não. Foram usados diferentes algoritmos de aprendizado de máquina, como Árvores de Decisão, **KNN!** (**KNN!**) e Flo-

restas Aleatórias, para treinar a classificação de SPAM. Os resultados mostraram que o algoritmo Florestas Aleatórias teve o melhor desempenho na classificação de SPAM, alcançando uma acurácia de 98,7%.

Martins, Souza e Pereira (2019) experimentam um algoritmo de classificação de SPAM em servidores de email, por meio de ML, para aprimorar a precisão da filtragem. Foi analisado um conjunto de dados coletado de mensagens de email classificadas como SPAM e não SPAM, no qual foram aplicados algoritmos de aprendizagem supervisionada, como K-NN e o *Naive Bayes*. Os resultados mostraram uma taxa de acerto de mais de 90%.

Gomes, Cardoso e Campista (2018) apresentam uma abordagem para identificação de SPAM, em fluxos de emails, utilizando aprendizagem de máquina e engenharia de características É utilizado o algoritmo de *Naive Bayes*, juntamente com a técnica de Análise de Componentes Principais (*Principal Component Analysis* (PCA)), para seleção das características mais relevantes. Foi utilizado um conjunto de dados de e-mails reais e os resultados indicaram uma melhora significativa na taxa de detecção de SPAM em relação aos métodos tradicionais de filtragem.

Deng et al. (2018) apresentam uma abordagem híbrida de Aprendizado Profundo e Florestas Aleatórias (RF) para classificação de SPAM, que consiste em usar CNN, como extrator de características, e alimentar um classificador de Florestas Aleatórias. Os experimentos foram realizados em três conjuntos de dados diferentes, demonstrando que a abordagem proposta é capaz de obter desempenho superior em comparação com outros métodos de classificação de SPAM, incluindo métodos baseados apenas em CNN ou apenas em RF. Além disso, a abordagem proposta é capaz de lidar eficientemente com um grande volume de dados de e-mail.

Li e Zhu (2019) apresentam um filtro de SPAM adaptativo aprimorado, baseado em Múltiplos Classificadores ponderados, oferecendo um novo método que combina vários classificadores para aumentar a eficácia do filtro de SPAM. O filtro foi aplicado em um conjunto de dados de e-mail real e os resultados mostram que o filtro aprimorado tem uma taxa de detecção de SPAM mais alta do que outros filtros convencionais.

Liu, Xu e Liu (2019) reportam a aplicação de uma Rede Neural Convolucional (CNN), que utiliza a técnica de *pooling* máximo para extrair características de mensagens de email e, em seguida, usa essas características para classificar o email, como SPAM ou não SPAM. O modelo foi treinado em um conjunto de dados de emails rotulados e os resultados mostram que a abordagem proposta é eficaz na detecção de SPAM, com uma precisão superior a 95%. Os autores também comparam o desempenho da CNN, demostrando ela supera esses algoritmos em termos de precisão e eficiência computacional.

Até onde se pode observar, a eficiência dos filtros de SPAM é uma questão cada vez mais importante no mundo de mensagens. Os autores de pesquisas e trabalhos correlatos estão empenhados em aumentar a capacidade de bloqueio de SPAMs nos MTAs de destino, sendo que o filtro de mensagens em si são parte do desafio, não podendo desprezar

que a origem também deve ser considerada para fins de garantir a legitimidade da mensagem. Uma visão centralizada de agentes de sistemas MHSs, garantindo que a gestão de provisionamentos necessários sejam feitos de modo orquestrado por um plano de controle.

No entanto, a falta de padrões procedimentais e a má configuração de MTAs emissores ainda representam um grande desafio. Embora os filtros de SPAM em MTAs Receptores estejam em constante aprimoramento, a especificação de um padrão de configuração, incluindo boas práticas, ainda não foi abordada com a devida profundidade.

A constituição de um plano de controle é fundamental para que um repositório de informações central possa ser disponibilizado para processamentos, incluindo a aplicação de técnicas de inteligência artificial - tais como aprendizado de máquina e aprendizado profundo - sejam aplicadas com sucesso. Configurações padronizadas a partir de um plano de controle é fundamental para reduzir a quantidade de SPAM que circula na internet.

## 2.3 Fundamentação Tecnológica

Qualquer que seja o serviço a ser oferecido na Internet, são necessários alguns fatores para determinar a autenticidade do servidor. Serviços de Correios Eletrônicos não são diferentes, com o agravante de e-mails serem serviços muito utilizados em relações comerciais em organizações. Os servidores de e-mails (MTA) precisam se relacionar com outros MTAs e, nessas interações, esses MTAs precisam ser autenticados, para evitar que mensagens enviadas por eles sejam classificadas como SPAMs nos MTAs receptores, chegando ao ponto que MTAs podem ser bloqueados.

A reputação do IP (leia-se do MTA) é um fator crítico para garantir que mensagens enviadas por servidores de e-mail sejam entregues com sucesso. Um MTA com boa reputação tende a ser considerado como confiável e suas mensagens são consideradas legítimas. Por outro lado, um MTA com má reputação pode culminar com o bloqueio de mensagens legítimas, sendo encaminhadas para o repositório de SPAM ou lixeira.

### 2.3.1 IP Público Estático

Todos os dispositivos que estão conectados à internet possuem um endereço IP exclusivo que os identifica na rede. Seja um computador, um celular, uma TV Smart ou qualquer outro dispositivo, cada um possui um IP único que o diferencia dos demais. No entanto, quando se trata da implementação de um servidor de e-mails, simplesmente estar conectado à internet com um IP dinâmico não é suficiente.

Isso ocorre porque o IP utilizado pelos dispositivos comuns é dinâmico e pode mudar a qualquer momento, o que impede o acesso ao servidor de e-mails por parte dos clientes. Além disso, os IPs públicos dinâmicos não podem receber a configuração PTR (DNS Reverso), que é um pré-requisito necessário para que o servidor de e-mails possa ser reconhecido pelo destinatário como autêntico.

O PTR é um registro de DNS que associa um endereço IP a um nome de domínio. Essa configuração é importante porque ajuda a confirmar a autenticidade do servidor de e-mails. Quando um servidor de e-mails envia uma mensagem para outro servidor, o receptor verifica o registro PTR do remetente para garantir que a mensagem é legítima e não é um SPAM ou um e-mail fraudulento. Se o PTR não estiver configurado corretamente, a mensagem poderá ser bloqueada ou encaminhada para a caixa de SPAM.

Portanto, para implementar um servidor de e-mails de forma eficaz, é necessário possuir um IP estático, ou seja, um IP que não muda com frequência. Isso garante que o servidor possa ser acessado pelos clientes sem problemas e permite a configuração do registro PTR. Além disso, é importante seguir outras boas práticas, como a configuração de autenticação e reputação do IP, para garantir que as mensagens enviadas sejam entregues com sucesso na caixa de entrada dos destinatários.

### 2.3.2 DNS Reverso

A configuração correta do DNS Reverso (rDNS) é essencial para garantir a legitimidade do servidor e aumentar sua confiabilidade. É necessário que o DNS Reverso aponte para o *Fully Qualified Domain Name* (FQDN) do MTA, sendo esta uma consulta frequente, para provar que o IP sendo utilizado pelo remetente da mensagem pertence de fato ao domínio do MTA enviador.

Para obter a configuração correta do DNS reverso, é necessário entrar em contato com a empresa fornecedora do serviço de IP Estático e solicitar a configuração PTR do IP público. É importante verificar se a configuração foi realizada corretamente utilizando o comando NSLOOKUP, por exemplo.

A configuração do DNS reverso deve ser realizada antes da implementação do servidor de e-mails, uma vez que essa configuração influencia diretamente no envio e recebimento de e-mails. Caso haja dúvidas em relação à configuração do DNS Reverso, é possível utilizar serviços online, como o "*mxtoolbox reverse* DNS", para realizar testes e garantir que a configuração foi realizada corretamente.

### 2.3.3 Política para Verificar Remetentes

O Protocolo SPF (KUCHERAWY, 2014) é utilizado para auxiliar a proteger seu domínio contra o envio de e-mails falsificados ou maliciosos. Ele funciona apoiado no cadastro, de MTAs habilitados (confiáveis), utilizando uma entrada do Tipo TXT, no registro SPF do seu domínio, que lista servidores autorizados. Quando uma mensagem é recebida, ele verifica se o MTA, que enviou a mensagem, está nessa lista. Isso pode ajudar a verificar a confiabilidade do remetente e reduzir a quantidade de SPAM.

Durante testes em laboratório, foi observado que mesmo com um registro SPF configurado, mensagens podem ser marcadas como SPAM, se o registro estiver configurado

de forma incorreta. Portanto, é importante configurar corretamente a cláusula "PTR"no registro SPF para garantir que suas mensagens sejam verificadas corretamente e entregues sem problemas.

Configurar SPF requer a inserção de linhas do Tipo TXT no servidor de DNS autoritativo do seu domínio. Todos os servidores de e-mail autorizados a enviar mensagens em nome de seu domínio, incluindo servidores de terceiros, se você usar provedores de serviços de e-mail, devem ser nomeados nesta lista. Certifique-se de que a linha esteja formatada corretamente e que inclua a cláusula "PTR"para verificar a autenticidade do remetente.

### 2.3.4 Política de Confidencialidade entre MTAs

O Protocolo DKIM (LEVINE; KUCHERAWY, 2011)permite encriptar mensagens trocadas entre MTAs por meio de infraestrutura de chaves públicas (*Public Key Infrastructure* (PKI)). O processo de instalação do DKIM começa com a geração das duas chaves no MTA Remetente. A chave pública (*Public Key*) é inserida em uma entrada TXT no DNS autoritativo do domínio, enquanto a chave privada (*Private Key*) é instalada no MTA. É importante frisar que MTAs são o *core* de um Sistema MHS, conforme se pode observar na Fig. 1.

Apesar de existirem diversas opções no mercado, para este projeto, foi utilizado o pacote OpenDkim disponível no sistema operacional Ubuntu Server 20.04 e instalado por meio do script Iredmail.

### 2.3.5 Autenticação baseada em Domínio & Conformidade

O protocolo DMARC (HANSEN; SCUDDER; KUCHERAWY, 2015)foi especificado para complementar as funcionalidades de segurança oferecidas pelo SPF e DKIM. DMARC define regras tratar mensagens bloqueadas pelos SPF e DKIM. Sem o DMARC, provedores decidem livremente o que fazer com essas mensagens rejeitadas pelos SPF e DKIM, por exemplo, descartar.

DMARC precisa de duas definições em sua implementação, sendo: 1) definir como mensagens bloqueadas pelo SPF ou DKIM serão tratadas; e 2) definir o endereço (e-mail) para onde serão enviados relatórios, com as falhas que levaram à não entrega da mensagem coretamente.

Ao contrário dos protocolos SPF e DKIM, DMARC não exige nenhuma configuração no MTA, sendo necessário apenas a inserção de uma entrada do tipo TXT no DNS do domínio em questão.

É importante destacar que a configuração do DMARC pode ajudar a melhorar a reputação do domínio, uma vez que, ao garantir a autenticidade das mensagens, é possível reduzir a quantidade de SPAM e *phishing* enviadas em nome do domínio. Isso pode ser

especialmente útil para empresas que enviam um grande número de e-mails marketing, por exemplo.

Capítulo 3

# SPAM-K: Proposta de uma Aplicação do Plano de Controle MHS

Muitos esforços têm sido envidados para combater SPAM e, consequentemente, diversos protocolos para autenticação e configuração foram especificados com o objetivo de permitir a implementação de boas práticas no envio de e-mails, tais como os protocolos DKIM, SPF, DMARC, entre outros. Tais protocolos têm por finalidades disponibilizar uma interface padrão para configurações importantes nos hospedeiros de agentes, como os arquivos `hostname, hosts, main.cf` e DNS Reverso (rDNS).

Todavia, atualmente, as implementações desses protocolos são feitas em plataformas distintas, sem preocupação expressa com interoperabilidade, e as respectivas configurações, em geral, são feitas a partir de valores "*default*", o que gera discrepâncias comportamentais de provedores de correio eletrônico, culminando com o aumento de falsos positivos.

Considerando que MHSs de diferentes provedores, eventualmente, podem trocar interações durante envios de envelopes, seria importante uma visão de controle logicamente centralizada que permita a gestão (monitoramento, configuração, controle) de artefatos e parâmetros para minimizar falsos, positivos ou negativos, no tangente a SPAMs. Nesse contexto, torna-se essencial o desenvolvimento de um plano de controle, logicamente centralizado, que faça a gestão das configurações do plano de dados, materializado pelos agentes MHSs, representado na Fig. 1. O Plano de Controle proposto permitirá o uso automático de serviços desses protocolos, com as configurações requeridas, assegurando a segurança e confiabilidade no envio de e-mails.

SPAM-K é uma aplicação do plano de controle com a finalidade de monitorar e controlar parâmetros dos agentes por meio dos protocolos de autenticação e configuração incorporados à aplicação desenvolvida. O monitoramento e controle são feitos sistematicamente, sem a necessidade de intervenção manual. Evidentemente, atuações de um administrador são possíveis para fins de análise e, eventualmente, alguma configuração necessária. SPAM-K garante uma implementação normatizada desses protocolos e con-

figurações, evitando discrepâncias entre provedores de correio eletrônico, isto é, entre MHSs. A gestão desempenhada pelo SPAM-K permite, rapidamente, identificar e corrigir possíveis erros de configuração em agentes MHS, contribuindo para minorar falsos, positivos ou negativos.

Para implementar um plano de controle centralizado que permita a implementação automática dos protocolos de autenticação e configurações necessários para garantir a segurança e a confiabilidade no envio de e-mails, foram desenvolvidos algoritmos com a linguagem de programação Python e JSON.

Esses algoritmos permitem que todas as configurações e protocolos sejam definidos de forma clara e objetiva, garantindo a padronização na implementação desses protocolos e configurações. Além disso, o plano de controle foi alocado em uma VPS EC2 da AWS, garantindo a escalabilidade e a disponibilidade necessárias para a implementação em larga escala.

## 3.1 Visão Geral MHS: Planos de Dado e de Controle

A visão apresentada nesta seção se baseia na filosofia SDN, em que um plano de controle ortogonal, logicamente centralizado, gere (monitora e controla) o plano de dados composto pelos agentes de um sistema MHS. Este plano centralizará em um único lugar todas as ações de controle necessárias para manter a saúde de MHSs, conforme está representado na Fig. 1. SPAM-K é uma aplicação da Camada de Aplicação do Plano de Controle para fins de controle de sistemas MHSs.

## 3.2 Plano de Controle

Como mencionado anteriormente, o Plano de Controle centraliza todos os aspectos de controle dos elementos de um sistema distribuído. Como pode ser observado na Fig. 1, o Plano de Controle é organizado em 3 camadas, sendo:

- ❑ **Camada Física**: responsável por gerir informações relativas a elementos físicos da infraestrutura da rede tais como roteadores, servidores, *switches*, *firewalls*, *proxies*, topologia, zonas militarizadas etc;
- ❑ **Camada de Controle**: responsável por provisionar (aplicar, modificar, consultar etc) as configurações que regem o funcionamento dos elementos da infraestrutura; e
- ❑ **Camada de Aplicação**: responsável por aplicações de controle[1], isto é, aplicações que desempenham a lógica de gestão dos parâmetros de configuração, fazendo uso de serviços da camada de Controle.

[1] Aplicações do Plano de Controle executam lógicas associadas a controle, isto é, não confundir com a camada de aplicação do Plano de Dados

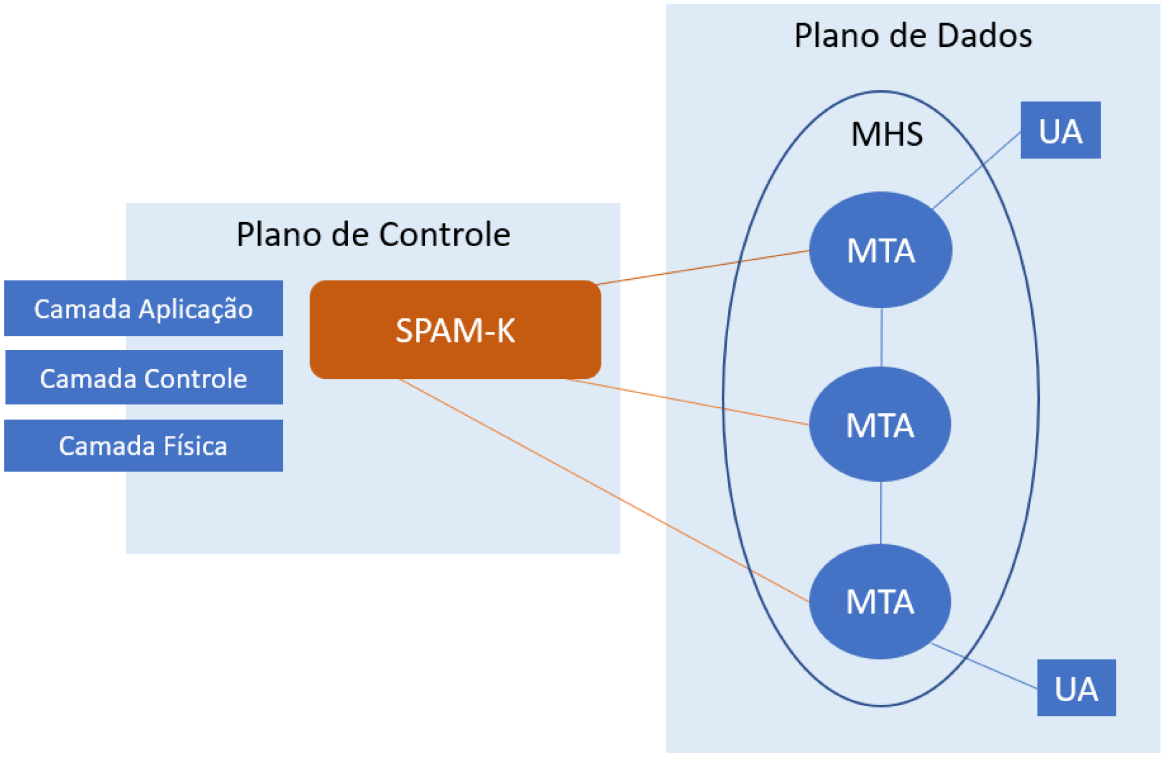



Figura 1 – Modelo para Plano de Controle MHS

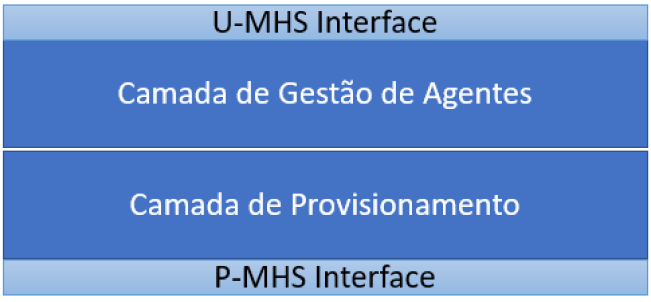



Figura 2 – Arquitetura da Aplicação SPAM-K

Observe que pela descrição das camadas, pode-se deduzir que SPAM-K é uma aplicação da camada de Aplicação, que inclui aspectos da camada de Controle do Plano de Controle. Isto é, a arquitetura de software da SPAM-K tem pelo menos duas subcamadas, sendo uma camada responsável pela lógica de controle anti SPAM e a segunda responsável pelos aspectos de controle (provisionamento) dos Agentes MHS. A Fig. 2 apresenta a arquitetura da aplicação de controle SPAM-K.

A Interface superior (U-MHS-Interface) funciona como uma *East Bound Interface* (EBI) permitindo que agentes MHS (Plano de Dados), em particular MUAs, possam trocar notificações de eventos e outros serviços afim de posicionar o plano de controle sobre eventuais ações a serem desempenhadas pela SPAM-K. Embora faça parte da modelagem,

a U-MHS-Interface está fora do escopo deste trabalho.

A Interface inferior (P-MHS-Interface) funciona como uma *South Bound Interface* (SBI) e é utilizada pela SPAM-K para controlar agentes MHS, em particular MTAs. A SBI neste projeto atua como uma arquitetura *hub-and-spoke* ou *controller-and-agents*, maiores detalhes são apresentados na Seção 3.2.4.

### 3.2.1 SPAM-K: Camada de Gestão de Agentes

Esta camada tem o objetivo de gerir os agentes no tocante a seus comportamentos relativos à categorização de mensagens, visando a eliminação ou minimização de falsos. Deste modo, esta camada deve manter um repositório de informações que permita uma análise da ocorrência de tais mensagens. Baseada em limiares de parâmetros chaves, a lógica implementada por esta camada deve tomar decisões de controle (alteração de configurações) usando serviços da camada de Provisionamento de Agentes.

A evolução desta camada poderia envolver diversas ferramentas de inteligência artificial e de análise de dados. Poderia, inclusive, disponibilizar uma API que permitisse a MUAs (clientes de email) trocar interações com a SPAM-K (plano de controle) para oferecer/buscar informações que poderia influenciar no comportamento de clientes de e-mail, com vistas a desempenho, segurança etc. Como dito anteriormente, nesta versão não será disponibilizada API para interações com MUAs, isto é, não foi especificada a Interface U-MHS-Interface.

Todavia, para esta dissertação, como prova de conceito da proposta, foi limitada, pelo imperativo do prazo, a uma lógica simples, que consiste em identificar o agente, especificar o serviço e os respectivos parâmetros a ser provisionados (no agente identificado). Conforme será possível verificar no Capítulo 5, os resultados obtidos permitem deduzir que a abordagem escolhida é capaz de provar a aplicabilidade da proposta.

### 3.2.2 Interface de Admin

Esta (*spam-k.py*) é a interface por meio da qual usuários podem fazer solicitações. O código é escrito em *Python* com o uso do *framework Flask*. A rota principal ("/") é definida para o método POST, o que significa que quando o formulário é enviado, a função `site()` é invocada. Dentro desta função, todos os dados de cadastramento do provedor, preenchidos pelo usuário, são recuperados a partir do objeto *request*.

Uma vez recuperados, os dados são passados via serviços requisitados a P-MHS-Interface, que invoca serviços específicos necessários para configurar o serviço de e-mail. Essas tarefas incluem a configuração de rDNS, SPF, DKIM, DMARC, que foram introduzidos na Seção 2.3, e os comandos `hostname, hosts, Postfix`.

A função `chave()` é chamada para gerar uma chave de criptografia para o DKIM, que é usado para garantir que e-mails enviados sejam autênticos e não tenham sido alterados

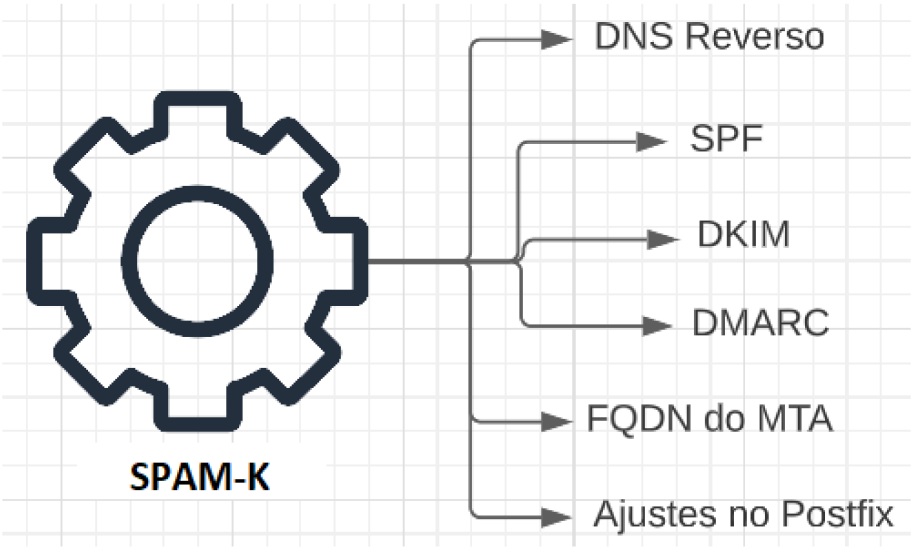



Figura 3 – SPAM-K: Interfaces da Camada de Provisionamento

durante a transmissão. As funções `dkim()`, `dmarc()`, `hostname()`, `hosts()`, `postfix()`, `rdns()` e `spf()` são invocadas para configurar os registros DNS necessários para que o serviço de e-mail funcione corretamente.

Finalmente, uma mensagem é retornada ao usuário confirmando se o provedor foi configurado com sucesso. A *spam-k.py* também inicia um servidor *Flask* local na `porta 80`, permitindo que o usuário acesse os serviços por meio do navegador.

### 3.2.3 SPAM-K: Camada de Provisionamento de Agentes

A camada de Provisionamento da SPAM-K reúne aspectos de controle da Camada de Controle[2], sendo, portanto, responsável por se comunicar com os agentes MHS, por meio da Interface Inferior (P-MHS-Interface), que abstrai o uso dos protocolos SPF, DKIM, DMARC e DNS Reverso, citados na Seção 2.3, e a configuração do FQDN de MTAs e ajustes necessários ao Postfix, conforme pode ser visto na Fig. 3.

A Seção 2.3 apresenta os principais protocolos atualmente desenvolvidos para minimizar os falsos, todavia, a camada de Provisionamento deve ter a habilidade de incorporar novos protocolos que venham a ser especificados com esta finalidade. Os serviços desses novos protocolos serão incorporados àqueles correntemente disponibilizados pelos protocolos atualmente especificados, representados na Fig. 3.

Nesta camada, o serviço requisitado pela Camada de Gestão de Agentes (ver Seção 3.2.1), passará pelo processamento com vistas a extrair os parâmetros necessários para que o serviço requisitado seja provisionado no agente correto. Deste modo, o serviço deve especificar:

[2] Provisionamento foi escolhido para nomear esta camada da SPAM-K para evitar confusão com a Camada de Controle do Plano de Controle

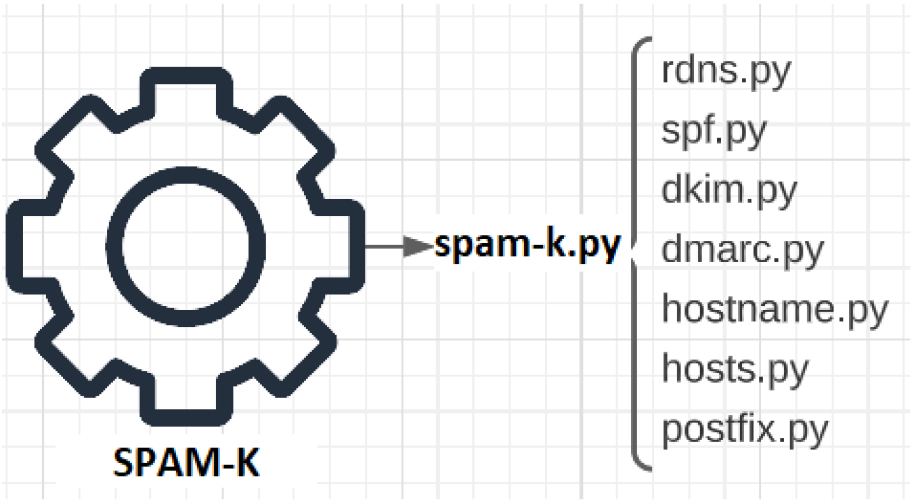



Figura 4 – SPAM-K: Interface Inferior P-MHS-Interface

- *Agente*: serve para identificar o agente (MTA), localizar o endereço, porta e aspectos de segurança, necessários para se conectar ao agente sendo configurado;
- *Serviço*: detectar o protocolo da Interface Inferior (P-MHS-Interface) e o serviço a ser requerido nessa interface; e
- *Parâmetros*: identificar os parâmetros e extrair os respectivos valores a ser provisionados no agente especificado (identificado).

Identificados os Agente, Protocolo, Serviço e Parâmetros a ser provisionados, deve-se proceder a invocação do serviço da P-MHS-Interface de modo que a ação especificada possa ser desempenhada no agente especificado. A P-MHS-Interface contém um conjunto de APIs com os serviços necessários para as invocações de provisionamento.

### 3.2.4 SPAM-K: Interface Inferior P-MHS-Interface

Essa interface SBI congrega as APIs dos protocolos (ver Seção 2.3) correntemente existentes para os provisionamentos de parâmetros em agentes MHS, notadamente MTAs. Para este trabalho, foram selecionadas API construídas em Python/JSON em função da base de software e pela estabilidade das APIs selecionadas. A Fig. 4 apresenta os símbolos disponíveis para as respectivas invocações. Maiores detalhes serão apresentados no Capítulo 4.

Estratificar as APIs nesta interface inferior (denominada spam-k.py) permite que novos protocolos sejam adicionados facilmente, bem como, se houver necessidade de troca de tecnologia (linguagem, orientação de serviço, *frameworks* etc), tais mudanças não impactem na camada de Provisionamento.

Em particular, em ambiente genuinamente SDN, com um controlador OpenFlow (OF), por exemplo, os serviços da SBI/OF seriam utlizados para estabelecer os enlaces lógicos

(*flows*) entre a SPAM-K e agentes MHS, notadamente os MTAs. Considerando que são camadas independentes e que o uso da SBI/OF é uma tecnologia dominada, este projeto dedicou-se à camada de aplicação, comunicando-se com agentes MHS por meio de circuitos virtuais TCP.

## 3.3 Diagrama de Casos de Uso MHS

Como é sabido, diagramas de casos de uso (*Use Case*) permitem relacionar todos os atores (*stakeholders*), tornando possível a análise do problema sob diferentes pontos de vista. É importante ressaltar que, neste trabalho, o escopo é limitado a atores envolvidos em atividades de controle (administrador). A Fig. 5 apresenta o diagrama de casos de uso que representa as interações de três atores relacionados ao processo de cadastro do provedor de serviços de correios eletrônicos.

Do lado esquerdo da Fig. 5, está o analista responsável pelo serviço de correio eletrônico (1), que proverá as informações para cadastro na plataforma de controle SMPAM-K, descritas na Seção 4.1.1. Ao submeter a solicitação, as informações serão passadas via requisição de serviço para a Camada de Provisionamento (Seção 3.2.3). Como resposta, receberá a confirmação se o serviço foi provisionado com êxito ou não.

Do lado direito da Fig. 5, estão os outros dois atores, sendo: (2) analista responsável pelo registro do domínio; e (3) analista responsável pelo provimento de VPS. O ator (2) é responsável pelo processo que envolve registro do domínio, incluindo as entradas de registros (RR – *Resource Record*) de DNS importantes. O ator (3), responsável por prover o VPS, onde serão realizadas as alterações no Postfix e no DNS Reverso.

O ator (1), responsável pelo serviço de correio eletrônico, deverá garantir aos usuários a capacidade enviar e receber e-mails, de forma precisa, eficiente e segura. O ator (2), responsável pelo registro do domínio, por sua vez, é responsável por garantir que o domínio esteja registrado corretamente e que as entradas DNS necessárias estejam presentes. Ele é o responsável por garantir que o endereço de e-mail possa ser resolvido corretamente no DNS. O ator (3), é responsável por provimento do VPS e, assim, garantir que o servidor de e-mail Postfix e a respectiva entrada de DNS estejam configurados corretamente. Além de garantir a entrega correta de e-mails, assegura que o servidor de e-mail esteja protegido contra spam e outras ameaças.

Ao orquestrar as ações desses atores, é possível garantir que o processo de cadastro de provedor de correio eletrônico (MHS) seja realizado de forma eficiente e segura. As funções de SPF, DKIM, DMARC e Postfix ajudam a garantir que e-mails sejam entregues corretamente e que o servidor de e-mail esteja protegido contra spam e outras ameaças. O DNS Reverso também é importante para garantir que o servidor de e-mail seja considerado confiável por outros servidores de e-mails.

Em resumo, o diagrama de caso de uso descrito nesta seção é uma representação

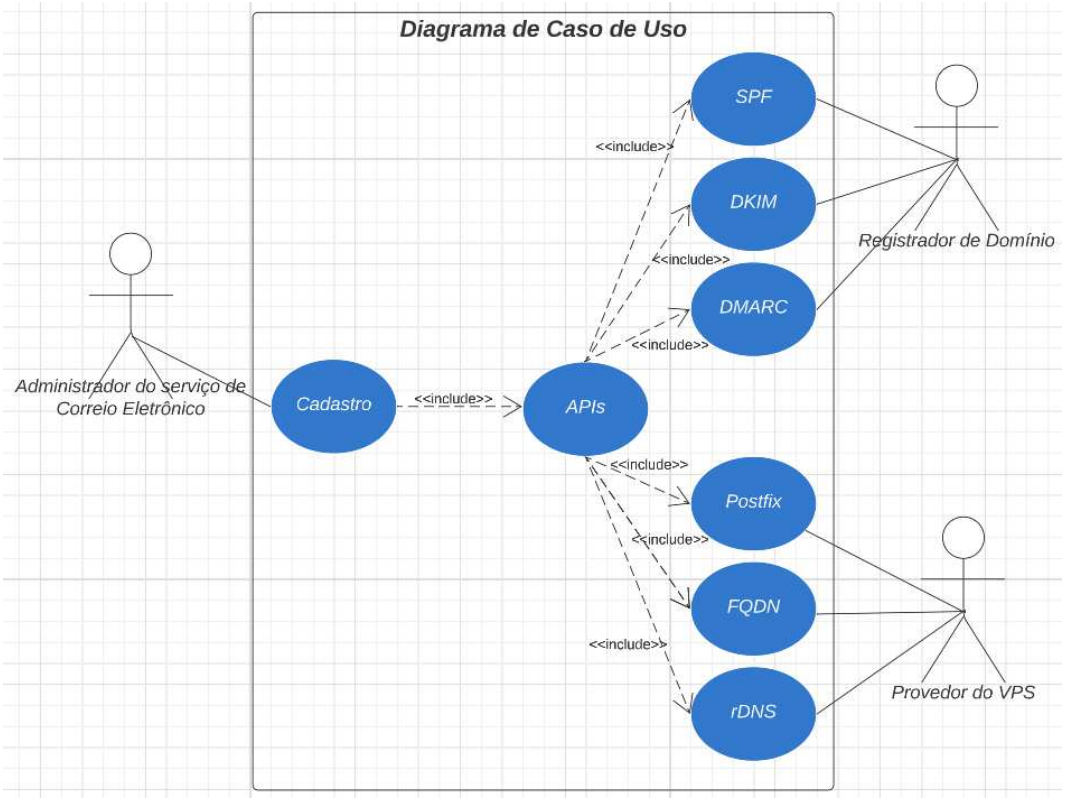



Figura 5 – MHS: Diagrama de Casos de Uso

visual, importante para entender como os atores envolvidos interagem para garantir que o processo de cadastro de correio eletrônico seja realizado de forma eficiente e segura. Cada ator desempenha um papel importante nesse processo, e entender como cada um deles se encaixa no processo global é essencial para garantir que tudo funcione corretamente.

A autenticidade de e-mails é uma questão cada vez mais importante nas comunicações, principalmente, corporativas, especialmente quando envolve fraudes e *phishing scams*. Para combater esses males, diversas empresas de tecnologia desenvolveram padrões de autenticação de e-mails, como o SPF, DKIM e DMARC. No entanto, a implementação desses padrões ainda não é universal e muitos provedores de e-mail ainda não os configuram de maneira adequada.

A SPAM-K tem como objetivo implementar e orquestrar a configuração desses padrões de autenticação de e-mails em todos os provedores de e-mail do mundo. Isso é essencial para garantir que e-mails enviados por remetentes legítimos, sejam entregues com sucesso, e que e-mails mal-intencionados, sejam bloqueados antes de chegarem a caixas de entrada de usuários.

A Fig. 6 ilustra o cenário em que provedores de correio eletrônico têm suas regras de autenticidade gerenciadas pela SPAM-K. Isso significa que o plano de controle terá autoridade para impor padrões de autenticação de e-mails em todos os provedores de e-mail, independentemente da localização ou tamanho.

Todavia, a implementação de um plano tão ambicioso não é tarefa fácil. Provedo-

res de e-mails têm seus próprios processos de autenticação e podem ter resistência em adotar novos procedimentos. Além disso, a implementação de novas regras de autenticação pode afetar a entrega de e-mails legítimos, especialmente se essas regras não forem implementadas corretamente.

Para resolver esses desafios, o plano de controle precisará trabalhar em colaboração com os provedores de e-mail para implementar os padrões de autenticação de e-mails de maneira eficaz e minimizar as interrupções na entrega de e-mails legítimos. Isso pode envolver a realização de testes em ambientes de produção limitados antes de implementar as regras em todo o sistema.

Além disso, a implementação de padrões de autenticação de e-mails também pode exigir uma maior conscientização e educação de usuários para identificar e-mails legítimos ou suspeitos. Isso pode incluir treinamento para usuários sobre como verificar a autenticidade de um e-mail, bem como o desenvolvimento de ferramentas que ajudem os usuários a identificar e-mails mal-intencionados.

Embora a implementação de padrões de autenticação de e-mails possa ser desafiadora, os benefícios potenciais são significativos. Ao reduzir a quantidade de e-mails mal-intencionados, que chegam às caixas de entrada dos usuários, os padrões de autenticação de e-mails podem ajudar a aumentar a confiança na comunicação eletrônica.

Além disso, a implementação de padrões de autenticação de e-mails pode ajudar a melhorar a eficácia do marketing por e-mail, reduzindo o risco de e-mails legítimos serem filtrados como spam. Isso pode ajudar empresas a alcançar seus públicos-alvo com mais eficácia e aumentar o *Return on Investiment* (ROI) de suas campanhas de marketing por e-mail.

Em resumo, a implementação de padrões de autenticação de e-mails pode trazer benefícios significativos para a segurança cibernética e eficácia do marketing por e-mail. No entanto, a implementação de tais padrões requer esforços colaborativos e pode enfrentar desafios técnicos e educacionais. É importante que provedores de e-mail trabalhem em conjunto com o plano de controle para garantir que a implementação seja feita de forma eficaz e eficiente, garantindo que os usuários recebam e-mails legítimos em suas caixas de entrada e reduzindo o risco de ataques cibernéticos.

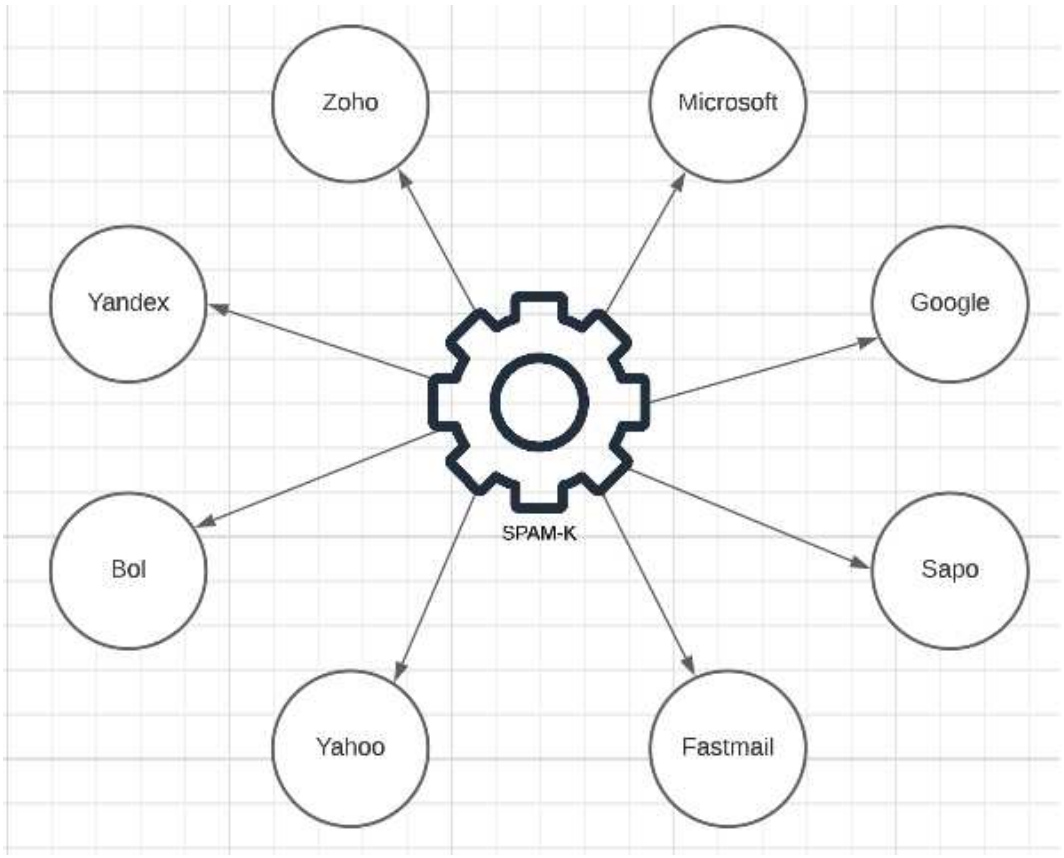



Figura 6 – Plano de controle e os provedores com suas regras padronizadas

Capítulo 4

# Desenvolvimento da Aplicação de Controle SPAM-K

Este capítulo tem por objetivo lançar alguma luz sobre o processo de desenvolvimento, sendo que os detalhes, tais como códigos fontes, serão adicionados a este trabalho na forma de apêndices. Deste modo, será dada maior ênfase a decisões de projeto (*design*) e não nas implementações propriamente ditas.

Além do desenvolvimento da SPAM-K, foi também necessário o desenvolvimento de um MTA de referência para fazer os testes, uma vez que não poderiam ser utilizados os MTAs de provedores tais como UFU, Google, Yahoo, Outlook, entre outros, para esta finalidade. Na Seção 4.4 é descrita a parte do desenvolvimento que foi necessária para o referido MTA.

## 4.1 SPAM-K: Camada de Gestão

Como introduzido na Seção 3.2.1, neste trabalho, será desenvolvido o substrato suficiente para provar a hipótese deste trabalho. Deste modo, serão feitos cadastros e telas de entrada/saída de informações de configuração, necessários para a verificação da proposta.

### 4.1.1 Cadastro de Provedores (MHS)

Esta seção descreve como os provedores de serviços de e-mails poderão cadastrar seus MHSs, de tal forma que esta camada de Gestão possa saber quais são os agentes gerenciados pela SPAM-K. As seguintes informações são necessárias para o provisionamento de parâmetros relativos a SPAM:

- **Domínio**: nome do domínio principal do provedor de correio eletrônico, é um parâmetro chave para fins de referência ao provedor MHS;

- ***Hostname***: nome do equipamento hospedeiro do MTA, responsável por enviar Envelopes (mensagens);
- **Endereço IP**: endereço IP do equipamento hospedeiro do MTA, responsável por enviar Envelopes (mensagens);
- **Administrador**: nome de usuário (*username*) administrador, responsável pelo MTA, responsável por enviar Envelopes (mensagens);
- **Senha Admnistrador**: credencial de acesso do usuário administrador do MTA, responsável por enviar Envelopes (mensagens);
- **DNS Reverso (rDNS)**: URL da empresa de registro de domínios responsável por fornecer o IP público ao MTA, responsável por enviar Envelopes (mensagens);
- **Chave de API**: chave gerada pela empresa de registro de domínios;
- **Senha de API**: assim como a chave, esta senha é fornecida pela empresa de registro de domínios;
- **URL Empresa Domínios**: o *Endpoint CPanel* requer a URL da empresa de Registro de Domínios, responsável pela autoridade do domínio principal;
- ***Username* Empresa Domínios**: nome de usuário da empresa responsável pelo registro de domínios;
- **Chave de API do usuário**: chave de API relativa ao *Username* da empresa responsável pelo registro de domínios; e,
- **E-mail**: endereço de correio eletrônico do administrador do MHS, sendo registrado.

