Implementação de Controles de Segurança Cibernética nos Serviços DNS e E-mail

EDMAR DA SILVA BRAGA JUNIOR
Universidade de Brasília - UnB
edmar.junior@unb.br

ÉDER SOUZA GUALBERTO
Universidade de Brasília - UnB
Eder.gualberto@unb.br

RESUMO

A evolução dos ataques cibernéticos e das violações de dados, principalmente aos órgãos da Administração Pública Federal (APF), tem apresentado a necessidade de implementação de controles de segurança cibernética nos serviços DNS e E-mail. Relatório de auditoria do Tribunal de Contas da União (TCU) apontam um porcentual de domínios governamentais que não implementaram às configurações de segurança recomendadas pelas boas práticas, esses sistemas são os principais vetores de ataques que poderá ocorrer manipulação de tráfego de rede, vazamento de credenciais, perda de dados e indisponibilidade de sistemas organizações. Nesse contexto, os protocolos Domain Name System Security Extensions (DNSSEC), Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) e Domain-based Message Authentication, Reporting and Conformance (DMARC) surgem como um mecanismo de mitigar as vulnerabilidades e proteger as informações sensíveis. Este artigo tem como objetivo disseminar a importância de implementar os controles que trazem um aumento no nível de segurança nas instituições e os riscos da não implementação. A pesquisa baseia-se em um levantamento bibliográfico, artigos científicos, relatórios técnicos, analise de casos reais de falhas e ataques. Os resultados indicam que os controles de segurança reduzem vulnerabilidades causadas por má configuração. Este artigo contribui para o aumento do controle de segurança, maturidade e resiliência.

Palavras-chave: Programa de Privacidade e Segurança da Informação (PPSI); Segurança Cibernética; DNS; E-mail, DNSSEC, SPF, DKIM, DMARC.

ABSTRACT

The evolution of cyberattacks and data breaches, particularly targeting Federal Public Administration (APF) bodies, has highlighted the need to implement cybersecurity controls in DNS and email services. Audit reports from the Brazilian Federal Court of Accounts (TCU) indicate a percentage of government domains that have not implemented security configurations recommended by best practices. These systems are the main vectors for attacks that can lead to network traffic manipulation, credential leaks, data loss, and system unavailability. In this context, the Domain Name System Security Extensions (DNSSEC), Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) protocols emerge as mechanisms to mitigate vulnerabilities and protect sensitive information. This article aims to disseminate the importance of implementing controls that increase the level of security in institutions and the risks of non-implementation. This research is based on a literature review, scientific articles, technical reports, and analysis of real-world cases of failures and attacks. The results indicate that security controls reduce vulnerabilities caused by misconfiguration. This article contributes to increasing security control, maturity, and resilience.

Keywords: Privacy and Information Security Program (PPSI); Cybersecurity; DNS; E-mail, DNSSEC, SPF, DKIM, DMARC.

1. INTRODUÇÃO

A comunicação digital moderna depende fortemente de serviços como o Domain Name System (DNS) e o correio eletrônico (E-mail). O e-mail continua sendo o principal ponto de entrada para ataques cibernético [8]. Segundo o relatório *Threat Landscape*, publicado pela *European Union Agency for Cybersecurity* (ENISA), O Phishing continua como o principal método de intrusão inicial.[9]

De acordo com o relatório *Threat Landscape 2025,* a administração pública continua a ser o setor mais visado (38%), representando um aumento significado referente ao *Threat Landscape 2024 (19%) [9].*

Em 2025, O Centro de Prevenção, Tratamento e Resposta a incidentes Cibernéticos de Governos (CTIR Gov) notificou 14.045, sendo 8.466 incidentes e 5.578 vulnerabilidades. O número de 681 notificações de Phishing e o número de 140 de abuso no serviço de e-mail, chama a atenção e destaca a exposição do setor público aos riscos cibernéticos [10].

Com o uso de inteligência artificial (IA), intensificou o desenvolvimento de malware e conteúdo falsos com aparência mais autêntica, o que aumentou a eficiência de ataques como phishing e ransomware. [7]

Nesse sentido, foram criados mecanismos para mitigar tais vulnerabilidades. No âmbito do DNS, o protocolo DNS Security Extensions (DNSSEC) que foi desenvolvido para prover autenticação de origem e integridade de respostas. [11]. No campo de e-mail, foram padronizados protocolos como o Sender Policy Framework (SPF) [13] para autenticação de remetente, o DomainKeys Identified Mail (DKIM) [14] para assinatura criptográfica de mensagens e o Domain-based Message Authentication, Reporting and Conformance (DMARC)[15] para definição de política e reporte de falhas de autenticação[12]

Segundo o Tribunal de Contas da União (TCU), por meio do acórdão 523/2024 [2], o relatório evidencia a baixa porcentagem de domínios governamentais que não implementaram as configurações de segurança recomendadas pelas boas práticas para serviços de DNS e e-mail. Muitos domínios testados estão com alto risco de ataques ao serviço de resolução de nomes que apoiam no serviço de e-mail (81% e 86%).

