



DISSERTAÇÃO DE MESTRADO PROFISSIONAL

**STOPEMAILSPOOFING:
PROTEGENDO A ADMINISTRAÇÃO PÚBLICA FEDERAL BRASILEIRA
CONTRA A FALSIFICAÇÃO DE ENDEREÇOS DE E-MAIL**

Guilherme Dieguez Cândido

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

**STOPEMAILSPOOFING:
PROTEGENDO A ADMINISTRAÇÃO PÚBLICA FEDERAL BRASILEIRA
CONTRA A FALSIFICAÇÃO DE ENDEREÇOS DE E-MAIL**

Guilherme Dieguez Cândido

*Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia
Elétrica como requisito parcial para obtenção
do grau de Mestre em Engenharia Elétrica*

Banca Examinadora

Prof. João Souza Neto, Ph.D, FT/UnB

Orientador

Prof. Éder Souza Gualberto, Ph.D, FT/UnB

Examinador Interno

Prof. Ana Paula Bernardi da Silva, Ph.D, UCB

Examinador Externo

FICHA CATALOGRÁFICA

CÂNDIDO, GUILHERME DIEGUEZ

STOPEMAILSPOOFING: PROTEGENDO A ADMINISTRAÇÃO PÚBLICA FEDERAL BRASILEIRA CONTRA A FALSIFICAÇÃO DE ENDEREÇOS DE E-MAIL [Distrito Federal] 2026.

xvi, 196. Publicação: PPEE.MP.125., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2026).

Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.

Departamento de Engenharia Elétrica

1. Falsificação de e-mail

2. Spoofing de e-mail

3. SPF

4. DMARC

I. ENE/FT/UnB

II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

CÂNDIDO, G. D. (2026). *STOPEMAILSPOOFING: PROTEGENDO A ADMINISTRAÇÃO PÚBLICA FEDERAL BRASILEIRA CONTRA A FALSIFICAÇÃO DE ENDEREÇOS DE E-MAIL*. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 196. Publicação: PPEE.MP.125.

CESSÃO DE DIREITOS

AUTOR: Guilherme Dieguez Cândido

TÍTULO: STOPEMAILSPOOFING: PROTEGENDO A ADMINISTRAÇÃO PÚBLICA FEDERAL BRASILEIRA CONTRA A FALSIFICAÇÃO DE ENDEREÇOS DE E-MAIL.

GRAU: Mestre em Engenharia Elétrica ANO: 2026

É concedida à Universidade de Brasília permissão para reproduzir cópias desta Dissertação de Mestrado e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. Do mesmo modo, a Universidade de Brasília tem permissão para divulgar este documento em biblioteca virtual, em formato que permita o acesso via redes de comunicação e a reprodução de cópias, desde que protegida a integridade do conteúdo dessas cópias e proibido o acesso a partes isoladas desse conteúdo. O autor reserva outros direitos de publicação e nenhuma parte deste documento pode ser reproduzida sem a autorização por escrito do autor.

Guilherme Dieguez Cândido

Depto. de Engenharia Elétrica (ENE) - FT

Universidade de Brasília (UnB)

Campus Darcy Ribeiro

CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Àqueles que, mesmo diante das adversidades, se empenham em sustentar a linha invisível de defesa do Estado brasileiro.

AGRADECIMENTOS

Meus agradecimentos mais sinceros à Alice, à Helena, ao Anderson, à Verônica e à Carolina pelo amor, apoio e incentivo incondicionais. Ao Eder pela amizade e suporte durante este período. E, em especial, ao Prof. Dr. João Souza Neto por todos os ensinamentos transmitidos e pela forma cortês, humilde e profissional com que me conduziu nesta jornada; é o mestre que todo discente gostaria ter.

DECLARAÇÃO DE USO DE INTELIGÊNCIA ARTIFICIAL

Declara-se que ferramentas de Inteligência Artificial Generativa foram utilizadas neste trabalho exclusivamente como suporte à revisão textual abrangendo traduções, organização textual, revisões gramaticais, ortográficas, de estilo e de adequação ao padrão ABNT.