Após o preenchimento dos dados nos formulários e a submissão do mesmo pelo usuário, as informações dos provedores são armazenadas em variáveis previamente declaradas no arquivo spam-k.py. Neste arquivo, ocorre a separação das informações de cada provedor nas suas respectivas variáveis, com base nos campos definidos nos formulários.

Vale ressaltar que não há a utilização de um banco de dados nesse processo. As informações são armazenadas randomicamente nas variáveis do arquivo spam-k.py e sequencialmente transportadas para os arquivos responsáveis por cada função de API.

É importante mencionar que a falta de um banco de dados pode tornar o processo de recuperação de informações mais complexo, especialmente em situações que exijam a recuperação de dados de forma rápida e eficiente. No entanto, para o escopo do projeto Spam-K, a decisão de não utilizar um banco de dados se justifica pela simplicidade do processo e pela necessidade de agilidade no disparo das APIs.

Após a coleta e armazenamento das informações dos provedores, ocorre o tratamento dos dados, com a finalidade de garantir que as informações estejam em conformidade com

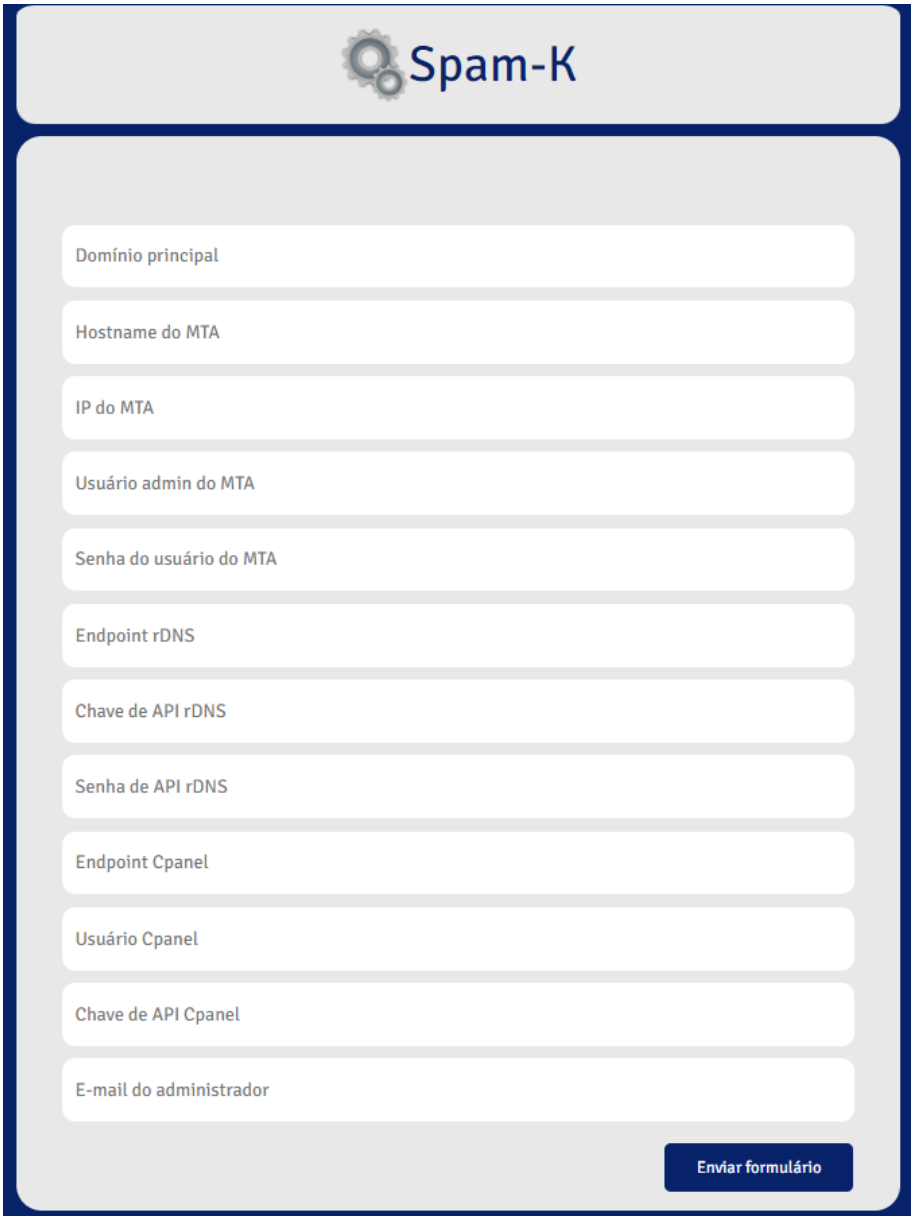



Figura 7 – Cadastro de provedores de E-Mails

os requisitos de cada API. Em seguida, é realizada a chamada de cada API, utilizando as informações previamente armazenadas nas variáveis.

Reconhece-se que estas informações são sensíveis e, principalmente, a introdução de um plano de controle, para tais tipos de atividades, é, até onde se pode pesquisar, novidade.

Essas informações são essenciais para que a gestão de agentes possa realizar alterações e configurações importantes em provedores, objetivando-se maior eficácia no envio de mensagens. A Fig. 7 apresenta uma tela de cadastro oferecida pela camada de Gestão da SPAM-K.


Figura 8 – Operação da SPAM-K


Figura 9 – Consultar SPAM-K

### 4.1.2 Cadastro de Operação

Na Seção 4.1.1 foi especificado cadastro de provedores de e-mails, sendo que as informações para cadastro podem ser vistas na Fig. 7. Para fins de prova de conceito, foi desenvolvida uma aplicação que permite (i) fazer consultas e (ii) solicitar tarefas de provisionamento em provedores MHS.

Deste modo, o administrador da SPAM-K deve definir se a atividade é uma atividade de consulta ou uma atividade de provisionamento. Também deve fornecer o parâmetro chave para identificar o domínio do provedor sobre o qual a atividade será executada.

Se for uma consulta, devem ser especificados os parâmetros a ser buscados no(s) agente(s) do provedor definido para a atividade.

Se for uma solicitação de provisionamento, além dos parâmetros, devem ser oferecidos os novos valores a ser provisionados no(s) agente(s) do provedor definido para a atividade.

Em ambos os casos, o administrador receberá uma tela de resposta com as respectivas informações especificadas na atividade. A Fig. 10 oferece uma representação da operação da SPAM-K.

## 4.2 SPAM-K: Camada de Provisionamento

A camada de Gestão (Seção 4.1) usa os serviços desta camada para consultar ou provisionar parâmetros em MTAs de provedores de e-mail. Basicamente, os serviços pro-


Figura 10 – Consultar SPAM-K

vidos por esta camada são especificados por atividades de operação solicitadas conforme descritas na Seção 4.1.2.

Ao receber a solicitação, esta camada é responsável por identificar o tipo da requisição (consulta ou provisionamento) e extrair os parâmetros relativos ao tipo da requisição.

É responsabilidade desta camada identificar qual o protocolo e qual o serviço da API P-MHS-Interface será invocado para executar o serviço requerido. Quando foi recebida a resposta, será responsabilidade desta camada formatar a resposta nos moldes requeridos pela interface desta camada, de tal modo que seja interpretado pela Camada de Gestão.

Esta camada foi desenvolvida em Python e usa os serviços da API P-MHS-Interface (JSON) para a invocação dos serviços pertinentes.

## 4.3 SPAM-K: Interface P-MHS-Interface

A Interface especificada nesta seção engloba os protocolos introduzidos na Seção 2.3 e reúne as chamadas de serviços no artefato Spam-K.py, desenvolvida na Linguagem Python, cuja representação pode ser apreciada na Fig. 4. Além dos protocolos, esta interface reúne serviços auxiliares para resolução de nomes, entre outras coisas. Como já mencionado anteriormente, a criação desta interface é fundamental para desacoplar as camadas superiores dos aspectos de implementação desses protocolos.

### 4.3.1 Resolução de Nomes

A resolução de nomes será desempenhada pelas bibliotecas *hostname.py* e *hosts.py*, com o objetivo de resolver FQDN (Fully Qualified Domain Name), lembrando que o FQDN representa nome de domínio, com informações precisas em uma rede sobre localização, nome do *host*, nome do domínio e, opcionalmente, nomes de subdomínios.

*hostname.py* permite definir o *hostname* do servidor. Isso é feito por meio de uma conexão SSH com o servidor, utilizando a biblioteca Python paramiko. O serviço especifica as informações de conexão, incluindo o endereço IP do servidor, o nome de usuário e senha

do administrador, bem como o nome do host que deve ser configurado. Em seguida, ele executa um comando SSH para modificar o arquivo /etc/hostname com o nome do hostname definido.

*hosts.py* tem a função de resolver o FQDN quando solicitado, usando a biblioteca Python paramiko, para estabelecer uma conexão SSH com o servidor e limpar o arquivo /etc/hosts. Em seguida, ele executa dois comandos SSH para modificar o arquivo /etc/hosts, sendo: 1) adiciona a entrada "127.0.0.1 [hostname_mta].[dominio_principal] [hostname_mta]"ao arquivo /etc/hosts, que mapeia o endereço IP local para o FQDN do servidor; e 2) cria a entrada "[ip_mta] [hostname_mta].[dominio_principal] [hostname_mta]"ao arquivo /etc/hosts, que mapeia o endereço IP do servidor para o FQDN do servidor.

Esses comandos garantem que o servidor MTA estará configurado corretamente para fornecer o FQDN quando solicitado, por exemplo quando solicitado por servidores de correio eletrônico, sistemas de autenticação, entre outros.

### 4.3.2 DNS Reverso

Disponível por meio de um script Python *rdns.py*, que utiliza a biblioteca *Python Requests*, para solicitar HTTP POST para um *endpoint* específico, com o objetivo de realizar uma configuração de DNS Reverso (rDNS – *reverse* DNS). DNS Reverso é uma técnica utilizada para garantir que um endereço IP é de fato associado a um nome de domínio.

O protocolo especifica vários parâmetros, incluindo: endpoint_rdns, que é o endereço do servidor que oferece o serviço de rDNS; chave_api_rdns e senha_api_rdns, que são as credenciais de autenticação para acessar o serviço; ip_mta, que é o endereço IP do servidor para o qual se deseja configurar o rDNS; hostname_mta, que é o nome do host que será associado ao endereço IP; e, dominio_principal, que é o nome do domínio ao qual o host pertence.

O algoritmo oferecido pela biblioteca começa construindo o *endpoint* completo a ser usado para a solicitação POST. Ele inclui as informações de autenticação e define o formato de resposta como JSON. Em seguida, é construído o *payload*, que contém as informações necessárias para se configurar o rDNS. O valor 'rdns' igual a 1 indica que a ação a ser realizada é configurar o rDNS. O valor 'rdns_ip' é o endereço IP do servidor para o qual se deseja configurar o rDNS, e 'rdns_domain' é o nome completo do host que será associado ao endereço IP.

Após construir o *endpoint* e o *payload*, o algoritmo envia a solicitação HTTP POST usando a função requests.post(). A opção "verify=False"é usada para desabilitar a verificação do certificado SSL, o que é útil para *endpoints* que usam certificados auto-assinados.

A resposta em formato de texto é impressa usando a função print(), que apresentará a resposta do *endpoint*, com as informações retornadas em formato JSON. Essas informações

podem incluir uma confirmação de que a configuração de rDNS foi bem sucedida ou informações de erro, dependendo do retorno do *endpoint*.

### 4.3.3 SPF - Sender Policy Framework

SPF se autentica na API do cPanel e adiciona uma entrada de registro TXT no DNS do domínio principal, a fim de configurar o SPF (Sender Policy Framework) do domínio. SPF é uma tecnologia de autenticação de e-mail que ajuda a prevenir o envio de spam e e-mails falsificados. Ele permite que o servidor de e-mail do destinatário verifique se o servidor que enviou o e-mail está autorizado a enviar e-mails para o domínio em questão.

SPF requer os parâmetros: *endpoint* da API do cPanel; o usuário cPanel; a chave de API cPanel; o domínio principal; e o endereço IP do servidor MTA. Em seguida, ele especifica o nome e valor da entrada TXT DNS com base nas informações recebidas. O valor da entrada TXT é definido como "v=spf1 a mx ip4: IP_do_servidor_MTA -all", que indica que o servidor de e-mail permitirá o envio de e-mails para o domínio especificado, a partir do próprio domínio (a), de qualquer servidor de correio (mx) e do endereço IP do servidor MTA (ip4).

Finalmente, o SPF verifica se a solicitação foi concluída com sucesso ou erro, dependendo do resultado da solicitação. Se houver algum erro, o algoritmo imprime uma mensagem de erro indicando que ocorreu um problema na criação da entrada TXT DNS. Se a solicitação for bem-sucedida, ele imprime uma mensagem indicando que a entrada TXT DNS foi criada com sucesso.

### 4.3.4 DKIM - DomainKeys Identified Mail

O protocolo DKIM é disponibilizado por meio de duas bibliotecas Python, sendo (1) *public_kay_dkim.py* e (2) *dkim.py*.

A (1) utiliza a biblioteca paramiko para estabelecer uma conexão SSH com um servidor de e-mail (MTA) especificado pelo usuário e obter a chave pública DKIM do domínio configurado no servidor.

São especificadas as informações de conexão SSH (YLONEN; LONVICK, 2006), SSH - *Secure Shell*(endereço IP do servidor, nome de usuário e senha) e, em seguida, o objeto SSHClient é criado e conectado ao servidor remoto com as informações fornecidas. O comando *amavisd-new showkeys* é enviado ao servidor para obter a chave pública DKIM. A execução resulta na chave pública DKIM do domínio configurado no servidor A conexão SSH é encerrada e o método é concluído.

O segundo (*dkim.py*) é utilizado para se autenticar na API do cPanel e adicionar uma entrada TXT DNS para o domínio especificado. O valor da entrada TXT é a chave pública DKIM obtida por (1) – na primeira biblioteca.

São definidas as informações de autenticação da API do cPanel (URL de *endpoint*, nome de usuário e chave de API). Em seguida, são definidas as informações do domínio (nome do domínio e nome da entrada TXT DNS a ser adicionada). O valor da entrada TXT é definido como a chave pública DKIM obtida anteriormente.

A solicitação inclui as informações de autenticação e os parâmetros necessários para adicionar a entrada TXT DNS para o domínio especificado. Se a solicitação for bem-sucedida (status HTTP *Hyper Text Transfer Protocol*, (FIELDING et al., 1999) 200), a resposta JSON é analisada e verificada se houve algum erro ao criar a entrada TXT DNS. Se não houver erros, a entrada foi criada com sucesso.

Em resumo, o primeiro serviço extrai a chave pública DKIM de um servidor de e-mail e o segundo serviço usa essa chave para criar uma entrada TXT DNS para o domínio usando a API do cPanel. Isso ajuda a autenticar e-mails enviados a partir desse domínio e aumenta a probabilidade de que eles sejam entregues com sucesso na caixa de entrada do destinatário.

### 4.3.5 DMARC - Domain-Based Message Authentication Message Conformance

O protocolo DMARC tem por objetivo auxiliar o plano de controle para um melhor sucesso da inserção DMARC no domínio em questão.

Para utilizar o serviço, é necessário informar o *endpoint* do cPanel, o usuário e a chave de API para autenticação, o domínio principal – onde a entrada DMARC será adicionada – e o email do administrador para onde os relatórios de DMARC devem ser enviados. Além disso, a função também define o nome e o valor da entrada TXT DNS a ser adicionada.

Ao ser executado, o algoritmo utiliza os parâmetros informados para criar uma entrada TXT DNS para a adição da DMARC no domínio especificado. A partir da autenticação na API do cPanel, a função utiliza os parâmetros informados para realizar a inserção da entrada TXT DNS por meio da chamada da API ZoneEdit.

Assim, ao utilizar este serviço, é possível facilitar o processo de inserção da DMARC no domínio em questão, aumentando as chances de sucesso e, consequentemente, melhorando o plano de controle para garantir a segurança e integridade do domínio.

### 4.3.6 Postfix

Este serviço permite modificar o arquivo de configuração principal do Postfix (POSTEL, 1982), que é armazenado em /etc/postfix/main.cf. Especificamente, ele substitui duas linhas do arquivo de configuração para garantir que a configuração do servidor de correio eletrônico esteja correta.

A primeira linha substituída é a *mydomain*. Por padrão, essa linha está definida com o FQDN do servidor. No entanto, para que a configuração esteja correta, a linha deve

conter apenas a definição do domínio principal. Portanto, o algoritmo substitui o FQDN pelo domínio principal.

A segunda linha modificada é a *mynetworks*. Essa linha define quais redes podem enviar e-mails através do servidor. Por padrão, essa linha está definida apenas com o endereço IP loopback, 127.0.0.1. No entanto, para que a configuração esteja correta, a linha deve conter a rede do servidor, além do endereço IP local. Portanto, o serviço adiciona a rede do servidor à lista de redes confiáveis.

Essas mudanças são importantes para garantir que o Postfix esteja configurado corretamente para o domínio principal e para o servidor específico em questão. Isso ajuda a garantir que o servidor possa enviar e receber e-mails corretamente e que a segurança esteja configurada corretamente para evitar atividades maliciosas, como spam.

## 4.4 Controle do Plano de Dados MHS

O plano de dados MHS é composto por agentes responsáveis por enviar e entregar envelopes (mensagens) desde o emissor até o(s) destinatário(s), conforme foi representado na Fig. 1. Controlar o plano de dados MHS consiste em identificar o(s) agente(s) que deve(m) ser provisionado(s), como pode ser observado nas relações (linhas laranjas) da SPAM-K com os MTAs, na referida Fig. 1.

O Plano de Dados MHS permite ter uma visão global dos estados dos agentes, incluindo agentes de diferentes provedores, e isto permite controlar de forma orquestrada e padronizada, seus comportamentos (dos agentes), reduzindo os falsos, positivos ou negativos. As adições (*Add-ons*) devem ser implementadas nos responsáveis por autenticações, onde (também) serão coletados dados, para posterior utilização em filtros, afim de determinar se uma mensagem é autentica ou não. Essas adições são implementadas nos servidores/agentes pertencentes ao plano de dados, sendo eles: DNS Autoritativo e MTA de Origem.

### 4.4.1 DNS Autoritativo

O servidor de DNS Autoritativo (SOA - *Start of Authority*) é responsável pelas informações originais do domínio, no qual os protocolos de autenticação SPF (*Sender Policy Framework*), DKIM (*Domain Keys Identified Mail*) e DMARC (*Domain-based Message Authentication Reporting e Conformance*), devem ser implementados. DNS Autoritativos pertencem ao provedor, onde o domínio foi contratado, ou podem ser de responsabilidade do administrador do domínio.

Se o servidor de DNS pertencer ao provedor, o administrador terá uma interface de administração para realizar as configurações. Caso seja um VPS de responsabilidade do

administrador, ele poderia optar por utilizar o comando *BIND* [1] ou o comando Role [2] no Windows Server.

### 4.4.2 MTA de Origem

MTA de origem é o agente responsável por receber o Envelope enviado por um UA (*User Agente* – cliente de e-mail) e iniciar o envio de Envelopes num plano de Dados MHS. Neste trabalho, o papel de MTA será desempenhado pelo servidor Postfix, disponível na distribuição do Sistema Operacional Linux Ubuntu Server 20.04. Além do MTA Postfix, o sistema operacional escolhido disponibiliza os outros pacotes necessários, tais como o Dovecot[3], RoundCube[4], entre outros, que foram instalados e configurados usando o *script iRedMail*.

A instalação padrão guiada pelo *script iRedMail*, por si só, realiza as configurações básicas necessárias para que o servidor MTA funcione corretamente. Todavia, em função da evolução das pesquisas realizadas neste trabalho, conforme descritas no Capítulo 3, percebeu-se que alguns ajustes seriam necessários para que o MTA (leia-se Postfix) tivesse resultados mais favoráveis, isto é, reduzisse de forma significativa os falsos.

Como mencionado acima, as pesquisas mostraram que alguns ajustes seriam necessários no MTA Postfix e, portanto, a seguir são descritas as alterações necessárias nos respectivos artefatos de configuração:

- `/etc/hostname`: deverá ser inserida uma entrada especificando apenas o nome do *host* do servidor, por exemplo `mx-01`;
- `/etc/hosts`: deverão ser inseridas duas linhas para especificar os valores de *loopback* e o FQDN do servidor, por exemplo:
  - `127.0.0.1 mx-01.projetoppgco.com.br mx-01`
  - `130.185.238.110 mx-01.projetoppgco.com.br mx-01`
- `/etc/postfix/main.cf`: o arquivo main.cf contém as principais configurações do servidor MTA, sendo que as seguintes linhas se mostraram importantes:
  - `mydomain = projetoppgco.com.br`
  - `mynetworks = 130.185.238.110/32, 127.0.0.0/8`
  - `relay_domains = $mydomain`

[1] BIND (MOCKAPETRIS, 1987a) (MOCKAPETRIS, 1987b), pode ser usado para executar um servidor de nomes autoritativo e fornece recursos como balanceamento de carga, notificação, atualização dinâmica, DNS dividido, DNSSEC, IPv6 etc

[2] O comando Role desempenha o papel de Servidor de DNS

[3] Dovecot é um servidor de IMAP (CRISPIN, 2003) e POP3 (ROSE; MYERS, 1996)*open source* para sistemas operacionais Linux

[4] Roundcube é uma aplicação Web IMAP, cliente de e-mail

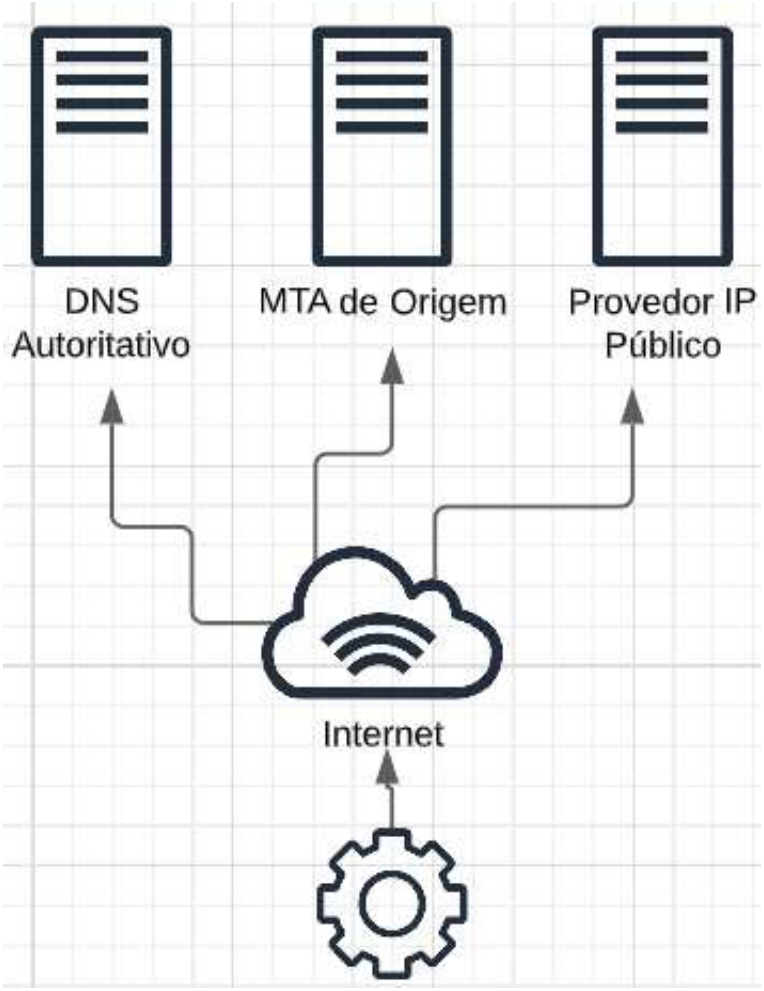



Figura 11 – SPAM-K controlando Plano de Dados MHS

Estas são alterações necessárias e que se mostraram eficazes para um melhor tratamento de mensagens pelos vários MTAs receptores. De acordo com os resultados apresentados no Capítulo 5, é possível afirmar que o desempenho aumenta consideravelmente no tangente à eliminação de falsos.

A Fig. 11 mostra a aplicação de controle desenvolvida no âmbito deste projeto, a SPAM-K, solicitando provisionamentos ao plano de dados MHS, notadamente: servidores de DNS Autoritativos, responsáveis pelo domínio, recebendo as entradas TXT relativas ao SPF, DKIM e DMARC; o servidor MTA responsável por envios, sendo atualizado com as alterações de *hostname*, FQDN e o servidor Postfix; e, por último, a configuração do DNS Reverso do provedor IP público.

É interessante ressaltar que todos esses provisionamentos são feitos, a todos os provedores MHS, que se inscrevam no Plano de Controle, isto é, na aplicação da camada de aplicação do plano de controle, SPAM-K, sendo que todas essas alterações são feitas automaticamente, sem a interação humana. Isto torna o processo de controle muito mais ágil e menos suscetível a erros ou esquecimentos.

## 4.5 SPAM-K: Implantação

Nesta fase do projeto, será executada a implantação do servidor de e-mail Postfix (MTA), que foi desenvolvido para atender às demandas específicas do projeto. Com a finalidade de garantir um funcionamento eficiente e seguro, serão realizadas as instalações e configurações necessárias. Todas essas atividades serão conduzidas após uma análise criteriosa dos resultados obtidos nos experimentos realizados no Capítulo 5.

Além disso, nesta etapa, serão realizadas as configurações de domínio e protocolos de autenticação e validação de e-mails. Isso é fundamental para garantir a integridade e a autenticidade das mensagens enviadas e recebidas pelo servidor. Os métodos que serão empregados aqui foram definidos com base em exigências mundiais de boas práticas no desenvolvimento de serviços de envio e recebimento de e-mails.

É importante ressaltar que a implementação adequada desses métodos é essencial para evitar que as mensagens dos clientes sejam banidas ou enviadas para a caixa de spam. Isso pode resultar em uma experiência negativa para os usuários, além de prejudicar a reputação da empresa. Portanto, é fundamental que todos os procedimentos sejam realizados com cuidado e atenção aos detalhes.

Nesse sentido, serão seguidos os padrões de configuração de DNS para garantir que os registros de DNS estejam corretamente configurados e atualizados. Além disso, serão realizadas as configurações de autenticação, tais como SPF, DKIM e DMARC, que garantem a autenticidade e a integridade das mensagens enviadas e recebidas pelo servidor.

Por fim, todas as configurações serão testadas para garantir que o servidor esteja funcionando de acordo com as especificações do projeto. Serão realizados testes de envio e recebimento de mensagens, bem como testes de autenticação e validação de e-mails.

Em suma, a etapa de implantação do servidor de e-mail é uma das mais críticas do projeto. Com a implementação adequada das configurações necessárias, será possível garantir a integridade, autenticidade e segurança das mensagens enviadas e recebidas pelo servidor, proporcionando uma experiência positiva para os usuários e protegendo a reputação da empresa.

### 4.5.1 Registro do Domínio

Para o registro do domínio "projetoppgco.com.br", foi escolhido o **Registro.br** como provedor de registro, uma vez que é muito utilizado no Brasil e possui servidores de DNS com delay bem menor em comparação com outros provedores fora do país.

Servidores de DNS do próprio Registro.br foram utilizados para o projeto, uma vez que, por estarem no Brasil, possuem um tempo de resposta menor, mesmo que em frações de segundos. Essa redução no tempo de resposta é muito importante, pois um "*delay* excessivo" pode fazer com que o servidor de destino interprete a mensagem de forma negativa.

Além disso, o Registro.br oferece uma plataforma de gerenciamento de domínios muito robusta e confiável, que permite aos usuários gerenciar seus domínios de forma simples e intuitiva. Essa plataforma oferece uma ampla gama de recursos e funcionalidades, incluindo a capacidade de gerenciar servidores de DNS, registros de MX, entre outras.

Outra vantagem do Registro.br é que ele oferece suporte técnico de alta qualidade, com uma equipe altamente qualificada e experiente. Isso garante que qualquer problema ou dúvida possa ser resolvido de forma eficiente.

É importante destacar que a escolha de um provedor de registro confiável é essencial para garantir a segurança do domínio. Um provedor de registro confiável pode ajudar a proteger o domínio contra ameaças como ataques de phishing e roubo de identidade, além de garantir que o domínio esteja sempre disponível para usuários.

### 4.5.2 Implementação do protocolo SPF

Como relatado na Seção 2.3.3, SPF é um protocolo de autenticação e validação de e-mails, para evitar falsos em entregas a destinatários. Neste projeto, as configurações do SPF foram realizadas, seguindo as boas práticas sugeridas pelo site "https://www.antispam.br", que consta nas referências desta obra.

Para implementar o SPF, foi adicionada registro do tipo TXT no arquivo da zona direta autoritativa do domínio "projetoppgco.com.br". Essa entrada segue as referências padrão de implementação, garantindo que o SPF esteja configurado corretamente e seguindo as boas práticas sugeridas pelo site "https://www.antispam.br".

Essa implementação do SPF é fundamental para garantir que mensagens de e-mail enviadas a partir do domínio "projetoppgco.com.br"sejam autenticadas e validadas corretamente, reduzindo assim a probabilidade de essas mensagens serem filtradas como spam pelos sistemas de e-mail dos destinatários. Além disso, essa implementação também ajuda a proteger a reputação do domínio, garantindo que ele seja reconhecido como um remetente confiável e legítimo.

Abaixo está a configuração desenhada para o projeto e a descrição de sua estrutura:

```
TXT projetoppgco.com.br "v=spf1 a mx ip4:130.185.238.110/24 -all"
```

Esse registro contém informações sobre as políticas de autenticação de e-mail para o domínio, permitindo que os servidores de e-mail dos destinatários verifiquem se uma mensagem de e-mail enviada a partir do domínio "projetoppgco.com.br"é legítima ou não. A estrutura da entrada SPF é composta por três elementos, sendo:

- i) **Versão**: neste caso indica o uso do SPF Versão 1 (`"v=spf1"`);
- ii) **Autenticação**: indica mecanismos de autenticação e validação de e-mail (`"a mx ip4:130.185.238.110/24"`), isto é, indica os mecanismos `"a"`, `"mx"`e `"ip4"`, que

significam, respectivamente, servidores de e-mail autorizados listados nos registros de endereço do domínio, servidores de e-mail autorizados listados nos registros `MX` e endereços IP autorizados que começam com "`130.185.238.110`"e pertencem à sub-rede com máscara de rede "`/24`"; e,

- iii) Ação Final de verificação de autenticação ("`-all`").

### 4.5.3 Implementação do protocolo DKIM

Foi utilizado o protocolo de autenticação de e-mail DKIM disponibilizado pelo OpenDKIM. A seleção se deve ao fato de ser uma implementação de código aberto, ser recomendado pelo *Signing Technology Group* (ESTG) e ser uma ferramenta padronizada pelo RFC 6376 (**??**). Além disso, o OpenDKIM possui implementações de padrões propostos pelo RFC 5617 (ALLMAN et al., 2009). Essas RFCs foram desenvolvidas para melhorar a eficácia da autenticação de e-mails, garantindo maior segurança e reduzindo a possibilidade de fraudes eletrônicas.

Para a instalação do MTA, utilizou-se o *script* "iRedMail", que é capaz de instalar e configurar automaticamente todos os componentes necessários para o servidor de correio eletrônico. Dessa forma, o componente responsável pela instalação do método de autenticação DKIM é o Amavis, que é instalado pelo script do iRedMail.

Amavis é responsável por instalar o método de autenticação DKIM, que por sua vez, é instalado automaticamente pelo *script* do iRedMail, garantindo que o servidor de correio eletrônico já esteja configurado com o DKIM no momento da instalação.

Em resumo, a escolha do OpenDKIM como método de autenticação de e-mail, aliado à utilização do iRedMail para a instalação do MTA e a instalação automática do Amavis para configuração do DKIM, garantem maior segurança e eficácia na autenticação de e-mails. A chave privada foi gerada através do comando abaixo:

```
amavisd-new genrsa /etc/dkim/keys/projetoppgco.com.br.pem
```

A chave pública será informada pelo comando abaixo:

```
amavisd-new showkeys
```

Para os primeiros testes, serão utilizadas configurações de forma padrão, sendo assim, será criada, no servidor de DNS Autoritativo do domínio "`projetoppgco.com.br`", uma entrada do tipo `TXT`, informando a chave pública da forma especificada abaixo, sendo que o servidor manterá sua chave privada, para, quando necessário, realizar a checagem da chave pública recebida com sua chave privada, confirmando assim a autenticidade do e-mail.

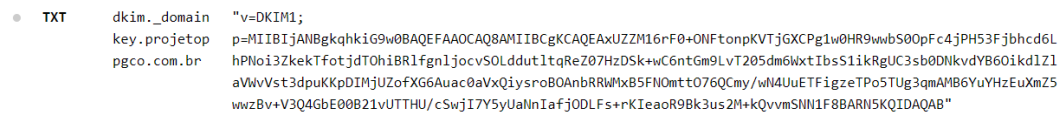



Figura 12 – Entrada Dkim contida no DNS Autoritativo do domínio

### 4.5.4 Implementação do protocolo DMARC

Na Seção 2.3.5 foi apresentado o protocolo DMARC, especificado para garantir a integridade de mensagens e determinar ações que o(s) destinatário(s) deve(m) tomar em caso de falha de autenticação dos protocolos SPF ou DKIM. A configuração DMARC utilizada nos primeiros experimentos foi adicionada como uma entrada do tipo `TXT` no DNS Autoritativo do domínio.

A entrada DMARC especifica que, caso ocorra falha na autenticação do SPF ou DKIM, a mensagem deve ser enviada para quarentena. Além disso, um relatório será enviado ao emissor da mensagem pelo e-mail "`wesley@projetoppgco.com.br`". A configuração também indica que os subdomínios não serão verificados e que todas as mensagens enviadas devem ser verificadas com um nível de verificação de 100%.

Essa configuração garante que apenas mensagens autenticadas pelo SPF ou DKIM serão entregues aos destinatários, reduzindo o risco de e-mails fraudulentos ou mal-intencionados. Ao enviar mensagens não autenticadas para quarentena, a configuração DMARC ajuda a proteger os usuários finais contra ameaças cibernéticas, garantindo a integridade da mensagem e aumentando a confiança do usuário no domínio.

Para implementar essa configuração, foi necessário adicionar a entrada DMARC como um registro TXT no servidor DNS Autoritativo do domínio. Essa configuração foi testada e ajustada para atender às necessidades do projeto. Além disso, foi importante garantir que a equipe responsável pelo domínio estivesse ciente da importância do DMARC e de como ele funciona para manter a segurança do domínio e dos usuários finais.

Com a implementação do DMARC, o domínio agora tem uma camada adicional de proteção contra ameaças cibernéticas, garantindo que apenas mensagens autênticas sejam entregues aos destinatários. Além disso, a configuração DMARC permite que o emissor da mensagem seja informado caso ocorra uma falha de autenticação, aumentando a transparência e a responsabilidade no processo de envio de mensagens.

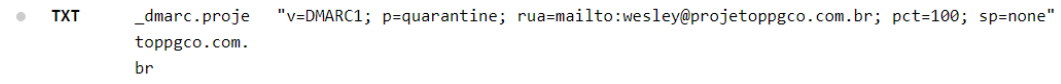



Figura 13 – Entrada Dmarc contida no DNS Autoritativo do domínio

### 4.5.5 Escolha do VPS (*Virtual Private Server*)

No desenvolvimento de um projeto, é essencial escolher um provedor de VPS/Cloud que atenda às necessidades da aplicação, especialmente quando se trata de servidores de e-mails (MTA). Todavia, encontrar uma empresa que permita a locação de servidores sem restrições pode ser um desafio, já que muitos provedores temem que seus servidores sejam utilizados para a propagação de spam.

Um VPS (*Virtual Private Server*) é uma tecnologia de virtualização que permite a locação de servidores com acesso total via SSH. O usuário tem a liberdade de realizar as configurações necessárias para criar o servidor que desejar. No entanto, para a criação de um servidor de e-mail, é necessária a liberação da porta 25 para a comunicação entre os MTAs.

Muitos *Data Centers*, que alugam VPSs, não liberam a porta 25 por questões de segurança. O motivo é que, se uma porta não for bloqueada, um usuário mal-intencionado pode utilizar o servidor para enviar spam ou realizar outros tipos de ataques. Por isso, a liberação da porta 25 é bloqueada por padrão em muitas empresas de hospedagem de servidores virtuais.

Por exemplo, a AWS (*Amazon Web Services*) bloqueia a porta 25. Nela, é necessária uma solicitação para a liberação da porta 25, que pode demorar bastante tempo e envolver muita burocracia.

Foi escolhido o *Data Center B Host Brasil*, que oferece total liberdade para uso de todas as portas necessárias, inclusive a porta 25. Basicamente, a escolha da *B Host Brasil* se deveu por ela permitir a configuração total do servidor, sem restrições e com a liberação da porta 25, o que é fundamental para o funcionamento de um servidor de e-mails.

As configurações da VPS são as seguintes:

- ❑ **Hostname Atual:** `mx-01.projetoppgco.com.br`
- ❑ **IP Público Primário:** `130.185.238.110`
- ❑ **Processador:** 2 vCore
- ❑ **Memória RAM:** 6GB
- ❑ **Espaço em Disco:** 70GB SSD
- ❑ **Rede:** 1Gbps Burst
- ❑ **Tráfego Mensal:** Ilimitado (FUP*)

Entende-se que não são configurações ideais para um ambiente de produção, porém, em se tratando de pesquisas, capacidade é bem razoável, pois os testes são executados em ambiente de laboratório, simulando a realidade.

## 4.6 Configurações do Servidor

Na Seção 4.1.1 foram introduzidos os parâmetros de configuração de um provedor MHS, sendo que alguns daqueles parâmetros são utilizados diretamente na configuração do servidor. Esta seção tem o objetivo de dirigir pelos arquivos de configurações para que o servidor funcione adequadamente.

### 4.6.1 Configuração de `hostname`

O `hostname` é um arquivo, em sistemas operacionais Unix, responsável por armazenar o nome do servidor. O conteúdo do arquivo `hostname` deve ser **tão somente o nome do servidor**, como por exemplo "`mx-01`".

No entanto, em alguns servidores analisados, foi observada uma prática comum em que o nome do servidor era seguido pelo seu domínio, um FQDN (*Fully Qualified Domain Name*), tal como "`mx-01.projetoppgco.com.br`". Essa prática é incorreta, pois o sufixo do `hostname` é de responsabilidade do arquivo `hosts`, que é descrito em outro tópico.

Em algumas distribuições Linux, como o Ubuntu, o arquivo `hostname` é utilizado apenas para exibição de informações, sendo que as informações de resolução de nomes são obtidas exclusivamente a partir do arquivo `hosts`. Entretanto, para criar um padrão de configuração, que funcione em quaisquer distribuições Linux, é importante seguir a prática recomendada de preencher o arquivo `hostname` apenas com o nome do servidor, sem adicionar o sufixo do domínio.

Dessa forma, é possível garantir que a configuração do servidor será correta e que a resolução de nomes ocorrerá da maneira adequada. É importante lembrar que o arquivo `hostname` pode ser encontrado em diferentes diretórios, dependendo da distribuição Linux utilizada. Em geral, ele é encontrado em `/etc/hostname`.

Em resumo, a utilização correta do arquivo hostname é fundamental para a correta configuração de servidores Linux. É importante preencher o arquivo apenas com o nome do servidor, sem adicionar o sufixo do domínio. Dessa forma, é possível garantir uma configuração adequada e uma resolução de nomes eficiente.

### 4.6.2 Configuração de `hosts`

O arquivo `hosts` é responsável por informar o FQDN do servidor, que nada mais é do que o nome do servidor (*hostname*) seguido do domínio, por exemplo:

```
130.185.238.110 mx-01.projetoppgco.com.br mx-01
```

Parece uma coisa corriqueira, mas a configuração nestes moldes garante que o nome do servidor será corretamente especificado e, assim, torna-se uma abordagem sumamente importante para sucesso no servidor de e-mails, reduzindo bastante os falsos positivos.

Durante as pesquisas, pode-se observar que alguns servidores de e-mail tiveram suas mensagens enviadas para o lixo eletrônico, pois houve uma informação não coerente com seu FQDN, precisamente, pela falha de configuração do arquivo `hosts`.

A correta configuração deste arquivo é muito importante, pois ele informa ao MTA receptor qual é o FQDN do servidor de e-mails remetente, e, dessa forma, o receptor faz uma checagem no DNS Reverso referente ao domínio do remetente, para comparar com o valor especificado no arquivo `hosts`.

Um fato que também foi observado, durante as pesquisas, é que a informação referente ao endereço de *loopback*, contido no arquivo `hosts`, em sua forma tradicional seria:

```
127.0.0.1          localhost
```

Em algumas literaturas, são recomendados os seguintes ajustes na especificação do *localhost*, complementando a segunda coluna com o FQDN e na terceira coluna com o `hostname` *localhost*, como pode ser observado a seguir:

```
127.0.0.1      localhost.localdomain      localhost
```

Até onde foi possível testar, esta abordagem está correta, todavia, há provedores de correio eletrônico, como por exemplo a Microsoft, que entende que esta informação é

talvez desnecessária, uma vez que *localhost* significa computador local, mas não especifica com clareza o IP relacionado ao FQDN, cuja informação é comparada com o seu respectivo DNS Reverso, mesmo contendo uma segunda linha explicada a posteriori.

A correta especificação da linha referente ao *localhost*, para o domínio `projetoppgco.com.br` tem a seguinte forma:

```
127.0.0.1      mx-01.projetoppgco.com.br      mx-01
```

A segunda linha que deve ser configurada no arquivo `hosts`, especifica a relação direta do endereço IP com o FQDN, sendo essa a principal informação fornecida, quando o receptor a solicitar. Entretanto, existem provedores que analisam também a linha relacionada ao *localhost* como explicado anteriormente. Deste modo, a seguir é apresentada uma configuração do arquivo *hosts*, contendo as duas linhas especificadas anteriormente:

```
127.0.0.1           mx-01.projetoppgco.com.br      mx-01
130.185.238.110     mx-01.projetoppgco.com.br      mx-01
```

A adoção deste padrão de configuração do arquivo *hosts*, até onde foi possível observar nos testes em laboratório, resultou em uma redução importante dos falsos positivos de mensagens enviadas aos provedores de correio eletrônico relacionados.

### 4.6.3 Configuração do Postfix

O principal arquivo de configuração do Postfix (MTA deste projeto) é denominado por `mail.cf`. Este arquivo contém linhas de configuração para envio e recebimento de envelopes pelo Postfix.

Na instalação *default* do Postfix, o arquivo `mail.cf` é configurado com as configurações padrão, que não suficientes para diminuir os falsos. Deste modo, são necessários ajustes para melhorar o desempenho do servidor em vários aspectos, inclusive no aspecto de interesse deste trabalho, isto é, reduzir falsos positivos de spam.