Nesse contexto, destaca-se a conformidade com políticas nacionais, como o Framework do Programa de Privacidade e Segurança da Informação (PPSI), que tem como objetivo orientar instituições públicas no sentido de auxiliar a identificação, o acompanhamento e o preenchimento das lacunas de segurança da informação e privacidade [3].

Diante deste cenário, este artigo tem como objetivo difundir os mecanismos e protocolos de segurança em DNS e e-mail, propondo de forma

integrada os controles recomendados pelo framework PPSI. O trabalho também visa explorar os benefícios, bem como expor os riscos com a falta de implementação desses mecanismos em conjunto que pode comprometer os serviços de comunicação.

2. REFERENCIAL TEÓRICO

2.1 Sistemas de Proteção.

Ragheb et al. 2023 [1], enfatiza que a “falsificação de e-mails tornou-se extremamente comum, pois os criminosos dependem para realizar ataques de phishing, campanhas de spam, e distribuição de malware”.

O Atacante se faz passar por alguém que a vítima conhece ou em que confia. Ao falsificar o endereço de e-mail, o atacante tem mais chance de engalhar a vítima, segundo Hu et al. [10].

Diante nisso, foram desenvolvidos protocolos de segurança de e-mail como DNSSEC, SPF, DKIM e DMARK, que ajudam a mitigar as ameaças. Juntos, esses controles reduzem os riscos de ataques e aumentam a confiança na comunicação por e-mail.

2.1.1 Domain Name System (DNS)

O Domain Name System (DNS) ou Sistema de Nomes de Domínio é uma tecnologia fundamental para o funcionamento da internet, pois permite a comunicação usando nomes de domínio.

Acessar recursos da internet por nomes de domínio em vez de endereços IP requer um sistema de tradução, que é a principal tarefa do Sistema de Nomes de Domínio (DNS). O processo de traduzir nomes de domínio em endereços IP é chamado de resolução de nomes [11]

Segundo Kim and Reeves [7] enfatiza que a falta de segurança é a principal vulnerabilidade do DNS. Uma resposta corrompida ou interceptada pode fornecer informações maliciosas a qualquer solicitante. O DNS não verifica se a tradução do endereço IP recebida é autentica. Diante disso, DNSSEC foi desenvolvido para mitigar ameaças cibernéticas.

2.1.2. Domain Name System Security Extensions (DNSSEC)

O DNSSEC é uma extensão ao protocolo DNS, que fornece autenticação de origem, integridade de dados e negação autenticada para informações fornecidas por um servidor. São assinadas digitalmente todas as respostas de servidores DNSSEC, segundo Ariyapperuma and Mitchell [1].

As extensões de segurança do sistema de nome de domínio (DNSSEC) são um conjunto de especificações de extensão da Internet Engineering Task Force (IETF), para proteger dados trocados no sistema de nome de domínio (DNS), em redes de protocolo de internet (IP).

Além disso, de acordo com o Secure Domain Name System (DNSSEC) Deployment Guide, do NIST, o DNSSEC pode fornecer autenticação de origem de dados e verificação de integridade de dados a partir de solicitações e respostas de servidores de nomes [16].

A RFC 3833 (Threat Analysis of the Domain Name System (DNS), IETF) Analisa as ameaças ao sistema DNS e descreve as principais funcionalidades para se manter as integridades dos dados, além da autenticação da origem dos dados. Diante disso, o DNSSEC é um protocolo relevante na defesa contra ameaças.

De acordo com Ariyapperuma and Mitchell [1] A falta de solução para gerenciamento e a necessidade de um nível mais alto de sincronização de tempo entre os servidores, continuam sendo alguns dos obstáculos mais significativos à sua implantação. O DNSSEC não protege contra configurações incorretas no servidor de nomes autoritativo, e não protege contra ataques DDoS.

Estudo recentes Suela [3], Misell [4], Rawat and Jhanwar[5], demostram a evolução dos computadores quânticos que representam ameaças para os serviços atuais, protocolos que dependem de algoritmos RSA e ECDSA, como o DNSSEC, em que exige novas técnicas resistentes à computação quântica para manter a segurança. Esses resultados demostram um desempenho entre segurança e eficiência.

2.2. Mecanismos de autenticação de e-mail: SPF, DKIM e DMARC.

Os protocolos SPF, DKIM e DMARK desempenham um papel fundamental na proteção contra falsificação de domínios de rementes de e-mails. Para mitigar essas ameaças, foi desenvolvido os mecanismos que se concentram na autenticação no nome do domínio Liu, Enze et al [8].

O Domain Name System (DNS) mantém registros públicos associados a um domínio, como os endereços IP correspondentes. O DNS é fundamental para que os usuários possam acessar sites e enviar e-mails, sem a necessidade de decorar longos endereços IP alfanuméricos [18].

Existem tipos especializados de registros de DNS que ajudam a garantir que os e-mails sejam de uma origem legítima, e não de um falsificador: registros SPF, registros DKIM e registros DMARC. Provedores de serviços e-mail verificam todos esses registros para ver se os e-mails realmente vieram do local de origem e se não foram alteradas em trânsito.[12][18].

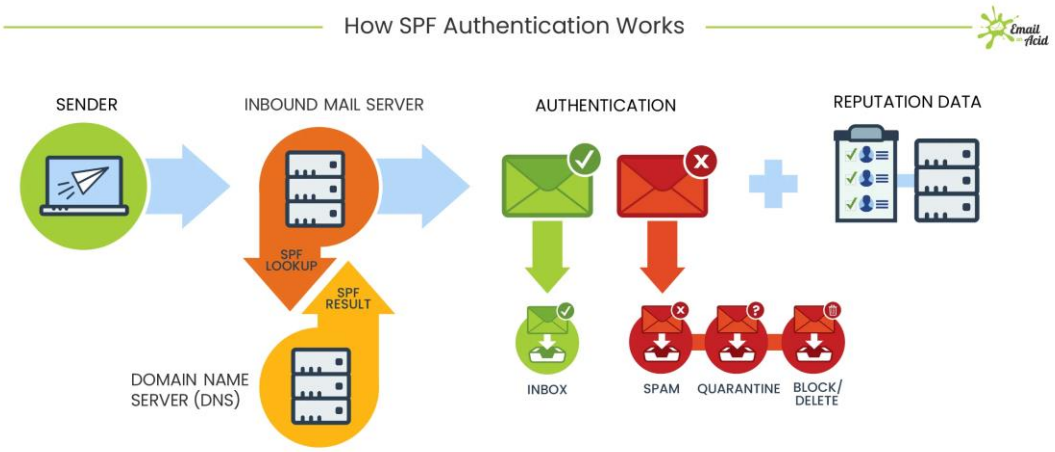
De acordo com Ragheb et al. 2023 [1], enfatiza a importância da utilização dos protocolos de autenticação para aprimorar a segurança e resiliência contra ameaças.

O PPSI recomenda a implementação dos protocolos e mecanismos de autenticação, que abrange controles e metodologias para identificação e mitigação de lacunas presentes nos órgãos e entidades da APF [11].

2.2.1. Sender Policy Framework (SPF)

O Sender Policy Framework (SPF) é um mecanismo que evita ou domínios enviarem e-mails não autorizados em nome de um domínio. Um domínio pode ou não autorizar que outros IP foram desta relação enviem e-mails em seu nome. O administrador configura esta relação na entrada TXT da zona de DNS, seguindo as regras da RFC 7208 [12][16] [20]. O SPF é especificado pela RFC 8616, e sua implementação é recomendada por diversas organizações, como o NIST [12] e o CTIR gov. [19]. O fluxo é ilustrado na Figura 1.

Figura 1 – Fluxo SPF



Fonte – media.emailocacid.com (2021)

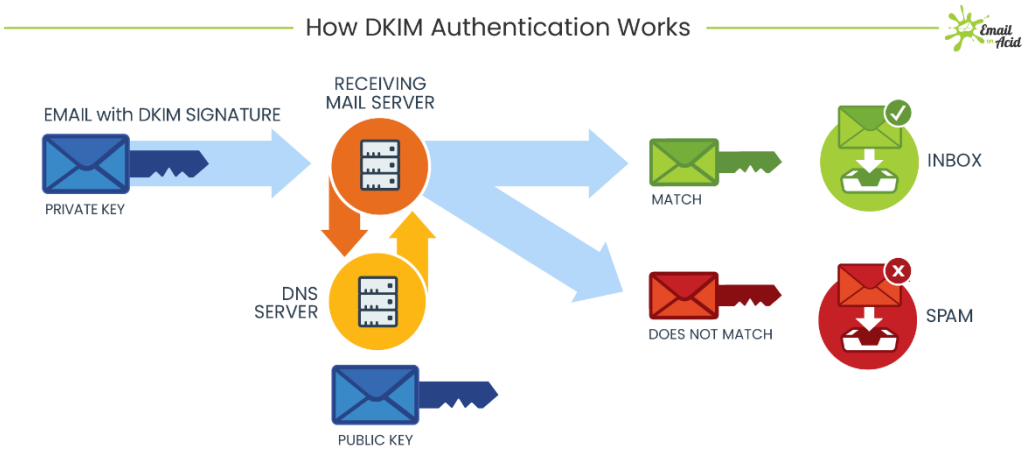
Na figura 1 é apresentado o processo de autenticação do protocolo SPF no recebimento de e-mails. O processo ocorre em etapas:

1. O Remetente (SENDER) envia um e-mail para o servidor de entrada (INBOUND MAIL SERVER).
2. O servidor de entrada realiza a consulta SPF (SPF LOOKUP) junto ao servidor DNS do domínio do remente, verificando se o IP que enviou o e-mail está autorizado na politica SPF registrada (SPF RESULT)
3. Se a autenticação SPF por positiva, a mensagem segue para a caixa de entrada (INBOX), se for negativa, pode ser redirecionada para SPAM, em QUARENTENA ou BLOQUEADA/DELETADA.

2.2.2 - DomainKeys Identified Mail (DKIM)

DKIM é um método de autenticação de e-mail projetado para detectar endereços de remetente falsos em e-mail, uma técnica frequentemente usada em phishing e spam. O DKIM é especificado pela RFC 8616, e sua implementação é recomendada por diversas organizações, como o CTIR gov. [19] e NIST [12]. O fluxo é ilustrado na Figura 2.