Testes realizados com as configurações *default* do arquivo `mail.cf`, havidas por meio do *script iRedMail*, apresentaram a ocorrência de falsos positivos, mesmo considerando que os outros arquivos de configuração (`hostname` e `hosts`) já estavam configurados adequadamente. Isto nos mostrou que customizações no arquivo `mail.cf` são necessárias para atingir o objetivo deste trablaho.

Deste modo, vários outros ajustes foram necessários para a redução significativa de falsos positivos, como serão apresentados no decorrer desta seção, destacando as configurações adicionais realizadas no arquivo `main.cf`, conforme são descritas abaixo.

Padrão de configuração do *script iRedMail*:

```
mydomain = mx-01.projetoppgco.com.br
```

Alteração necessária:

```
mydomain = projetoppgco.com.br
```

Linhas a serem necessariamente adicionadas:

```
mynetworks = 130.185.238.110/32, 127.0.0.0/8
relay_domains = $mydomain
```

O parâmetro "mydomain"informa qual é o domínio principal responsável por enviar mensagens, informação essa que será solicitada por alguns filtros *antispam* de alguns MTA receptores. Se a resposta é o FQDN e não o Domínio, então o MTA Receptor pode entender que esta inconsistência é um problema, podendo o e-mail ser enviado para o lixo eletrônico.

O parâmetro "`mynetworks`"determina quais redes estão autorizadas a encaminhar e-mails, sendo importante especificar que somente sua rede tem essa autorização. Isso impõe uma maior confiança, sendo que alguns filtros analisam esta informação.

Por fim, o parâmetro "relay_domains"especifica que apenas ao domínio principal será permitida a retransmissão. Essa informação é consultada por diversos filtros *antispam*. Deste modo, a forma final da configuração do arquivo `main.cf` seria, por exemplo:

```
mydomain = projetoppgco.com.br
mynetworks = 130.185.238.110/32, 127.0.0.0/8
relay_domains = $mydomain
```

## 4.7 Boas Práticas

Durante as pesquisas bibliográficas, análise de trabalhos correlatos e, mormente, investigação de provedores estabelecidos na Internet, foi possível observar que algumas práticas, até simples, não são observadas no projeto e implantação de soluções de correios eletrônicos. Esta constatação reforça a importância de um plano de controle, como a SPAM-K, e evidências algumas práticas que podem ser categorizadas como "boas práticas", que são relatadas nas próximas seções.

### 4.7.1 Gerência de Porta 25

Com a adoção de criptografia por aplicações clientes de e-mail, inclusive para uso particular doméstico, a porta 587 passou a ser obrigatória, por razões de segurança, em particular, de confidencialidade. No caso de WebMails (cliente de e-mail no navegador), também não é utilizada a porta 25, sendo neste caso, utilizada a porta de serviços Web. Após essas considerações de clientes de e-mail (UA), as seguintes considerações são pertinentes em relação à porta 25:

- ❏ Alteração da porta 25 para a porta 587 em UAs (clientes de e-mail), pelas razões de segurança e confidencialidade, apontadas no início deste parágrafo;
- ❏ Adoção de autenticação para submissão de mensagens, conforme recomendado pela RFC 4954 (SIEMBORSKI; MELNIKOV, 2007);
- ❏ Realizar o bloqueio da saída para a porta 25, para máquinas (todas) que executam clientes de e-mail, que não sejam, portanto, MTAs.

A gerência da porta 25 é importante para mitigar aspectos de segurança e da qualidade de serviço percebida por usuários, podendo ser citadas:

- ❏ Redução de envios de spams;
- ❏ Com a redução de mensagens indevidas, usuários tendem a reclamar menos em relação a utilização de sua banda; e
- ❏ Reduz a possibilidade de fraudes (*fishing*), entre outros males;

### 4.7.2 Programa Junk Mail da Microsoft

JMRP (*Junk Mail Report Program*) é uma iniciativa da Microsoft para diminuir a incidência de falsos em seus provedores, tais como Hotmail e Outlook. Com mais de 60 filtros dinâmicos para barrar mensagens indesejáveis, o desafio é entregar mensagens fidedignas na caixa de entrada do Hotmail. Devido a esses filtros, muitas mensagens importantes são classificadas erroneamente e endereçadas para a caixa de spam ou para a lixeira (*Junk Mail*).

JMRP permite que provedores façam parte do programa de combate a spams. Esta iniciativa da Microsoft permite que provedores se cadastrem no programa e comecem a receber relatórios especificando os motivos pelos quais mensagens de seus provedores foram categorizadas como spam. Dessa forma, ao fazer parte do programa[5], os filtros da Microsoft aumentam sua confiança e mensagens importantes sejam entregues normalmente na Caixa de Entrada.

Vale destacar que, além dos desafios específicos relacionados ao Hotmail, é importante que provedores de e-mail estejam em conformidade com práticas de segurança, implementando protocolos de autenticação de e-mails, tais como o SPF, DKIM e DMARC, introduzidos na Seção 2.3. Esses protocolos são essenciais para evitar spams, garantindo a autenticidade de remetentes e aumentando a confiança em e-mails enviados.

### 4.7.3 *Relays* Abertos

*Relay* é uma capacidade que MTAs podem ter de retransmitirem mensagens recebidas de outros MTAs. *Relay* Aberto é dito quando o MTA está apto a retransmitir mensagens de MTAs desconhecidos. *Relays* Abertos são uma fraqueza para MHSs, uma vez que MTAs mal-intencionados usam esta fragilidade para enviar spams através de MTAs com boa reputação. Além disso, o uso de *relays* abertos por servidores mal-intencionados também permite que remetentes de spams permaneçam anônimos, uma vez que e-mails chegam a destinatários contendo cabeçalhos de origem do servidor MTA com *Relay* Aberto e não do spammer.

Todavia, existem MTAs, como o Postfix, que possuem por *default* configurações que bloqueiam tais retransmissões, isto é, "fecham o *relay*". Isso significa que, nos dias atuais tende a ser cada vez menos comum encontrar servidores de e-mail com *relays* abertos. No entanto, ainda é possível configurar o servidor para permitir retransmissões de domínios e IPs especificados pelo administrador de redes.

Ao implantar um servidor de e-mails, é fundamental verificar se o *relay* está realmente fechado. Isso pode ser facilmente feito por meio de plataformas confiáveis, como a `mxtoolbox.com`, que fornece ferramentas de diagnóstico para verificação de servidores

[5] Para participar deste programa acesse o link https://postmaster.live.com/snds/data.aspx

de e-mail. Abaixo é apresentado um teste de *Relay* Aberto, realizado pela plataforma https://mxtoolbox.com.

```
Connecting to 130.185.238.x
220-mx-01.projetoppgco.com.br ESMTP Postfix
220 mx-01.projetoppgco.com.br ESMTP Postfix [6969 ms]
EHLO keeper-us-east-1d.mxtoolbox.com
250-mx-01.projetoppgco.com.br
250-PIPELINING
250-SIZE 15728640
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING [250 ms]
MAIL FROM: <supertool@mxtoolboxsmtpdiag.com>
250 2.1.0 Ok [459 ms]
RCPT TO:<test@mxtoolboxsmtpdiag.com>
554 5.7.1 <test@mxtoolboxsmtpdiag.com>:  Relay access denied [454 ms]
```

O resultado acima descrito apresenta as informações do teste de *Relay* e, na última linha, é possível verificar o resultado que interessa, que o *relay* do servidor está com acesso negado.

### 4.7.4 Reputação do MTA

Manter o MTA com uma boa reputação é fundamental para aumentar as chances de entrega de mensagens na caixa de entrada de destinatários. Quando a reputação de um servidor de e-mails diminui, a possibilidade de ter suas mensagens barradas aumenta significativamente.

A reputação de servidores de e-mails é medida por vários fatores, como a quantidade de spam reportado pelos destinatários, a quantidade de endereços inválidos ou inexistentes utilizados nas mensagens enviadas, o histórico de envio de mensagens, a autenticação dos e-mails (SPF, DKIM e DMARC), entre outros. É importante lembrar que os filtros anti-spam estão sempre atualizando suas regras para barrar o máximo de spam possível e um servidor de e-mails com má reputação pode ser facilmente detectado e bloqueado.

Para manter uma boa reputação do servidor de e-mails, é importante tomar algumas medidas como:

- ❏ Verificar regularmente as listas de spam reportadas por destinatários e tomar providências rapidamente em relação a elas, removendo, por exemplo, endereços inválidos ou inexistentes;

- ❏ Implementar e manter atualizadas as políticas de autenticação de e-mails (SPF, DKIM e DMARC), para garantir que mensagens sejam enviadas apenas por servidores autorizados;

- ❏ Evitar o envio de mensagens em massa para listas de contatos, listas compradas por exemplo, pois isso aumenta a possibilidade de mensagens serem consideradas spam; e,

- ❏ Ter uma boa estratégia de conteúdo para e-mails, evitando palavras ou termos que sejam frequentemente associados a spam.

Em resumo, manter uma boa reputação do servidor de e-mails é essencial para garantir a entrega das mensagens na caixa de entrada dos destinatários, evitar falsos positivos de spam e aumentar a credibilidade da empresa ou organização. Por isso, é importante adotar boas práticas de segurança e envio de e-mails, e estar sempre atento às atualizações e mudanças nos filtros anti-spam. Abaixo está descrito os fatos que mais interferem para a conquista e permanência de uma boa reputação:

#### 4.7.4.1 Aquecimento do Domínio

O processo de atribuição de um novo endereço IP a um servidor de e-mails pode trazer problemas de entrega. Isso se deve ao fato de que o endereço IP (leia-se Domínio) não possui nenhuma reputação, o que significa que, se enviar e-mails através dele, é muito provável que a mensagem seja entregue no lixo eletrônico ou bloqueada pelo receptor.

Para evitar esse problema é importante "aquecer" o endereço IP ou Domínio. O aquecimento consiste em enviar e-mails de forma programada, começando com volumes menores nos primeiros dias e aumentando gradualmente com o passar do tempo. É importante manter uma constância nos envios durante o período de aquecimento para evitar que uma variação brusca resulte na queda da reputação que está sendo adquirida.

Além disso, o processo de aquecimento deve ser feito de forma estratégica e com cautela, evitando enviar grandes volumes de e-mails de uma só vez, o que pode ser interpretado pelos provedores de e-mails como um comportamento suspeito ou mal-intencionado.

É preciso lembrar que o processo de aquecimento do IP ou do domínio é uma parte essencial da estratégia de e-mail marketing e deve ser planejada cuidadosamente. É importante também monitorar constantemente a reputação do IP ou do domínio, para garantir que ela esteja sempre positiva e, caso necessário, fazer ajustes na estratégia de envio de e-mails.

#### 4.7.4.2 Higienização das Listas

A entrega adequada a destinatários é fundamental para o sucesso do envio de e-mails. Isso porque, se os receptores marcarem os e-mails como spam, a reputação do remetente será afetada negativamente, o que pode prejudicar a entrega na Caixa de Entrada. Portanto, é importante manter uma lista de destinatários saudável e com boa reputação para garantir que os e-mails sejam entregues com sucesso.

A entrega positiva a destinatários é essencial para o sucesso do envio de e-mails. Essa entrega pode ser medida por meio da abertura, leitura, resposta, remoção orgânica de mensagens que forem consideradas como spam e cadastro na lista de contatos. Quanto mais entrega positiva houver, maior será a reputação do remetente e, consequentemente, maior será o sucesso dos envios.

Para evitar que os e-mails sejam considerados spam pelos destinatários, é importante seguir algumas boas práticas, como enviar apenas para os destinatários que deram permissão para receber os e-mails, personalizar o conteúdo de acordo com o perfil dos destinatários e evitar enviar e-mails em massa sem segmentação adequada.

Além disso, é importante monitorar constantemente a interação de destinatários com e-mails enviados, para identificar possíveis problemas e ajustar a estratégia de envio de e-mails, caso necessário. É possível utilizar ferramentas de análise de métricas para medir a interação dos destinatários com os e-mails e identificar quais são os e-mails que estão sendo mais bem recebidos pelo público-alvo.

Capítulo 5

# Experimentos e Análise dos Resultados

Este capítulo é dedicado à descrição dos procedimentos de implantação do ambiente desenvolvido, dos experimentos realizados e à análise dos resultados obtidos durante os experimentos. Foram avaliadas a efetividade dos provisionamentos a partir do Plano de Controle materializado pela SPAM-K, bem como, foram levantados dados relativos aos envios propriamente ditos de mensagens, e foram verificadas a eficácia da boas práticas e configurações de MHSs.

A preparação dos experimentos começa com a escolha de provedores de Correio Eletrônico (MHS) disponíveis na Internet, e a criação de contas nesses provedores, sendo que a Tabela 1 relaciona os 10 provedores utilizados nos experimentos e especifica o número de contas criadas em cada um deles.

Tabela 1 – Relação de Provedores MHS

| | **Provedor** | **Número de Contas** |
|---|---|---|
| 1 | AOL | 7 |
| 2 | Sapo | 3 |
| 3 | Fastmail | 7 |
| 4 | GMX | 3 |
| 5 | Google | 10 |
| 6 | Microsoft | 7 |
| 7 | Protonmail | 4 |
| 8 | UFU | 1 |
| 9 | Yahoo | 10 |
| 10 | Yandex | 4 |

A escolha dos provedores da Tabela 1 foi baseada no fornecimento de e-mails gratuitos a usuários, pela amplitude de oferta mundial, sendo que cada um deles conta com particularidades em relação ao comportamento de seus filtros anti-SPAM. No entanto, todos seguem regras de validação adotadas mundialmente, como sendo realmente eficientes.

O MHS da UFU foi utilizado por meio da conta institucional do mestrando. A relação de provedores MHS, bem como a quantidade e a identificação das contas de e-mails criadas

nestes provedores podem ser encontradas no Apêndice A.

Foi elaborado um plano contendo uma sequencia de envio de e-mails, incluindo todos os provedores (Tabela 1) e contas nomeadas no Anexo A, com o seguinte critério. Primeiramente, foi executado o plano sem o envolvimento do plano de controle materializado pela SPAM-K. O resultado da execução desse plano é relatado na Seção 5.1.

Depois, considerando que o *iRedMail* é um *script* largamente utilizado para a implantação de servidores de email por provedores, a Seção 5.2 apresenta a aplicação do plano utilizando um MTA configurado pelo referido *script*.

Como descrito no Capítulo 3, para a verificação da efetividade do proposto neste trabalho, foi necessária a implementação de um MTA de referência, para desempenhar o papel de uma agente que pertença a um MHS controlado pela SPAM-K. A Seção 5.3 apresenta a execução do plano a partir do MTA de Referência, controlado pela SPAM-K.

## 5.1 Envio entre Provedores sem SPAM-K

Nesta primeira fase foram realizados envios entre os provedores enumerados na Tabela 1, sendo que os experimentos foram feitos usando os referidos provedores sem os provisionamentos orquestrados pela SPAM-K. Os envios de mensagens foram realizados tendo como alvos os provedores Yahoo, Google e Microsoft, a partir de domínios públicos e gratuitos como GMX, AOL, Sapo, Fastmail, Protonmail, Yandex, e UFU. Este experimento inicial está relacionado à importância de se entender as falhas por parte dos emissores, sem orquestração de provisionamentos pela SPAM-K, formando assim a base inicial para comparação.

Serão analisados, através do cabeçalho das mensagens recebidas pelos provedores Google, Microsoft e Yahoo com origem em AOL, GMX, Fastmail, Protonmail, Yandex, UFU e também Google, Microsoft e Yahoo, observando-se a correta configuração dos autenticadores SPF, DKIM e DMARC, também através do *header* é possível verificar o FQDN e o endereço IP do servidor MTA emissor e, posteriormente através do comando NSLOOKUP, pode-se constatar se o DNS Reverso informado bate com aquele informado pelo *header*.

Outras verificações se fazem importantes, como a presença do IP do MTA emissor em listas de bloqueio e em banco de dados importantes. Outro fato seria verificar se seu *relay* está aberto e verificar o score de reputação do MTA, uma vez que diversos receptores, como a Microsoft, analisam esta informação para tomar decisões sobre mensagens recebidas.

Será dada ênfase a envios destinados aos 3 maiores provedores, sendo Microsoft, Gmail e Yahoo, considerando que reclamações de clientes reportam um grande percentual de falsos positivos relativos a esses 3 provedores.

### 5.1.1 Envios de AOL, Fastmail, Microsoft e Yahoo para GMail

Nesta seção, serão analisados os experimentos de envios a partir dos provedores AOL, Fastmail, Microsoft e Yahoo tendo como destino o provedor GMail. Para facilitar a compreensão, cada um dos provedores enviadores mencionados terão uma seção na qual serão reportados os achados dos experimentos realizados.

#### 5.1.1.1 Envios do AOL para GMail

Os resultados reportados nesta seção se referem a envios a partir do provedor AOL (`aol.com`), com base em análises de leituras realizadas a partir dos resultados obtidos através do *header* informado pelo Google (Fig. 14), pertencente ao e-mail recebido por um cliente AOL, pode-se observar que não houve insuficiência de parâmetros para a validação, que causariam falsos positivos, isto é, os protocolos SPF, DKIM e DMARC foram configurados de forma correta.

A análise subsequente informa que o endereço IP do servidor MTA da AOL, aponta corretamente para o FQDN informado pelo *header* (Fig. 14), indicando uma correta configuração de seu DNS Reverso, conforme pode ser observado na Fig. 15.

A análise subsequente detecta a presença do endereço IP do servidor MTA do AOL listado no *Spam and Open Relay Blocking System* (SORBS) SPAM[1], doravante referenciado como SORBS SPAM. A presença nesta lista indica que o servidor de e-mails do AOL está contido em uma lista de bloqueio importante (`mxtoolbox.com`). Esta ocorrência pode ocasionar a presença de falsos positivos de SPAM, conforme pode ser observado na Fig. 16.

A próxima análise seria para verificar se o servidor está com seu *relay* aberto, o que não foi possível, pois o servidor não permitiu a consulta, como mostra a Fig. 17. Todavia, como consta na lista de bloqueio do SORBS SPAM, e se trata de um banco de dados que também informa MTAs com *relays* abertos, é possível que o servidor esteja com seu *relay* aberto.

O resultado da análise, realizada pelo site `mail-tester.com`, mostra o AOL com 9 de 10 pontos possíveis, conforme pode ser visto na Fig. 18. De acordo com o referido site, o principal motivo de não ter obtido 100% da pontuação é devido ao fato de seu endereço IP estar contido em duas listas de bloqueio importantes, conforme pode ser observado na Fig. 19

Foram enviadas diversas mensagens a partir do AOL para os provedores mencionados neste capítulo. Os relatórios aqui descritos foram obtidos por amostragem, sendo que os experimentos foram monitorados durante um período de 4 meses. Os resultados auferidos são apresentados na Fig. 20.

[1] Proofpoint, Inc. (`sorbs.net`) é proprietária e opera o SORBS

É interessante observar que mesmo sendo o AOL um provedor conhecido, houve mensagens oriundas de seus servidores que foram classificadas como lixo eletrônico. Provavelmente, o fato de seu endereço IP estar contido em duas listas de bloqueio, e isto ter influenciado na sua pontuação, contribuiu para essas classificações.


```
Delivered-To: ricardosoaresitba@gmail.com
Received: by 2002:adf:ed06:0:0:0:0:0 with SMTP id a6csp3283217wro;
        Tue, 1 Nov 2022 17:07:33 -0700 (PDT)
X-Google-Smtp-Source: AMsMyM7uoEsBfqS5/o8Q7DNtdPFrSf7gidBahu2fJh9AZ6mnAd3w1AkYJ+RqGiHzlWgST1J/HCJq
X-Received: by 2002:a05:622a:252:b0:3a5:73a:1aa3 with SMTP id c18-20020a05622a025200b003a5073a1aa3mr17687278qtx.482.1667347653540;
        Tue, 01 Nov 2022 17:07:33 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1667347653; cv=none;
        d=google.com; s=arc-20160816;
        b=j1UfwfZTDECGjpGdtLEvNchsr0u61hhLUMPrMn5Jpcue19JqLK5LpH1CnjldaJVcC6
         tNC7PNfi/H+OyrlVd1Mz200FQuMc9n+usfmP4BTcbgWmD79YXih16nvPDMgY2T3ONpKR
         bRGNjJL9gvH7OEnK/ozh82XjRbkEYowkxnbiJsFAtXQ1LHN1F34K8jih9m/W0rsZg7hK
         vFDOm37nZqcENOMICTz/orF+wmrYvOhAT4ROcL4wQLPg3l1fdhpwD4CG1rfjX3BiOJmW
         +0pJdMgW5KoYO5hUCgqVcOq/SOC3OJ4Dy4tsKNxpVJ2Sd75cA8+0amTnEPh6BDpXtfWQ
         dRng==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=references:mime-version:subject:message-id:to:reply-to:from:date
         :dkim-signature;
        bh=a69hPVrCmWG8uyM6GjsroOVrDkqEOLvsay/d7AFbCTw=;
        b=cxX4kEGFzcAaIw/rsC6KkWve4p/UC3PF3DcGDOLMKubKC6eMsG7+BnRTBXJrUKfxGy
         V3XbnLQQk/XOl9bxhbOBA52TUzRXc0Gpu8SMIL0IoIutAuiAEP0gEgL2SLyIsA72f2n4
         8BRf8ZjBEM/vxhVJzrxu/FUsGXuvcu6gypZ++kQe3ePQymNkapNPPdljRPeRt7hjVKuw
         YUtGxpz577WGtFVp/vLXPVtpXuWw7kycb/WItm0GhDwq3cRjap9/nF7/DpRyuCOfa5iC
         QNBfupx7x7l2qaup8swA22oJydbjglpRS9uQlcSQB2W/SVGTooCEAfEhLzF8BSO5iKqP
         KaUw==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@aol.com header.s=a2048 header.b=X94PxjH5;
       spf=pass (google.com: domain of andrealimaitba@aol.com designates 66.163.187.147 as permitted sender) smtp.mailfrom=andrealimaitba@aol.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=aol.com
Return-Path: <andrealimaitba@aol.com>
Received: from sonic316-21.consmr.mail.ne1.yahoo.com (sonic316-21.consmr.mail.ne1.yahoo.com. [66.163.187.147])
        by mx.google.com with ESMTPS id kj23-20020a056214529700b004acbe62d31fsi6629650qvb.183.2022.11.01.17.07.33
        for <ricardosoaresitba@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
        Tue, 01 Nov 2022 17:07:33 -0700 (PDT)
Received-SPF: pass (google.com: domain of andrealimaitba@aol.com designates 66.163.187.147 as permitted sender) client-ip=66.163.187.147;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@aol.com header.s=a2048 header.b=X94PxjH5;
       spf=pass (google.com: domain of andrealimaitba@aol.com designates 66.163.187.147 as permitted sender) smtp.mailfrom=andrealimaitba@aol.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=aol.com
```


Figura 14 – *Header* Google - Mensagem recebida do AOL


Figura 15 – DNS Reverso do AOL

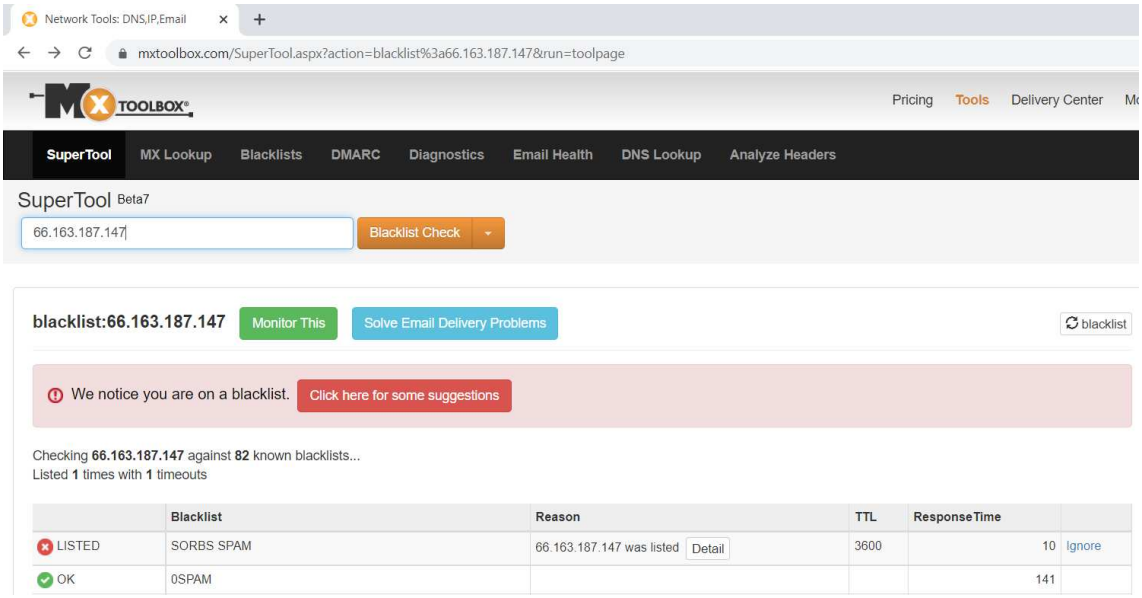



Figura 16 – mxtoolbox.com - lista de bloqueio AOL

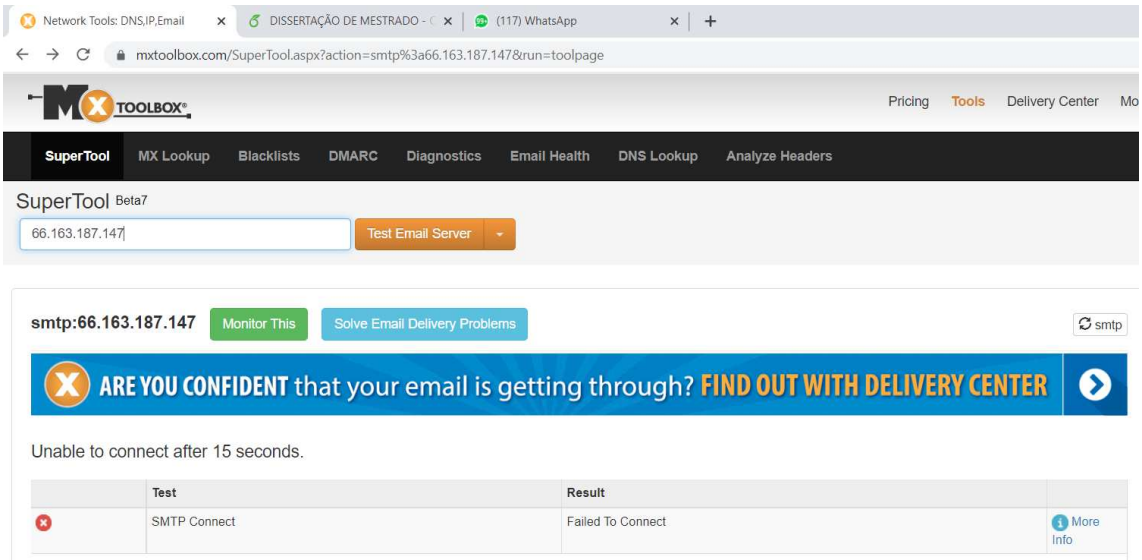



Figura 17 – AOL: *Relay* Possivelmente Aberto


Figura 19 – AOL: Listado em listas de bloqueio


Figura 18 – AOL: Pontuação auferida pelo *Mail Tester*

**1º Mês**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| andrealimaitba@aol.com | x | x | x | x | x | x | x | x | x | x |
| olionmastus@aol.com | x | | x | x | x | x | x | x | x | x |
| palomalisten@aol.com | | x | x | x | x | x | x | x | x | x |
| eduardomazola@aol.com | x | x | x | x | x | x | x | | x | x |
| danielleliman@aol.com | x | x | x | x | x | x | x | x | x | x |
| brissalisboa@aol.com | x | x | x | x | x | x | x | x | x | x |
| anagarcia99@aol.com | | x | x | x | x | x | x | x | x | x |

**2º Mês**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| andrealimaitba@aol.com | x | x | x | x | x | x | | x | x | x |
| olionmastus@aol.com | x | x | x | x | x | x | x | x | x | x |
| palomalisten@aol.com | | x | x | x | x | x | x | x | x | x |
| eduardomazola@aol.com | | x | x | x | | x | x | x | x | x |
| danielleliman@aol.com | x | x | x | x | x | x | x | x | x | x |
| brissalisboa@aol.com | x | x | | x | x | x | x | x | x | x |
| anagarcia99@aol.com | x | x | x | x | x | x | x | x | x | x |

**3º Mês**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| andrealimaitba@aol.com | x | x | x | x | x | x | x | x | x | x |
| olionmastus@aol.com | x | x | x | x | x | x | x | x | x | x |
| palomalisten@aol.com | x | x | x | x | x | x | x | x | x | x |
| eduardomazola@aol.com | x | | x | | x | x | x | x | x | x |
| danielleliman@aol.com | | x | x | x | x | x | x | x | x | x |
| brissalisboa@aol.com | | x | x | x | x | x | x | x | x | x |
| anagarcia99@aol.com | x | x | x | x | x | x | x | x | x | x |

**4º Mês**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| andrealimaitba@aol.com | x | | x | x | | x | x | x | x | x |
| olionmastus@aol.com | x | x | x | x | x | x | x | x | x | x |
| palomalisten@aol.com | x | x | x | x | x | x | | x | x | x |
| eduardomazola@aol.com | x | x | x | x | x | x | x | x | x | x |
| danielleliman@aol.com | x | x | x | x | x | x | x | x | x | x |
| brissalisboa@aol.com | x | x | | x | x | x | x | x | | x |
| anagarcia99@aol.com | x | x | x | x | x | x | x | x | x | x |

| | | |
|---|---|---|
| Caixa de entrada | 262 | 100% |
| Lixo eletrônico | 18 | 6,9% |

Figura 20 – AOL: Envios monitorados por 4 meses

#### 5.1.1.2 Envios do Fastmail para GMail

Os resultados reportados nesta seção se referem a envios a partir do provedor Fastmail (`fastmail.com`), com base em análises de leituras realizadas a partir dos resultados obtidos através do *header* informado pelo Google (Fig. 21), pertencente ao e-mail recebido por um cliente Fastmail, pode-se observar que não houve insuficiência de parâmetros para a validação, que causariam falsos positivos, isto é, os protocolos SPF, DKIM e DMARC foram configurados de forma correta.

A análise subsequente informa que o endereço IP do servidor MTA do Fastmail, aponta corretamente para o FQDN informado pelo *header*, indicando uma correta configuração de seu DNS Reverso, conforme pode ser observado na Fig. 22.

A análise subsequente informa que o endereço IP do servidor MTA do Fastmail não está registrado em banco de dados relevantes para SPAM, indicando que o servidor de e-mails da Fastmail não está contido em nenhuma lista de bloqueio importante, conforme pode ser observado na Fig. 23.

Não foi possível verificar se o servidor está com seu *relay* aberto, pois o servidor não permitiu a consulta, conforme pode ser observado na Fig. 24.

A análise realizada por meio do *Mail Tester* (`mail-tester.com`) mostra o Fastmail (`fastmail.com`) com 9,9 de 10 pontos possíveis, conforme pode ser visto na Fig. 25.

A ausência de alguns ajustes pode ser apontado como o motivo para o não atingimento de 100%. Observando a Fig. 26, pode-se ver que a autenticação DKIM não foi corretamente configurada, além de outras linhas de observação não muito relevantes, fica entendido que os ajustes em sua autenticação DKIM foi o fato principal para a pontuação auferida.

Foram realizados vários envios a partir do Fastmail, tendo como destino os provedores relacionados neste capítulo. Os relatórios foram obtidos por amostragem, sendo que os experimentos foram observados por um período de 4 meses, conforme pode ser observado na Fig. 27. É possível observar que o Fastmail obteve um bom percentual em suas entregas.

Envios a partir do provedor Fastmail (`fastmail.com`), tendo como destino o GMail, acusaram alguns falsos. De acordo com as análises, deduz-se que um dos principais fatores para algumas mensagens serem categorizadas como lixo eletrônico pelo Google, foi possivelmente a falta de inscrição em programas de combate a SPAM, uma vez que a Microsoft, Google e Yahoo sempre orientam seus clientes a se inscreverem nestes programas. Não foi possível efetuar tais verificações, mas como houve falsos positivos, essa seria uma possibilidade.

```
Delivered-To: ricardosoaresitba@gmail.com
Received: by 2002:adf:ed06:0:0:0:0:0 with SMTP id a6csp3531593wro;
        Wed, 2 Nov 2022 03:58:37 -0700 (PDT)
X-Google-Smtp-Source: AMsMyM56CHa3Ppk8gmQNhH8SLGgNCcrS/JNbfVQwmYhFkhr82tsqrFlBuu+MuMKckt2qCGzNKNBQ
X-Received: by 2002:a17:907:6e1a:b0:7ad:ba0b:538c with SMTP id sd26-20020a1709076e1a00b007adba0b538cmr20216822ejc.111.1667386717789;
        Wed, 02 Nov 2022 03:58:37 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1667386717; cv=none;
        d=google.com; s=arc-20160816;
        b=oT8/JglMh3sVHePVh3Z9jQG2FEYvjHeeUZV7fyMggYQEP4wPZRQo0p4gMIaoJNj+SA
         T6I/7UBetqOVhlrrykyRZ7HFQRIUz3VfkzP3d7tP3Jtrnsb5ybQ/H3k79q1pm+FABNJ4
         zinEgf71iYNBlnyj8KAGb3f8LrzKA99mXWU9LyYLeu5jo++zlXpgcRLkq2ABMKJvl/eB
         vqTxcIto3Om69F5MzaX+080eXdtmDK0TEWAPlog04Xuiqnf/XF8Azsu3zIXQsTw8l2kJ
         mG3yEz9NNRgMMDhth5d5rzqLc5eCQJahm07pkZqWDCbx+3lHID1/uAFRy8v1Q9Cu0xhK
         5Bsg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=subject:to:from:date:message-id:mime-version:user-agent:feedback-id
         :dkim-signature:dkim-signature;
        bh=eE9g8fo0ZELy27WCPFUZ0vk6Q1aqoTS1CL+8OCYweJY=;
        b=rNgDG1H5lvZ1vtmUTcCCBwQrRLrdgZGndY20Y+Mc39Bk70TOzafYjM9ThGkWpohg2z
         k4pxidm86LB+kzuYYbg2iMF6os+SyzozrLA9ALKp/D+nuuo9RpwQvjLKdpPoIWcQSbxB
         vbZtTdKE2x8ciPgP+bUJkHOxsBOFyUtdYZxG5esY9bsTycEZdx6IOCsNTA6z8PPYwfDf
         uURkoJuNliwWZmCb1L+VsF2TzSOdZ+h+2TyrdA8sv/wEJzh4/0gAiMz1klzY0CGDGPp5
         hxz1g4e+erZLAYuGdiSHASJg4kwhO0leLwCuAqUkYvTT0ubVpIoCD1QfSLB0DXmSG1Ga
         vl0A==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@fastmail.com header.s=fm3 header.b=bAhH7dDi;
       dkim=pass header.i=@messagingengine.com header.s=ice21466c.fm3 header.b=cqnfajNP;
       spf=pass (google.com: domain of mariojacobcostaitba@fastmail.com designates 64.147.123.27 as permitted sender)
smtp.mailfrom=mariojacobcostaitba@fastmail.com;
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=fastmail.com
Return-Path: <mariojacobcostaitba@fastmail.com>
Received: from wnew2-smtp.messagingengine.com (wnew2-smtp.messagingengine.com. [64.147.123.27])
```


Figura 21 – *Header* Google - Mensagem recebida do Fastmail

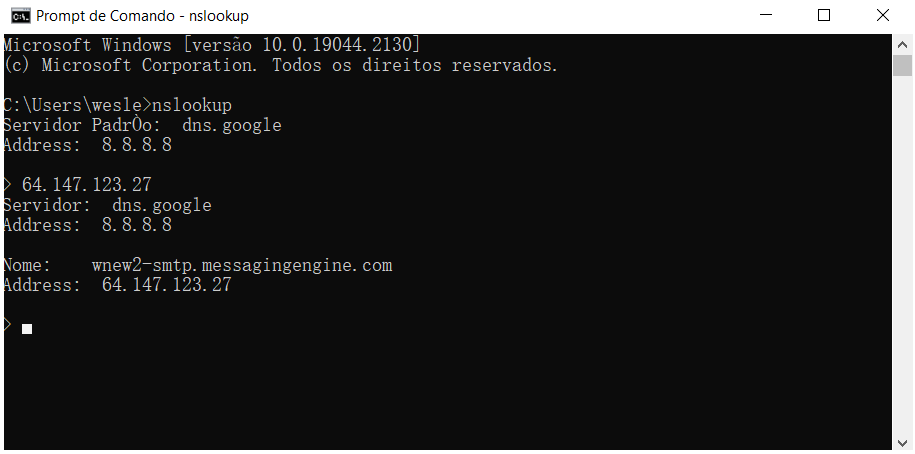



Figura 22 – DNS Reverso do Fastmail

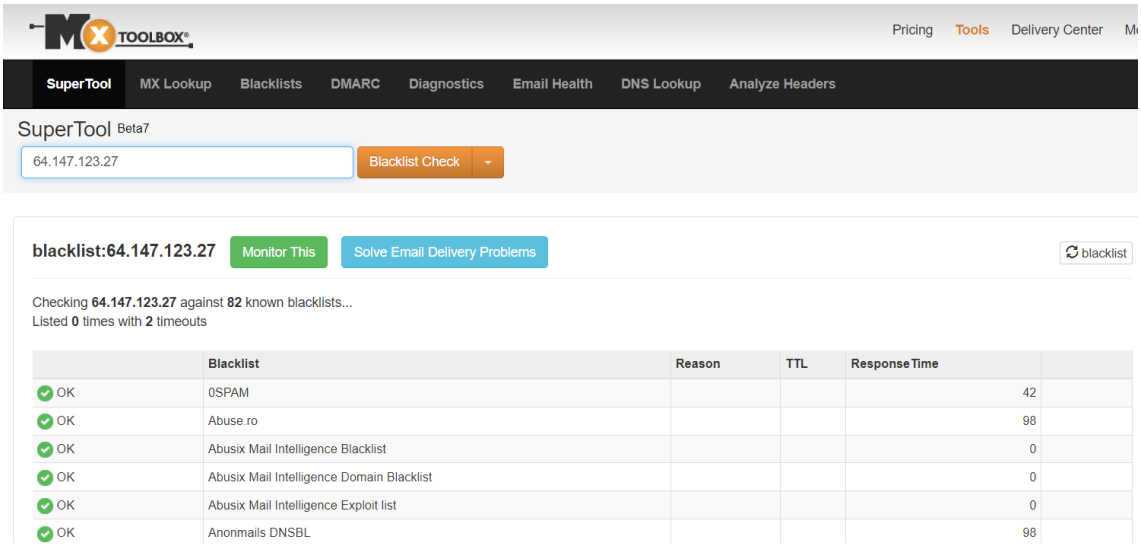



Figura 23 – Fastmail: Não listado em listas de bloqueio

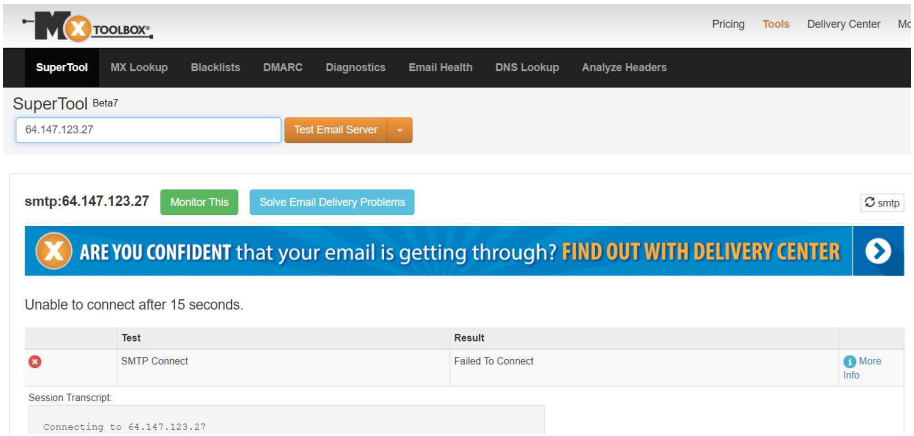



Figura 24 – Fastmail: *Relay* Possivelmente Aberto


Figura 25 – Fastmail: Teste de Pontuação

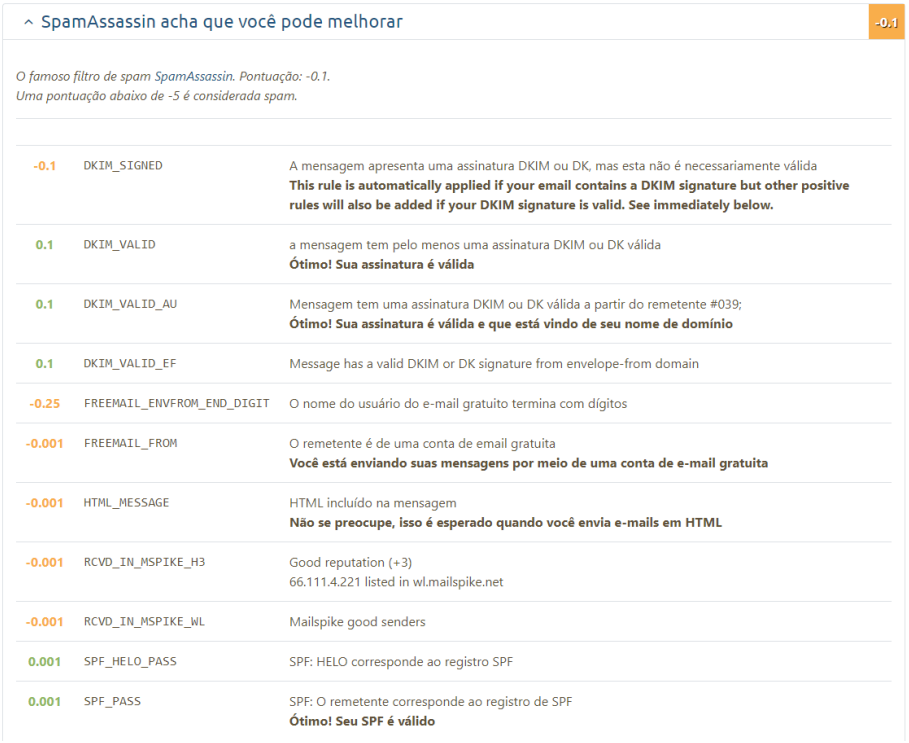
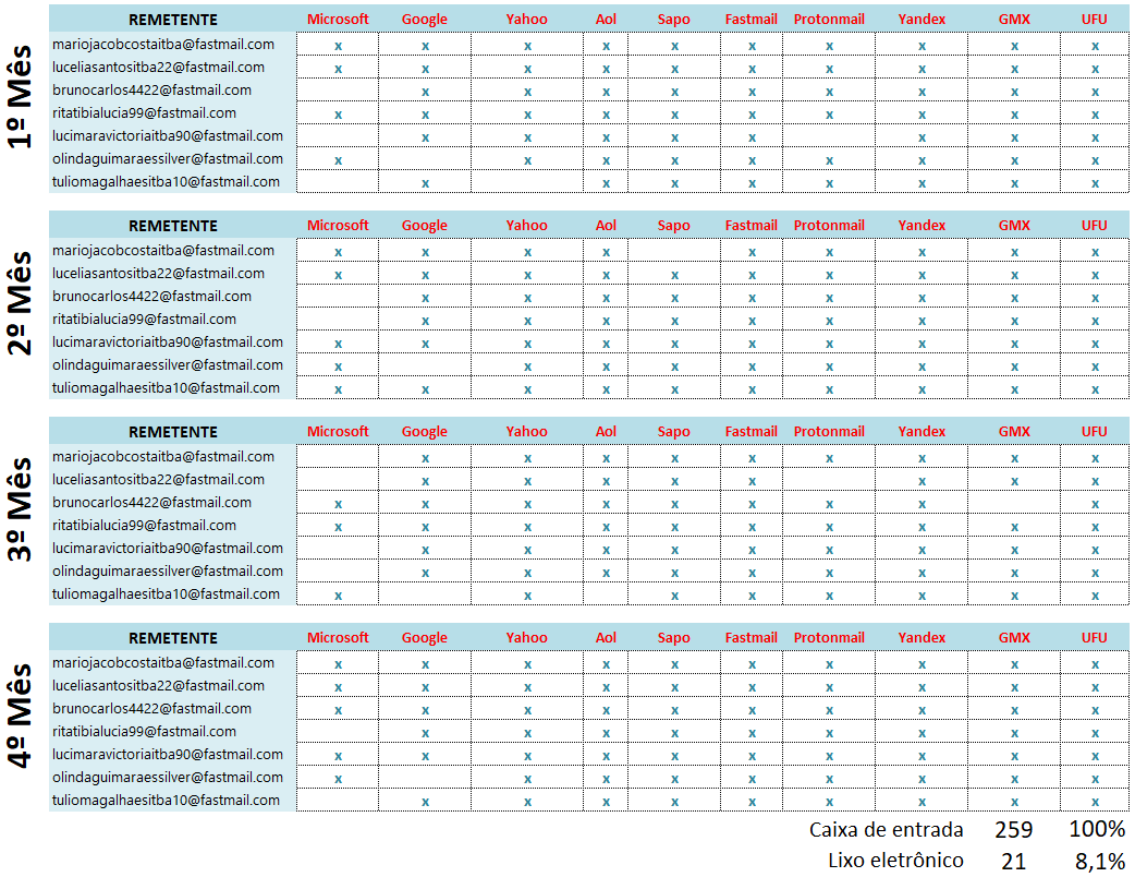



Figura 26 – Fastmail: Relatório *SpamAssassin*



1º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| mariojacobcostaitba@fastmail.com | x | x | x | x | x | x | x | x | x | x |
| luceliasantositba22@fastmail.com | x | x | x | x | x | x | x | x | x | x |
| brunocarlos4422@fastmail.com | | x | x | x | x | x | x | x | x | x |
| ritatibialucia99@fastmail.com | x | x | x | x | x | x | x | x | x | x |
| lucimaravictoriaitba90@fastmail.com | | x | x | x | x | x | | x | x | x |
| olindaguimaraessilver@fastmail.com | x | | x | x | x | x | x | x | x | x |
| tuliomagalhaesitba10@fastmail.com | | x | | x | x | x | x | x | x | x |

2º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| mariojacobcostaitba@fastmail.com | x | x | x | x | | x | x | x | x | x |
| luceliasantositba22@fastmail.com | x | x | x | x | x | x | x | x | x | x |
| brunocarlos4422@fastmail.com | | x | x | x | x | x | x | x | x | x |
| ritatibialucia99@fastmail.com | | x | x | x | x | x | x | x | x | x |
| lucimaravictoriaitba90@fastmail.com | x | x | x | x | x | x | x | x | x | x |
| olindaguimaraessilver@fastmail.com | x | | x | x | x | x | x | x | x | x |
| tuliomagalhaesitba10@fastmail.com | x | x | x | x | x | x | x | x | x | x |

3º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| mariojacobcostaitba@fastmail.com | | x | x | x | x | x | x | x | x | x |
| luceliasantositba22@fastmail.com | | x | x | x | x | x | | x | x | x |
| brunocarlos4422@fastmail.com | x | x | x | x | x | x | x | x | | x |
| ritatibialucia99@fastmail.com | x | x | x | x | x | x | x | x | x | x |
| lucimaravictoriaitba90@fastmail.com | | x | x | x | x | x | x | x | x | x |
| olindaguimaraessilver@fastmail.com | | x | x | x | x | x | x | x | x | x |
| tuliomagalhaesitba10@fastmail.com | x | | x | | x | x | x | x | x | x |

4º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| mariojacobcostaitba@fastmail.com | x | x | x | x | x | x | x | x | x | x |
| luceliasantositba22@fastmail.com | x | x | x | x | x | x | x | x | x | x |
| brunocarlos4422@fastmail.com | x | x | x | x | x | x | x | x | x | x |
| ritatibialucia99@fastmail.com | | x | x | x | x | x | x | x | x | x |
| lucimaravictoriaitba90@fastmail.com | x | x | x | x | x | x | x | x | x | x |
| olindaguimaraessilver@fastmail.com | x | | x | x | x | x | x | x | x | x |
| tuliomagalhaesitba10@fastmail.com | | x | x | x | x | x | x | x | x | x |



Figura 27 – Fastmail: Envios monitorados por 4 meses

#### 5.1.1.3 Envios do Microsoft para GMail

Esta seção relata envios do Microsoft (`microsoft.com`), para o GMail. O *header* informado pelo Google, conforme Fig. 28, referente ao e-mail enviado pelo Microsoft, mostra que não há insuficiência de parâmetros para a validação e os protocolos SPF, DKIM e DMARC foram configurados corretamente.