Figura 2 – Fluxo DKIM



Fonte – media.emailocacid.com (2021)

Na figura 2 é apresentado o processo de autenticação do protocolo DKIM no recebimento de e-mails. O processo ocorre em etapas:

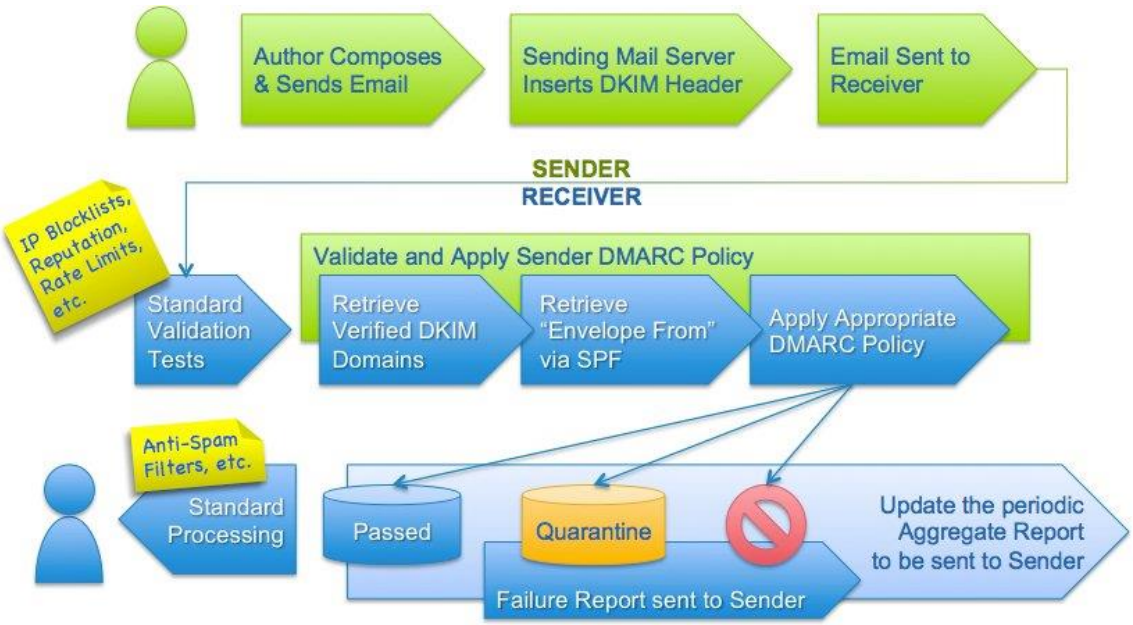
1. O e-mail é enviado já com uma assinatura DKIM, gerada pela chave privada do remetente.
2. O servidor de e-mail de destino recebe a mensagem e, para verificar a autenticidade, consulta o servidor DNS do domínio remetente para obter a chave pública correspondente.
3. O servidor faz a validação, comparando a assinatura DKIM do e-mail recebido com a chave pública encontrada no DNS.
4. Se houver correspondência (“MATCH”), o e-mail é considerado autêntico e direcionado à caixa de entrada (“INBOX”).
5. Se não houver correspondência (“DOES NOT MATCH”), indicando possível falsificação ou alteração, o e-mail é tratado como spam (“SPAM”).

2.2.3 - Domain-Based Message Authentication, Reporting, and Conformance (DMARC)

O Domain-Based Message Authentication, Reporting, and Conformance DMARC é um protocolo de segurança de e-mail que ajuda a proteger contra a falsificação de remetentes e combater o phishing e o spoofing de e-mails. Ele permite que os remetentes autentiquem seus e-mails com o Sender Policy

Framework – SPF e o Domain Keys Identified Mail – SPF e fornece instruções aos servidores de e-mail sobre como lidar com mensagens não autenticadas. O DMARC também oferece relatórios detalhados sobre os resultados das autenticações, permitindo que os remetentes monitorem e corrijam eventuais problemas de configuração [16]. Além disso, é especificado pela RFC 8616, e sua implementação é recomendada por diversas organizações, como o CTIR gov. [19] e NIST [12]. O fluxo é ilustrado na Figura 3.

Figura 3 – Processo de autenticação.



Fonte: dmarc.org (2015

Na figura 3 é apresentado o processo de autenticação do protocolo DMARC no recebimento de e-mails. O processo ocorre em etapas:

1. O remetente compõe e envia o e-mail, e o servidor de envio insere um cabeçalho DKIM na mensagem.
2. O e-mail é então enviado ao destinatário.
3. O servidor do destinatário realiza validações padrão, como verificar listas de IP bloqueados, reputação e limitações de taxa.
4. Em seguida, são buscados os domínios validados com DKIM e o “Envelope From” (remetente real) via SPF.
5. O servidor aplica a política DMARC do remetente, analisando os resultados das validações DKIM e SPF.

6. Conforme o resultado, a mensagem pode ser aprovada (“Passed”), direcionada à quarentena (“Quarantine”), ou rejeitada (bloqueada).
7. Para mensagens que falham na verificação, um relatório de falha é enviado ao remetente. Relatórios agregados também são atualizados periodicamente e enviados ao administrador do domínio.

3. BENEFÍCIOS DA IMPLEMENTAÇÃO.

A implementação dos protocolos traz benefícios significativos para a segurança da comunicação por e-mail e previne ataques de spoofing e phishing. Assim, a configuração dos mecanismos aumenta a segurança do e-mail e a resiliência contra ameaças de acordo Ragheb et al. [1]. Diante disso, desataca-se os relevantes benéficos:

- **DNSSEC**: soluciona alguns problemas encontrados na atual tecnologia DNS. Falsas informações DNS criam oportunidades para roubo de informações de terceiros ou alteração de dados em diversos tipos de transações como, por exemplo, compras eletrônicas. O objetivo da extensão DNSSEC é assegurar o conteúdo do DNS e impedir estes ataques validando os dados e garantindo a origem das informações. [5].
- **SPF:** A importância está em combater o problema de spoofing e phishing, que é quando alguém envia um e-mail se passando por outra pessoa ou organização. Isso é comumente usado em ataques de phishing, onde o remetente finge ser uma empresa legítima para enganar os destinatários e obter informações confidenciais.[2]
- **DKIM**: é usado principalmente para combater o spam e o phishing, já que essas técnicas de envio de e-mails falsos se aproveitam da falta de autenticidade dos remetentes. Ao implementar o DKIM, os remetentes podem provar que são legítimos, aumentando a confiança na entrega do e-mail.
- **DMARC**: Permite que os proprietários de domínios de e-mail definam políticas e recebam feedback sobre seus e-mails por meio de relatórios. Ao analisar esses relatórios do DMARC, os administradores podem identificar maneiras de aprimorar a autenticidade de seus e-mails,

melhorar as configurações de SPF e DKIM, e também impedir e-mails falsificados que abusam de seu domínio Ragheb et al. 2023 [1].

4 . DESAFIOS DA IMPLEMENTAÇÃO.

> Segundo Hu et al. [10] “Mesmo que um administrador de e-mail decidisse implementar o protocolo, haveria outros desafios no caminho. Resumimos as respostas dos participantes em três aspectos: (1) falta de controle sobre o DNS ou mesmo os servidores de e-mail, (2) o grande número de serviços dependentes, (3) falta de compreensão do protocolo e das dificuldades de implementação.
>
> Outro desafio é que a aplicação rigorosa de certos protocolos de e-mail exige esforços significativos de coordenação em grandes instituições. Um sistema de e-mail possui muitos serviços dependentes (por exemplo, ferramentas de marketing) distribuídos em diferentes departamentos em uma grande instituição. A implementação de um novo protocolo de e-mail requer um esforço de colaboração considerável de diferentes departamentos.
>
> Por fim, os participantes mencionaram que havia uma falta de compreensão aprofundada dos protocolos anti-spoofing, especialmente dos novos protocolos como o DMARC. É difícil estimar o esforço necessário para implementar e manter o protocolo na prática.”

Diante disso, a implementação dos protocolos enfrenta desafios significativos como o conhecimento técnico e configuração adequada. No entanto, destacam-se os riscos:

4.1. DNSSEC

- **Ataque de envenenamento de cache (Cache Poisonig):** um invasor corrompe o cache de um servidor DNS com informações falsas, fazendo que os usuários sejam redirecionados para sites maliciosos [17].
- **b. DNS Spoofing:** redireciona os usuários de sites legítimos para sites falsos que parecem idênticos, por exemplos bancos. A diferença entre o DNS spoofing e o cache poisoning é que na primeira, o ataque é diretamente no usuário, enquanto no segundo, a fraude é direcionada ao servidor [1]

- **Ataque distribuído de negação de serviço (DDoS):** inunda um servidor com tráfego de várias fontes, tornando-o indisponível para usuários legítimos. Embora o DNSSEC possa ajudar a prevenir certos tipos de ataques ao sistema DNS, não pode impedir diretamente ataques DDoS. [16].

4.1.2. SPF

- Risco de disponibilidade na comunicação, pois sem o mecanismo, os e-mails podem ser rejeitados pelos servidores de destinos.
- Aumenta o risco de spoofing [21] e phishing [22], pois o SPF verifica os servidores de e-mail autorizados:[12]

4.1.3. DKIM

- A falha na implementação de DKIM deixa os e-mails suscetíveis a modificações por atacantes, potencialmente levando a mudanças não autorizadas no conteúdo ou nos anexos
- Risco de disponibilidade na comunicação, pois seus e-mails podem ser rotulados ou rejeitados pelos servidores recipientes

4.1.4. DMARC

- Sem a implementação do DMARC, criminosos podem passar-se pelo seu domínio (domain spoofing) e enviar e-mails fraudulentos, aumentando as chances de sucesso de ataques de phishing. O DMARC ajuda a proteger-se desses ataques, ao permitir que donos de domínios especifiquem políticas de autenticação de e-mail.