A análise do DNS Reverso mostra, conforme a Fig. 29, que o endereço IP do servidor Microsoft resolve para o FQDN:

```
ail-bn8nam12olkn2059.outbound.protection.outlook.com
```

Note-se que essa informação diverge da mensagem `Hello` informada no cabeçalho pela cláusula `Received: From` da Fig. 28, cuja resposta é:

```
NAM12-BN8-obe.outbound.protection.outlook.com
```

Tal discrepância pode ser um ponto importante para a ocorrência de falsos positivos, uma vez que a boa prática seria configurar o DNS Reverso exatamente como o FQDN do MTA.

A Fig. 30 aponta que o endereço IP do servidor MTA da Microsoft aparece na lista de bloqueio do SORBS SPAM (`mxtoolbox.com`), indicando que o servidor de e-mails da Microsoft está em uma lista de bloqueio importante, que pode implicar em falsos positivos de SPAM.

Não foi possível verificar se o provedor Microsoft está com seu *relay* aberto, pois o servidor na permitiu a consulta, conforme mostra a Fig. 31. Todavia, como o provedor está registrado na lista de bloqueio do SORBS SPAM, que também informa MTAs com *relays* abertos, é possível deduzir que o servidor esteja com seu *relay* aberto.

A investigação com o *Mail Tester* (`mail-tester.com`) mostra o provedor Microsoft com 9,5 de 10 pontos possíveis, conforme pode ser visto na Fig. 32. De acordo com a análise, o principal motivo para não alcançar 100% da pontuação foi exatamente a discrepância de informações entre a mensagem `Helo` de seu FQDN (ver Fig. 28) e o DNS Reverso (ver Fig. 29).

A discrepância mencionada no parágrafo anterior pode ser verificada pelo resultado do experimento desempenhado com o *Mail Tester* e apresentado na Fig. 33.

Foram realizados vários envios do Microsoft para os provedores relacionados neste capítulo. Os relatórios foram obtidos por amostragem, sendo que os experimentos foram observados durante 4 meses, e podem ser vistos na Fig. 34.

A Fig. 34 mostra que o Microsoft obteve um bom percentual em suas entregas, exitem muitos fatores que influenciam ao resultado final, que foram aqui descritos e estão devidamente relatados em cada análise de envios através dos diversos provedores.

```
Delivered-To: didaticatioficial@gmail.com
Received: by 2002:a59:b261:0:b0:324:98fe:472c with SMTP id p1csp3910809vqr;
        Wed, 2 Nov 2022 05:39:21 -0700 (PDT)
X-Google-Smtp-Source: AMsMyM7O+IycQgpsc0tIMduwVTOsRJychnBqAgONdu5eY6Kk/41kF/dwp2W8Q/5AhDXu/YDCPLvB
X-Received: by 2002:a05:620a:1a99:b0:6ee:c795:46a6 with SMTP id bl25-20020a05620a1a9900b006eec79546a6mr17135361qkb.286.1667392760438;
        Wed, 02 Nov 2022 05:39:20 -0700 (PDT)
ARC-Seal: i=2; a=rsa-sha256; t=1667392760; cv=pass;
        d=google.com; s=arc-20160816;
        b=thEKj+1bojdixGL88SdcdtcT9vwOdwxa2pygu0b3htyhRXe8QMLeQ/4kbTdebSdizg
         sfunME8VuaN9cyddeVHeOy0RBNSuQCtqxOGs1YK1F9+R0b7Dppk4ryG6+BQ2GwnLCriy
         xtFEc0iXdmD5/efUajgT8DZA8GuahSG97W73SlBxrcFM7M5cTSuHJlNVL4neHoXoZckV
         hZ/wGoyeMrOJ4l4PhOP6LuRBhpGwMU+fqmDaiLYaWmXWG8U0HCW1tUrmq8hcr0vbb+Zi
         W5qEQj5JjnuxEyijMMc+7XqkHco7Dao8A+Dq0Da6zg3SNerB9zXrNplkzG3zQRAUhfQX
         /kFg==
ARC-Message-Signature: i=2; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=mime-version:msip_labels:content-language:accept-language
         :message-id:date:thread-index:thread-topic:subject:to:from
         :dkim-signature;
        bh=sPeDCkh9BFVwqP77uIKyUEsleOVyP94nEMzi+3SCk1c=;
        b=osLE9v1B2l+IQQub4v55QR6RnYNqyB/EEyYEU3mKJZov0LEDDqSNfrHVvRMY4f4b5W
         S44sWcdwvqSH59W1s5eLb6Ern6M5JzubxpIjSOZVsAueS9YcLwSjR9dmnA1k6heQQKL0
         BHz8g2mHAHJpz/HfPzLSkoykxUkeHvEfirIDNYQa+ZODApofDp1vLsvqpMaWRxHj4NUz
         Nc+cz68jVNhABqXkM5D+gNfQNCoNYrabv4pLSzFeWYeIZBJFdsgT9vFhzXyTJC9j/aHi
         upvfNsulthHtKy7orRzY3w8zsiSZO58ZizkraZodQeH7faHC7aSI+pIDfmKt854TEnl7
         6G6g==
ARC-Authentication-Results: i=2; mx.google.com;
       dkim=pass header.i=@outlook.com header.s=selector1 header.b="AbYZ/ATg";
       arc=pass (i=1);
       spf=pass (google.com: domain of wesley.silverio@outlook.com designates 40.92.21.59 as permitted sender)
smtp.mailfrom=wesley.silverio@outlook.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=outlook.com
Return-Path: <wesley.silverio@outlook.com>
Received: from NAM12-BN8-obe.outbound.protection.outlook.com (mail-bn8nam12olkn2059.outbound.protection.outlook.com. [40.92.21.59])
        by mx.google.com with ESMTPS id 7-20020ad45ba7000000b004bb69dd32b9si7860384qvq.141.2022.11.02.05.39.20
        for <didaticatioficial@gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Wed, 02 Nov 2022 05:39:20 -0700 (PDT)
```

Figura 28 – *Header* Google - Mensagem recebida do Microsoft

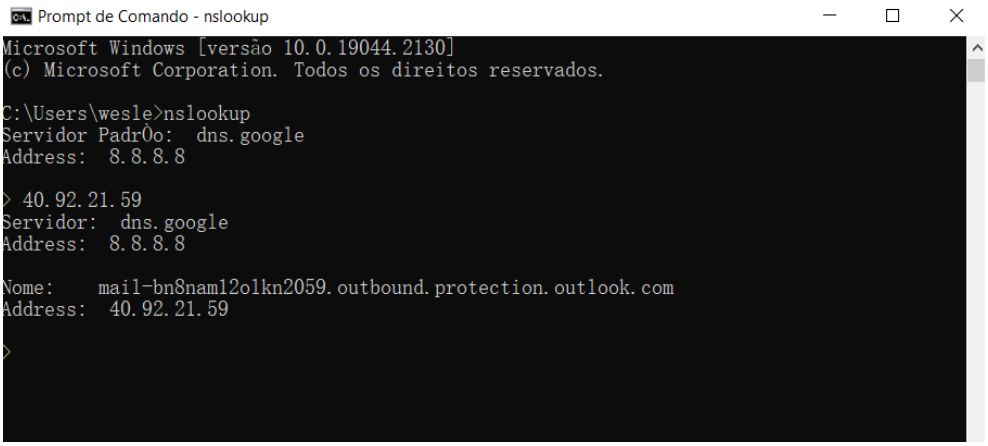



Figura 29 – DNS Reverso Microsoft

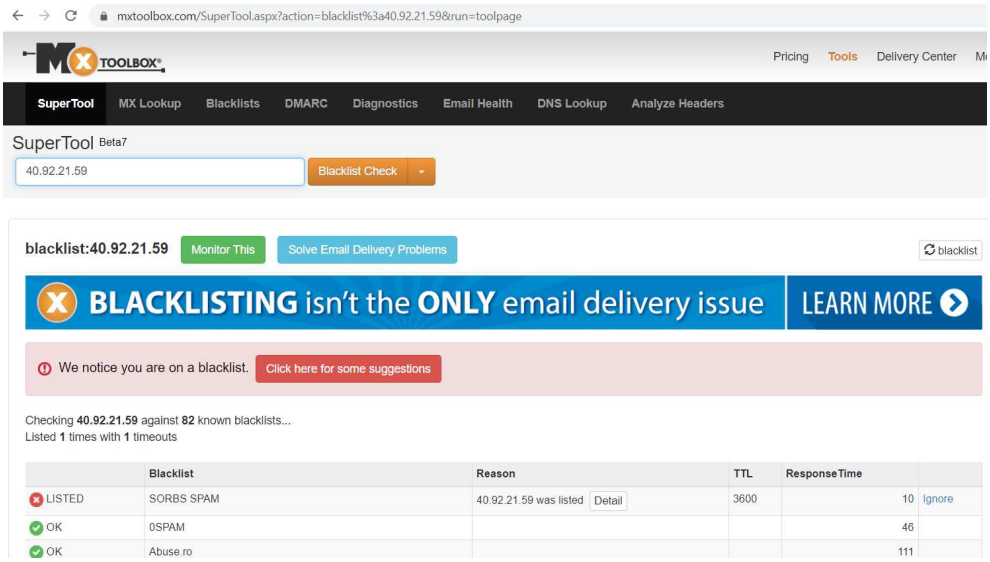



Figura 30 – Microsoft: Registro em lista de bloqueio

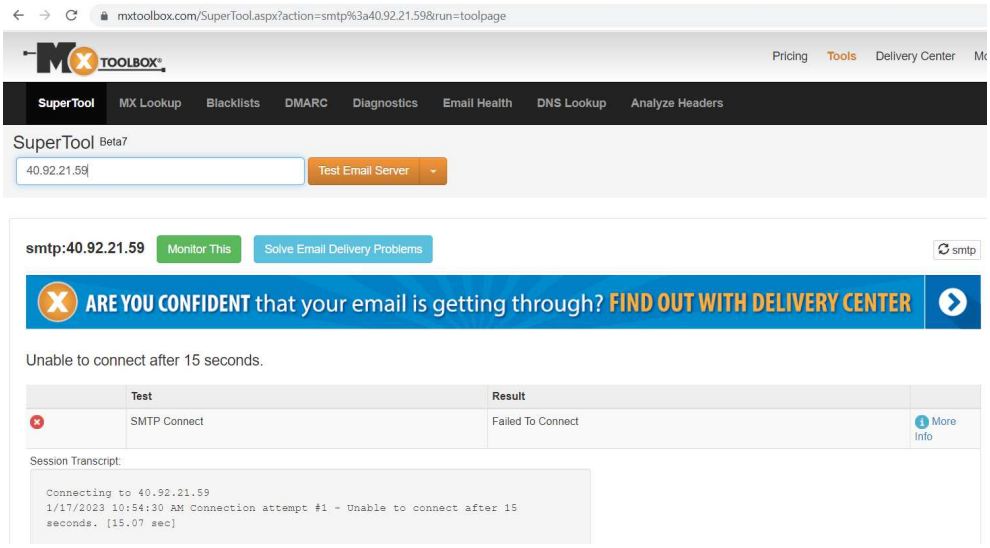
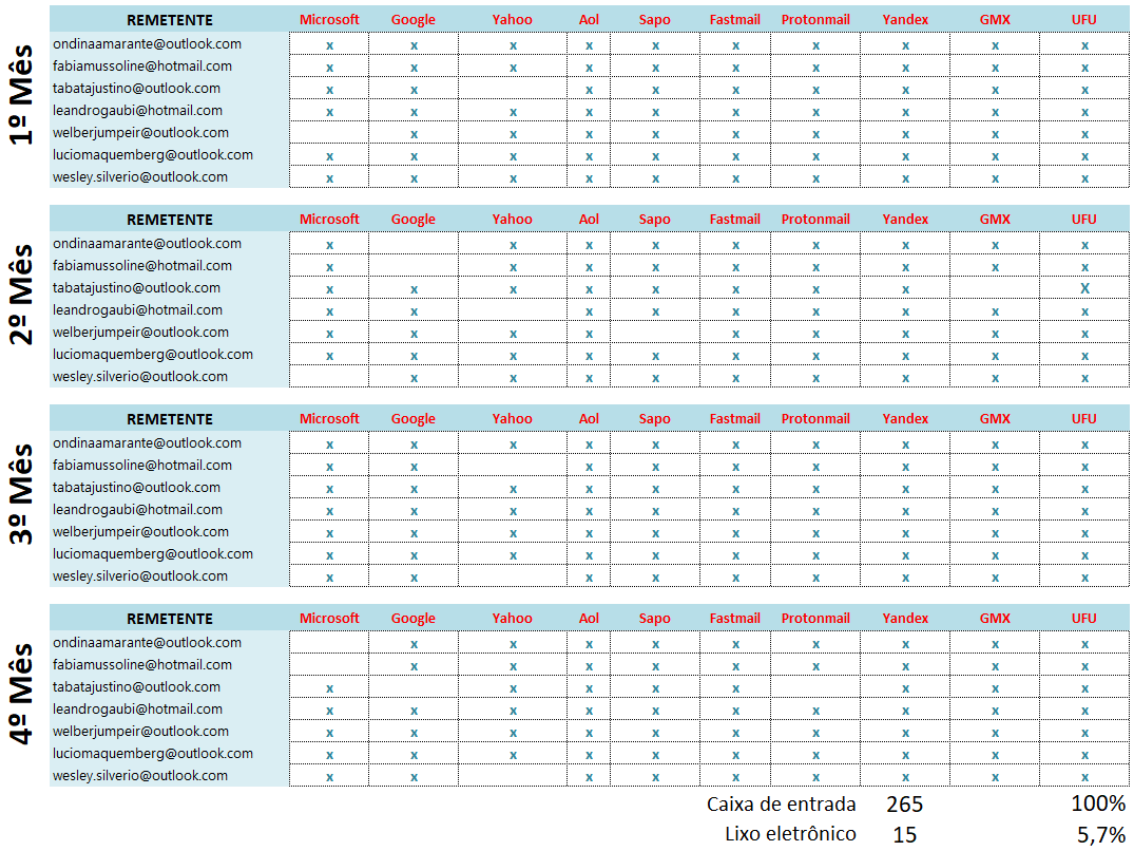



Figura 31 – Microsoft: *Relay* Possivelmente Aberto


Figura 32 – Microsoft: Pontuação


Figura 33 – Microsoft: Discrepâncias *Mail Tester*



1º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| ondinaamarante@outlook.com | x | x | x | x | x | x | x | x | x | x |
| fabiamussoline@hotmail.com | x | x | x | x | x | x | x | x | x | x |
| tabatajustino@outlook.com | x | x | | x | x | x | x | x | x | x |
| leandrogaubi@hotmail.com | x | x | x | x | x | x | x | x | x | x |
| welberjumpeir@outlook.com | | x | x | x | x | x | x | x | x | x |
| luciomaquemberg@outlook.com | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@outlook.com | x | x | x | x | x | x | x | x | x | x |

2º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| ondinaamarante@outlook.com | x | | x | x | x | x | x | x | x | x |
| fabiamussoline@hotmail.com | x | | x | x | x | x | x | x | x | x |
| tabatajustino@outlook.com | x | x | x | x | x | x | x | x | | x |
| leandrogaubi@hotmail.com | x | x | | x | x | x | x | x | x | x |
| welberjumpeir@outlook.com | x | x | x | x | | x | x | x | x | x |
| luciomaquemberg@outlook.com | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@outlook.com | | x | x | x | x | x | x | x | x | x |

3º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| ondinaamarante@outlook.com | x | x | x | x | x | x | x | x | x | x |
| fabiamussoline@hotmail.com | x | x | | x | x | x | x | x | x | x |
| tabatajustino@outlook.com | x | x | x | x | x | x | x | x | x | x |
| leandrogaubi@hotmail.com | x | x | x | x | x | x | x | x | x | x |
| welberjumpeir@outlook.com | x | x | x | x | x | x | x | x | x | x |
| luciomaquemberg@outlook.com | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@outlook.com | x | x | | x | x | x | x | x | x | x |

4º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| ondinaamarante@outlook.com | | x | x | x | x | x | x | x | x | x |
| fabiamussoline@hotmail.com | | x | x | x | x | x | x | x | x | x |
| tabatajustino@outlook.com | x | | x | x | x | x | | x | x | x |
| leandrogaubi@hotmail.com | x | x | x | x | x | x | x | x | x | x |
| welberjumpeir@outlook.com | x | x | x | x | x | x | x | x | x | x |
| luciomaquemberg@outlook.com | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@outlook.com | x | x | | x | x | x | x | x | x | x |



Figura 34 – Microsoft: Envios monitorados por 4 meses

#### 5.1.1.4 Envios do Yahoo para GMail

Esta seção relata envios do Yahoo (`yahoo.com`), para o GMail. O *header* informado pelo Google, conforme Fig. 35, referente ao e-mail enviado pelo Yahoo, mostra que não há insuficiência de parâmetros para a validação e os protocolos SPF, DKIM e DMARC foram configurados corretamente.

A análise subsequente informa que o endereço IP do servidor MTA do Yahoo, resolve corretamente para o FQDN informado pelo *header* (Fig. 35), indicando que configuração de seu DNS Reverso está correto (Fig. 36).

A busca no SORBS SPAM, conforme pode ser visto na Fig. 37, retorna que o endereço IP do servidor MTA se encontra registrado, indicando que o servidor de e-mails do Yahoo consta em sua lista de bloqueio. Este registro pode implicar em falsos positivos de SPAM.

O próximo experimento verifica se o servidor está com seu *relay* aberto, sendo que não foi possível obter tal resposta, devido ao servidor não permitir a consulta, conforme pode ser visto na Fig. 38. Todavia, há registro na lista de bloqueio do SORBS SPAM, que também informa sobre *relays* abertos, é possível que o servidor esteja com seu *relay* aberto.

O resultado do *Mail Tester* (`mail-tester.com`) mostra o Yahoo com 9,5 de 10 pontos possíveis, conforme pode ser observado na Fig. 39.

De acordo com a verificação, o motivo de não ter alcançado 100% é devido a seu endereço IP de envios estar contido em duas listas de bloqueio importantes, conforme se pode ver na Fig. 40, e isso possivelmente pode ter implicado na ocorrência de alguns falsos positivos.

Foram realizados vários envios do Yahoo para os provedores relacionados neste capítulo. Os relatórios foram obtidos por amostragem, sendo que os experimentos foram observados durante 4 meses, sendo o resultado final apresentado na Fig. 41.

Os resultados dos envios mostram que o Yahoo obteve um bom percentual em suas entregas, sendo possível verificar que exitem muitos fatores que influenciam ao resultado final, que foram aqui descritos e estão devidamente relatados em cada análise de envios através dos diversos provedores.

```
Delivered-To: ricardosoaresitba@gmail.com
Received: by 2002:adf:ed06:0:0:0:0:0 with SMTP id a6csp2668278wro;
        Mon, 31 Oct 2022 17:41:00 -0700 (PDT)
X-Google-Smtp-Source: AMsMyM405X0emQhn8xJ4PgLKW/MDNI1LrpJg7pcq9T31nggAzJvliDo8LZnki0uQ5mBmGr1O9fwk
X-Received: by 2002:ad4:5de9:0:b0:4bb:83a6:10bf with SMTP id jn9-20020ad45de9000000b004bb83a610bfmr13654370qvb.49.1667263259710;
        Mon, 31 Oct 2022 17:40:59 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1667263259; cv=none;
        d=google.com; s=arc-20160816;
        b=oyygumMfkE4sLbBJrOyI1lFtYpgqyKobwgFzfhcXFwPwy3LUeNosUUp7LKxLschkDB
         j131gqa6z0gPRgyLnrEy/41IP+3aserNABSWG1QzDKZ2g6Z9aVZpNZCFprlC0TgqBAqV
         B6wZvXLpF14I6fr+A10J+OHKkpg6n5w85x2+d1jbGZihz+eU7jnJlG11xUiugIdD8MSe
         DdZfDLvFyy6PqGAXxwZCh0HWJgQ02ZU2z3klAo/hG5R50O6j44BzbBPip5O8IMn2lHqd
         vbvlGuBX3I4rebLPnOieES2Jp1yc0+NIgOkGJ1Kn4tnQ2mgGyeqqP3a+zcR2GykFjLYf
         d3/Q==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=references:mime-version:subject:message-id:to:from:date
         :dkim-signature;
        bh=ROoj+sYxpFsI1zhdqGVT98JYXjOjdNNXeUlv+KE9Xlk=;
        b=p3dgZKfnqFRbGaeMb7N5qeEEHZ/eaKn723JAYj4jRTlZZONHeYKjQdnAbQBGDN1oKx
         ptlvT8LSFNUU00mSLwbs5kPtsxsm5LUaHS1r13dzfV4x333CcOFGrfwm3SvSKVksDtNU
         6anH4U6RAG7iXMnUCzicyChPOdUbbicrTo0KCYdh4HXrtLCqZhNrDI5Cz4uDP2FltZyu
         2jzf1+/4OKiUzxwU5lCwmSF74JBagVn1eNlnQ9Ra6ND4frR3II/6O4pFl3W2OF5z1FLk
         K1R2zT4K7cwDwrzkcIv9xdlEXGeMPmYuUp76jZ2dFH1rJGWdfHLY0QGVSAHo9EA8PFoB
         tbMQ==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@yahoo.com header.s=s2048 header.b=cmJ7S06I;
       spf=pass (google.com: domain of gilbertolealcunha@yahoo.com designates 66.163.189.32 as permitted sender)
smtp.mailfrom=gilbertolealcunha@yahoo.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
Return-Path: <gilbertolealcunha@yahoo.com>
Received: from sonic322-9.consmr.mail.ne1.yahoo.com (sonic322-9.consmr.mail.ne1.yahoo.com. [66.163.189.32])
        by mx.google.com with ESMTPS id js11-20020a0562142aab00b004bb6e7d6c77si3984350qvb.69.2022.10.31.17.40.59
        for <ricardosoaresitba@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
        Mon, 31 Oct 2022 17:40:59 -0700 (PDT)
Received-SPF: pass (google.com: domain of gilbertolealcunha@yahoo.com designates 66.163.189.32 as permitted sender) client-ip=66.163.189.32;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@yahoo.com header.s=s2048 header.b=cmJ7S06I;
       spf=pass (google.com: domain of gilbertolealcunha@yahoo.com designates 66.163.189.32 as permitted sender)
```

Figura 35 – *Header* Google - Mensagem recebida do Yahoo

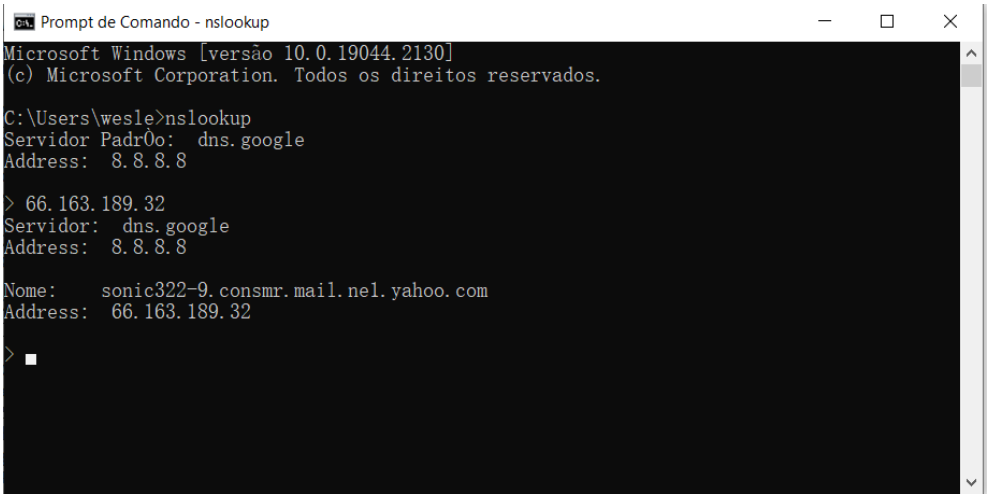



Figura 36 – DNS Reverso Yahoo

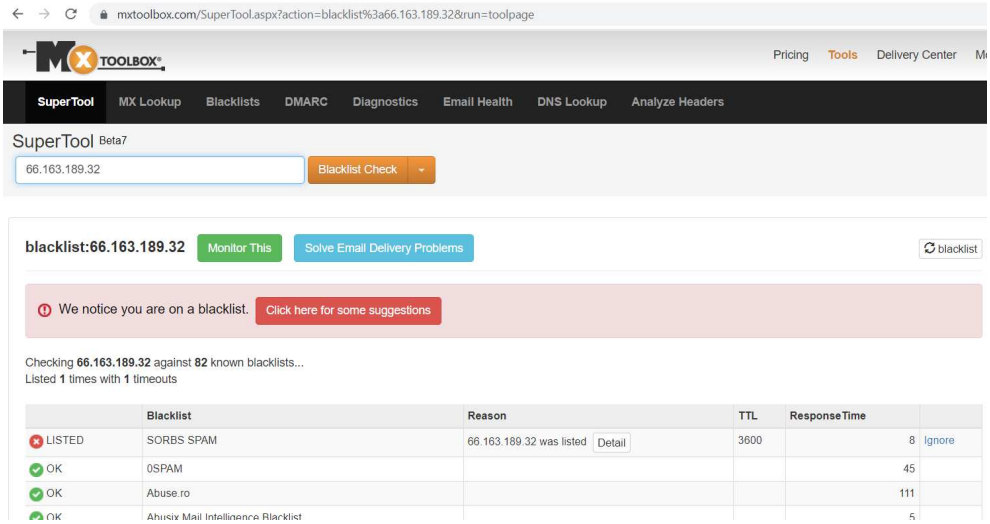



Figura 37 – Yahoo: lista de bloqueio

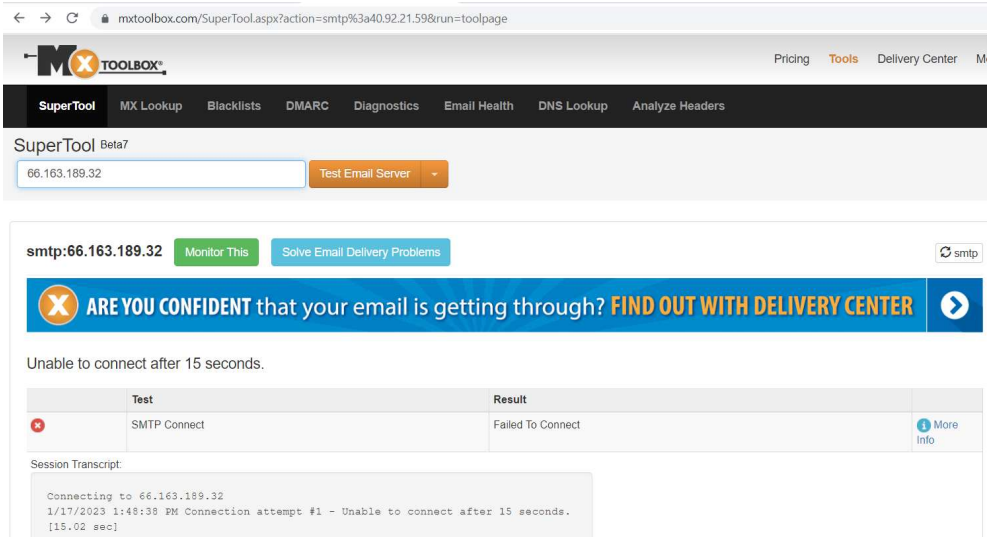



Figura 38 – Yahoo: *Relay* Possivelmente Aberto

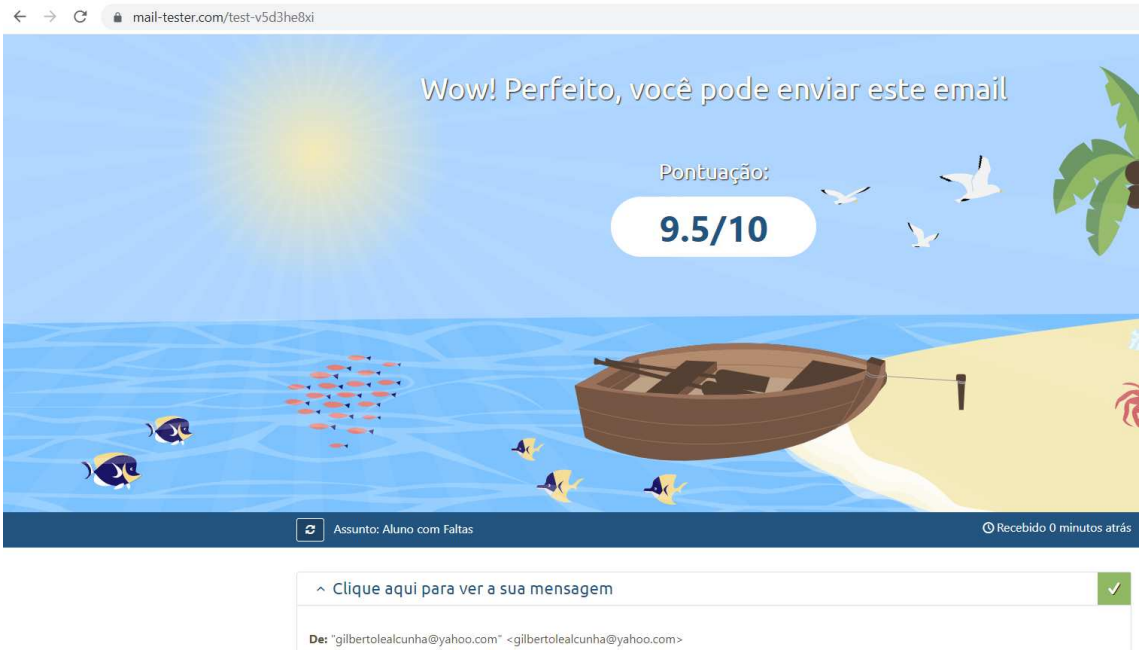



Figura 39 – Yahoo - Pontuação

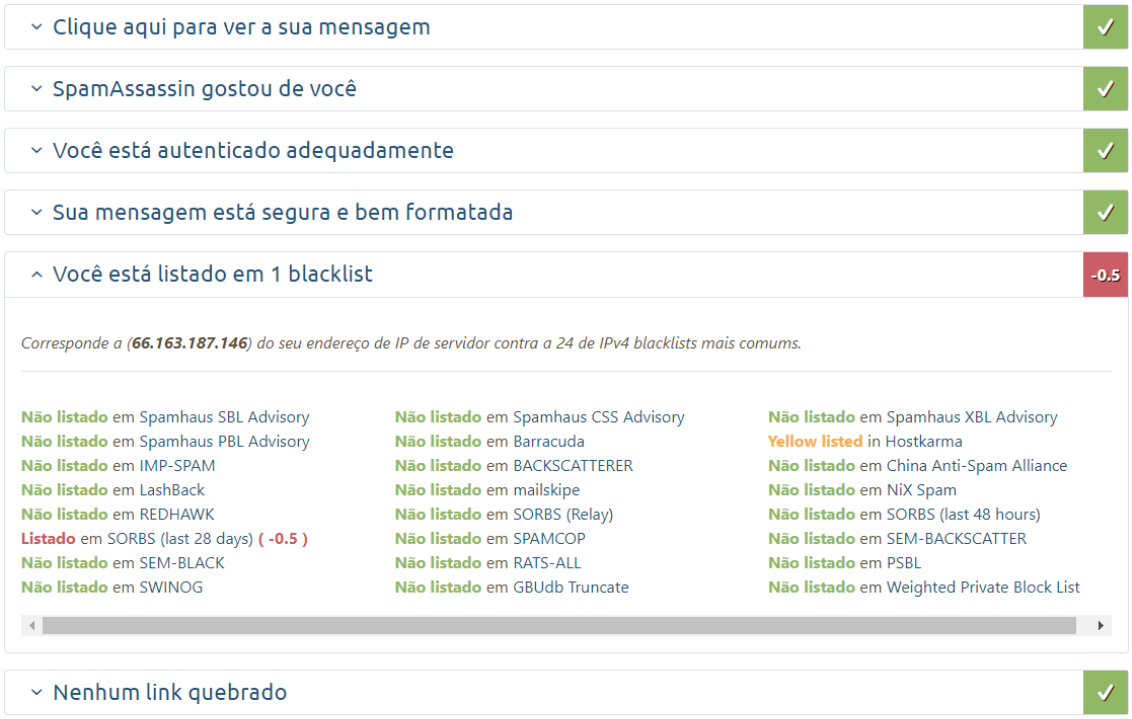
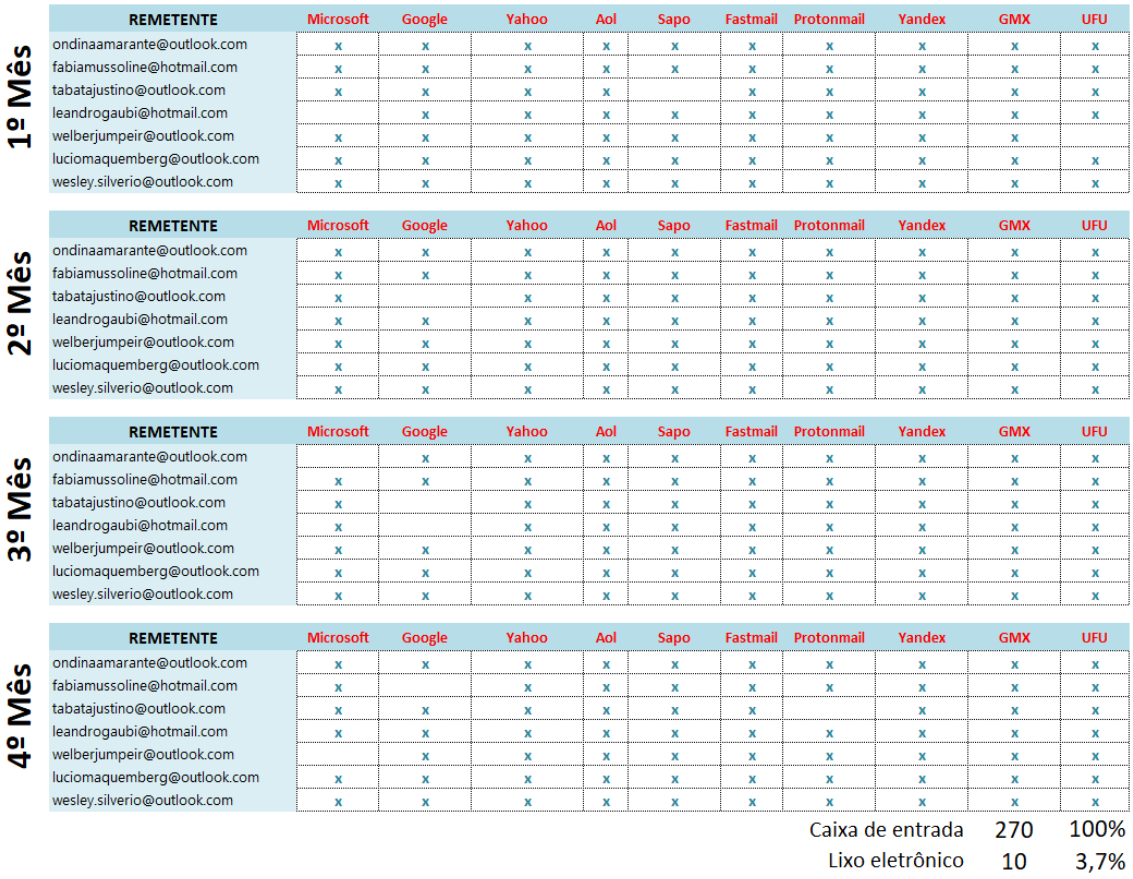



Figura 40 – Yahoo: Discrepâncias *Mail Tester*



1º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| ondinaamarante@outlook.com | x | x | x | x | x | x | x | x | x | x |
| fabiamussoline@hotmail.com | x | x | x | x | x | x | x | x | x | x |
| tabatajustino@outlook.com | x | x | x | x | | x | x | x | x | x |
| leandrogaubi@hotmail.com | | x | x | x | x | x | x | x | x | x |
| welberjumpeir@outlook.com | x | x | x | x | x | x | x | x | x | |
| luciomaquemberg@outlook.com | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@outlook.com | x | x | x | x | x | x | x | x | x | x |

2º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| ondinaamarante@outlook.com | x | x | x | x | x | x | x | x | x | x |
| fabiamussoline@hotmail.com | x | x | x | x | x | x | x | x | x | x |
| tabatajustino@outlook.com | x | | x | x | x | x | x | x | x | x |
| leandrogaubi@hotmail.com | x | x | x | x | x | x | x | x | x | x |
| welberjumpeir@outlook.com | x | x | x | x | x | x | x | x | x | x |
| luciomaquemberg@outlook.com | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@outlook.com | x | x | x | x | x | x | x | x | x | x |

3º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| ondinaamarante@outlook.com | | x | x | x | x | x | x | x | x | x |
| fabiamussoline@hotmail.com | x | x | x | x | x | x | x | x | x | x |
| tabatajustino@outlook.com | x | | x | x | x | x | x | x | x | x |
| leandrogaubi@hotmail.com | x | | x | x | x | x | x | x | x | x |
| welberjumpeir@outlook.com | x | x | x | x | x | x | x | x | x | x |
| luciomaquemberg@outlook.com | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@outlook.com | x | x | x | x | x | x | x | x | x | x |

4º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| ondinaamarante@outlook.com | x | x | x | x | x | x | x | x | x | x |
| fabiamussoline@hotmail.com | x | | x | x | x | x | x | x | x | x |
| tabatajustino@outlook.com | x | x | x | x | x | x | | x | x | x |
| leandrogaubi@hotmail.com | x | x | x | x | x | x | x | x | x | x |
| welberjumpeir@outlook.com | | x | x | x | x | x | x | x | x | x |
| luciomaquemberg@outlook.com | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@outlook.com | x | x | x | x | x | x | x | x | x | x |



Figura 41 – Yahoo: Envios monitorados por 4 meses

### 5.1.2 Envios de GMX, UFU, UFU365 e Yandex para Microsoft

Nesta seção, serão analisados os experimentos de envios a partir dos provedores GMX, UFU, UFU365[2] e Yandex tendo como destino o provedor Microsoft. Para facilitar a compreensão, cada um dos provedores enviadores terão uma seção na qual serão reportados os achados dos experimentos realizados.