5. CENÁRIOS EMERGENTES

A Internet depende fortemente de esquemas de criptografia de chave pública e de assinaturas digitais para garantir a confidencialidade e autenticidade das comunicações digitais. No entanto, criptografias amplamente utilizadas poderão ser quebradas por algoritmos quânticos segundo Liu and Moody [34]

No entanto, os novos padrões de chave pública do NIST fornecerão segurança pós quântica para aplicações, protocolos de internet como TLS, SSH, IKE, IPsec e DNSSEC e certificados digitais [34].

Liu and Moody [34] enfatiza que a criptografia de chave pública e assinaturas digitais como RSA (Rivest-Shamir-Adleman), serão vulneráveis a ataques quânticos.

Neste contexto desafiador, o estudo [3] recente apresenta a implementação do plugin dnssec_pqc que integra algoritmos criptográficos pós-quânticos (PQC) ao CoreDNS que permitirá assinatura de DNS resistente a computação quântica.

O CoreDNS é um servidor rápido e flexível que cada vez mais importante dentro do ecossistema DNS moderno, principalmente devido ao seu papel como servidor DNS padrão para clusters Kubernetes e ao seu design e recursos [3].

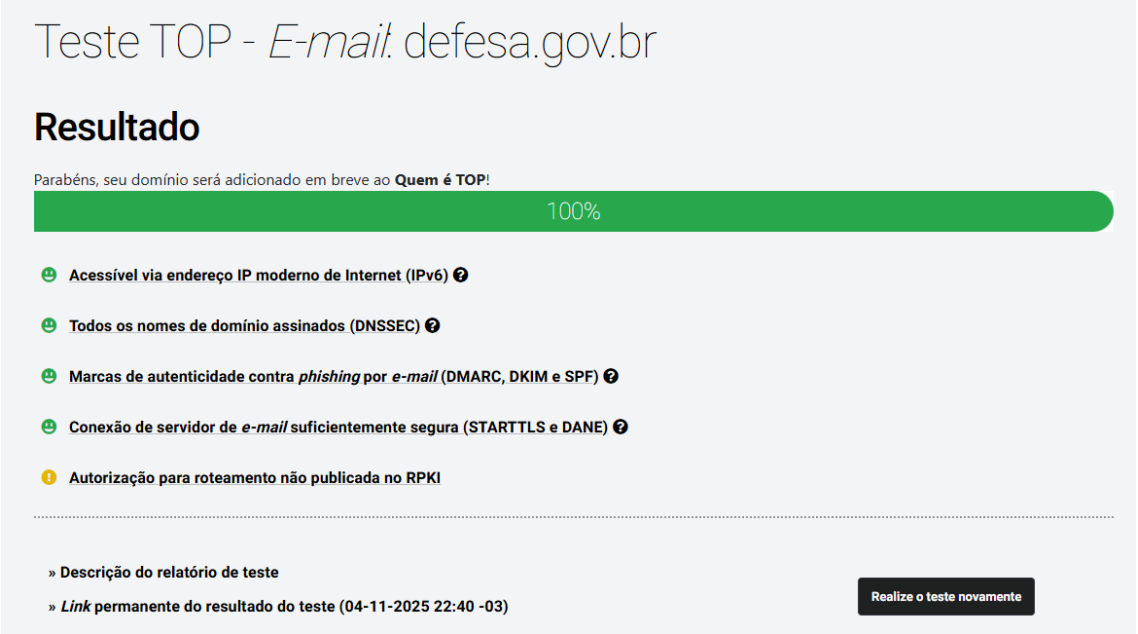
Diante do contexto, Suela at al. [3], demostram que o plugin integra algoritmos criptográficos pós-quânticos e estende o processo de geração de registros para suportar algoritmos PQC.

Dessa forma, o estudo demonstra com sucesso a integração de algoritmos criptográficos pós-quânticos no CoreDNS, resistentes à computação quântica.

6. FERRAMENTA TOP NIC

A ferramenta de testes TOP foi adaptada pelo NIC.br utilizando como base o site Internet.nl, que é uma iniciativa da holandesa Internet Standards Platform. A Internet Society também recomenda a utilização do Internet.nl para testar como os servidores de e-mail e os serviços de acesso à Internet atendem aos padrões abertos mais recentes de Internet.[26]

Figura 4 – Resultado



Fonte top.nic.br (2025)

Na figura 4 é apresentado o resultado da verificação dos padrões técnicos mais modernos e confiáveis de internet.

Figura 5: E-mail

Fonte top.nic.br (2025)

Na figura 5 é apresentado os domínios que pontuaram 100% no teste de e-mail e somente 4 órgãos com o domínio gov.br

7. DISCUSSÃO

A análise dos resultados desde estudo evidencia a importância da implementação dos controles de segurança cibernéticas nos serviços de DNS e e-mail, especialmente no âmbito da APF, onde cresce exponencialmente as ameaças. Estudos recentes, Ragheb and Elmedany [1], Enze et al [9], Hang et al [10] evidenciam a implantação dos protocolos SPF, DKIM, DMARC. Esses resultados indicam uma eficiência na mitigação contra ameaças.

Esse cenário ressalta a necessidade de atualização constantes frente às ameaças, como ataques sofisticados utilizando inteligência artificial e o ponto de vista em computação quântica, que podem comprometer a segurança das criptografias atual utilizada, por exemplo, no DNSSEC. Assim os estudos, Suela [3], Misell [4], Rawat and Jhanwar [6], Liu and moody [34] apontam para A transição para a criptografia pós-quântica não é apenas uma necessidade técnica, mas um imperativo estratégico para garantir a segurança e a integridade das comunicações digitais na era quântica.

Por fim, o PPSI tem como principal objetivo orientar e monitorar a implementação dos controles recomendados, elevando a maturidade e a resiliência dos órgãos.

8. Conclusão

Este artigo demostrou a crescente necessidade da implementação de controles de segurança cibernética nos serviços de DNS e e-mail, especialmente no contexto da Administração Pública Federal, onde a exposição a ataques é significativa e crescente. Os protocolos como DNSSEC, SPF, DKIM e DMARC mostram-se fundamental para mitigar vulnerabilidades, ataques de spoofing e phishing, protegendo informações sensíveis que garante a integridade e autenticidade das comunicações digitais.

A baixa implementação de configurações recomendadas pelas boas práticas, apontado por auditoria como a do Tribunal de Contas da União, reforça a importância de implementar os mecanismos de segurança. Assim, a disseminação do estudo e a implementação integrada dos controles

recomendados pelo framework PPSI, são essenciais para fortalecer a maturidade e resiliência dos órgãos públicos contra ameaças cibernéticas.

Cada camada de segurança digital construída sobre criptografia de chave pública deve eventualmente mudar para permanecer segura na era quântica. A computação quântica não representa apenas um risco à segurança cibernética. Ele abrange criptografia, identidade e confiança.

Dessa forma, conclui-se que a implementação dos controles de segurança é fundamental para garantir que os serviços de DNS e e-mail estejam adequadamente protegidos contra ameaças atuais. Como trabalhos futuros, propõe-se a implementação de criptografia pós-quântica no serviço DNSSEC visando mitigar ataques cibernéticos avançados e aumentar a eficiência do sistema.

5 - REFERÊNCIAS BIBLIOGRÁFICAS

[1] RAGHEB, Mohamed Sami; ELMEDANY, Wael; SHARIF, Mhd Saeed. The effectiveness of dkim and spf in strengthening email security. In: 2023 10th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, 2023. p. 422-426.

[2] ARIYAPPERUMA, Suranjith; MITCHELL, Chris J. Security vulnerabilities in DNS and DNSSEC. In: The Second International Conference on Availability, Reliability and Security (ARES'07). IEEE, 2007. p. 335-342.

[3] SUELA, Julio Gento et al. Implementing and Evaluating Post-Quantum DNSSEC in CoreDNS. arXiv preprint arXiv:2507.09301, 2025.

[4] MISELL, Q. et al. Measuring the Deployment of DNSSEC Bootstrapping Using Authenticated Signals. In: 25th ACM Internet Measurement Conference. ACM, 2025

[5] Tribunal de Contas da União. (2024). *Acórdão 523/2024 – plenário.* Brasília. Fonte: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/NUMACORDAO%253A523%2520ANOACORDAO%253A20

24%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0

[6] RAWAT, Aditya Singh; JHANWAR, Mahabir Prasad. Quantum-safe signatureless dnssec. In: Proceedings of the 20th ACM Asia Conference on Computer and Communications Security. 2025. p. 267-282.

[7] REIS, Rafael Santos; THOMAZ, Leonardo Santiago Spíndula. DNSSEC: aspectos gerais de segurança, eficiência e estatísticas de uso no contexto brasileiro. 2015. xv, 55 f., il. Monografia (Bacharelado em Engenharia de Redes de Comunicação) —Universidade de Brasília, Brasília, 2015.

[8] KIM, Tae Hyun; REEVES, Douglas. A survey of domain name system vulnerabilities and attacks. Journal of Surveillance, Security and Safety, v. 1, n. 1, p. 34-60, 2020

[9] LIU, Enze et al. Forward pass: On the security implications of email forwarding mechanism and policy. In: 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P). IEEE, 2023. p. 373-391

[10] HU, Hang; PENG, Peng; WANG, Gang. Towards understanding the adoption of anti-spoofing protocols in email systems. In: 2018 IEEE Cybersecurity Development (SecDev). IEEE, 2018. p. 94-101.

[11] Ministério da Gestão e da Inovação em Serviços Públicos (Brasil), “Programa de privacidade e segurança da informação (PPSI),” https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos, 2023, secretaria de Governo Digital. Acesso em: 14 out. 2025.

[12] MITRE ATT&CK Framework. Disponível em: https://attack.mitre.org/. Acesso em: 14 out. 2025.