#### 5.1.2.1 Envios do GMX para Microsoft

Esta seção relata envios do GMX (`gmx.com`) para o Microsoft. O *header* informado pela Microsoft, conforme Fig. 42, pertencente ao e-mail recebido por um cliente GMX, no qual não foi observado a presença do protocolo DKIM, que é essencial para redução dos falsos positivos (mensagens legitimas são classificadas como lixo eletrônico. Os protocolos SPF e DMARC estão presentes e configurados corretamente no *header*.

A análise do DNS informa que o endereço IP do servidor MTA do GMX resolve corretamente para o FQDN informado pelo *header* (Fig. 42), indicando que seu DNS Reverso foi configurado corretamente, conforme pode ser observado na Fig. 43.

[2] UFU aparece duas vezes nos experimentos em função da migração de serviços para Microsoft, havida durante o projeto.

O MxToolBox (`mxtoolbox.com`) reporta a presença do endereço IP do servidor MTA do GMX na lista de bloqueio do SORBS SPAM e SORBS NEW, indicando que o GMX está registrado em duas listas de bloqueio importantes, conforme pode ser observado na Fig. 44. Esta ocorrência pode ocasionar a presença de falsos positivos de SPAM.

A verificação de *relay* aberto, com o MxToolBox, indica que o servidor do GMX não permitiu a consulta, como mostra a Fig. 45. Todavia, como o endereço do GMX está registrado nas listas de bloqueio do SORBS SPAM e SORBS NEW e não utiliza o protocolo DKIM, é possível que esteja com seu *relay* aberto, embora não seja possa afirmar.

A avaliação da pontuação feita por meio do *Mail Tester* (`mail-tester.com`) aponta o GMX com 8.4 de 10 pontos possíveis, conforme pode ser observado na Fig. 46.

De acordo com o *SpamAssassin*, dois dos principais motivos para não ter alcançado 100% da pontuação, conforme consulta apresentada na Fig. 47, se devem a: (i) ausência do protocolo de autenticação DKIM; e (ii) presença do endereço IP do MTA em duas listas de bloqueio. Embora haja aspectos importantes corretamente configurados, essas duas falhas concorrem para a incidência de falsos positivos.

A Fig. 48, feita a partir de resultados do *Mail Tester*, apresenta mais evidências de falhas/faltas de configuração no provedor GMX, o que permite deduzir que mensagens enviadas a partir de seu MTA são, eventualmente, classificadas como falsos positivos.

Foram realizados envios do GMX para os provedores relacionados neste capítulo, sendo que os relatórios foram obtidos por amostragem, observados durante 4 meses, sendo que a Fig. 49 apresenta os resultados colhidos.

Os resultados mostram que o provedor GMX obteve um bom percentual em suas entregas, existindo muitos fatores que influenciam ao resultado final, que foram aqui descritos e estão devidamente relatados em cada análise de envios através dos diversos provedores.

```
Received: from DM8PR12MB5496.namprd12.prod.outlook.com (::1) by
 MW2PR12MB2554.namprd12.prod.outlook.com with HTTPS; Wed, 2 Nov 2022 11:37:43
 +0000
Received: from MW3PR06CA0002.namprd06.prod.outlook.com (2603:10b6:303:2a::7)
 by DM8PR12MB5496.namprd12.prod.outlook.com (2603:10b6:8:38::11) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5769.19; Wed, 2 Nov
 2022 11:37:42 +0000
Received: from MW2NAM10FT050.eop-nam10.prod.protection.outlook.com
 (2603:10b6:303:2a:cafe::f0) by MW3PR06CA0002.outlook.office365.com
 (2603:10b6:303:2a::7) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5769.18 via Frontend
 Transport; Wed, 2 Nov 2022 11:37:42 +0000
Authentication-Results: spf=pass (sender IP is 212.227.15.19)
 smtp.mailfrom=gmx.com; dkim=none (message not signed)
 header.d=none;dmarc=pass action=none header.from=gmx.com;compauth=pass
 reason=100
Received-SPF: Pass (protection.outlook.com: domain of gmx.com designates
 212.227.15.19 as permitted sender) receiver=protection.outlook.com;
 client-ip=212.227.15.19; helo=mout.gmx.net; pr=C
Received: from mout.gmx.net (212.227.15.19) by
 MW2NAM10FT050.mail.protection.outlook.com (10.13.155.13) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.5791.20 via Frontend Transport; Wed, 2 Nov 2022 11:37:42 +0000
X-IncomingTopHeaderMarker:

OriginalChecksum:D5DC47DA898FC383E78EC2C0BCBDE1876127FC982568BF91919D505B32E17901;UpperCasedChe
32A9EF2E227BD2F1E98B6EA69B185E7C24494;SizeAsReceived:1859;Count:14
Received: from [191.54.207.79] ([191.54.207.79]) by web-mail.gmx.net
 (3c-app-mailcom-bs12.server.lan [172.19.170.180]) (via HTTP); Wed, 2 Nov
 2022 12:37:40 +0100
Message-ID: <trinity-8da37c2f-5742-431c-a7ac-9686c9ebb370-1667389060572@3c-app-mailcom-bs12>
From: Gilberto Carlos <gilbertoitba@gmx.com>
To: wesley.silverio@outlook.com
Subject: =?UTF-8?Q?Confraterniza=C3=A7=C3=A3o?=
Content-Type: text/html; charset=UTF-8
Date: Wed, 2 Nov 2022 12:37:40 +0100
```

Figura 42 – *Header* Microsoft - Mensagem recebida do GMX

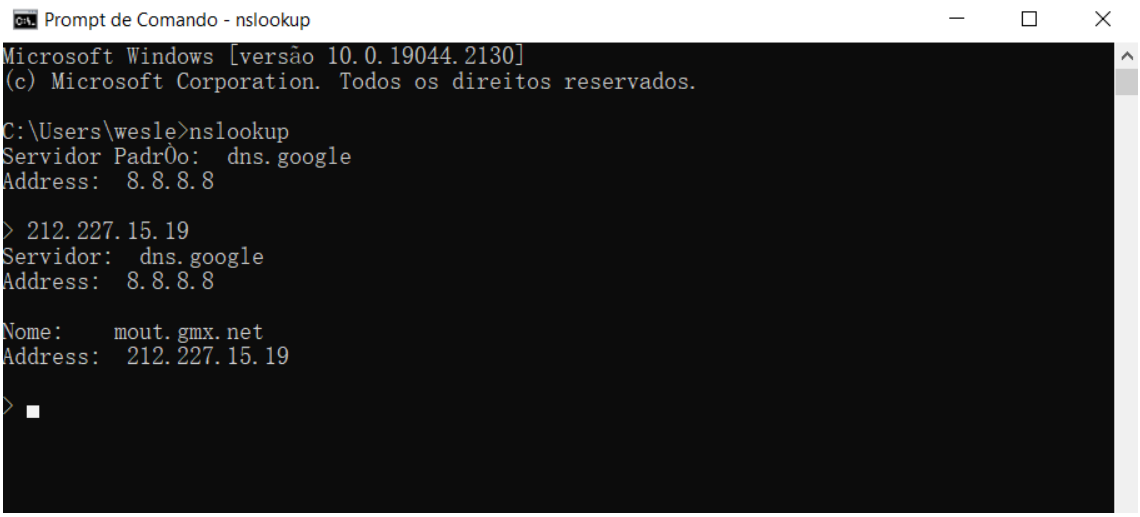



Figura 43 – GMX - DNS Reverso

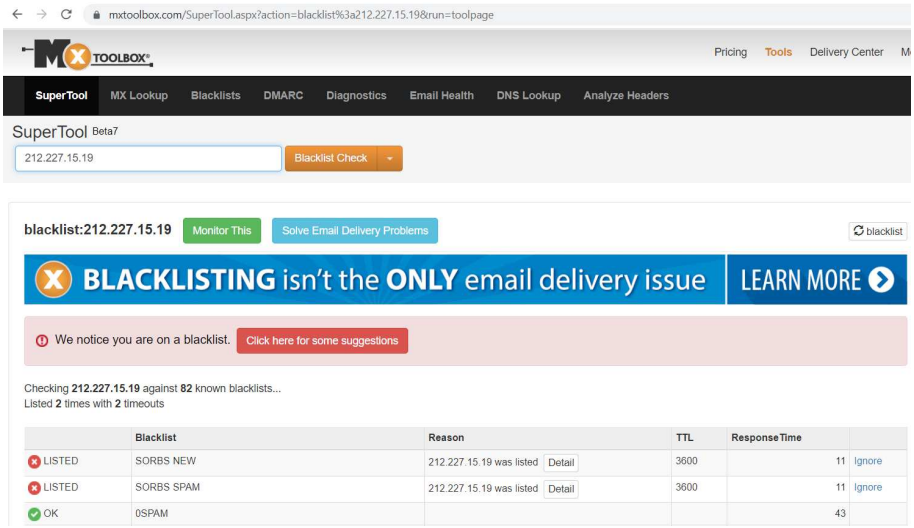



Figura 44 – GMX - lista de bloqueio

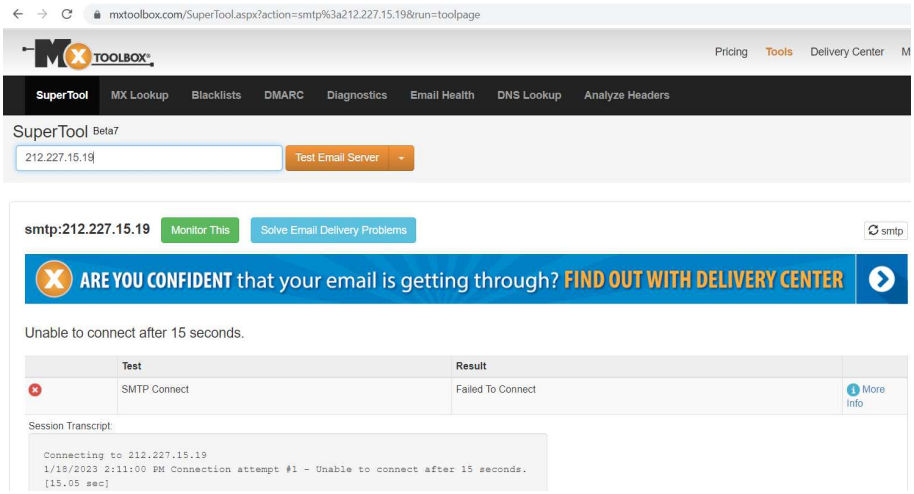
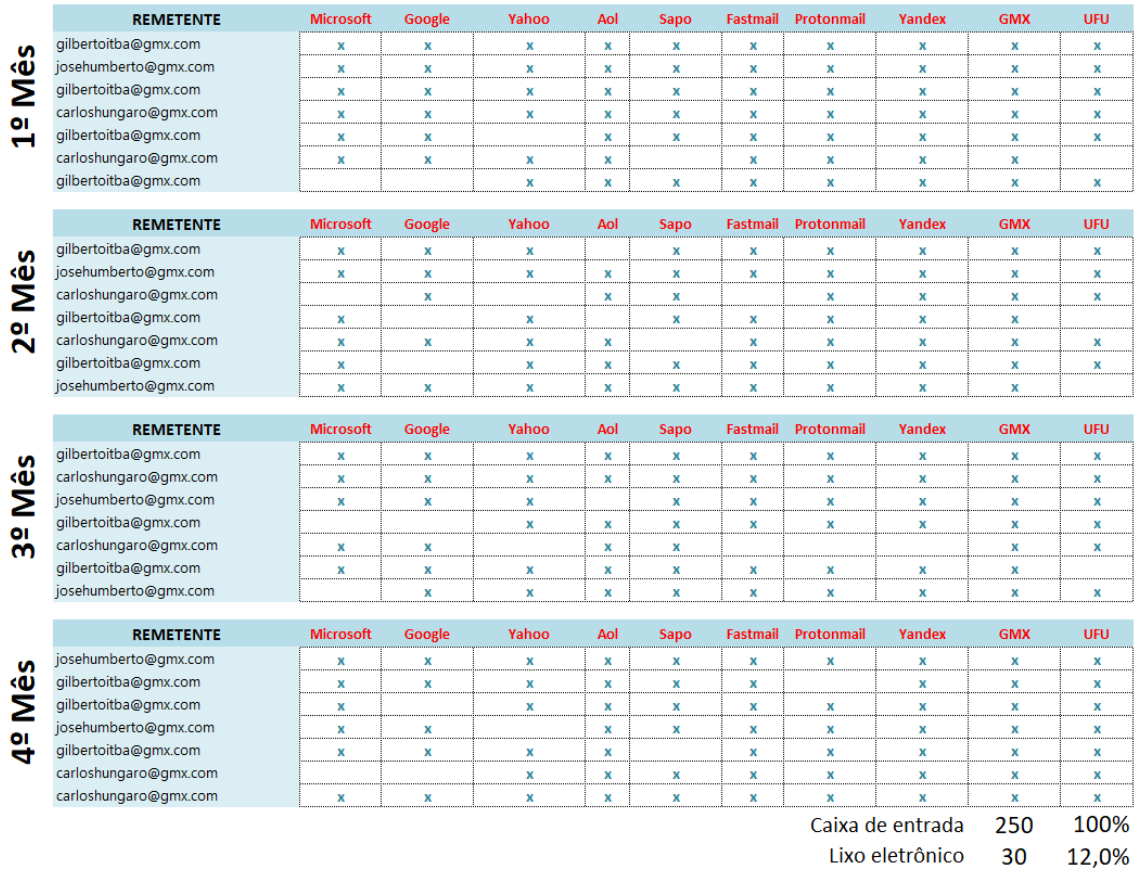



Figura 45 – GMX - *Relay* Possivelmente Aberto


Figura 46 – GMX - Pontuação


Figura 47 – GMX - Falhas de configuração


Figura 48 – GMX - Mais falhas de configuração



1º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| gilbertoitba@gmx.com | x | x | x | x | x | x | x | x | x | x |
| josehumberto@gmx.com | x | x | x | x | x | x | x | x | x | x |
| gilbertoitba@gmx.com | x | x | x | x | x | x | x | x | x | x |
| carloshungaro@gmx.com | x | x | x | x | x | x | x | x | x | x |
| gilbertoitba@gmx.com | x | x | | x | x | x | x | x | x | x |
| carloshungaro@gmx.com | x | x | x | x | | x | x | x | x | |
| gilbertoitba@gmx.com | | | x | x | x | x | x | x | x | x |

2º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| gilbertoitba@gmx.com | x | x | x | | x | x | x | x | x | x |
| josehumberto@gmx.com | x | x | x | x | x | x | x | x | x | x |
| carloshungaro@gmx.com | | x | | x | x | | x | x | x | x |
| gilbertoitba@gmx.com | x | | x | | x | x | x | x | x | |
| carloshungaro@gmx.com | x | x | x | x | | x | x | x | x | x |
| gilbertoitba@gmx.com | x | | x | x | x | x | x | x | x | x |
| josehumberto@gmx.com | x | x | x | x | x | x | x | x | x | |

3º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| gilbertoitba@gmx.com | x | x | x | x | x | x | x | x | x | x |
| carloshungaro@gmx.com | x | x | x | x | x | x | x | x | x | x |
| josehumberto@gmx.com | x | x | x | | x | x | x | x | x | x |
| gilbertoitba@gmx.com | | | x | x | x | x | x | x | x | x |
| carloshungaro@gmx.com | x | x | | x | x | | | | x | x |
| gilbertoitba@gmx.com | x | x | x | x | x | x | x | x | x | |
| josehumberto@gmx.com | | x | x | x | x | x | x | x | x | x |

4º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| josehumberto@gmx.com | x | x | x | x | x | x | x | x | x | x |
| gilbertoitba@gmx.com | x | x | x | x | x | x | | x | x | x |
| gilbertoitba@gmx.com | x | | x | x | x | x | x | x | x | x |
| josehumberto@gmx.com | x | x | | x | x | x | x | x | x | x |
| gilbertoitba@gmx.com | x | x | x | x | | x | x | x | x | x |
| carloshungaro@gmx.com | | | x | x | x | x | x | x | x | x |
| carloshungaro@gmx.com | x | x | x | x | x | x | x | x | x | x |

| | | |
|---|---|---|
| Caixa de entrada | 250 | 100% |
| Lixo eletrônico | 30 | 12,0% |

Figura 49 – GMX - Envios durante 4 meses

#### 5.1.2.2 Envios de UFU para Microsoft

Esta seção relata envios do provedor de e-mail UFU (`ufu.br`) para o Microsoft. O *header* informado pelo Microsoft, conforme Fig. 50, pertence a e-mail recebido de um cliente UFU, onde se verifica que os protocolos SPF, DKIM foram configurados corretamente. No entanto, o protocolo DMARC não foi configurado adequadamente.

A análise do DNS informa que o endereço IP do servidor MTA do UFU resolve para o FQDN `mx.ufu.br`, conforme se pode ver pela Fig. 51, sendo que essa informação diverge da mensagem `Helo`, informada pela cláusula `Received: From`, apresentada na Fig. 50, que reporta `rufus.dr.ufu.br`. Tal discrepância pode implicar em falsos positivos, uma vez que a boa prática recomenda configurar o rDNS exatamente como é o FQDN do MTA.

O MxToolBox (`mxtoolbox.com`) reporta que o endereço IP do servidor MTA responsável pelos envios UFU não consta em nenhuma lista de bloqueios, conforme mostra a Fig. 52. Isso implica na melhoria da reputação do servidor.

A verificação de *relay* aberto, com o MxToolBox, indica que o servidor do UFU não permitiu a consulta, como mostra a Fig. 53.

Não foi possível realizar o experimento para a obtenção da pontuação do MTA UFU, uma vez que durante o desenvolvimento deste projeto, houve a migração de servidores *on premise* da UFU para Microsoft 365, que será apresentada na Seção 5.1.2.3.

Foram realizados envios do UFU para os provedores relacionados neste capítulo, sendo que os relatórios foram obtidos por amostragem, observados durante 4 meses. A Fig. 54 apresenta os resultados colhidos.

Os resultados apresentados na Fig. 54 mostram que o provedor UFU obteve um percentual razoável em suas entregas, mesmo considerando que o protocolo DMARC não estivesse devidamente configurado. Isso pode ter contribuído para o grande número de mensagens que destinadas ao lixo eletrônico.

```
Received: from DM5PR15MB1116.namprd15.prod.outlook.com (2603:10b6:3:b7::14) by
 BN8PR15MB2961.namprd15.prod.outlook.com with HTTPS; Wed, 20 Oct 2021 17:43:19
 +0000
Received: from DB6PR07CA0115.eurprd07.prod.outlook.com (2603:10a6:6:2c::29) by
 DM5PR15MB1116.namprd15.prod.outlook.com (2603:10b6:3:b7::14) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.4608.18; Wed, 20 Oct 2021 17:43:17 +0000
Received: from DB8EUR05FT051.eop-eur05.prod.protection.outlook.com
 (2603:10a6:6:2c:cafe::af) by DB6PR07CA0115.outlook.office365.com
 (2603:10a6:6:2c::29) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.4628.9 via Frontend
 Transport; Wed, 20 Oct 2021 17:43:16 +0000
Authentication-Results: spf=pass (sender IP is 200.19.146.227)
 smtp.mailfrom=ufu.br; outlook.com; dkim=pass (signature was verified)
 header.d=ufu.br;outlook.com; dmarc=bestguesspass action=none
 header.from=ufu.br;compauth=pass reason=109
Received-SPF: Pass (protection.outlook.com: domain of ufu.br designates
 200.19.146.227 as permitted sender) receiver=protection.outlook.com;
 client-ip=200.19.146.227; helo=rufus.dr.ufu.br;
Received: from rufus.dr.ufu.br (200.19.146.227) by
 DB8EUR05FT051.mail.protection.outlook.com (10.233.239.141) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.4628.16 via Frontend Transport; Wed, 20 Oct 2021 17:43:15 +0000
X-IncomingTopHeaderMarker:
```

Figura 50 – *Header* Microsoft - Mensagem recebida do UFU

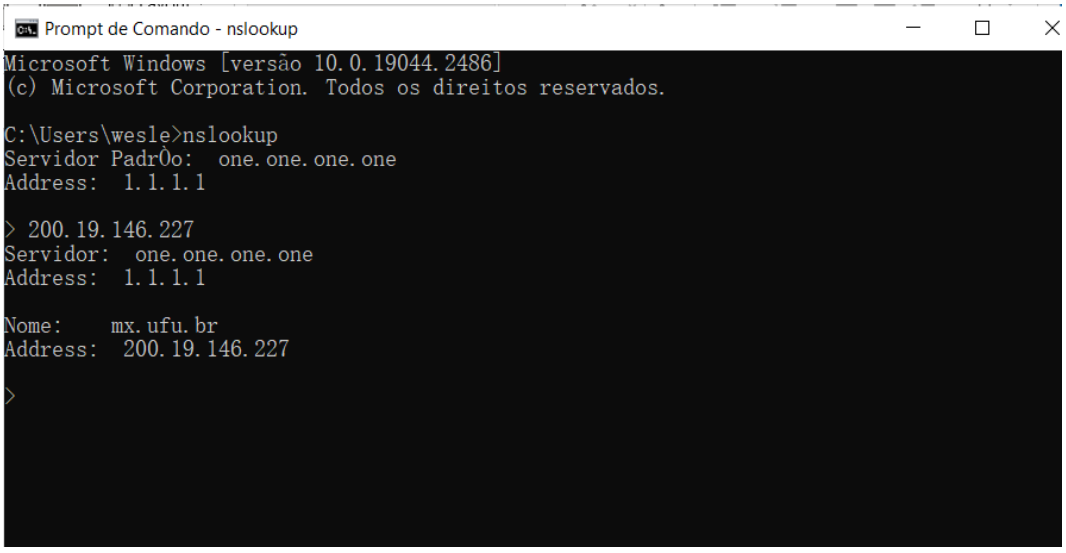



Figura 51 – UFU - DNS Reverso

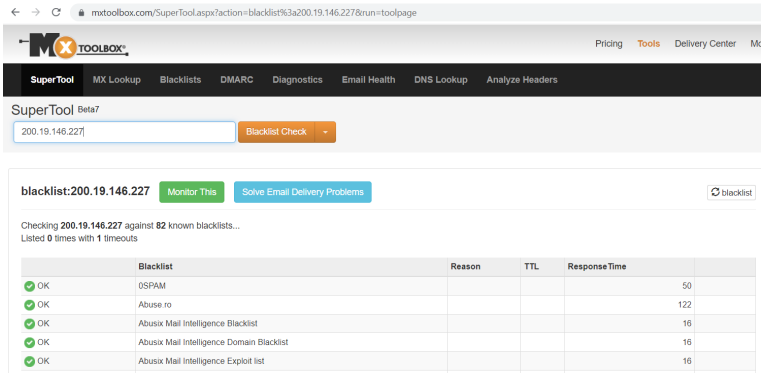



Figura 52 – UFU - Lista de bloqueio

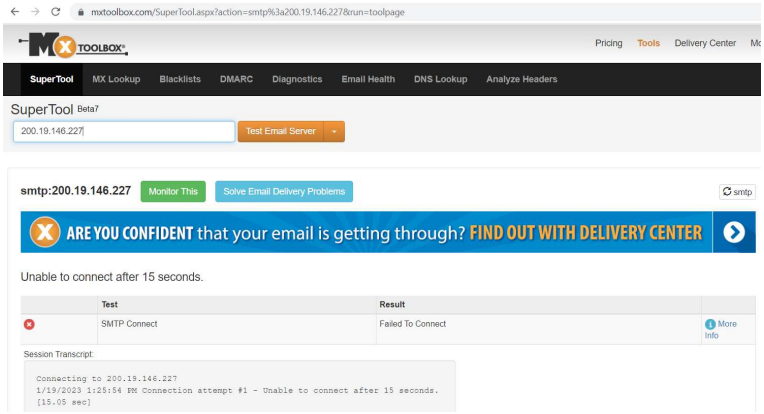



Figura 53 – UFU - *Relay* Possivelmente Aberto

**1º Mês**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | | | | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | | x | | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | | | x | x | x | x | x | | x | x |
| wesley.silverio@ufu.br | x | x | | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | | x | x | | x | | x | x |
| wesley.silverio@ufu.br | | | x | x | x | x | x | x | x | x |

**2º Mês**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | | | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | | x | x | x | x | x | | x | x | x |
| wesley.silverio@ufu.br | | | x | | x | x | x | | x | x |
| wesley.silverio@ufu.br | | x | | x | x | | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | | x | x | x | x | | x |
| wesley.silverio@ufu.br | | | x | x | | x | | x | x | x |

**3º Mês**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| wesley.silverio@ufu.br | | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | | x | x | x |
| wesley.silverio@ufu.br | | | | x | | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | | | x | x |
| wesley.silverio@ufu.br | x | x | x | | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | | | x | x | | x | | x | x |
| wesley.silverio@ufu.br | | x | | | x | x | x | x | x | x |

**4º Mês**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | | x | | | | x | x | | x | x |
| wesley.silverio@ufu.br | | | x | x | x | x | x | | x | x |
| wesley.silverio@ufu.br | | | x | | x | x | | x | x | |
| wesley.silverio@ufu.br | x | x | | x | | | x | x | x | x |
| wesley.silverio@ufu.br | x | x | | | x | | x | x | x | x |
| wesley.silverio@ufu.br | | x | x | x | x | x | x | x | x | x |

| | | |
|---|---|---|
| Caixa de entrada | 213 | 100% |
| Lixo eletrônico | 67 | 31,5% |

Figura 54 – UFU - Envios durante 4 meses

#### 5.1.2.3 Envios de UFU 365 para Microsoft

Esta seção relata envios do provedor de e-mail UFU (`ufu.br`) para o Microsoft. O *header* informado pelo Microsoft, conforme Fig. 55, recebido do UFU, onde se verifica que os protocolos SPF, DKIM e DMARC foram configurados corretamente.

Na fase inicial das pesquisas o MTA da UFU estava locado em um provedor em que havia diversas insuficiências as quais estão mencionadas no capitulo 5.1.2.2, contudo foram observados um grande número de falsos positivos e negativos, posteriormente houve uma migração do seus servidores para a plataforma 365 da Microsoft, os resultados foram positivos e houve uma redução acentuada das inconsistências, certamente a alteração de plataforma foi devido a diversas reclamações pelos seus clientes.

A análise do DNS informa que o endereço IP do servidor MTA do UFU resolve corretamente para o FQDN informado pelo *header* (Fig. 55), indicando que seu DNS Reverso foi configurado corretamente, conforme pode ser observado na Fig. 56.

O MxToolBox (`mxtoolbox.com`) mostra que o endereço IP do servidor MTA responsável pelos envios do UFU não está registrado em nenhuma lista de bloqueio, conforme pode ser observado na Fig. 57. Isto contribui para aumentar a reputação do servidor.

A verificação de *relay* aberto, com o MxToolBox, indica que o servidor do UFU não permitiu a consulta, como mostra a Fig. 58, não permitindo fazer qualquer avaliação sobre este quesito.

A Fig. 59, feita a partir de resultados do *Mail Tester*, mostra o provedor UFU com 10 de 10 pontos válidos. O motivo pelo qual o servidor obteve esse resultado está relacionado à sua reputação é consequência do conjunto de padrões adotados.

A única divergência encontrada pelo *Mail Tester* se refere ao endereço IP e FQDN informados pelo *header*, conforme pode ser observado na Fig. 60. Essa diferença é devida ao fato que o Microsoft possui vários servidores de e-mail para atender à quantidade de usuários que ela hospeda. Todavia, isto pode implicar em falsos positivos.

Foram realizados vários envios do UFU para os provedores relacionados neste capítulo, sendo que os relatórios foram obtidos por amostragem, em testes observados durante 4 meses, conforme apresentado na Fig. 61.

Os envios do provedor UFU obteve um bom percentual em suas entregas, sendo que existem muitos fatores que influenciam ao resultado final, que foram aqui descritos e estão devidamente relatados em cada análise de envios através dos diversos provedores.

```
Received: from MW3PR12MB4554.namprd12.prod.outlook.com (2603:10b6:303:55::21)
 by MW2PR12MB2554.namprd12.prod.outlook.com with HTTPS; Wed, 2 Nov 2022
 12:04:38 +0000
ARC-Seal: i=2; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=pass;
 b=k57LX/KMyeU3PNX7GzUYwKuNbRR
+ONVqI/alqCPtv5LaaILZ6bEhVU/cENEx9YUHHtKOA1OE1ghPBk5duMKabgYtCSboQy/vw/hWOfKhR2lwz0kahcolA2eG5ihbjnpcPDPjoEQgKFh8NBMfUFeNjuqgYTR
pth9YxCjrs+oPuQcB6vbxcrfCXnpwU7T3q/XsNoaaNRK9N5q1pz+5vfKnNhNvHf6mXOlGt8naX8nXZaUgPAV7AA0IbAj9w5yJD
+qNF2LDDRjnyTTQbQkl0p/krrZmfIq88GOWBglnKvRGo6eP0jRw+uYRiiis+dzqbOA9y69C6mNBpCwZBkR6eLjnVQ==
ARC-Message-Signature: i=2; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
 s=arcselector9901;
 h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-
MessageData-0:X-MS-Exchange-AntiSpam-MessageData-1;
 bh=QkckrcfSpL1b8x96PRDy2deoAGm3xBRSfrdP0L3CnlU=;
 b=NE2AAKqf/B4waj/Erq5t3xGI/WHaV+OvTpH282euI9I/nPdLko7i9YpQo4UUPSiKXZA
+cmhduBHQsJ/Ou594dVDAl0YQWE20ZUBI6kS2Wi/vmJF9ArIfYbSSw8KI1xrXHCCIGsC0ZPE4Zzgyg4R3sc3PJlevj0KqJgjt8ExM4MlSpEot6wHPNphytD
+Os8pwax9dWWPOiyqhmWSW4tErSL8GhcPj/KW
+gBbpoFzFVMzlnWOPSu/8A8C5WbbsC67f84w3zzH/VyDkEZJjW/VGWwoCBvQOQUdUokq1RJNP1oD4zd16m75lJy53PjNJUzo/IFvOQQxJba/YO4ekDGvyPQ==
ARC-Authentication-Results: i=2; mx.microsoft.com 1; spf=pass (sender ip is
 40.107.101.83) smtp.rcpttodomain=outlook.com smtp.mailfrom=ufu.br;
 dmarc=bestguesspass action=none header.from=ufu.br; dkim=pass (signature was
 verified) header.d=ufu.br; arc=pass (0 oda=1 ltdi=1
 spf=[1,1,smtp.mailfrom=ufu.br] dkim=[1,1,header.d=ufu.br]
 dmarc=[1,1,header.from=ufu.br])
Received: from DB6PR07CA0086.eurprd07.prod.outlook.com (2603:10a6:6:2b::24) by
 MW3PR12MB4554.namprd12.prod.outlook.com (2603:10b6:303:55::21) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.5769.21; Wed, 2 Nov 2022 12:04:37 +0000
Received: from DB8EUR06FT041.eop-eur06.prod.protection.outlook.com
 (2603:10a6:6:2b:cafe::8b) by DB6PR07CA0086.outlook.office365.com
 (2603:10a6:6:2b::24) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5791.22 via Frontend
 Transport; Wed, 2 Nov 2022 12:04:37 +0000
Authentication-Results: spf=pass (sender IP is 40.107.101.83)
 smtp.mailfrom=ufu.br; dkim=pass (signature was verified)
 header.d=ufu.br;dmarc=bestguesspass action=none
 header.from=ufu.br;compauth=pass reason=109
Received-SPF: Pass (protection.outlook.com: domain of ufu.br designates
 40.107.101.83 as permitted sender) receiver=protection.outlook.com;
 client-ip=40.107.101.83; helo=NAM04-MW2-obe.outbound.protection.outlook.com;
```

Figura 55 – *Header* Microsoft - Mensagem recebida do UFU/365


Figura 56 – UFU365: DNS Reverso

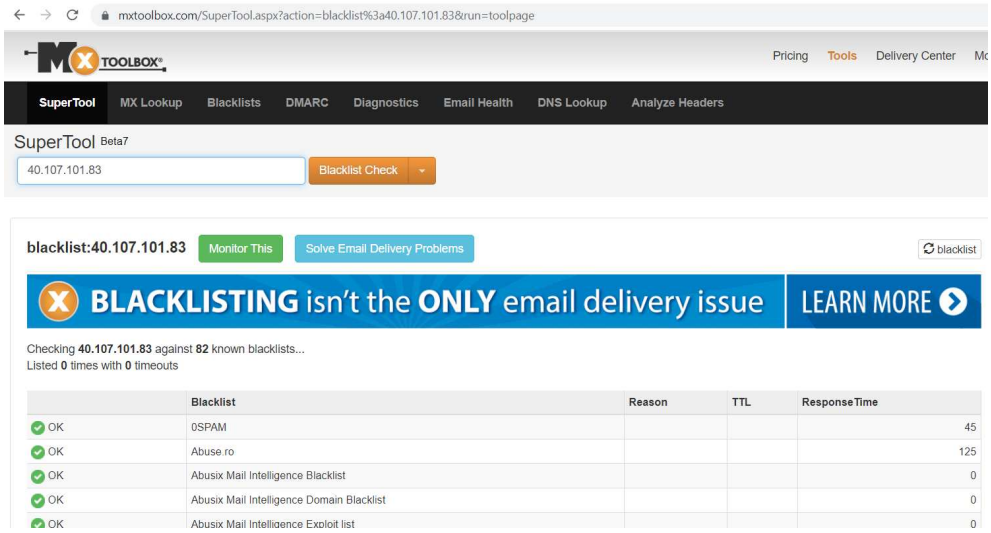



Figura 57 – UFU365 - Negativo para lista de bloqueio

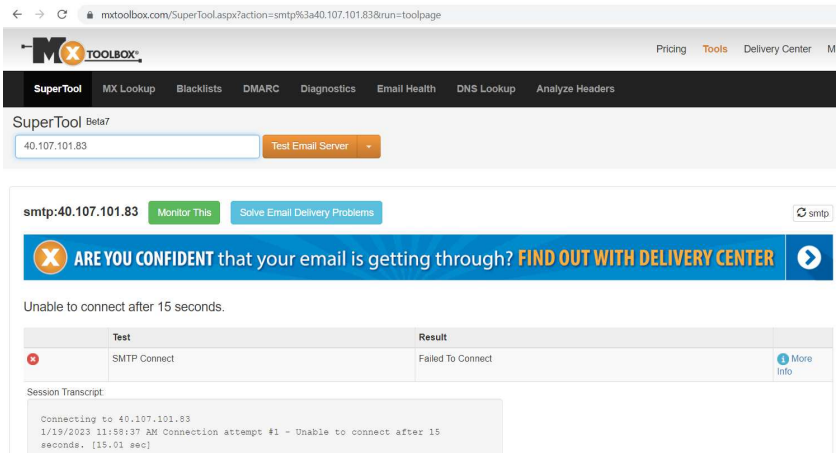
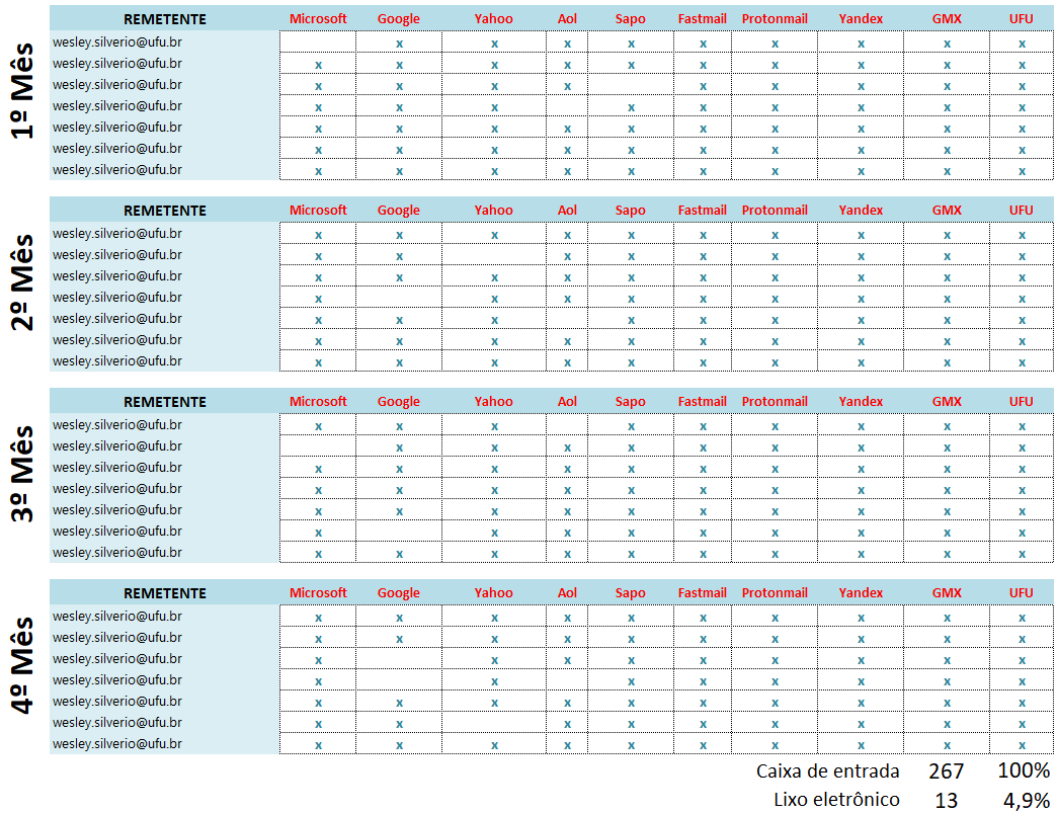



Figura 58 – UFU365 - *Relay* Possivelmente Aberto


Figura 59 – UFU365 - Pontuação


Figura 60 – UFU365 - Resultados *Mail Tester*



1º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| wesley.silverio@ufu.br | | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |

2º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |

3º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| wesley.silverio@ufu.br | x | x | x | | x | x | x | x | x | x |
| wesley.silverio@ufu.br | | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |

4º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | | x | | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | | x | x | x | x | x | x | x |
| wesley.silverio@ufu.br | x | x | x | x | x | x | x | x | x | x |

| | | |
|---|---|---|
| Caixa de entrada | 267 | 100% |
| Lixo eletrônico | 13 | 4,9% |

Figura 61 – UFU365 - Envios durante 4 meses

#### 5.1.2.4 Envios do Yandex para Microsoft

Esta seção relata envios do Yandex (`yandex.com`), para Microsoft. O *header* apresentado na Fig. 62, recebido do Yandex, onde se verifica que os protocolos SPF, DKIM e DMARC foram configurados corretamente.

A análise do DNS mostra que o endereço IP do servidor MTA do Yandex resolve corretamente para o FQDN informado pelo *header* (Fig. 62), indicando que seu DNS Reverso foi configurado corretamente, conforme pode ser observado na Fig. 63.

O MxToolBox (`mxtoolbox.com`) reporta o endereço IP do MTA do Yandex em 4 listas de bloqueio, conforme pode ser observado na Fig. 64, sendo: *Sender Score Reputation Network*; UCE *Protect* Nível 1 (UCEPROTECTL1)[3]; UCE *Protect* Nível 2 (UCEPROTECTL2)[4]; e UCE *Protect* Nível (UCEPROTECTL3)[5]. Isto indica que o Yandex possui grande chance de problemas em entregas.

A verificação de *relay* aberto, com o MxToolBox, indica que o servidor do Yandex não permitiu a consulta, como mostra a Fig. 65. Todavia, como consta em 4 listas de bloqueio, em particular a UCE *Protect* Nível 1 indica a presença de *relay* aberto.

[3] Indica problema de *Relay* Aberto ou DNS reverso
[4] Indica endereço IP ou sub-rede em lista de bloqueio
[5] Bloqueia todos endereços IP de um Provedor, caso tenha incorrido em 50 diferentes casos de SPAMs e tenha 50 casos de IPs na lista de bloqueios de Nível 1

A Fig. 66, feita pelo *Mail Tester*, mostra o provedor Yandex com 10 de 10 pontos possíveis.

Contudo, o MxToolBox mostra o Yandex em 4 listas de bloqueio, mostrando que as listas de bloqueio não são analisadas pelo *Mail Tester*, conforme se pode observar na Fig. 67. Infelizmente, no momento, não há uma ferramenta que avalie todos os quesitos necessários.

Foram realizados envios do Yandex para os provedores relacionados neste capítulo e os resultados obtidos por amostragem, durante 4 meses, são apresentados na Fig. 68.

Os resultados mostram que o Yandex obteve um bom percentual em suas entregas, apesar dos problemas relatados. Isto pode ser explicado pelo fato de existirem muitos fatores que influenciam ao resultado final, permitindo concluir que as listas de bloqueio não foram checadas pela maioria dos receptores. No entanto, note-se que Yahoo e AOL rejeitaram um número elevado de mensagens do Yandex, muito provavelmente em função de estar nas listas de bloqueio.

```
Received: from PH8PR12MB7229.namprd12.prod.outlook.com (2603:10b6:510:227::20)
 by MW2PR12MB2554.namprd12.prod.outlook.com with HTTPS; Wed, 2 Nov 2022
 11:25:21 +0000
Received: from BN8PR07CA0035.namprd07.prod.outlook.com (2603:10b6:408:ac::48)
 by PH8PR12MB7229.namprd12.prod.outlook.com (2603:10b6:510:227::20) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5769.19; Wed, 2 Nov
 2022 11:25:20 +0000
Received: from BN8NAM04FT017.eop-NAM04.prod.protection.outlook.com
 (2603:10b6:408:ac:cafe::77) by BN8PR07CA0035.outlook.office365.com
 (2603:10b6:408:ac::48) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5791.22 via Frontend
 Transport; Wed, 2 Nov 2022 11:25:20 +0000
Authentication-Results: spf=pass (sender IP is 77.88.28.105)
 smtp.mailfrom=yandex.com; dkim=pass (signature was verified)
 header.d=yandex.com;dmarc=pass action=none
 header.from=yandex.com;compauth=pass reason=100
Received-SPF: Pass (protection.outlook.com: domain of yandex.com designates
 77.88.28.105 as permitted sender) receiver=protection.outlook.com;
 client-ip=77.88.28.105; helo=forward400p.mail.yandex.net; pr=C
Received: from forward400p.mail.yandex.net (77.88.28.105) by
 BN8NAM04FT017.mail.protection.outlook.com (10.13.161.136) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.5791.20 via Frontend Transport; Wed, 2 Nov 2022 11:25:19 +0000
X-IncomingTopHeaderMarker:
 OriginalChecksum:04601FF98506626A7410D3B8950ABE537DF67DAFD0061647E66905B69CDA296A;UpperCasedChecksum:B8FB3C665951C360D7531B9238CC45I
Received: from vla1-cdca1270eaaa.qloud-c.yandex.net (vla1-cdca1270eaaa.qloud-c.yandex.net [IPv6:2a02:6b8:c0d:4e8f:0:640:cdca:1270])
        by forward400p.mail.yandex.net (Yandex) with ESMTP id 5B3E964190E
        for <wesley.silverio@outlook.com>; Wed,  2 Nov 2022 14:25:18 +0300 (MSK)
Received: from mail.yandex.com (mail.yandex.com [191.54.207.79])
        by vla1-cdca1270eaaa.qloud-c.yandex.net (mxback/Yandex) with HTTP id FPQIde1fwGk1-PIfKQ1iQ;
        Wed, 02 Nov 2022 14:25:18 +0300
X-Yandex-Fwd: 1
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yandex.com; s=mail; t=1667388318;
        bh=CkQoeHHBleXj9ZMH5z68hXtmvc54VXp2a7QQk+q1kA4=;
        h=Message-Id:Date:Subject:To:From;
        b=wS1nAjzsPR7WjdPqHHIB1pkBlq8e/njC+sH859Ldl6oiz80bPRbJfy2ALVjAAJYDY
```

Figura 62 – *Header* Microsoft - Mensagem recebida do Yandex

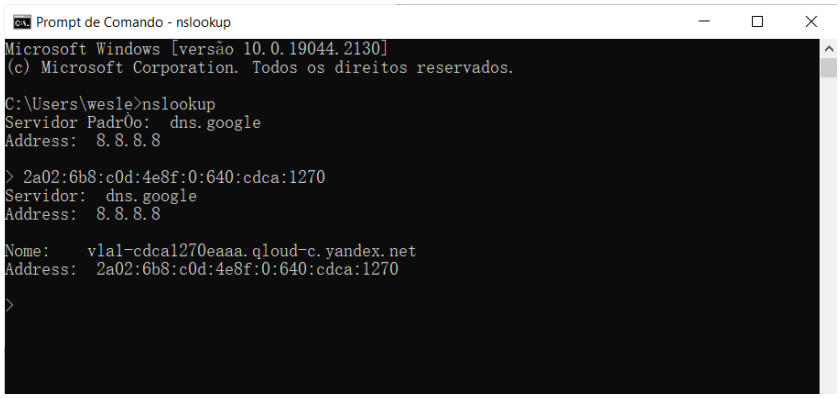



Figura 63 – Yandex - DNS Reverso

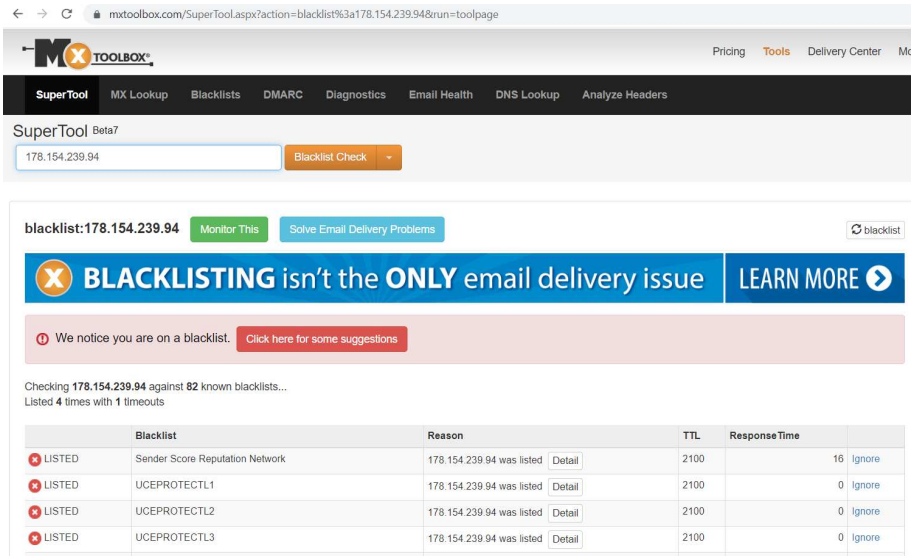



Figura 64 – Yandex - Lista de Bloqueio

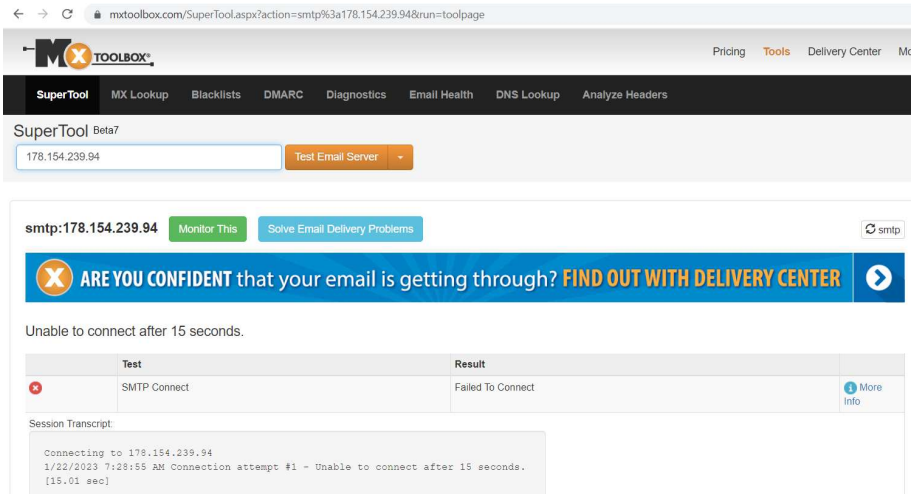
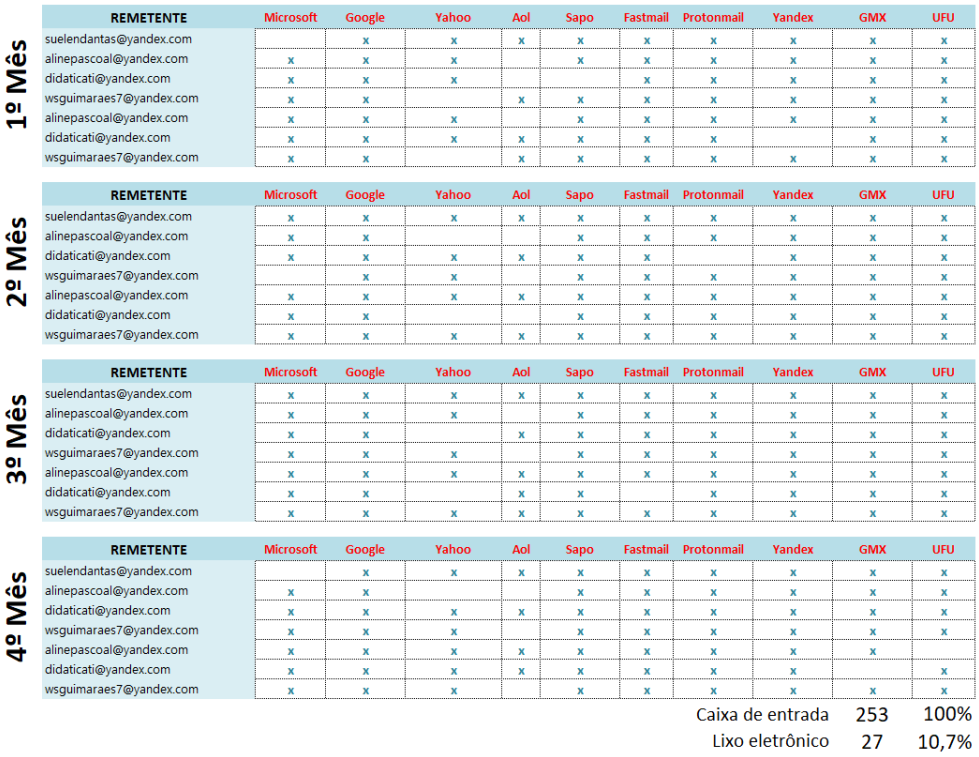



Figura 65 – Yandex - *Relay* Possivelmente Aberto


Figura 66 – Yandex - Pontuação


Figura 67 – Yandex - *Mail Tester*



1º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| suelendantas@yandex.com | | x | x | x | x | x | x | x | x | x |
| alinepascoal@yandex.com | x | x | x | | x | x | x | x | x | x |
| didaticati@yandex.com | x | x | x | | | x | x | x | x | x |
| wsguimaraes7@yandex.com | x | x | | x | x | x | x | x | x | x |
| alinepascoal@yandex.com | x | x | x | | x | x | x | x | x | x |
| didaticati@yandex.com | x | x | x | x | x | x | x | | x | x |
| wsguimaraes7@yandex.com | x | x | | x | x | x | x | x | x | x |

2º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| suelendantas@yandex.com | x | x | x | x | x | x | x | x | x | x |
| alinepascoal@yandex.com | x | x | | | x | x | x | x | x | x |
| didaticati@yandex.com | x | x | x | x | x | x | | x | x | x |
| wsguimaraes7@yandex.com | | x | x | | x | x | x | x | x | x |
| alinepascoal@yandex.com | x | x | x | x | x | x | x | x | x | x |
| didaticati@yandex.com | x | x | | | x | x | x | x | x | x |
| wsguimaraes7@yandex.com | x | x | x | x | x | x | x | x | x | x |

3º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| suelendantas@yandex.com | x | x | x | x | x | x | x | x | x | x |
| alinepascoal@yandex.com | x | x | x | | x | x | x | x | x | x |
| didaticati@yandex.com | x | x | | x | x | x | x | x | x | x |
| wsguimaraes7@yandex.com | x | x | x | | x | x | x | x | x | x |
| alinepascoal@yandex.com | x | x | x | x | x | x | x | x | x | x |
| didaticati@yandex.com | x | x | | x | x | | x | x | x | x |
| wsguimaraes7@yandex.com | x | x | x | x | x | x | x | x | x | x |

4º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| suelendantas@yandex.com | | x | x | x | x | x | x | x | x | x |
| alinepascoal@yandex.com | x | x | | | x | x | x | x | x | x |
| didaticati@yandex.com | x | x | x | x | x | x | x | x | x | x |
| wsguimaraes7@yandex.com | x | x | x | | x | x | x | x | x | x |
| alinepascoal@yandex.com | x | x | x | x | x | x | x | x | x | |
| didaticati@yandex.com | x | x | x | x | x | x | x | x | | x |
| wsguimaraes7@yandex.com | x | x | x | | x | x | x | x | x | x |

| | | |
|---|---|---|
| Caixa de entrada | 253 | 100% |
| Lixo eletrônico | 27 | 10,7% |

Figura 68 – Yandex - Envios durante 4 meses

### 5.1.3 Envios de Google, Protonmail e Sapo para Yahoo

Nesta seção, serão analisados os experimentos de envios a partir dos provedores Google, Protonmail e Sapo tendo como destino o provedor Yahoo. Para facilitar a compreensão, cada um dos provedores enviadores terão uma seção na qual serão reportados os achados dos experimentos realizados.

#### 5.1.3.1 Envios do Google para Yahoo

Esta seção relata envios do Google (`google.com`), para a Yahoo. O *header* informado pela Yahoo, conforme Fig. 69, recebido do Yahoo, podendo-se verificar os protocolos SPF, DKIM e DMARC foram configurados corretamente.

A análise do DNS informa que o endereço IP do servidor MTA da Google aponta corretamente para o FQDN informado pelo *header* apresentado na Fig. 69 (**??**), indicando que o DNS Reverso está correto, conforme se pode observar na Fig. 70.

O MxToolBox (`mxtoolbox.com`) reporta o endereço IP do MTA do Google em duas listas de bloqueio, sendo: SORBS NEW e SORBS SPAM, conforme mostra a Fig. 71. Isto indica que o servidor de e-mails da Google pode experimentar a ocorrência de falsos positivos de SPAM.

A verificação de *relay* aberto, com o MxToolBox, indica que o servidor do Google não permitiu a consulta, como mostra a Fig. 72. Todavia, como consta em 2 listas de bloqueio, é possível que o servidor esteja com *relay* aberto.

O *Mail Tester* mostra o Google com 9,5 de 10 pontos possíveis, conforme se pode observar na Fig. 73.

De acordo com o MxToolBox, o principal motivo de não ter alcançado 100% reside em sua presença em duas listas de bloqueio importantes, conforme Fig. 74.

Foram realizados envios Google para os provedores relacionados neste capítulo, sendo que os relatórios foram obtidos por amostragem e os experimentos observados durante 4 meses, como é apresentado na Fig. 75.

Os resultados mostram que o Google obteve um bom percentual em suas entregas, exitindo muitos fatores que influenciam ao resultado final, que foram aqui descritos e estão devidamente relatados em cada análise de envios através dos diversos provedores.

```
Received: from 10.222.142.149
 by atlas321.free.mail.ne1.yahoo.com pod-id NONE with HTTPS; Wed, 2 Nov 2022 12:49:27 +0000
Return-Path: <didaticatioficial@gmail.com>
X-Originating-Ip: [209.85.217.54]
Received-SPF: pass (domain of gmail.com designates 209.85.217.54 as permitted sender)
Authentication-Results: atlas321.free.mail.ne1.yahoo.com;
 dkim=pass header.i=@gmail.com header.s=20210112;
 spf=pass smtp.mailfrom=gmail.com;
 dmarc=pass(p=NONE,sp=QUARANTINE) header.from=gmail.com;
X-Apparently-To: gilbertolealcunha@yahoo.com; Wed, 2 Nov 2022 12:49:28 +0000
X-YMailISG: nCX2fe4WLDtOimnd6MqMKTb4xeiMQYoaNAFPbIGl.dP5PdCz
 VDHzacoXHANAgXTm1_LveQ_H7FWzdDbrfBlfBgjd1TRt1vTyafAdbOV7a1NF
 NAnzurlFkGgGAqIobGSXdb6SGoUSvXNSqQYm2hC53iyfc50_0dtVaZuvO6Ht
 vsmLDchqlyTDBWaTODxDj0F5whZPPn9CznKr_FtXDKaTzalwUfY2Ho78raH7
 b.uEJeX_AiB7CbuYtwU3sfYCqXHBRF5irTpfYssj7xoQcDAYvYDyFHfzIIAJ
 N7XBKvtIw16cqXf5wrYW0Q67qfNynbbSNxN3WAFKLvW1tR0YpELWWi5jAjok
 OUA34flevn_6MDyP15NHnAaggv5L1cKpbCDN8IOWf.rlTyrnP8JMdfoueIcj
 hqyI0vdpniKxXxmFMBZfCAVb8vmrS9VEs61XwPVG4iZycEIVJ4eYRR2kGFIp
 b9TxY7zJSr7RJOxRjS3fM3Vs.a62CgMTMdTvWvS.gUeqpBJKQcobM9LouZ6S
 FrNf5N1aLzUTxccL4rqf82md7VxSZIYY6sAgrfhXFf6m5iLJiFvKvRER5Elx
 IRwJiSbatu5Vu.JGdlrdHXYenTpGFx4Gao5ZnN.l9n1TQ50mq7Xyd9VuMcld
 XxCYTMw.XmGFFoqPKCulX82e231KvDQ21xk_T81mfu7jPKy2H3pWdunCbKkT
 Tc8dUFJeoQs2RDCVO15k294iNxA30yDUHcUAPvBlJa1PneIOySBBV2swVcRT
 2Y5mcAfcPc38mnMc9ab_hyi9Xx9ajR82EM_Yls7OGvpxW58iE1nYrk7AU6CG
 1C5cLFuw44PqCTmeH.lCMtQ..pGT02RKhu14_hB5q9zcbDiVoYi9.2sa0Fag
 z.QFtvdLqY.m0ecStc9IDmwtCfmJHm9PgiYWbaqgCU51BibeRlcfp3wsHoGA
 GV9VhzqduuSBwW5wPlHaJDZoLQ.bfpfDcCwWwyqed1X25XSw36XVTyVz.JMU
 hdJ5VkIIUp_MK3eDHZtt6V56GCZj1AQIWOhr9T0wLy4HwyWGJvgomZqmO9Ii
 DfVuPl4plCnVCbXBlN8s43b3Jcux.foNwkJny21yOB4EI2J9ROKNnR_IlUF4
 2ql1bhXd9vsDCxtjm2N1VbrIzanpLdDNmd6BSJEdHpfsLzAw1OIfFZiBUjL7
 yHM69ddzwmsqyKLZw4FKR2wP
Received: from 209.85.217.54 (EHLO mail-vs1-f54.google.com)
 by 10.222.142.149 with SMTPs
 (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256);
 Wed, 02 Nov 2022 12:49:27 +0000
Received: by mail-vs1-f54.google.com with SMTP id z189so16464693vsb.4
        for <gilbertolealcunha@yahoo.com>; Wed, 02 Nov 2022 05:49:27 -0700 (PDT)
```

Figura 69 – *Header* Yahoo - Mensagem recebida do Google

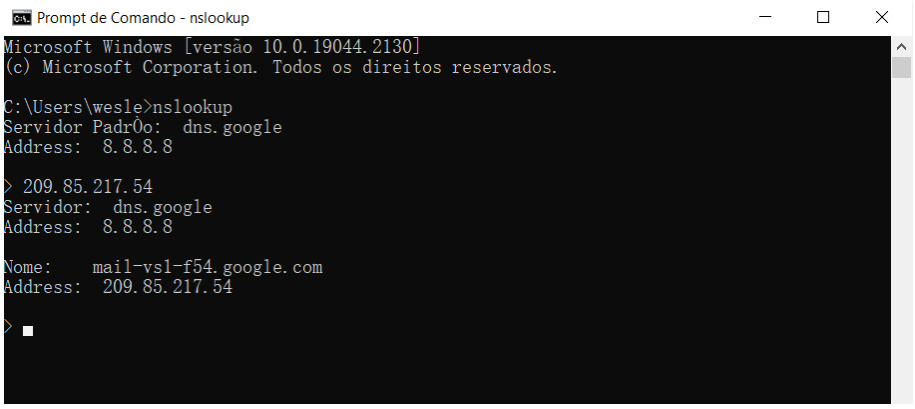



Figura 70 – Google - DNS Reverso

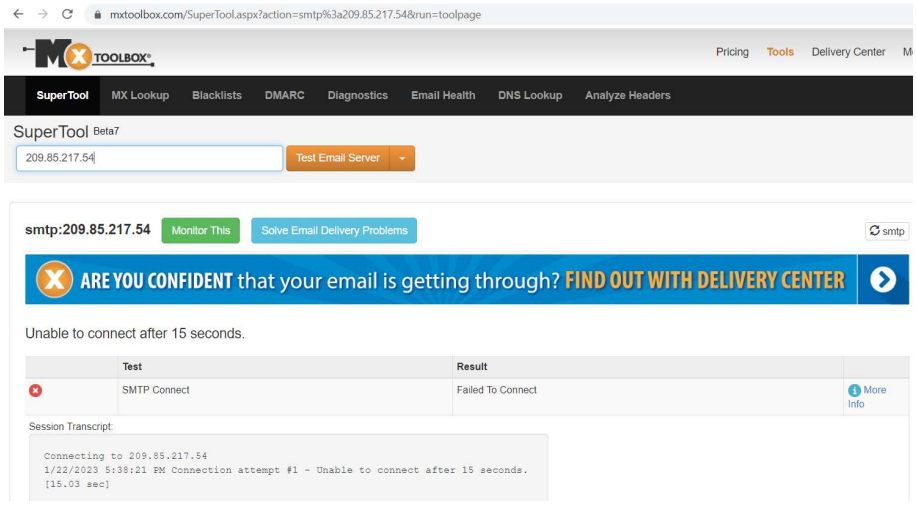



Figura 71 – Google - Lista de Bloqueio

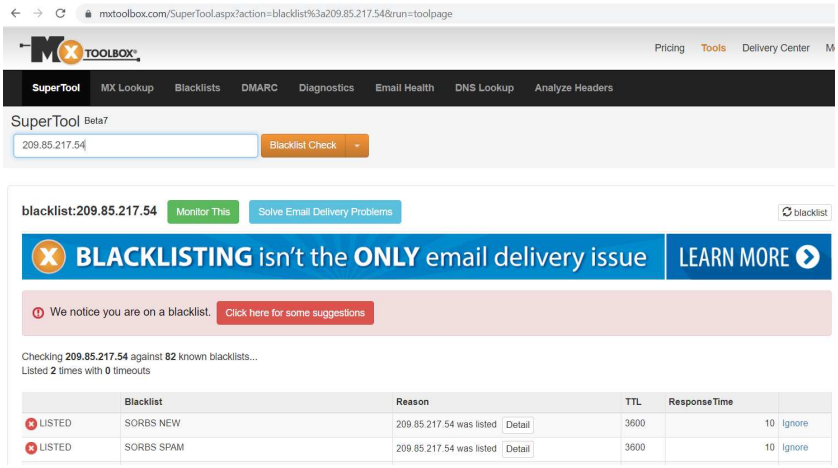
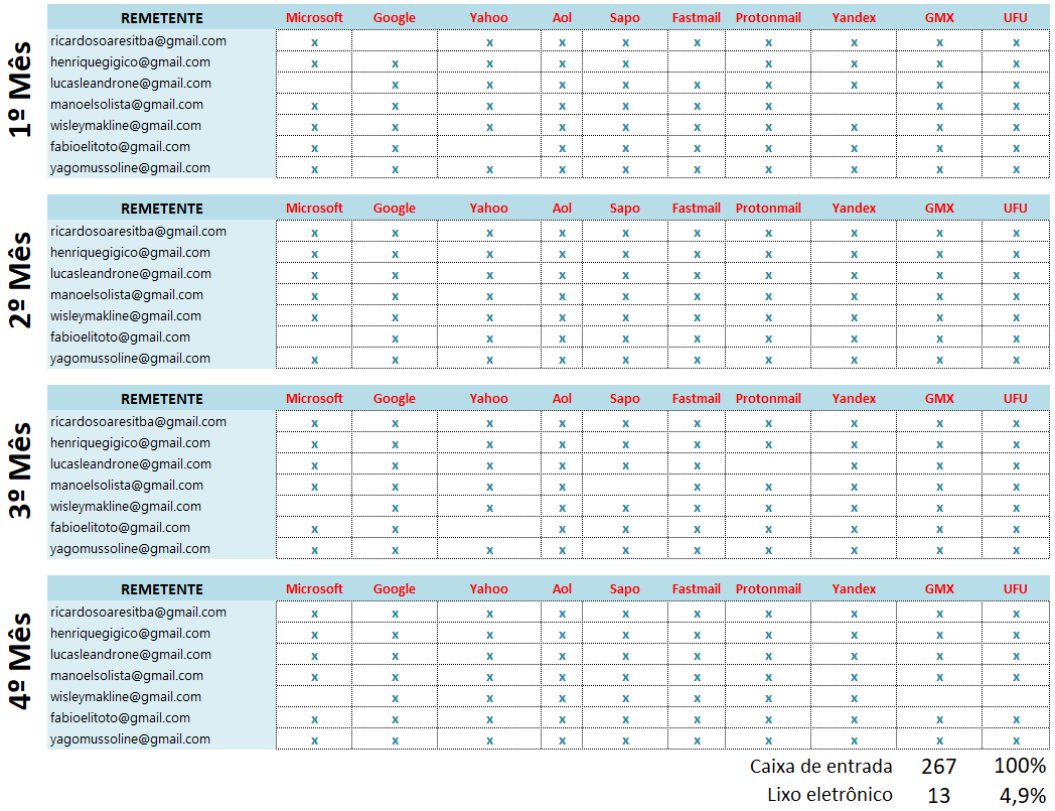



Figura 72 – Google - *Relay* Possivelmente Aberto


Figura 73 – Google - Pontuação


Figura 74 – Google - *Mail Tester*



1º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| ricardosoaresitba@gmail.com | x | | x | x | x | x | x | x | x | x |
| henriquegigico@gmail.com | x | x | x | x | x | | x | x | x | x |
| lucasleandrone@gmail.com | | x | x | x | x | x | x | x | x | x |
| manoelsolista@gmail.com | x | x | x | x | x | x | x | | x | x |
| wisleymakline@gmail.com | x | x | x | x | x | x | x | x | x | x |
| fabioelitoto@gmail.com | x | x | | x | x | x | x | x | x | x |
| yagomussoline@gmail.com | x | x | x | x | x | x | x | x | x | x |

2º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| ricardosoaresitba@gmail.com | x | x | x | x | x | x | x | x | x | x |
| henriquegigico@gmail.com | x | x | x | x | x | x | x | x | x | x |
| lucasleandrone@gmail.com | x | x | x | x | x | x | x | x | x | x |
| manoelsolista@gmail.com | x | x | x | x | x | x | x | x | x | x |
| wisleymakline@gmail.com | x | x | x | x | x | x | x | x | x | x |
| fabioelitoto@gmail.com | | x | x | x | x | x | x | x | x | x |
| yagomussoline@gmail.com | x | x | x | x | x | x | x | x | x | x |

3º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| ricardosoaresitba@gmail.com | x | x | x | x | x | x | x | x | x | x |
| henriquegigico@gmail.com | x | x | x | x | x | x | x | x | x | x |
| lucasleandrone@gmail.com | x | x | x | x | x | x | | x | x | x |
| manoelsolista@gmail.com | x | x | x | x | | x | x | x | x | x |
| wisleymakline@gmail.com | | x | x | x | x | x | x | x | x | x |
| fabioelitoto@gmail.com | x | x | | x | x | x | x | x | x | x |
| yagomussoline@gmail.com | x | x | x | x | x | x | x | x | x | x |

4º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| ricardosoaresitba@gmail.com | x | x | x | x | x | x | x | x | x | x |
| henriquegigico@gmail.com | x | x | x | x | x | x | x | x | x | x |
| lucasleandrone@gmail.com | x | x | x | x | x | x | x | x | x | x |
| manoelsolista@gmail.com | x | x | x | x | x | x | x | x | x | x |
| wisleymakline@gmail.com | | x | x | x | x | x | x | x | | |
| fabioelitoto@gmail.com | x | x | x | x | x | x | x | x | x | x |
| yagomussoline@gmail.com | x | x | x | x | x | x | x | x | x | x |

| | | |
|---|---|---|
| Caixa de entrada | 267 | 100% |
| Lixo eletrônico | 13 | 4,9% |

Figura 75 – Google - Envios durante 4 meses

#### 5.1.3.2 Envios do Protonmail para Yahoo

Esta seção relata envios do Prontonmail (`protonmail.com`) para a Yahoo. O *header* informado pela Yahoo, conforme Fig. 76, recebido do Protonmail. Pode-se observar que os protocolos SPF, DKIM e DMARC foram configurados de forma correta.

A consulta ao DNS mostra que o endereço IP do servidor MTA do Protonmail resolve adequadamente para o FQDN especificado no *header*, conforme apresenta a Fig. 76, permitindo verificar que o DNS Reverso está configurado adequadamente, como mostra a Fig. 77.

A análise com o MxToolBox mostra que o MTA do Protonmail não está relacionado em nenhuma lista de bloqueio, conforme é possível verificar pela Fig. 78.

Em relação a *Relay*, não foi possível verificar se o Protonmail tem seu *relay* aberto, pois o servidor não permitiu a consulta, conforme pode ser observado na Fig. 79.

A verificação da pontuação do Protonmail pela ferramenta *Mail Tester* mostra o provedor com 10 de 10 pontos possíveis, conforme aponta a Fig. 94.

Foram realizados envios do Protonmail para os provedores relacionados neste capítulo, sendo que os relatórios foram obtidos por amostragem, em experimentos observados durante 4 meses, conforme é apresentado na Fig. 95.

Os resultados mostram que o Protonmail obteve um bom percentual em suas entregas. É interessante notar que apesar de ter todos os parâmetros necessários, ainda assim houve

a presença de falsos positivos, talvez merecendo uma investigação mais aprofundada.

```
Received: from 10.197.39.201
 by atlas220.free.mail.bf1.yahoo.com with HTTPS; Mon, 31 Oct 2022 13:17:37 +0000
Return-Path: <zehumberto@protonmail.com>
X-Originating-Ip: [185.70.40.135]
Received-SPF: pass (domain of protonmail.com designates 185.70.40.135 as permitted sender)
Authentication-Results: atlas220.free.mail.bf1.yahoo.com;
 dkim=pass header.i=@protonmail.com header.s=protonmail3;
 spf=pass smtp.mailfrom=protonmail.com;
 dmarc=pass(p=QUARANTINE) header.from=protonmail.com;
X-Apparently-To: gilbertolealcunha@yahoo.com; Mon, 31 Oct 2022 13:17:37 +0000
X-YMailAVSC: 6V9WhWs3bBtWyyeUUpQtm5oNB9dXo6VXCpQve_kvgxRRvh4
Received: from 185.70.40.135 (EHLO mail-40135.protonmail.ch)
 by 10.197.39.201 with SMTPs
 (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256);
 Mon, 31 Oct 2022 13:17:37 +0000
Date: Mon, 31 Oct 2022 13:17:27 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=protonmail.com;
```

Figura 76 – *Header* Yahoo - Mensagem recebida do Protonmail

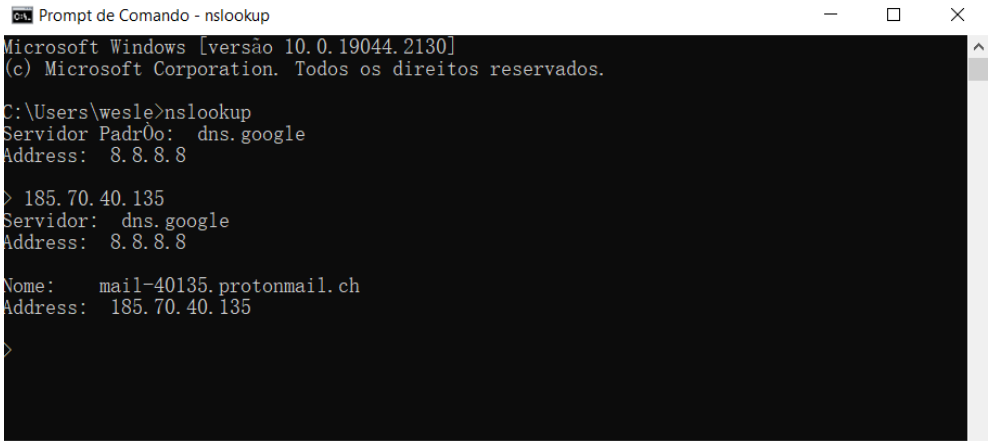



Figura 77 – Protonmail - DNS Reverso

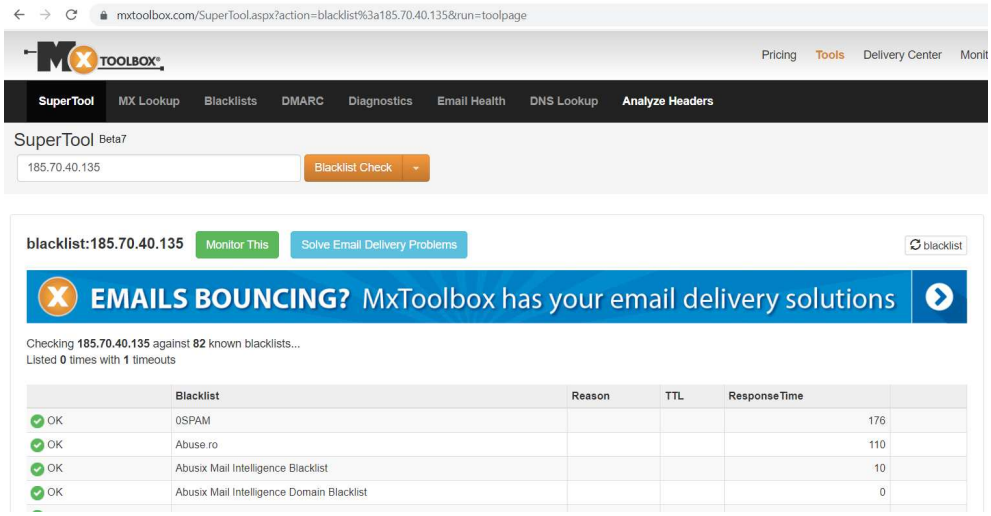



Figura 78 – Protonmail - Lista de Bloqueio

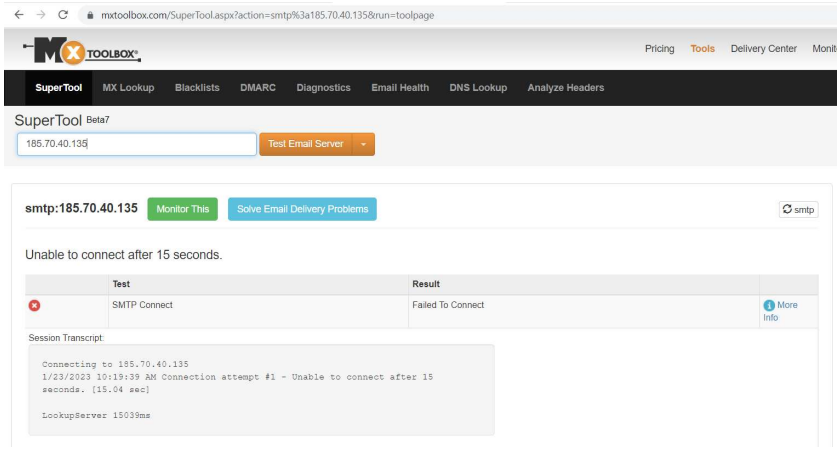



Figura 79 – Protonmail - *Relay* Possivelmente Aberto


Figura 80 – Protonmail - Pontuação

**1º Mês**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| brunamattos@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| juniorvilana@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| riquinha@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| wesleys@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| brunamattos@protonmail.com | x | | x | x | x | x | x | x | x | x |
| juniorvilana@protonmail.com | | x | x | x | x | x | x | x | x | x |
| riquinha@protonmail.com | x | x | x | x | x | x | x | x | x | x |

**2º Mês**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| brunamattos@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| juniorvilana@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| riquinha@protonmail.com | | x | x | x | x | x | x | x | x | x |
| wesleys@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| brunamattos@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| juniorvilana@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| riquinha@protonmail.com | | x | x | x | x | x | x | x | x | x |

**3º Mês**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| brunamattos@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| juniorvilana@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| riquinha@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| wesleys@protonmail.com | x | x | x | | x | x | x | x | x | x |
| brunamattos@protonmail.com | | x | x | | x | x | x | x | x | x |
| juniorvilana@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| riquinha@protonmail.com | x | x | x | x | x | x | x | x | x | x |

**4º Mês**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| brunamattos@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| juniorvilana@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| riquinha@protonmail.com | | x | x | x | x | x | x | x | x | x |
| wesleys@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| brunamattos@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| juniorvilana@protonmail.com | x | x | x | x | x | x | x | x | x | x |
| riquinha@protonmail.com | x | x | x | x | x | x | x | x | x | x |

| | | |
|---|---|---|
| Caixa de entrada | 272 | 100% |
| Lixo eletrônico | 8 | 2,9% |

Figura 81 – Protonmail - Envios durante 4 meses

#### 5.1.3.3 Envios do Sapo para Yahoo

Esta seção relata envios do Sapo (`sapo.pt`) para o Yahoo. O *header* informado pelo Yahoo, conforme Fig. 82, recebido do Sapo, nele sendo possível perceber que apenas o protocolo SPF foi configurado adequadamente. Os protocolos DKIM e DMARC não foram configurados, pois mão aparecem no cabeçalho.

A consulta ao DNS permite verificar que o endereço IP do servidor MTA do provedor Sapo resolve corretamente para o FQDN informado pelo *header* (Fig. 82), indicando que a configuração do DNS Reverso está correta, conforme mostra a Fig. 83.

O MxToolBox reporta a presença do endereço IP do provedor Sapo em três listas de bloqueio, conforme indica a Fig. 84, sendo: SORBS NEW; UCE *Protect* Nível 3; e ZapBL[6] - *Zap Block List* (`zapbl.net`).

O servidor do Sapo não permitiu verificar o estado de *relay*, pois não houve resposta à consulta conforme se pode observar na Fig. 85. Todavia, o fato de constar na UCE *Protect* Nível 3, além da SORBS NEW, é uma indicação forte de que seu *relay* está aberto.

A verificação da pontuação do Sapo com o *Mail Tester* mostra o provedor com 9 de 10 pontos possíveis, conforme mostra a Fig. 86.

O motivo pelo qual o servidor obteve esse resultado está relacionado à ausência dos protocolos DKIM e DMARC, conforme se pode verificar na Fig. 87, sendo que não somente estas insuficiências foram determinantes para a avaliação auferida, tais como os registros em programas de combate a SPAM.

```
Received: from 127.0.0.1
 by atlas-production.v2-mail-prod1-gq1.omega.yahoo.com with HTTP; Sat, 29 Oct 2022 23:54:28 +0000
Return-Path: <fabiolaandrade@sapo.pt>
X-Originating-Ip: [212.55.154.22]
Received-SPF: pass (domain of sapo.pt designates 212.55.154.22 as permitted sender)
Authentication-Results: atlas-production.v2-mail-prod1-gq1.omega.yahoo.com;
 dkim=unknown;
 spf=pass smtp.mailfrom=sapo.pt;
 dmarc=unknown header.from=sapo.pt;
X-Apparently-To: gilbertolealcunha@yahoo.com; Sat, 29 Oct 2022 23:54:28 +0000
Received: from 212.55.154.22 (EHLO relay2.ptmail.sapo.pt)
 by 10.214.173.215 with SMTPs
 (version=TLS1_2 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256);
 Sat, 29 Oct 2022 23:54:28 +0000
Received: (qmail 962 invoked from network); 29 Oct 2022 23:54:24 -0000
Received: from [::ffff:177.191.51.114] ([::ffff:177.191.51.114]) by
 mail.sapo.pt (Horde Framework) with HTTPS; Sun, 30 Oct 2022 00:54:23 +0100
Date: Sun, 30 Oct 2022 00:54:23 +0100
Message-ID: <20221030005423.Horde.NAmpe7YQ_3z1yKTCioihjk4@mail.sapo.pt>
From: fabiolaandrade@sapo.pt
```

Figura 82 – *Header* Yahoo - Mensagem recebida do Sapo

[6] Lista de bloqueio em tempo real baseada em DNS mantida por administradores sobre de onde eles não desejam receber e-mails.