[13] Núcleo de Informação e Coordenação do Ponto BR - Nic.br. Disponível em: https://nic.br/publicacoes/indice/guias/page:2/

[14] Centro de Prevenção, Tratamento e Resposta a incidentes Cibernéticos de Governo – CTIR Gov. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/recomendacoes/2023/recomendacao-17-2023

[15] https://news.microsoft.com/source/latam/ia-pt-br/extorsao-e-ransomware-impulsionam-mais-da-metade-dos-ataques-ciberneticos/?lang=pt-br

[16] TREND, Relatório de cenário de ameaças por e-mail: Ameaças em evolução em ataques baseados em e-mail. Disponível em: https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/email-threat-landscape-report-evolving-threats-in-email-based-attacks

[17] EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). ENISA Threat Landscape 2025. Heraklion: ENISA, 2025. Disponível em: https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025_0.pdf .Acesso em: 02 fev. 2025.

[18] CTIR Gov - Centro de Prevenção, Tratamento e Resposta a incidentes Cibernéticos de Governo. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros

[19] ROSE, Scott; LIU, Cricket; GIBSON, Ross. **Secure Domain Name System (DNS) Deployment Guide**. National Institute of Standards and Technology, 2025. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81r3.ipd.pdf. Acessado em: 03 nov. 2025.

[20] Nightingale, J. (2017), Email Authentication Mechanisms: DMARC, SPF and DKIM, Technical Note (NIST TN), National Institute of Standards and

Technology, Gaithersburg, MD. Disponível em: Email Authentication Mechanisms: DMARC, SPF and DKIM. Acessado em: 03 nov. 2025

[21] S. Kitterman. Sender Policy Framework (SPF) for Authorizing Use of Domains in Email Version 1. Internet Engineering Task Force Request for Comments 7208. Disponível em: https://www.rfc-editor.org/rfc/rfc7208

[22] D. Cocker, T. Hansen, M. Kucherawy. Domain Keys Identified Mail (DKIM) Signatures. Internet Engineering Task Force Request for Comments 6376 Disponível em: https://www.ietf.org/rfc/rfc6376.txt

[23] M. Kucherawy and E. Zwicky. Domain-based Message Authentication, Reporting and Conformance (DMARC). Internet Engineering Task Force Request for Comments 7489. March 2015 Disponível em: https://www.ietf.org/rfc/rfc7489.txt

[24] Matriz de Riscos e Controles para serviços de hospedagem WEB, e-mail e DNS. 2024 Tribunal de Contas da União (TCU). Disponível em: https://portal.tcu.gov.br/data/files/B2/F6/D8/64/13CB39100FB48339F18818A8/Matriz%20de%20risco%20e%20Controles%20para%20servicos%20de%20hospedagem%20WEB_%20e-mail%20e%20DNS_WEB.pdf

[25] Cloudflare, "O que é envenenamento de cache DNS? | Falsificação de DNS", 2025. Disponível em: https://www.cloudflare.com/pt-br/learning/dns/dns-cache-poisoning/ Acesso: 04 nov. 2025

[26] Cloudflare, "O que é segurança de e-mail?", 2025. Disponível em: https://www.cloudflare.com/pt-br/learning/email-security/what-is-email-security/ Acesso: 04 nov. 2025

[27] CTIR gov - Centro de Prevenção, Tratamento e Resposta a incidentes Cibernéticos de Governo – Recomendação 06/2025. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/alertas-e-

recomendacoes/recomendacoes/2025/recomendacao-06-2025
Acessado em 04 nov.2025

[28] MD Ishtiaq and W. li, V. Tech, T Fiebig,M. F. Inofrmatik and T. Chung. You've Got Report: Measurement and Security Implications of DMARC Reporting. USENIX Security, 2023. Disponível em: https://www.usenix.org/system/files/usenixsecurity23-ashiq.pdf Acesso em: 04 nov. 2025.

[29] MITRE ATT&CK Framework – Email Spoofing. Disponível em: https://attack.mitre.org/techniques/T1672/ .Acesso em: 04 nov. 2025.

[30] MITRE ATT&CK Framework – Phishing. Disponível em: https://attack.mitre.org/techniques/T1566/ .Acesso em: 04 nov. 2025.

[31] Top Teste de Padrões. Disponível em: https://top.nic.br/

[32] Threat Analysis of the Domain Name System (DNS) – RFC 3833, IET,https://tools.ietf.org/html/rfc3833. Acesso em 13 de nov de 2025.

[33] KULKARNI, Mehar et al. Mitigating email phishing: analytical framework, simulation models, and preventive measures. In: 2024 10th international conference on communication and signal processing (ICCSP). IEEE, 2024. p. 1459-1464.

[34] Liu, Y. and Moody, D. (2024), Post-Quantum Cryptography, and the Quantum Future of Cybersecurity, Physical Review Applied, [online], https://doi.org/10.1103/PhysRevApplied.21.040501, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=936706 (Accessed November 16, 2025)

[35] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, and Y.-K. Liu, Status report on the third round of the NIST postquantum

cryptography standardization process, NISTIR 8413, National Institute of Standards and Technology, 2022.https://doi.org/10.6028/NIST.IR.8413-upd1.

[36] DMARC.ORG, 2015. Disponível em: https://dmarc.org/wp-content/uploads/2015/02/DMARC_author-to-recipient_flow.jpg