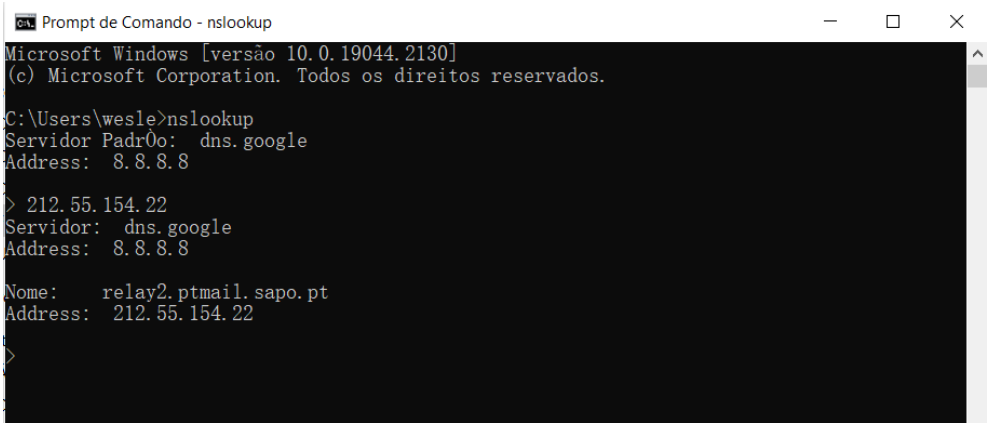



Figura 83 – Sapo - DNS Reverso

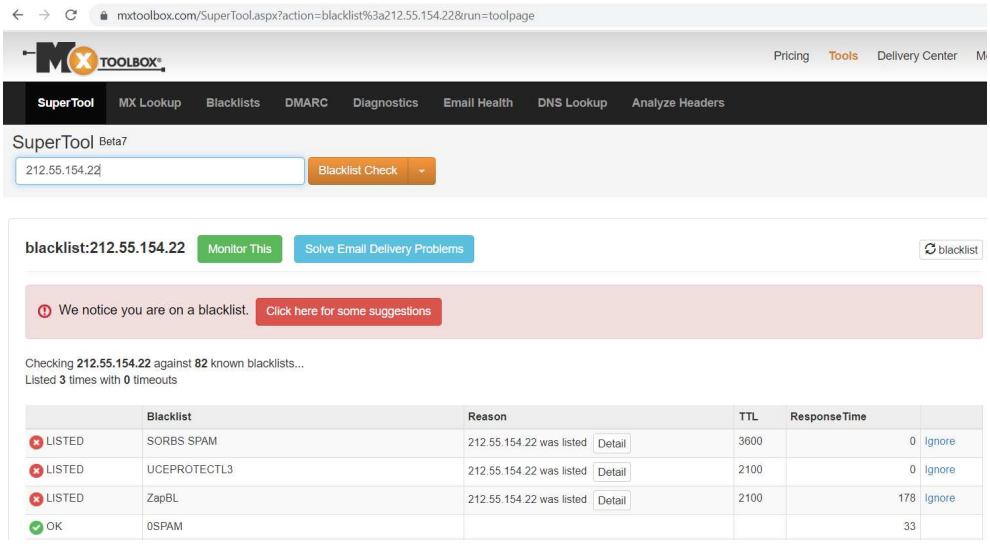



Figura 84 – Sapo - Lista de Bloqueio

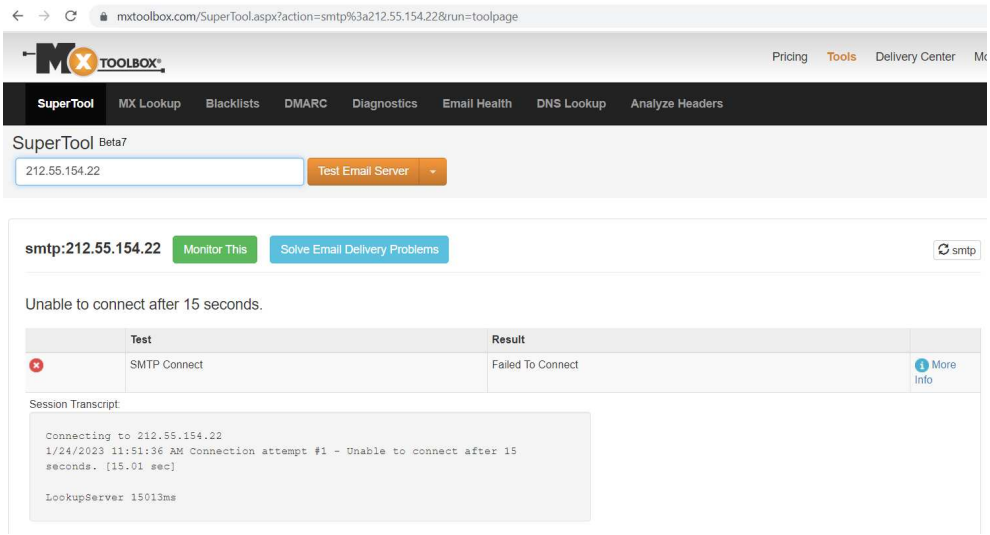



Figura 85 – Sapo - *Relay* Possivelmente Aberto

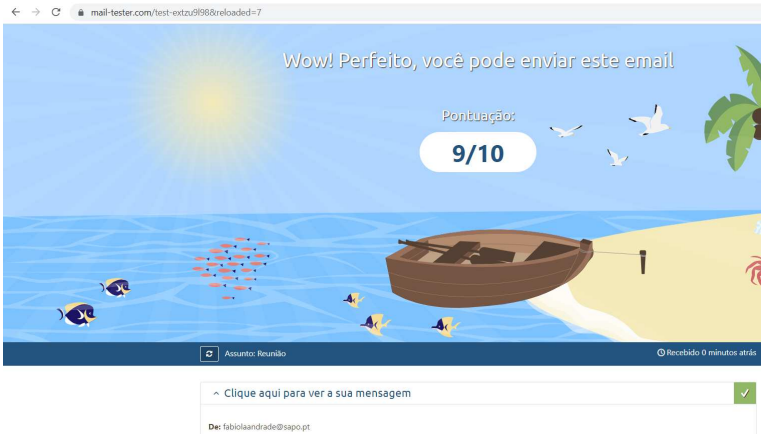
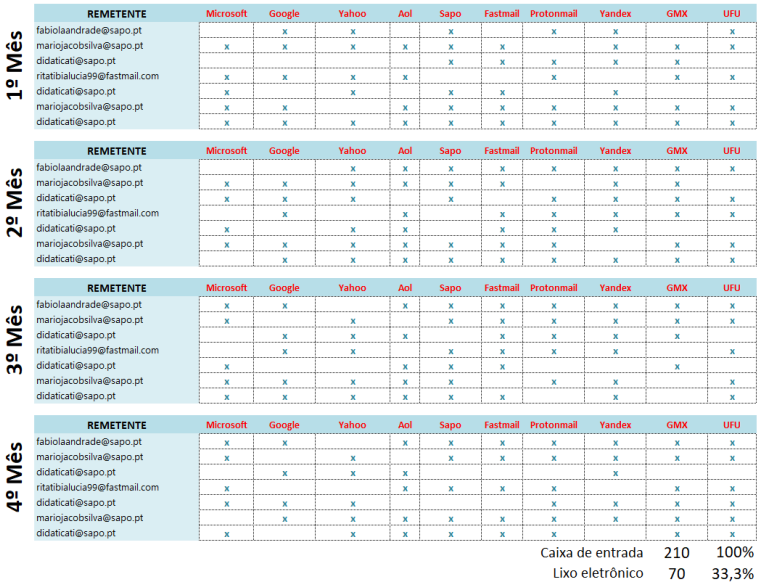



Figura 86 – Sapo - Pontuação


Figura 87 – Sapo - *Mail Tester*



1º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| fabiolaandrade@sapo.pt | | x | x | | x | | x | x | | x |
| mariojacobsilva@sapo.pt | x | x | x | x | x | x | | x | x | x |
| didaticati@sapo.pt | | | | | x | x | x | x | x | |
| ritatibialucia99@fastmail.com | x | x | x | x | | | x | | x | x |
| didaticati@sapo.pt | x | | x | | x | x | | x | | |
| mariojacobsilva@sapo.pt | x | x | | x | x | x | x | x | x | x |
| didaticati@sapo.pt | x | x | x | x | x | x | x | x | x | x |

2º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| fabiolaandrade@sapo.pt | | | x | x | x | x | x | x | x | x |
| mariojacobsilva@sapo.pt | x | x | x | x | x | x | | x | x | |
| didaticati@sapo.pt | x | x | x | | x | | x | x | x | x |
| ritatibialucia99@fastmail.com | | x | | x | | x | x | x | x | x |
| didaticati@sapo.pt | x | | x | x | | x | x | x | | |
| mariojacobsilva@sapo.pt | x | x | x | x | x | x | x | | x | x |
| didaticati@sapo.pt | | x | x | x | x | x | x | x | x | x |

3º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| fabiolaandrade@sapo.pt | x | x | | x | x | x | x | x | x | x |
| mariojacobsilva@sapo.pt | x | | x | | x | x | x | x | x | x |
| didaticati@sapo.pt | | x | x | x | | x | x | x | x | |
| ritatibialucia99@fastmail.com | | x | x | | x | x | x | x | | x |
| didaticati@sapo.pt | x | | | x | x | x | | | x | |
| mariojacobsilva@sapo.pt | x | x | x | x | x | | x | x | | x |
| didaticati@sapo.pt | x | x | x | x | x | x | | x | | x |

4º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| fabiolaandrade@sapo.pt | x | x | | x | x | x | x | x | x | x |
| mariojacobsilva@sapo.pt | x | | x | | x | x | x | x | x | x |
| didaticati@sapo.pt | | x | x | x | | | | x | | |
| ritatibialucia99@fastmail.com | x | | | x | x | x | x | | x | x |
| didaticati@sapo.pt | x | x | x | | | | x | x | x | x |
| mariojacobsilva@sapo.pt | | x | x | x | x | x | x | x | x | x |
| didaticati@sapo.pt | x | | x | x | x | x | x | | x | x |

| | | |
|---|---|---|
| Caixa de entrada | 210 | 100% |
| Lixo eletrônico | 70 | 33,3% |

Figura 88 – Sapo - Envios durante 4 meses

As análises feitas até este momento reforçam a importância da orquestração e da existência de padrões de provisionamentos, tirando dos provedores certas liberalidades, de aplicar ou não certos padrões, conforme lhes convier.

Cabe ressaltar que a análise apresentada para os envios mencionados, será baseada nos *headers*, considerando que as seções anteriores mostram os efeitos da configurações, ou não, dos protocolos SPF, DKIM e DMARC. A Tabela 2 apresenta um resumo dos achados durantes os experimentos. Nesta tabela, os campos têm os seguintes significados:

- **Provedor**: especifica o nome do provedor utilizado no experimento;
- ***Score***: denota a uma nota de sanidade, que varia de 0 a 10, em experimento realizado com a ferramenta MxToolBox;
- ***Relay***: é uma capacidade que os MTAs têm de encaminhar (Aberto), ou não (Fechado), mensagens oriundas de MTAs externos e destinadas a MTAs externos, de outros provedores, sendo que a boa prática indica que 'Fechado' é o correto;
- **rDNS**: especifica se o DNS Reverso está configurado corretamente (Sim), ou Não, permitindo verificar a veracidade do nome indicada no cabeçalho da mensagem;
- **BL**: indica a quantidade de listas de bloqueios (*Blocked List*) nas quais o provedor consta como bloqueado, sendo o ideal que não esteja relacionado em nenhuma lista de bloqueios (0);
- **Protocolos**: especifica quais protocolos, daqueles descritos na Seção 3.2.3, são utilizados pelo provedor, podendo ser SPF, DKIM e DMARC.

Tabela 2 – Resultado de Experimentos sem Plano de Controle

| **Provedor** | ***Score*** | ***Relay*** | **rDNS** | **BL** | **Protocolos** |
|---|---|---|---|---|---|
| AOL | 9,0 | Possivelmente Aberto | Sim | 1 | SPF DKIM DMARC |
| Sapo | 9,0 | Possivelmente Aberto | Sim | 3 | SPF |
| Fastmail | 9,9 | Não Permitiu Consulta | Sim | 0 | SPF DKIM DMARC |
| GMX | 8,4 | Possivelmente Aberto | Sim | 2 | SPF DMARC |
| Google | 9,5 | Possivelmente Aberto | Sim | 2 | SPF DKIM DMARC |
| Microsoft | 9,5 | Possivelmente Aberto | Não | 1 | SPF DKIM DMARC |
| Protonmail | 10,0 | Não Permitiu Consulta | Sim | 2 | SPF DKIM DMARC |
| UFU | | Não Permitiu Consulta | Não | 0 | SPF DKIM |
| UFU365 | 10,0 | Não Permitiu Consulta | Não | 0 | SPF DKIM DMARC |
| Yahoo | 9,5 | Possivelmente Aberto | Sim | 1 | SPF DKIM DMARC |
| Yandex | 10,0 | Possivelmente Aberto | Sim | 4 | SPF DKIM DMARC |

É interessante notar na Tabela 2 que provedores largamente conhecidos e utilizados por milhões de usuários, com imagem consolidada mundialmente, tais como Google, Microsoft, AOL e Yahoo apresentam pontuação (*Score*) de sanidade inferiores a 10 (nota

máxima). Nessa tabela, é possível ver que apenas três provedores mais conhecidos na Europa alcançaram 10.

A pontuação inferior a 10 é justificada em parte por apresentarem *Relays* possivelmente abertos e, também, por estarem em listas de bloqueios (BL) importantes, que são consultadas pelos provedores destinatários na categorização de mensagens. Observem que uma gestão sistemática, automatizada, poderia: 1) verificar se o provedor se encontra registrado nessas listas; e 2) caso estejam, tomar as providências para as respectivas remoções.

Chama a atenção também, o DNS Reverso (rDNS) não estar configurado devidamente em alguns desses provedores de classe mundiais. É uma coisa relativamente simples de se verificar e, igualmente, simples de resolver, por uma gestão automatizada.

Do ponto de vista dos protocolos de autenticação e autorização (SPF, DKIM e DMARC), é possível ver que, à exceção de três provedores (Sapo, GMX e UFU), todos os demais os implementam adequadamente. Todavia, também neste caso, há aspectos de gestão que poderiam melhorar ainda mais as autenticações.

A Tabela 2 apresenta uma análise das configurações, que podem ser gerenciadas e controladas à medida que haja necessidade de alterações em agentes MHS (Plano de Dados). Além disso, o projeto também fez uma análise dinâmica, a partir do envio de mensagens das contas criadas nos provedores enumerados na Tabela 1, para verificar o quão eficazes são os provedores em evitar falsos (negativos ou positivos).

## 5.2 Envio por Servidor configurado por *iRedMail*

Talvez o leitor esteja se perguntando do "por que da existência desta seção?". O *iRedMail* é, provavelmente, o *script* de instalação e configuração do MTA Postfix mais utilizado no mundo. O Brasil tem milhares de *Internet Service Provider* (ISP)s e a maioria massiva deles utiliza o *iRedMail*[7].

Por esta razão, o *iRedMail* será utilizado para instalar e configurar um MTA “padrão de mercado”, que será denominado *iRedMTA*, a partir do qual serão feitos testes para fins de comparação com os resultados da SPAM-K.

O iRedMTA é hospedado no servidor `mx-01.projetoppgco.com.br` no qual foram provisionados: os protocolos SPF, DKIM e DMARC; DNS Reverso (rDNS); e inscrições em programas de combate a SPAMs - tais como *Junk Mail Program Report* (JMPR) da Microsoft.

Foram feitas verificações que: o domínio (Endereço IP do MTA) não conste em nenhuma lista de bloqueio; a pontuação de sanidade seja 100% (*Mail Tester*); não haja contra indicação à confiabilidade do MTA; e, por fim, que o *Relay* esteja fechado.

[7] Este é um levantamento empírico, não havendo uma pesquisa formal.

Além das verificações, envelopes (mensagens) terão cabeçalhos formatados com cláusulas "amigáveis", que indicam a provedores de destinos que se originam em sites confiáveis, sendo que todos esses pré-requisitos foram utilizados nos experimentos envolvendo provedores públicos e gratuitos.

O objetivo da existência desta seção é avaliar um MTA '*default*', implantado pelo *iRedMail* com as configurações nativas, por esta razão, não foram feitas alterações nas configurações do `main.cf`, que é o principal arquivo de configuração do MTA Postfix, sendo isto que se denominou iRedMTA.

Esta abordagem permite analisar a acurácia dos primeiros experimentos, que serão comparados com aqueles da SPAM-K, relatados na Seção 5.3, que fará provisionamentos detalhados no artefato `main.cf`.

Como esperado, os experimentos mostraram que os resultados obtidos, em função de envios do iRedMTA para os demais provedores nominados neste capítulo, foram muito próximos, então, por este motivo, este trabalho relata os resultados obtidos com envios para os provedores de email Google (Seção 5.2.1) e Microsoft (Seção 5.2.2).

Cabe ressaltar que a análise apresentada para os envios mencionados, será baseada nos *headers*, considerando que as seções anteriores mostram os efeitos da configurações, ou não, dos protocolos SPF, DKIM e DMARC.

Escolhidos os provedores de destino mencionados, cabe frisar que houve alguns dados gerais, merecedores de um olhar, que são reportados na Seção 5.2.3.

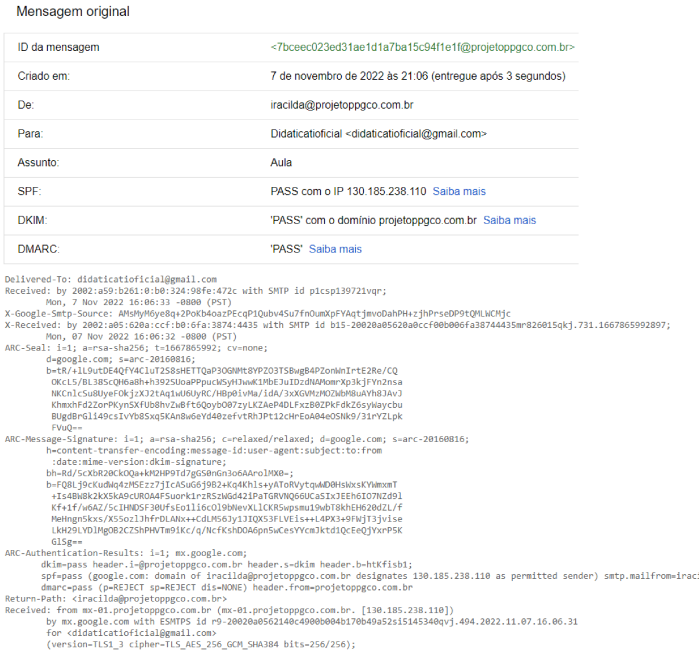
### 5.2.1 Envios do iRedMTA para Google

Nesta seção será relatado o experimento de envios a partir do iRedMTA para o Google. A Fig. 89 apresenta o *header* informado pelo Google, recebido da mensagem enviada pelo iRedMTA.

É possível verificar na Fig. 89, que os protocolos SPF, DKIM e DMARC foram configurados adequadamente e, então, é possível depreender aspectos tais como a pontuação do iRedMTA, feita pela MxToolBox.

### 5.2.2 Envios do iRedMTA para Microsoft

Esta seção relata os experimentos de envios a partir do iRedMTA para o Microsoft. A análise do *header* informado pelo Microsoft, a partir da mensagem recebida pelo iRedMTA, apresentado na Fig. 90, permite verificar que os protocolos SPF, DKIM e DMARC foram configurados adequadamente, do mesmo modo como foi reportado pelo Google na Seção 5.2.1.



Mensagem original

| | |
|---|---|
| ID da mensagem | <7bceec023ed31ae1d1a7ba15c94f1e1f@projetoppgco.com.br> |
| Criado em: | 7 de novembro de 2022 às 21:06 (entregue após 3 segundos) |
| De: | iracilda@projetoppgco.com.br |
| Para: | Didaticatiofícial <didaticatiofícial@gmail.com> |
| Assunto: | Aula |
| SPF: | PASS com o IP 130.185.238.110 Saiba mais |
| DKIM: | 'PASS' com o domínio projetoppgco.com.br Saiba mais |
| DMARC: | 'PASS' Saiba mais |


```
Delivered-To: didaticatiofícial@gmail.com
Received: by 2002:a59:b261:0:b0:324:98fe:472c with SMTP id p1csp139721vqr;
        Mon, 7 Nov 2022 16:06:33 -0800 (PST)
X-Google-Smtp-Source: AMsMyM6ye8q+2PoKb4oazPEcqP1Qubv4Su7fnOumXpFYAqtjmvoDahPH+zjhPrseDP9tQMLWCMjc
X-Received: by 2002:a05:620a:ccf:b0:6fa:3874:4435 with SMTP id b15-20020a05620a0ccf00b006fa38744435mr826015qkj.731.1667865992897;
        Mon, 07 Nov 2022 16:06:32 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1667865992; cv=none;
        d=google.com; s=arc-20160816;
        b=tR/+lL9utDE4QfY4C1uT2S8sHETTQaP3OGNMt8YPZO3TSBwgB4PZonWnIrtE2Re/CQ
         OKcL5/BL38ScQH6a8h+h392SUoaPPpucWSyHJwwK1MbEJuIDzdNAMomrXp3kjFYn2nsa
         NKCnlcSu8UyeFOkjzXJ2tAq1wU6UyRC/HBp0ivMa/idA/3xXGVMzMOZWbM8uAYh8JAvJ
         KhmxhFd2ZorPKymSXfUb8hvZwBftGQoybO07zyLKZAeP4DLFxzB0ZPkFdkZ6syWaycbu
         BUgdBrGll49csIvVb8SxqSKAn8w6eYd40zefvtRhJPt12cHrEoA04eOSNk9/31rYZLpk
         FVuQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=content-transfer-encoding:message-id:user-agent:subject:to:from
         :date:mime-version:dkim-signature;
        bh=Rd/5cXbR20CkDQa+KM2HP9TdZgG50n6n3o6AArolMX0=;
        b=FQ8Lj9cKudWq4zMSEzz7jIcASuG6j9B2+Kq4Khls+yATaRVytqwMD0HsWxsKYWmxmT
         +Is4Bw8k2kX5kA9cURO4AFSuork1rzRSzWGd42iPaTGRVNQ6GUCaSIxJEEh6IO7NZd9l
         Kf+1f/w6AZ/5cIHNDSF30UfsEo1li6cOl9bNevXLlCKRSwpsmu19wbT8khEH620dZL/f
         MeHngn5kxs/XS5ozlJhfrDLANx++CdLMS6Jy1JIQX53FiVEis++L4PX3+9FwjT3jvise
         ikH29LYDlMgOB2CZShPHVTm9lKc/q/NcFkShDOA6pn5wCesYVcm3ktd1QcEeQjYxrP5K
         Gl5g==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@projetoppgco.com.br header.s=dkim header.b=htKfisb1;
       spf=pass (google.com: domain of iracilda@projetoppgco.com.br designates 130.185.238.110 as permitted sender) smtp.mailfrom=iracilda@projetoppgco.com.br;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=projetoppgco.com.br
Return-Path: <iracilda@projetoppgco.com.br>
Received: from mx-01.projetoppgco.com.br (mx-01.projetoppgco.com.br. [130.185.238.110])
        by mx.google.com with ESMTPS id r9-20020a0562140c4900b004b170b49a52si5145340qvj.494.2022.11.07.16.06.31
        for <didaticatiofícial@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
```


Figura 89 – *Header* Google - Origem iRedMTA

**Origem da mensagem**


```
Received: from BL1PR12MB5753.namprd12.prod.outlook.com (::1) by
 MW2PR12MB2554.namprd12.prod.outlook.com with HTTPS; Mon, 29 Aug 2022 13:08:13
 +0000
Received: from DB6P191CA0021.EURP191.PROD.OUTLOOK.COM (2603:10a6:6:28::31) by
 BL1PR12MB5753.namprd12.prod.outlook.com (2603:10b6:208:390::15) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5566.21; Mon, 29 Aug
 2022 13:08:12 +0000
Received: from DB8EUR06FT053.eop-eur06.prod.protection.outlook.com
 (2603:10a6:6:28:cafe::8d) by DB6P191CA0021.outlook.office365.com
 (2603:10a6:6:28::31) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5566.14 via Frontend
 Transport; Mon, 29 Aug 2022 13:08:11 +0000
Authentication-Results: spf=pass (sender IP is 130.185.238.110)
 smtp.mailfrom=projetoppgco.com.br; dkim=pass (signature was verified)
 header.d=projetoppgco.com.br;dmarc=pass action=none
 header.from=projetoppgco.com.br;compauth=pass reason=100
Received-SPF: Pass (protection.outlook.com: domain of projetoppgco.com.br
 designates 130.185.238.110 as permitted sender)
 receiver=protection.outlook.com; client-ip=130.185.238.110;
 helo=mx-01.projetoppgco.com.br; pr=C
Received: from mx-01.projetoppgco.com.br (130.185.238.110) by
 DB8EUR06FT053.mail.protection.outlook.com (10.233.253.201) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.5566.15 via Frontend Transport; Mon, 29 Aug 2022 13:08:10 +0000
X-IncomingTopHeaderMarker:
 OriginalChecksum:E6101A9850010369762B8E7E7BB27C890D715CDCB36932A4CE5DBD12368447FB;UpperCa
Received: from mx-01.projetoppgco.com.br (mx-01.projetoppgco.com.br [127.0.0.1])
        by mx-01.projetoppgco.com.br (Postfix) with ESMTP id 4MGW2c5ymJz2wxl
        for <wesley.silverio@outlook.com>; Mon, 29 Aug 2022 10:08:08 -0300 (-03)
Authentication-Results-Original: mx-01.projetoppgco.com.br (amavisd-new);
        dkim=pass (2048-bit key) reason="pass (just generated, assumed good)"
        header.d=projetoppgco.com.br
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=
        projetoppgco.com.br; h=content-type:message-id:user-agent
        :subject:to:from:date:mime-version; s=dkim; t=1661778488; x=
        1664370489; bh=Y+jZTYwlW9b8ZgT8fst29znFTZZPbC7cXlAe70wTMjk=; b=d
        kSr5V+YHcJXmR1ri32WWn9eVkN/QCp1h67V6cmkQuOxY0KuuMvn13f9h53gdT7yo
        XK0Yvm8aviLwWPUkpWIc+UMwdWDsRIQo5xlDibAQvhDeQyFhjBLUiy1/B7goKhEq
```


Figura 90 – *Header* Microsoft - Origem iRedMTA

### 5.2.3 Análises Complementares

As análises desempenhadas nesta seção não possuem como pré-requisitos análises dos *headers*, que já foram apresentadas nas Seções 5.2.1 e 5.2.2. Nesta seção foram feitas análises de aspectos que são próprias do provedor iRedMTA e que não dependem de envios ou de seus destinatários.

A análise do DNS mostra que o endereço IP do iRedMTA resolve corretamente para o FQDN informado pelos *header*s apresentados nas Fig. 89 e Fig. 90, indicando que o DNS Reverso está configurado adequadamente como se pode verificar na Fig. 91.

A análise do experimento com o MxToolBox mostra que o endereço IP do iRedMTA não consta en nenhuma lista de bloqueio, conforme pode ser verificado na Fig. 92, tornando-o mais confiável para envios.

Nesse experimento com o MxToolBox, foi possível verificar o *status* do *Relay* do MTA, sendo que, como se pode observar na Fig. 93, o servidor iRedMTA não está com seu *relay* aberto. Isso reduz a ocorrência de falsos positivos, pois provedores receptores usam esta informação em seus filtros.

O experimento com o *Mail Tester* mostra o iRedMTA com 10 de 10 pontos possíveis, conforme pode ser visto na Fig. 94. Além da pontuação máxima, o *Mail Tester* não reporta nenhuma informação negativa, que necessitasse de ajustes. Os resultados mostram que mensaens enviadas a partir do servidor ProjetoPPGCO, denominado iRedMTA, tem grande chance de alcançar a caixa de entrada de destinatários.

Foram realizados envios do iRedMTA para os diversos provedores relacionados neste capítulo, no decorrer de quatro semanas. Os relatórios foram obtidos por amostragem, sendo seu resultado final apresentado na Fig. 95.

É interessante ressaltar que, apesar da pontuação de sanidade total - conforme demonstra a Fig. 94 - e a verificação de que os protocolos foram configurados corretamente, conforme mostra a Fig. 89, ainda houve evidências de falsos positivos.

Esse ressalto em relação ao iRedMTA, de acordo com as análises, permite considerar que um dos fatores, talvez principal, de algumas mensagens terem sido classificados como lixo eletrônico, pode estar relacionado à necessidade de ajustes em arquivos do servidor, como se discutiu na Seção 4.6.

O provisionamento gerenciado automaticamente e orquestrado a partir do Plano de Controle se mostra importante, uma vez que não depende de analistas, de diversos provedores, manualmente, cuidar de ajustes no MHS. Os resultados obtidos, a partir dos experimentos descritos neste capítulo, evidenciam cenários do mercado, com várias discrepância em seus processos provisionamentos, implicando em uma vasta quantidade de falsos, positivos e negativos.


Figura 91 – iRedMTA - DNS Reverso

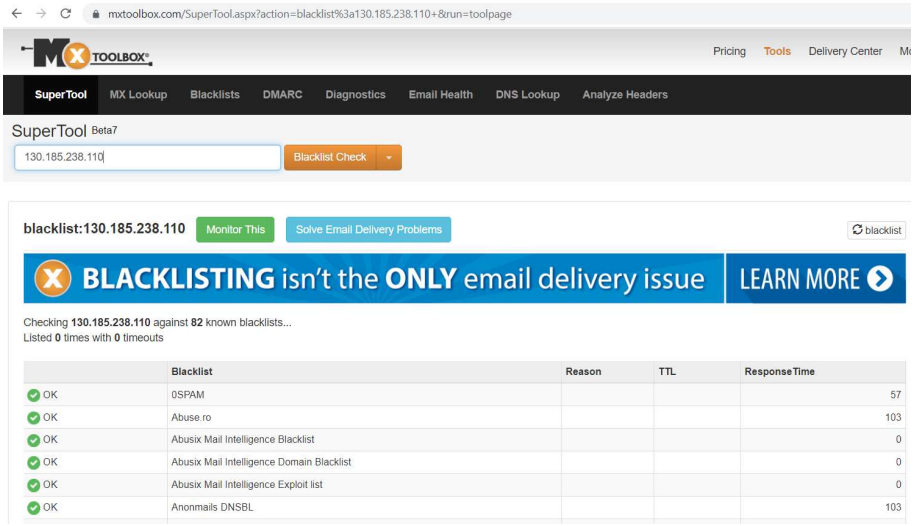



Figura 92 – iRedMTA - Lista de Bloqueio

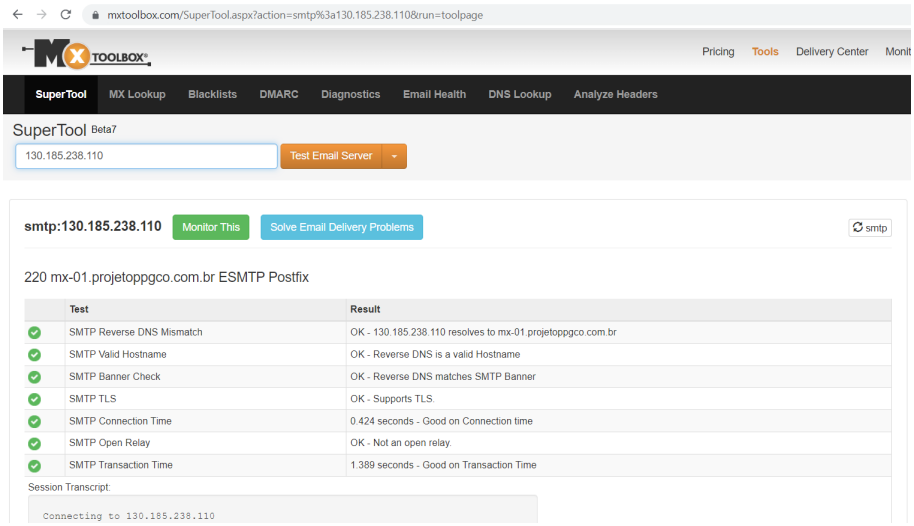



Figura 93 – iRedMTA - *Relay* Fechado

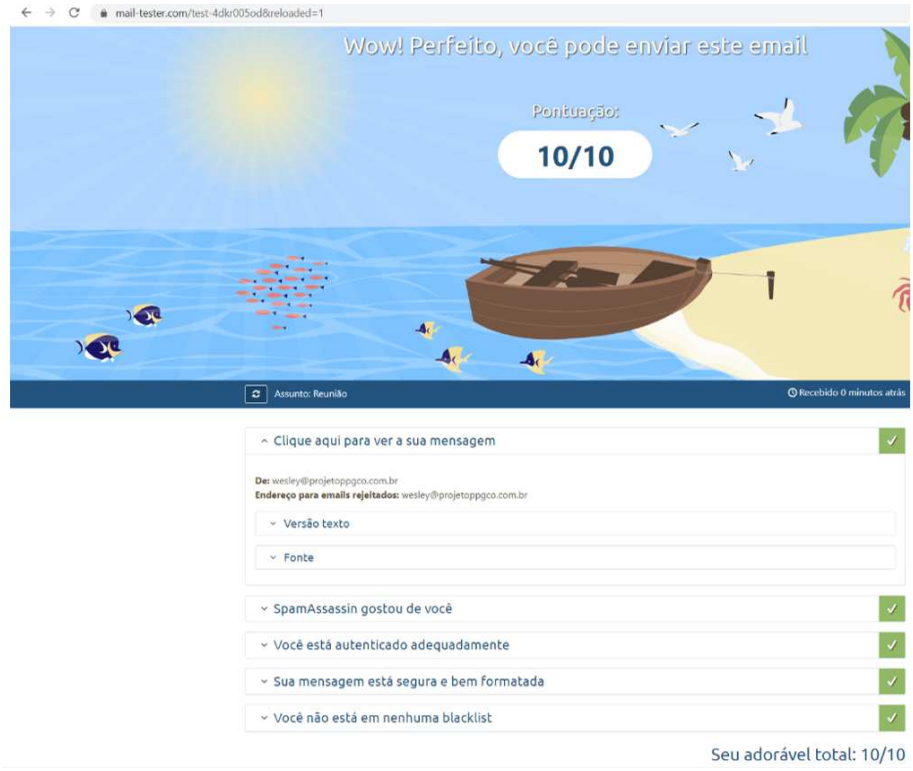



Figura 94 – iRedMTA - Pontuação

**1º Semana**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| alminda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| caio@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| diego@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| gabriel@projetoppgco.com.br | | x | x | | x | x | x | x | x | x |
| iracilda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| jenifer@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| wesley@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |

**2º Semana**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| alminda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| caio@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| diego@projetoppgco.com.br | x | | x | x | x | x | x | x | x | x |
| gabriel@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| iracilda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| jenifer@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| wesley@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |

**3º Semana**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| alminda@projetoppgco.com.br | x | x | x | | x | x | x | x | x | x |
| caio@projetoppgco.com.br | | x | x | x | x | x | x | x | x | x |
| diego@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| gabriel@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| iracilda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| jenifer@projetoppgco.com.br | x | x | x | | x | x | x | x | x | x |
| wesley@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |

**4º Semana**

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| alminda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| caio@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| diego@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| gabriel@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| iracilda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| jenifer@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| wesley@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |

| | | |
|---|---|---|
| Caixa de entrada | 274 | 100% |
| Lixo eletrônico | 6 | 2,2% |

Figura 95 – Envios - Origem ProjetoPPGCO

## 5.3 Envios por MHS gerido pela SPAM-K

Na Seção 5.2 foram apresentados experimentos envolvendo um MTA "*default*" configurado pelo iRedMail. Isto significa que o servidor Postfix foi implementado e, então, não sofreu quaisquer ajustes posteriores relativos a envio de mensagens, cono ocorre em boa parte de ISPs no Brasil e no mundo.

Nesta seção serão apresentados experimentos que começam com a implementação do plano de controle, por meio da implantação e configuração da aplicação de controle SPAM-K. Em seguida, é feita a implantação do MTA de referência, denominado *Kayrós* MTA - implementado para o projeto SPAM-K (K-MTA).

### 5.3.1 Implantação da infraestrutura SPAM-K

A interface P-MHS-Interface, introduzida na Seção 3.2.4, é responsável por interfacear com os protocolos descritos na Seção 2.3, que foram amplamente discutidos nas análises dos experimentos anteriores, tais como SPF, DKIM e DMARC. Deste modo, sistemas (servidores) alvos de provisionamentos devem prover credenciais de API disponíveis para que a SPAM-K possa se conectar e provisionar artefatos nesses alvos. A Fig. 96 apresenta o cenário de experimentação da SPAM-K.

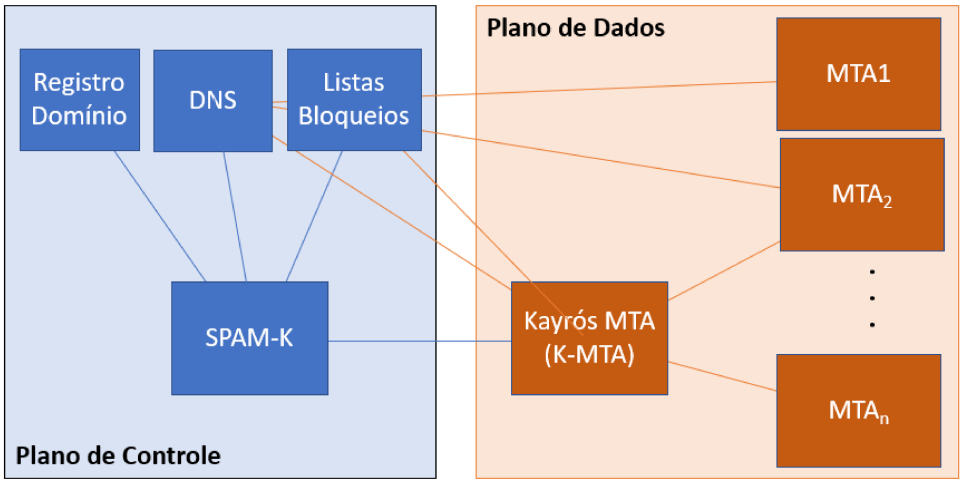



Figura 96 – SPAM-K: Cenário de Experimentação

A SPAM-K precisa interfacear com sistemas do plano de controle, como é o caso de Registro de Domínios, Listas de Bloqueio - tais como da *Real-time Blackhole List* (RBL) e UCE *Protect* etc, entre outros. Na Fig. 96, as linhas azuis representam interações do plano de controle e as linhas laranjas representam interações do plano de dados. É interessante notar que MTAs fazem acesso a sistemas do plano de controle e, por esta razão, faz sentido a SPAM-K existir, para orquestrar os provisionamentos do plano de controle.

Durante a implantação e testes de funcionamentos da infraestrutura, foi notado que alguns ´serviços', como o registro de domínio, não ofereciam acessos, como requerido pelo projeto. Por esta razão, foi necessária a transferência do domínio `projetoppgco.com.br`, registrado no **Registro.br** para o **cPanel**. Isto se deveu ao fato de o Registro.br não disponibilizar API para provisionamentos requeridos por sistemas externos, como requerido pela SPAM-K.

#### 5.3.1.1 cPanel: Criando a chave da API

Para criar uma chave de API, é necessário acessar o cPanel e localizar a funcionalidade *`Manage API Tokens`* ou `Gerenciamento de Chaves de API`, conforme é representada na Fig. 97.

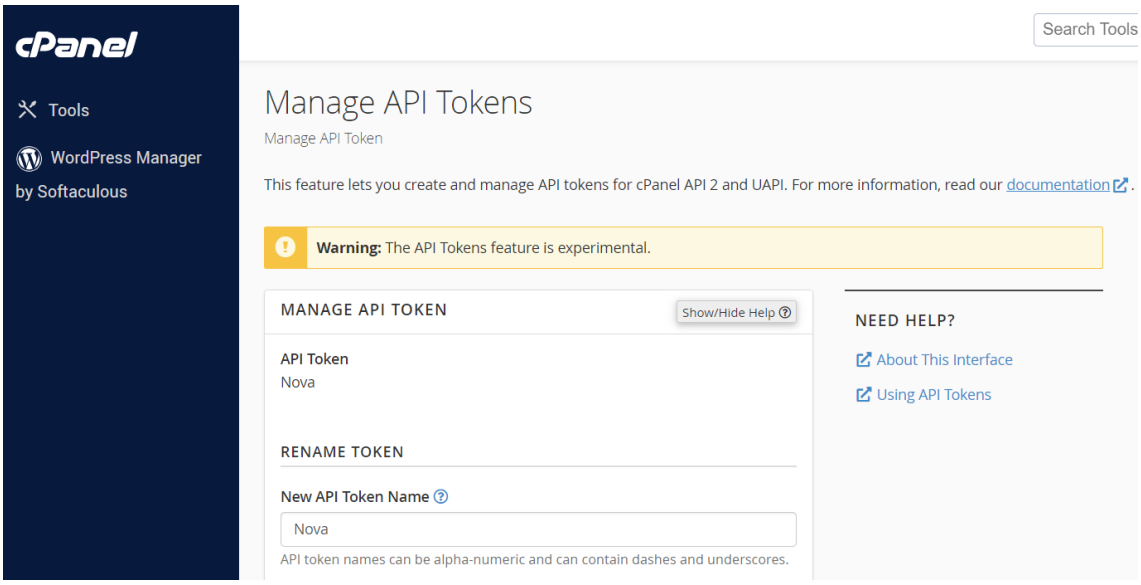



Figura 97 – cPanel - Gerencimaento de APIs

Em seguida, deve-se selecionar a opção `Gerar Chave da API` e preencher as informações necessárias, tais como o `Nome da Chave` e as `Permissões` que ela terá para acessar recursos do cPanel, conforme mostra a Fig. 98.

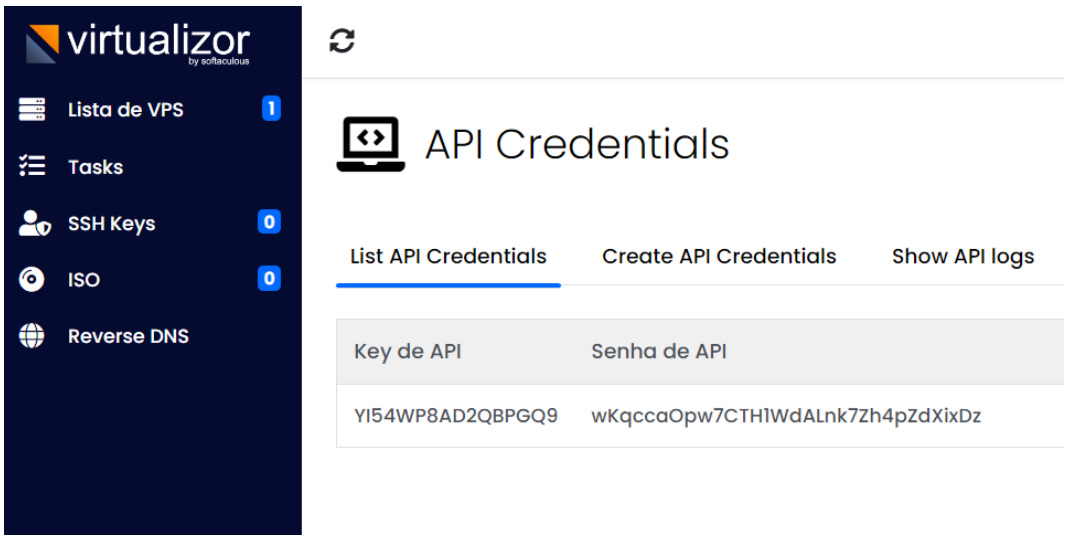



Figura 98 – cPanel - Criação da Chave de API

Frise-se que a escolha das permissões deve ser feita com cuidado, para garantir a segurança e a privacidade dos dados armazenados no cPanel. Recomenda-se que sejam concedidas apenas as permissões estritamente necessárias para o bom funcionamento do aplicativo ou serviço que utilizará a chave da API.

A chave da API deve ser armazenada em local seguro e não deve ser compartilhada com terceiros, de forma a evitar possíveis vulnerabilidades de segurança. Lembrando que no caso deste projeto, apenas a SPAM-K deve utilizar a chave da API gerada.

De posse do *Token* da API do cPanel, além do usuário e senha de acesso à plataforma cPanel, como mostrado na Fig. 98, a SPAM-K consegue se conectar e provisionar os protocolos SPF, DKIM e DMARC. O código fonte completo está disponível nos anexos.

#### 5.3.1.2 K-MTA: Implantação e Configuração de MTA

K-MTA é o agente MTA implementado no projeto e desempenhará o papel de MHS de Referência a ser provisionado pela SPAM-K. Foi utilizado um *Virtual Private Server* (VPS) fornecido pela BhostBrasil[8], sendo que sua escolha se deve ao fato de permiir acesso via APIs. A configuração do DNS Reverso é realizada pela plataforma *Virtualizor*, que é um painel de controle VPS baseado na web. Esta plataforma possui credenciais de APIs, sendo necessário apenas a configuração da chave e senha, que foram utilizadas para que o rDNS pudesse ser provisionado pela SPAM-K. A Fig. 98 apresenta a chave da API e sua respectiva senha.

[8] www.bhostbrasil.com.br

Para que a SPAM-K pudesse fazer os provisionamentos no K-MTA, envolvendo os arquivos `hostname`, `main.cf` e `hosts`, conforme detalhado na Seção 4.4.2, foi necessário informar o usuário e a senha do Administrador do servidor, para que a SPAM-K pudesse invocar as APIs.

Além dos provisionamentos K-MTA, há que, também, se realizar ajustes nos protocolos de autenticação, descritos na Seção 2.3. A centralização desse processo é muito importante, pois, como os provisionamentos são independentes e cada provedor se responsabiliza pelo seus procedimentos, muitos provedores deixam de realizar ou realizam de forma incorreta e isso ocasiona problemas a seus clientes, como falsos positivos ou negativos de SPAM.

### 5.3.2 SPAM-K: Experimentação com MHS K-MTA

Após completar os provisionamentos realizados pela SPAM-K, incluindo aspectos que vão além dos provisionamentos do K-MTA, por exemplo, provisionamento de DNS Reverso, foram realizados novos experimentos de envios.

Nesta seção serão apresentados os resultados obtidos com os experimentos de envios a partir do K-MTA, sendo que alguns resultados esperados, e já expostos na Seção 5.2, por óbvios, serão omitidos nesta seção.

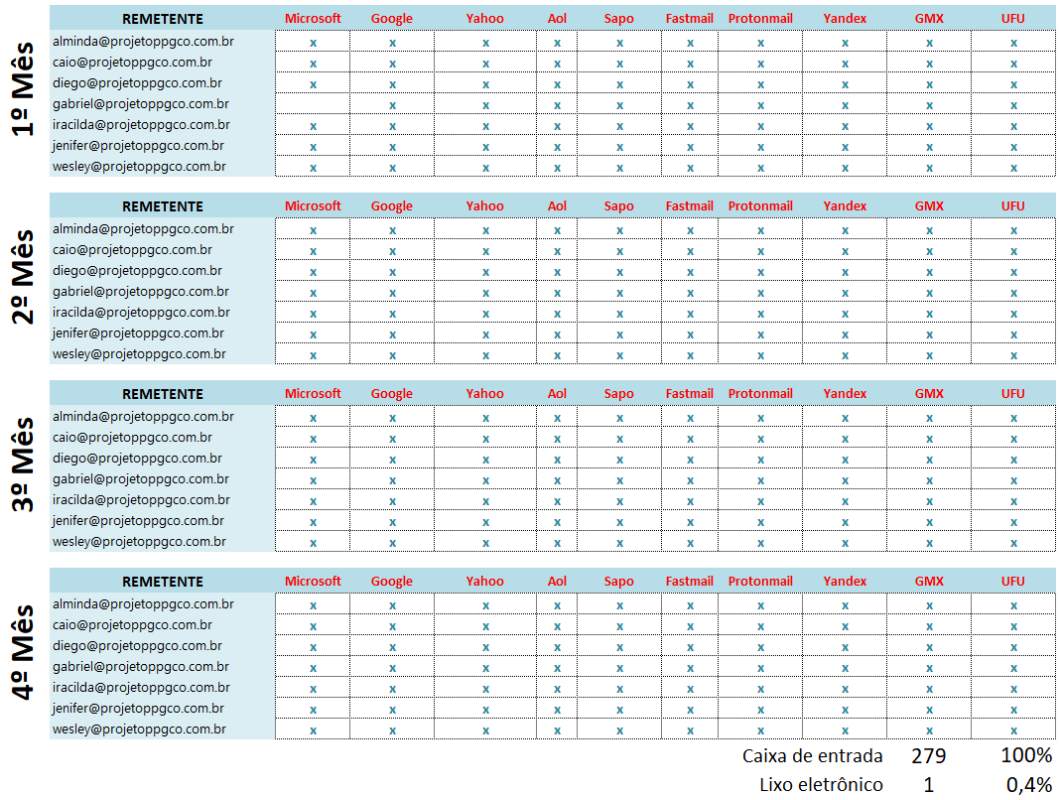
Os resultados obtidos confirmaram que os falsos, positivos e negativos, foram minimizados substancialmente, se comparados aos resultados obtidos nas abordagens expostas nas Seção 5.1 e Seção 5.2. A Fig. 99 sumariza os resultados obtidos com experimentos realizados durante 4 meses, nos quais foram feitos baterias de envios para os provedores de correio eletrônicos apresentados neste capítulo.

Os resultados foram minimizados significativamente, todavia, os falsos não foram eliminados. Há muitos casos que dependem de semântica e de contexto, então, a SPAM-K deve incorporar heurísticas baseadas em inteligência artificial, tais como ML e DL, de tal modo que a SPAM-K possa ir além de regras fixas.

De todo modo, há que se concordar que os resultados obtidos neste trabalho mostram uma base importante para construções mais eficazes. Os resultados comprovaram a eficacia da SPAM-K em reduzir falsos, sendo que resta evidente que a padronização de procedimentos é fundamental para a saúde dos sistemas de e-mails.

Por este motivo, foi desenvolvido o MTA *Kayrós* (K-MTA) para realizar os experimentos. É oportuno ressaltar que o cenário dos experimentos apresentado na Fig. 96 é exatamente aquele utilizado para a obtenção dos resultados a serem apresentados na corrente seção. Usando as mesmas ferramentas e técnicas descritas na Seção 5.1, foram feitas análises estáticas, cujas são apresentadas na Tabela 3.

A Tabela 3 mostra sanidade de 100% (*Score* 10) para o K-MTA. Esta pontuação é resultado da análise do MxToolBox que avalia aspectos como a presença em lista de bloqueios (BL=0). É possível perceber que a SPAM-K fez o controle adequado do K-MTA



1º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| alminda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| caio@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| diego@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| gabriel@projetoppgco.com.br | | x | x | x | x | x | x | x | x | x |
| iracilda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| jenifer@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| wesley@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |

2º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| alminda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| caio@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| diego@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| gabriel@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| iracilda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| jenifer@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| wesley@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |

3º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| alminda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| caio@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| diego@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| gabriel@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| iracilda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| jenifer@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| wesley@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |

4º Mês

| REMETENTE | Microsoft | Google | Yahoo | Aol | Sapo | Fastmail | Protonmail | Yandex | GMX | UFU |
|---|---|---|---|---|---|---|---|---|---|---|
| alminda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| caio@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| diego@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| gabriel@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| iracilda@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| jenifer@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |
| wesley@projetoppgco.com.br | x | x | x | x | x | x | x | x | x | x |

| | | |
|---|---|---|
| Caixa de entrada | 279 | 100% |
| Lixo eletrônico | 1 | 0,4% |

Figura 99 – K-MTA: Envios durante 4 meses

Tabela 3 – Resultado de Experimentos com Plano de Controle

| **Provedor** | ***Score*** | ***Relay*** | **rDNS** | **BL** | **Protocolos** |
|---|---|---|---|---|---|
| K-MTA | 10,0 | Fechado | Sim | 0 | SPF DKIM DMARC |

e, então, a Tabela 3 a facilidade de *Relay* fechado, isto é, nenhum provedor pode utilizar o K-MTA como um mero retransmissor de mensagens. O K-MTA apresenta a configuração do DNS Reverso (rDNS=Sim) adequada, garantindo que ninguém utiliza o endereço IP do servidor a não ser que seja o próprio domínio (`projetoppgco.com.br`) o remetente da mensagem. Por fim, o K-MTA especifica e utiliza dos os protocolos requeridos para autenticação/autorização nas conexões com outros MTAs e MUAs.

Os experimentos de envios apresentados na Fig. **??** mostram que durante 4 meses, houve 1 falso, que merece uma reflexão, mas que já mostra uma redução importante nos equívocos na classificação de mensagens.

A análise comparativa entre os experimentos de envios da seção 5.1 e 5.3 ambos monitorados durante 4 meses é apresentada na Tabela 4. A primeira coluna diz se os envios são (ou não) orquestrados pela SPAM-K, a quantidade de Caixas Postais utilizadas, o Total de Mensagens enviadas, a Quantidade (Qtde) e a Percentagem (%) de Falsos.

Entendemos que o volume de emails poderia ser maior, todavia, maior número de envios poderia ser classificado pelos provedores de forma negativa ao projeto. A quantidade enviada já mostra claramente uma melhora significativa na redução de falsos.

Tabela 4 – Comparação entre Envios Com/Sem Plano de Controle

| **SPAM-K** | **Provedor** | **Caixa Postal** | **Total Mensagens** | **Qtde Falso** | **% Falso** |
|---|---|---|---|---|---|
| **Não** | **AOL** | 262 | 280 | 18 | 6,9 |
| **Não** | **Sapo** | 210 | 280 | 70 | 33,3 |
| **Não** | **fastmail** | 259 | 280 | 21 | 8.1 |
| **Não** | **Microsoft** | 265 | 280 | 15 | 5.7 |
| **Não** | **Yahoo** | 270 | 280 | 10 | 3.7 |
| **Não** | **GMX** | 250 | 280 | 30 | 12.0 |
| **Não** | **UFU** | 213 | 280 | 67 | 31.5 |
| **Não** | **UFU365** | 267 | 280 | 13 | 4.9 |
| **Não** | **Yandex** | 253 | 280 | 27 | 10.7 |
| **Não** | **Google** | 267 | 280 | 13 | 4.9 |
| **Não** | **Protonmail** | 272 | 280 | 8 | 2.9 |
| **Sim** | **K-MTA** | 251 | 250 | 1 | 0,4 |

A SPAM-K reduziu a incidência de falsos, que, contudo, não foram eliminados. Isso era esperado, pois há muitos casos que dependem de semântica e de contexto, então, a SPAM-K deve incorporar heurísticas baseadas em inteligência artificial, tais como ML e DL, de tal modo que a SPAM-K possa ir além de regras fixas.

# Capítulo 6

# Conclusão

Este projeto foi motivado pela ineficácia de investimentos em plataformas de anti-spam. Tem-se aplicado técnicas de IA, contudo, a realidade é que falsos continuam a ocorrer. Em grande parte, esta ineficiência pode ser creditada à ausência de boas práticas nas instalação e configuração da infraestrutura de provedores de correio eletrônico. É importante ressaltar que, mesmo com a popularização de ferramentas de troca instantânea de mensagens, nossas pesquisas mostraram que o correio eletrônico ainda é amplamente utilizado no universo corporativo.

Existem milhares de provedores em todo o mundo e, portanto, as decisões de instalação e configuração são espalhadas nesses provedores. Para diminuir as ocorrências de falsos, alguns grandes provedores, como por exemplo a Microsoft, tem uma política de cadastro de provedores, e assim mitigar em parte esse problema.

A premissa deste projeto é a de que a gestão centralizada de agente(s) de Sistemas MHSs (provedores) é essencial para a mitigação de falsos. Isto se materializou com a construção da SPAM-K, uma aplicação do plano de controle SDN/NFV, que tem o propósito de gerir (monitorar, provisionar e orquestrar) planos de dados MHSs. Para verificar esta premissa foi necessária a implementação de um MTA capaz de interfacear com o plano de controle, que foi chamado de *Kayrós* (K-MTA), nos moldes apresentados na Fig. 96.

A Tabela 4 mostra que a SPAM-K, mesmo sendo uma aplicação ainda em fase inicial, se mostrou efetiva pelos resultados obtidos nos experimentos realizados. Evidentemente, é uma ambição ter uma aplicação do plano de controle MHS em escala mundial. De fato, há que se pensar em uma regulamentação, mas este trabalho demonstra que há um caminho.

Em face dos problemas apresentados pelo uso do correio eletrônico, a definição de padrões para autenticação é parte essencial de uma solução para minimizar falsos positivos na classificação de mensagens.

Para mitigar esses problemas, é necessária a implementação de servidores de e-mail eficientes, que possuem todas as regras e protocolos de autenticação de e-mails e boas práticas de configuração devidamente orquestrados.

Foram analisados diversos fatores, como o remetente da mensagem, o conteúdo, a linguagem utilizada, entre outros, a fim de desenvolver um padrão que possa ser aplicado a aos MTAs emissores. Espera-se que essa pesquisa possa contribuir para o desenvolvimento de servidores de e-mail mais eficientes e uma melhor gestão das comunicações eletrônicas.

A orquestração de métodos de autenticação também pode trazer benefícios adicionais, como a redução de custos de treinamento e a simplificação do processo de gerenciamento de qualidade. Com todos os atores seguindo os mesmos métodos autenticativos, é mais fácil identificar e corrigir problemas em potencial e garantir que as melhores práticas sejam adotadas em toda a organização.

Em conclusão, a implantação de um plano de controle é estratégico para melhorar a qualidade dos produtos e aumentar a satisfação de usuários. Comprovadamente eficaz através de experimentos, a padronização dos métodos de autenticação, a automação e o compromisso da equipe são elementos fundamentais para garantir o sucesso desse tipo de plano.

## 6.1 Principais Contribuições

Este trabalho traz à luz uma realidade de arquiteturas de software, que se baseiam numa suposição "meio verdadeira". Engenheiros de software partem da premissa de que a rede existe (o que é verdade) e vai entregar a qualidade de serviço que a aplicação sendo projetada requer (não vai, pelo menos, não por *default*). Esta discussão é uma importante contribuição deste trabalho, pois cada vez mais, o desenvolvimento de software vai precisar incorporar requisitos não funcionais atidos a planos de controle.

Protocolos importantes tais como SPF, DKIM, DMARC etc e listas de bloqueios importantes são negligenciados por provedores tais como Google, Yahoo, Microsoft, mostrando que a proposta deste trabalho tem fulcro numa realidade, sendo fundamental para indivíduos, corporações e governos.

Os experimentos realizados comprovaram a hipótese de que o Plano de Controle é eficaz em monitorar e controlar o plano de dados MHS, a gestão de padrões de configuração para servidores de envio de e-mail passa a residir em um centro. Através da análise de diversos casos, foi possível identificar que a gestão desses padrões a partir de um plano, é altamente eficaz para minimizar os prejuízos causados pela identificação equivocada de mensagens como SPAMs e garantir a entrega de mensagens autênticas.

Os resultados deste trabalho foram submetidos para publicação à revista "iSys - *Brazilian Journal of Information Systems*", da Sociedade Brasileira de Computação (SBC) e temos o primeiro retorno de '*major review*'.

## 6.2 Trabalhos Futuros

O presente trabalho se baseou em uma aplicação protótipo do plano de controle, com uma lógica simples, e se mostrou eficaz já em seus estágios iniciais. A arquitetura da aplicação SPAM-K, apresentada na Fig. 2, apresenta suas camadas e interfaces, mas entendemos que careça de maior refinamento para definir novas entidades dessas camadas e até mesmo novas camadas devam ser acrescentadas.

Podemos afirmar que a SPAM-K foi desenvolvida para gerir o plano de dados a partir da centralização do controle de protocolos essenciais, bem como, interfacear com listas de bloqueios. Essa é uma camada elementar, podendo ser considerada o ponto de partida, que, de resto, já se mostrou eficaz.

A partir da base introduzida pela SPAM-K, em termos do plano de controle, novas camadas podem se introduzidas para fazer uso de técnicas de inteligencia artificial e de análise de dados, podendo criar *datasets* que permitam fazer verificações ainda mais eficientes na direção de eliminação de falsos.

Em termos do plano de dados MHS, o projeto de novos agentes, tais como MTA, MDA, MUA etc, poderia fazer uso da EBI (*East Bound Interface*) para disponibilizar provedores naturalmente integrados ao plano de controle, o que poderia levar a almejar a eliminação de falsos. Provavelmente um dos grandes óbices para a eliminação de notícias falsas, para além de aspectos mercadológicos, é o fato de inexistir aplicações do plano de controle para as respectivas aplicações do plano de dados.

Como foi possível observar no desenvolvimento do trabalho, diversos protocolos foram introduzidos, basicamente, para autenticações, com algumas nuances entre eles. A criação de um método de autenticação universal pode melhorar a eficiência e a confiabilidade da autenticação das mensagens, mas também é importante garantir que ele possa ser integrado com outros sistemas de autenticação existentes.

A criação de um método inteligente que confirme a autenticidade das mensagens pode ser uma solução para reduzir falsos e melhorar a eficiência e a segurança da autenticação de mensagens. No entanto, é importante garantir que esse processo seja seguro, confiável e interoperável com outros sistemas de autenticação existentes. O avanço contínuo da tecnologia e a colaboração entre especialistas em inteligência artificial e segurança da informação são fundamentais para alcançar esse objetivo.

O desenvolvimento de processos inteligentes para confirmação da autenticidade dos e-mails também pode ajudar a reduzir o tempo gasto pelos usuários na triagem de mensagens, permitindo que eles se concentrem em mensagens importantes e relevantes. Isso também pode reduzir o risco de erros humanos na triagem de mensagens, o que pode levar a perda de informações valiosas ou prejuízos financeiros.

# Referências

ALLMAN, E. et al. **DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)**. IETF, 2009. RFC 5617 (Proposed Standard). (Request for Comments, 5617). Disponível em: <https://doi.org/10.17487/rfc5617>.

BIBI, A. et al. Spam mail scanning using machine learning algorithm. **J. Comput.**, v. 15, n. 2, p. 73–84, 2020. Disponível em: <https://doi.org/10.17706/jcp.15.2.73-84>.

BRITO, A. C. A.; COSTA, A. S.; SILVA, E. C. An'alise de filtragem de spam em servidores de email utilizando a ferramenta spamassassin. **Revista Cient'ifica Multidisciplinar N'ucleo do Conhecimento**, N'ucleo do Conhecimento, v. 6, n. 3, p. 27–38, 2021.

BUKHARI, S. M.; JAMEEL, S.; NAZ, S. Spam email detection using machine learning and data mining techniques. **International Journal of Advanced Computer Science and Applications**, The Science and Information Organization, v. 10, n. 2, p. 93–98, 2019.

CAI, R.; WU, Y.; ZHANG, S. Email spam detection model based on improved naive bayes algorithm. In: IEEE. **2021 2nd International Conference on Intelligent Computing**. [S.l.], 2021.

CAMPOS, R. C.; SOARES, A. C. Aplicação de machine learning para a classificação de spam em e-mails. In: **Anais do IX Congresso Brasileiro de Informática na Educação**. [S.l.: s.n.], 2018. p. 315–324.

CASADO, M.; MCKEOWN, N.; SHENKER, S. From ethane to sdn and beyond. **ACM SIGCOMM Computer Communication Review**, ACM Digital Library, v. 49, n. 1, p. 92–95, 2019. Disponível em: <https://doi.org/10.1145/3371934.3371963>.

CRISPIN, M. **INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1**. IETF, 2003. RFC 3501 (Proposed Standard). (Request for Comments, 3501). Updated by RFCs 4466, 4469, 4551, 5032, 5182, 5738, 6186, 6858. Disponível em: <https://doi.org/10.17487/rfc3501>.

CROCKER, D. **STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES**. IETF, 1982. RFC 822 (INTERNET STANDARD). (Request for Comments, 822). Obsoleted by RFC 2822, updated by RFCs 1123, 2156, 1327, 1138, 1148. Disponível em: <https://doi.org/10.17487/rfc0822>.

CROCKER, D. et al. **Proposed official standard for the format of ARPA Network messages**. IETF, 1977. RFC 724. (Request for Comments, 724). Obsoleted by RFC 733. Disponível em: <http://www.ietf.org/rfc/rfc724.txt>.

DALKILIÇ, G.; SIPAHI, D. Spam filtering with sender authentication network. **Computer Communications**, Elsevier, v. 98, p. 72–79, 2017.

DENG, H. et al. A hybrid approach for spam email classification using deep learning and random forest. **Neural Computing and Applications**, Springer, v. 29, n. 9, p. 677–685, 2018.

DOUZI, S. et al. Hybrid email spam detection model using artificial intelligence. **International Journal of Machine Learning and Computing**, v. 10, n. 2, p. 316–322, 2020.

FIELDING, R. et al. **Hypertext Transfer Protocol – HTTP/1.1**. IETF, 1999. RFC 2616 (Draft Standard). (Request for Comments, 2616). Updated by RFCs 2817, 5785, 6266, 6585. Disponível em: <http://www.ietf.org/rfc/rfc2616.txt>.

FOROUZAN, B. A. **Data Communications and Networking**. 6th. ed. [S.l.]: McGraw-Hill Education, 2018.

GAO, S. et al. An email spam filtering algorithm based on weighted trust vector machine. **Multimedia Tools and Applications**, Springer, v. 78, n. 9, p. 11525–11540, 2019.

GELLENS, R.; KLENSIN, D. J. C. **Message Submission**. RFC Editor, 1998. RFC 2476. (Request for Comments, 2476). Disponível em: <https://rfc-editor.org/rfc/rfc2476.txt>.

GOMES, R. F.; CARDOSO, V. S.; CAMPISTA, M. E. Uma abordagem para identificação de spam em fluxo de emails baseada em aprendizagem de máquina e engenharia de características. In: **Anais do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**. [S.l.: s.n.], 2018. p. 1–14.

GUPTA, R.; GUPTA, P. An overview of email spam filtering techniques. **International Journal of Computer Applications**, Foundation of Computer Science, v. 179, n. 22, p. 32–35, 2019.

HALEPLIDIS, A. et al. **Software-Defined Networking (SDN): Layers and Architecture Terminology**. IETF, 2015. RFC 7426. (Request for Comments, 7426). Disponível em: <https://tools.ietf.org/html/rfc7426>.

HAMEED, S.; KHAN, A. A comparative analysis of spam filtering techniques in email systems. **International Journal of Advanced Computer Science and Applications**, The Science and Information Organization, v. 10, n. 2, p. 165–171, 2019.

HANSEN, E. T.; SCUDDER, E. J.; KUCHERAWY, E. M. **Domain-based Message Authentication, Reporting, and Conformance (DMARC)**. IETF, 2015. RFC 7489. (Request for Comments, 7489). Disponível em: <https://tools.ietf.org/html/rfc7489>.

HOSSAIN, M. S.; KARIM, A.; RAHMAN, M. A. A hybrid machine learning approach for spam email detection. **Journal of Ambient Intelligence and Humanized Computing**, Springer, v. 12, n. 8, p. 8329–8345, 2021.

JIA, X. et al. A bayesian network model for email spam detection. In: IEEE. **2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)**. [S.l.], 2020. p. 2091–2095.

KLENSIN, J. **Simple Mail Transfer Protocol**. IETF, 2008. RFC 5321. (Request for Comments, 5321). Disponível em: <https://tools.ietf.org/html/rfc5321>.

KUCHERAWY, M. **Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1**. IETF, 2014. RFC 7208. (Request for Comments, 7208). Disponível em: <https://tools.ietf.org/html/rfc7208>.

KUROSE, J. F.; ROSS, K. W. **Computer Networking: A Top-Down Approach**. 8th. ed. [S.l.]: Pearson, 2020.

LEVINE, J.; KUCHERAWY, M. **DomainKeys Identified Mail (DKIM) Signatures**. IETF, 2011. RFC 6376. (Request for Comments, 6376). Disponível em: <https://tools.ietf.org/html/rfc6376>.

LI, X.; ZHU, H. Improved adaptive spam filter based on multiple weighted classifiers. **International Journal of Distributed Sensor Networks**, SAGE Publications Sage UK: London, England, v. 15, n. 6, 2019.

LIU, H.; XU, M.; LIU, Y. Application of convolutional neural network in spam email filtering. **Journal of Ambient Intelligence and Humanized Computing**, Springer, v. 10, n. 4, p. 1431–1441, 2019.

MAIA, G. F.; SANTOS, G. S.; AZEVEDO, H. C. Análise do desempenho do postfix como servidor de email. **Revista de Tecnologia da Informação e Comunicação**, v. 11, n. 1, p. 23–30, 2021.

MARTINS, E. F.; SOUZA, R. M. de; PEREIRA, E. A. Algoritmo de classificação de spam em servidores de email utilizando machine learning. In: **Anais do 5º Congresso de Pesquisa, Ensino e Extensão da UFG**. [S.l.: s.n.], 2019. p. 1536.

MOCKAPETRIS, P. **Domain names - concepts and facilities**. IETF, 1987. RFC 1034 (INTERNET STANDARD). (Request for Comments, 1034). Updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936. Disponível em: <http://www.ietf.org/rfc/rfc1034.txt>.

_____. **Domain names - implementation and specification**. IETF, 1987. RFC 1035. (Request for Comments, 1035). Disponível em: <https://tools.ietf.org/html/rfc1035>.

NIAZI, S. M. R.; BHATTI, A. I. A novel model for email spam detection using multiclass support vector machines. **Procedia Computer Science**, Elsevier, v. 159, p. 310–319, 2019.

OLIVEIRA, M. S.; SANTOS, T. M. L.; SOUZA, R. F. An'alise de efic'acia de filtro de spam baseado em t'ecnicas de aprendizado de m'aquina. **Revista Brasileira de Computaç ao Aplicada**, Sociedade Brasileira de Computaç ao, v. 11, n. 1, p. 16–24, 2019.

PETERSON, L. L.; DAVIE, B. S. **Computer Networks: A Systems Approach**. 6th. ed. [S.l.]: Morgan Kaufmann, 2021.

POONKODI, T. et al. E-mail spam filtering through feature selection using enriched firefly optimization algorithm. **Turkish Journal of Computer and Mathematics Education (TURCOMAT)**, v. 12, n. 5, p. 1248–1255, 2021.

POSTEL, J. **Simple Mail Transfer Protocol**. IETF, 1982. RFC 821 (INTERNET STANDARD). (Request for Comments, 821). Obsoleted by RFC 2821. Disponível em: <http://www.ietf.org/rfc/rfc821.txt>.

RAHMAD, F.; SURYANTO, Y.; RAMLI, K. Performance comparison of anti-spam technology using confusion matrix classification. In: IOP PUBLISHING. **IOP Conference Series: Materials Science and Engineering**. [S.l.], 2020. v. 879, n. 1, p. 012076.

RAMPRASAD, M. et al. Email spam detection using python & machine learning. **Turk. J. Phys. Rehabil**, v. 32, n. 3, 2019.

RIBEIRO, R. L. P.; SILVA, C. B. Análise de servidores de e-mail na nuvem. **Anais do Congresso Internacional de Gestão da Tecnologia e Sistemas de Informação**, v. 8, n. 1, p. 280–290, 2021.

ROSE, D. M. T.; MYERS, J. G. **Post Office Protocol - Version 3**. RFC Editor, 1996. RFC 1939. (Request for Comments, 1939). Disponível em: <https://rfc-editor.org/rfc/rfc1939.txt>.

SAHNI, R. Analysis of naıve bayes algorithm for email spam filtering. 2021.

SALAMON, A.; VIDA, R.; DUDA, P. Applying machine learning for spam email classification in a big data environment. **Computers Security**, Elsevier, v. 89, p. 101641, 2020.

SANTOS, A. F.; AZEVEDO, F. A.; ARAÚJO, R. G. Análise comparativa de servidores de email postfix e sendmail no ambiente de sistemas operacionais livres. In: **Anais do Simpósio Brasileiro de Sistemas de Informação**. [S.l.: s.n.], 2018. p. 1–12.

SIEMBORSKI, R.; MELNIKOV, A. **SMTP Service Extension for Authentication**. IETF, 2007. RFC 4954 (Proposed Standard). (Request for Comments, 4954). Updated by RFC 5248. Disponível em: <http://www.ietf.org/rfc/rfc4954.txt>.

SILVA, L. C. C.; LIMA, R. H. M.; FILHO, J. G. C. Uso de técnicas de machine learning para classificação de spam de e-mails. In: **Anais do 21º Workshop de Informática Médica**. [S.l.: s.n.], 2019. p. 40–47.

SOUSA, R. S.; SOUZA, F. B. de; TAVARES, J. M. Análise de desempenho do postfix em sistemas de correio eletrônico. **Revista Brasileira de Computação Aplicada**, v. 10, n. 2, p. 18–26, 2018.

STALLINGS, W. **Data and Computer Communications**. 10th. ed. [S.l.]: Pearson, 2019.

TANENBAUM, A. S.; WETHERALL, D. J. **Computer Networks**. 6th. ed. [S.l.]: Pearson, 2019.

VANNUCCI, L.; PROSPERI, M. A comprehensive analysis of the effectiveness of the spamassassin open-source anti-spam system. **Computer Networks**, Elsevier, v. 137, p. 75–92, 2018.

WANG, J.; LI, Q. An improved anti-spam model based on naive bayesian algorithm. **Procedia Computer Science**, Elsevier, v. 159, p. 1397–1406, 2019.

YLONEN, T.; LONVICK, C. **The Secure Shell (SSH) Protocol Architecture**. IETF, 2006. RFC 4251. (Request for Comments, 4251). Disponível em: <https://tools.ietf.org/html/rfc4251>.

ZHANG, T.; HU, X. Research on intelligent control method for email filtering system. **Journal of Computational Information Systems**, v. 16, n. 4, p. 1339–1349, 2020.

_____. An email filtering system based on machine learning and deep learning. **Journal of Ambient Intelligence and Humanized Computing**, Springer, v. 12, n. 1, p. 717–726, 2021.

APÊNDICE **A**

# Relação de Provedores e Contas

Este apêndice relaciona os provedores públicos de Correios Eletrônicos utilizados para fins de implantação e testes da aplicação de controle SPAM-K, nominalmente Microsoft (7 contas), Google (10 contas), Yahoo (10 contas), GMX (4 contas), AOL (7 contas), Fastmail (7 contas), Protonmail (4 contas), Yandex (4 contas), Sapo (3 contas) e UFU (1 conta).

## A.1 AOL

- ❏ anagarcia99@aol.com
- ❏ andrealimaitba@aol.com
- ❏ brissalisboa@aol.com
- ❏ danielleliman@aol.com
- ❏ eduardomazola@aol.com
- ❏ olionmastus@aol.com
- ❏ palomalisten@aol.com

## A.2 Sapo

- ❏ fabiolaandrade@sapo.pt
- ❏ didaticati@sapo.pt
- ❏ mariojacobsilva@sapo.pt

## A.3 Fastmail

- ❏ brunocarlos4422@fastmail.com
- ❏ luceliasantositba22@fastmail.com
- ❏ lucimaravictoriaitba90@fastmail.com
- ❏ mariojacobcostaitba@fastmail.com
- ❏ olindaguimaraessilver@fastmail.com
- ❏ ritatibialucia99@fastmail.com
- ❏ tuliomagalhaesitba10@fastmail.com

## A.4 GMX

- ❏ antoniamaia770@gmx.com
- ❏ carloshumberto9090@gmx.com
- ❏ gilbertoitba@gmx.com
- ❏ ritadecassiaitba50@gmx.com

## A.5 Google

- ❏ fabioelitoto@gmail.com
- ❏ gabizinhaitba09@gmail.com
- ❏ henriquegigico@gmail.com
- ❏ hugosanvico@gmail.com
- ❏ lucasleandrone@gmail.com
- ❏ lucianabrazuca@gmail.com
- ❏ manoelsolista@gmail.com
- ❏ ricardosoaresitba@gmail.com
- ❏ wisleymakline@gmail.com
- ❏ yagomussoline@gmail.com

## A.6 Microsoft

- ❏ fabiamussoline@hotmail.com
- ❏ leandrogaubi@hotmail.com
- ❏ luciomaquemberg@outlook.com
- ❏ ondinaamarante@outlook.com
- ❏ tabatajustino@outlook.com
- ❏ welberjumpeir@outlook.com
- ❏ wesley.silverio@outlook.com

## A.7 Protonmail

- ❏ brunamattos@protonmail.com
- ❏ juniorvilana@protonmail.com
- ❏ riquinha@protonmail.com
- ❏ wesleys@protonmail.com

## A.8 UFU

- ❏ wesley.silverio@ufu.br

## A.9 Yahoo

- ❏ daniellisandro12@yahoo.com
- ❏ fabioelioto17@yahoo.com
- ❏ gilbertolealcunha@yahoo.com
- ❏ janonessolista@yahoo.com
- ❏ lucasgirotoni@yahoo.com
- ❏ mariorizatty@yahoo.com
- ❏ mioranzasobretudo@yahoo.com
- ❏ ritasoares16@yahoo.com

- teoondilon@yahoo.com
- yurigarcia19@yahoo.com

## A.10 Yandex

- alinepascoal@yandex.com
- didaticati@yandex.com
- suelendantas@yandex.com
- wsguimaraes7@yandex.com

ANEXO A

# Códigos Fonte SPAM-K

```
------------------------------------------------------------
% O arquivo main.py
from flask import Flask, render_template
from flask.globals import request
from Apis import *

app = Flask(__name__)

@app.route("/", methods=['GET', 'POST'])
def site():
    if request.method == 'POST':
        dominio_principal = request.form["dominio_principal"]
        hostname_mta = request.form["hostname_mta"]
        ip_mta = request.form["ip_mta"]
        usuario_admin_mta = request.form["usuario_admin_mta"]
        senha_usuario_admin_mta = request.form["senha_usuario_admin_mta"]
        endpoint_rdns = request.form["endpoint_rdns"]
        chave_api_rdns = request.form["chave_api_rdns"]
        senha_api_rdns = request.form["senha_api_rdns"]
        endpoint_cpanel = request.form["endpoint_cpanel"]
        usuario_cpanel = request.form["usuario_cpanel"]
        chave_api_cpanel = request.form["chave_api_cpanel"]
        email_admin = request.form["email_admin"]

        CHAVE = chave(ip_mta,
            usuario_admin_mta,
            senha_usuario_admin_mta)
```

```
dkim(endpoint_cpanel,
     usuario_cpanel,
     chave_api_cpanel,
     dominio_principal,
     CHAVE)

dmarc(endpoint_cpanel,
    usuario_cpanel,
    chave_api_cpanel,
    dominio_principal,
    email_admin)

hostname(ip_mta,
    usuario_admin_mta,
    senha_usuario_admin_mta,
    hostname_mta)

hosts(ip_mta,
    usuario_admin_mta,
    senha_usuario_admin_mta,
    hostname_mta,
    dominio_principal)

postfix(ip_mta,
    usuario_admin_mta,
    senha_usuario_admin_mta,
    hostname_mta,
    dominio_principal)

rdns(endpoint_rdns,
    chave_api_rdns,
    senha_api_rdns,
    ip_mta,hostname_mta,
    dominio_principal)

spf(endpoint_cpanel,
    usuario_cpanel,
    chave_api_cpanel,
    dominio_principal,
```

```
            ip_mta)

        return f"DADOS ENVIADOS COM SUCESSO !!"


    return render_template("index.html", imagem="ufu.png")

if __name__ == "__main__":
#app.run()
    app.run(host="0.0.0.0", port=80)

-----------------------------------------------------
% O arquivo spf.py
import requests
import json

# Autenticação na API do cPanel
def spf(endpoint_cpanel, usuario_cpanel, chave_api_cpanel,
dominio_principal,
ip_mta):
    # https://cp01.srvcpanel.com.br:2083/json-api/cpanel é o
    ENDPOINT Cpanel
    # projetop é o USUÁRIO Cpanel
    # L3CB7ZIZXXYTWHTZ427YBYA1S4F9TRNF é a CHAVE DE API Cpanel
    URL = endpoint_cpanel
    USER = usuario_cpanel
    API_KEY = chave_api_cpanel

    # Nome do domínio
    DOMAIN = dominio_principal

    # Nome da entrada TXT DNS
    TXT_NAME = dominio_principal + '.'

    # Valor da entrada TXT DNS
    TXT_VALUE = 'v=spf1 a mx ip4:' + ip_mta + '-all'
```

```
    ########################################
    ##      NÃO ALTERAR A PARTIR DAQUI      ##
    ########################################
    headers = {
        'Authorization': F'cpanel {USER}:{API_KEY}',
    }

    params = {
        'cpanel_jsonapi_apiversion': '2',
        'cpanel_jsonapi_module': 'ZoneEdit',
        'cpanel_jsonapi_func': 'add_zone_record',
        'domain': DOMAIN,
        'name': TXT_NAME,
        'type': 'TXT',
        'txtdata': TXT_VALUE
    }

    response = requests.get(URL, params=params, headers=headers)

    if response.status_code == 200:
        data = response.json()
        if "error" in data.get("cpanelresult"):
            print("Houve um erro ao criar a entrada TXT DNS.")
        else:
            print("A entrada TXT DNS foi criada com sucesso.")

------------------------------------------------------------
% O arquivo public_key_dkim.py
import paramiko

def chave(ip_mta, usuario_admin_mta, senha_usuario_admin_mta):
    # Define as informações de conexão SSH
    host = ip_mta
    port = 22
    username = usuario_admin_mta
    password = senha_usuario_admin_mta

    # Estabelece uma conexão SSH
    ssh_client = paramiko.SSHClient()
```

```
    ssh_client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    ssh_client.connect(hostname=host, port=port, username=username,
    password=password)

    # Define o comando a ser executado para obter a chave pública DKIM
    # domain = 'projetoppgco.com.br'
    command = f'amavisd-new showkeys'

    # Executa o comando no terminal remoto
    stdin, stdout, stderr = ssh_client.exec_command(command)

    # Lê a saída do comando
    output = stdout.read().decode('utf-8')

    #Separa a chave
    chave = output.split('p="')[1]
    chave = chave.replace("\n", '').replace(" ", '').replace('"', '')
    .replace(")", '')
    # Imprime a chave pública DKIM
    #print(chave)

    # Fecha a conexão SSH
    ssh_client.close()
    return chave

-----------------------------------------------------
% O arquivo dkim.py
import requests
import json

# Autenticação na API do cPanel
def dkim(endpoint_cpanel, usuario_cpanel, chave_api_cpanel,
dominio_principal, CHAVE):
    # https://cp01.srvcpanel.com.br:2083/json-api/cpanel é o
    ENDPOINT Cpanel
    # projetop é o USUÁRIO Cpanel
    # L3CB7ZIZXXYTWHTZ427YBYA1S4F9TRNF é a CHAVE DE API Cpanel
    URL = endpoint_cpanel
    USER = usuario_cpanel
```

```
API_KEY = chave_api_cpanel

# Nome do domínio
DOMAIN = dominio_principal

# Nome da entrada TXT DNS
TXT_NAME = 'default._domainkey.' + DOMAIN + '.'

# Valor da entrada TXT DNS
TXT_VALUE = "v=DKIM1; k=rsa; p="+ CHAVE#'v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxUZZM16rF0+
ONFtonpKVTjGXCPg1w0HR9wwbS0OpFc4jPH53Fjbhcd6LhPNoi3ZkekTf
otjdTOhiBRlfgnljocvSOLddutltqReZ07HzDSk+wC6ntGm9LvT205dm6
WxtIbsS1ikRgUC3sb0DNkvdYB6OikdlZlaVWvVst3dpuKKpDIMjUZofXG
6Auac0aVxQiysr'

##########################################
##      NÃO ALTERAR A PARTIR DAQUI      ##
##########################################
headers = {
    'Authorization': F'cpanel {USER}:{API_KEY}',
}

params = {
    'cpanel_jsonapi_apiversion': '2',
    'cpanel_jsonapi_module': 'ZoneEdit',
    'cpanel_jsonapi_func': 'add_zone_record',
    'domain': DOMAIN,
    'name': TXT_NAME,
    'type': 'TXT',
    'txtdata': TXT_VALUE
}

response = requests.get(URL, params=params, headers=headers)

if response.status_code == 200:
    data = response.json()
    if "error" in data.get("cpanelresult"):
        print("Houve um erro ao criar a entrada TXT DNS.")
```

```
        else:
            print("A entrada TXT DNS foi criada com sucesso.")

-------------------------------------------------------
% O arquivo dmarc.py
import requests
import json

def dmarc(endpoint_cpanel, usuario_cpanel, chave_api_cpanel,
dominio_principal, email_admin):
    # Autenticação na API do cPanel

    # https://cp01.srvcpanel.com.br:2083/json-api/cpanel é o
    ENDPOINT Cpanel
    # projetop é o USUÁRIO Cpanel
    # L3CB7ZIZXXYTWHTZ427YBYA1S4F9TRNF é a CHAVE DE API Cpanel
    URL = endpoint_cpanel
    USER = usuario_cpanel
    API_KEY = chave_api_cpanel

    # Nome do domínio
    DOMAIN = dominio_principal

    # Nome da entrada TXT DNS
    TXT_NAME = '_dmarc.' + DOMAIN + '.'

    # Valor da entrada TXT DNS
    TXT_VALUE = 'v=DMARC1; p=none; rua=mailto:'
    + email_admin + '; ruf=mailto:'+ email_admin + '; fo=0'

    ##########################################
    ##      NÃO ALTERAR A PARTIR DAQUI      ##
    ##########################################
    headers = {
        'Authorization': F'cpanel {USER}:{API_KEY}',
    }

    params = {
        'cpanel_jsonapi_apiversion': '2',
```

```
        'cpanel_jsonapi_module': 'ZoneEdit',
        'cpanel_jsonapi_func': 'add_zone_record',
        'domain': DOMAIN,
        'name': TXT_NAME,
        'type': 'TXT',
        'txtdata': TXT_VALUE
    }

    response = requests.get(URL, params=params, headers=headers)

    if response.status_code == 200:
        data = response.json()
        if "error" in data.get("cpanelresult"):
            print("Houve um erro ao criar a entrada TXT DNS.")
        else:
            print("A entrada TXT DNS foi criada com sucesso.")

-----------------------------------------------
% O arquivo hostname.py
import paramiko

def hostname(ip_mta, usuario_admin_mta, senha_usuario_admin_mta,
hostname_mta):
    # Define as informações de conexão
    host = ip_mta
    username = usuario_admin_mta
    password = senha_usuario_admin_mta

    # Cria a conexão SSH
    ssh = paramiko.SSHClient()
    ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    ssh.connect(host, username=username, password=password)

    # Executa o comando para modificar o hostname
    command = f"echo '{hostname_mta}' > /etc/hostname"
    stdin, stdout, stderr = ssh.exec_command(command)

    # Fecha a conexão SSH
    ssh.close()
```

```
-----------------------------------------------------
% O arquivo hosts.py
import paramiko

def hosts(ip_mta, usuario_admin_mta, senha_usuario_admin_mta, hostname_mta,
dominio_principal):
    # Define as informações de conexão
    host = ip_mta
    username = usuario_admin_mta
    password = senha_usuario_admin_mta

    # Cria a conexão SSH
    ssh = paramiko.SSHClient()
    ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    ssh.connect(host, username=username, password=password)

    # Limpa o conteúdo do arquivo hosts
    command = "echo '' > /etc/hosts"
    stdin, stdout, stderr = ssh.exec_command(command)

    # Executa o comando para modificar o arquivo hosts
    command = f"echo '127.0.0.1' {hostname_mta}'.'{dominio_principal}
    {hostname_mta} >> /etc/hosts"
    stdin, stdout, stderr = ssh.exec_command(command)
    command = f"echo {ip_mta}     {hostname_mta}'.'{dominio_principal}
    {hostname_mta} >> /etc/hosts"
    stdin, stdout, stderr = ssh.exec_command(command)

    # Fecha a conexão SSH
    ssh.close()

-----------------------------------------------------
% O arquivo postfix.py
import paramiko

def postfix(ip_mta, usuario_admin_mta, senha_usuario_admin_mta,
hostname_mta, dominio_principal):
    # Define as informações de conexão SSH
```

```
host = ip_mta
port = 22
username = usuario_admin_mta
password = senha_usuario_admin_mta

# Cria a conexão SSH
client = paramiko.SSHClient()
client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
client.connect(hostname=host, port=port, username=username,
password=password)

# Define o arquivo que será modificado
filename = '/etc/postfix/main.cf'

# Lê o conteúdo do arquivo
stdin, stdout, stderr = client.exec_command(f'cat {filename}')
content = stdout.read().decode('utf-8')

# Substitui o texto desejado pelo novo texto
new_content = content.replace(f"mydomain =
{hostname_mta}.{dominio_principal}",
f"mydomain = {dominio_principal}").replace('mynetworks =
127.0.0.1 [::1]',
'mynetworks = ' + host + '/32, 127.0.0.0/8') +
'\nrelay\_domains = \$mydomain'
#new_content = content.replace('mynetworks = 127.0.0.1 [::1]',
'mynetworks = ' + hostname + '/32, 127.0.0.0/8') +
'\nrelay\_domains = \$mydomain'

# Escreve o novo conteúdo no arquivo
ftp = client.open_sftp()
with ftp.open(filename, 'w') as f:
    f.write(new_content)
ftp.close()

# Encerra a conexão SSH
client.close()
```

```
-----------------------------------------------------
% O arquivo rdns.py
import requests
import json

def rdns(endpoint_rdns,chave_api_rdns,senha_api_rdns,ip_mta,
hostname_mta,dominio_principal):

    endpoint = f"https://{endpoint_rdns}/index.php?act=rdns&api=
    json&apikey={chave_api_rdns}&apipass={senha_api_rdns}"

    payload = {'rdns': '1', 'rdns_ip': ip_mta, 'rdns_domain':
    hostname_mta + '.' + dominio_principal}

    response = requests.post(endpoint, data=payload, verify=False)
    print(response.text)

    # https://cloud.bhostbrasil.com.br é o ENDPOINT rDNS
    # YI54WP8AD2QBPGQ9 é a CHAVE DE API rDNS
    # wKqccaOpw7CTH1WdALnk7Zh4pZdXixDz é a SENHA DE API rDNS
    #url = f'https://{endpoint_rdns}/index.php?act=rdns&api=
    json&apikey={chave_api_rdns}&apipass={senha_api_rdns}'

    #data = {
    #   "rdns": "1",
    #  "rdns_ip": ip_mta,
    # "rdns_domain": f"{hostname_mta}'.'{dominio_principal}"
    #}

    #headers = {
    #   "Content-Type": "application/x-www-form-urlencoded"
    #}

    #response = requests.post(url, data=data, headers=headers,
    verify=False)
    #result = json.loads(response.text)
    #print(result)
---------------------------xxx----------------------------
```