Todo o conteúdo apresentado nesta dissertação é de autoria própria, foi revisado criticamente pelo autor e reflete exclusivamente os procedimentos, análises e conclusões por ele conduzidos. O autor assume integral responsabilidade pela originalidade, veracidade e integridade do texto final, inclusive por eventuais erros ou imprecisões, em conformidade com a Portaria CNPq nº 2.664, de 6 de março de 2026.

RESUMO

Esta dissertação investigou o estado de vulnerabilidade da Administração Pública Federal (APF) brasileira frente a ataques de *spoofing* de e-mail, problema que compromete a autenticidade das comunicações institucionais e favorece a personificação de entidades estatais em campanhas de *phishing*. Partiu-se da constatação de uma lacuna de conhecimento sobre a implementação dos mecanismos de autenticação SPF, DKIM e DMARC nos domínios governamentais e objetivou-se auxiliar na mitigação da vulnerabilidade, com fins de ampliar a resiliência cibernética das infraestruturas críticas e a proteção de conhecimentos sensíveis de interesse do Estado e da sociedade.

Adotou-se pesquisa aplicada, quantitativa, de caráter censitário e desenho prospectivo-longitudinal de natureza experimental, com dezoito coletas mensais — realizadas entre fevereiro de 2025 e julho de 2026 — dos registros DNS dos 281 domínios da APF que operam correio eletrônico. Para tanto, desenvolveu-se a ferramenta *StopEmailSpoofing*, que automatiza a coleta, classifica a vulnerabilidade e fornece sugestões de correção. Ao longo do período, conduziram-se ações de mitigação institucionais — em parceria com os órgãos públicos federais competentes — e individualizadas — por meio do envio direto de alertas aos órgãos em situação vulnerável.

Os resultados evidenciaram que a proporção de domínios vulneráveis caiu de 64,8% para 34,2%, ganho que relacionou-se temporalmente às intervenções realizadas. Destaca-se, ainda, que o repasse de achados parciais ao PNPC da ABIN culminou na atualização e republicação, pelo CTIR Gov, da Recomendação nº 06/2025, que considerou os parâmetros técnicos desta pesquisa e converteu-os, ainda que indiretamente, em um padrão de conformidade obrigatório para toda a APF, ampliando o alcance das contribuições deste trabalho.

Conclui-se que o objetivo geral foi atingido, restando ainda expostos 96 domínios, resíduo que se mostrou majoritariamente refratário às sucessivas ações de mitigação executadas. Entre as contribuições, destacam-se a disponibilização em código aberto da ferramenta desenvolvida e o desdobramento normativo que transformou os parâmetros da pesquisa em padrão de conformidade para a APF. Como principal limitação, aponta-se o enfoque dado apenas à perspectiva do domínio remetente — não abrangendo o igualmente relevante comportamento do servidor destinatário — restrição esta que pode ser abordada em trabalhos futuros.

Palavras-chave: Falsificação de e-mail; SPF; DMARC; segurança cibernética; segurança nas comunicações.

ABSTRACT

This dissertation investigated the state of vulnerability of the Brazilian Federal Public Administration (APF) to e-mail spoofing attacks, a problem that compromises the authenticity of institutional communications and facilitates the impersonation of state entities in phishing campaigns. The study started from the observation of a knowledge gap regarding the implementation of the SPF, DKIM, and DMARC authentication mechanisms across government domains, and aimed to help mitigate this vulnerability in order to enhance the cyber resilience of critical infrastructures and the protection of sensitive knowledge of interest to the State and society.

An applied, quantitative research approach was adopted, of a census-based nature and prospective-longitudinal and experimental design, comprising eighteen monthly collections — carried out between February 2025 and July 2026 — of the DNS records of the 281 APF domains operating e-mail services. To this end, the StopEmailSpoofing tool was developed, which automates data collection, classifies vulnerability, and provides remediation suggestions. Throughout the period, both institutional mitigation actions — carried out in partnership with the competent federal public agencies — and individualized actions — through direct alerts sent to vulnerable entities — were conducted.

The results showed that the proportion of vulnerable domains dropped from 64.8% to 34.2%, a gain that was temporally related with the interventions carried out. It is also worth noting that the disclosure of partial findings to ABIN's PNPC led to the update and republication, by CTIR Gov, of Recommendation No. 06/2025, which took into account the technical parameters of this research and converted them, albeit indirectly, into a mandatory compliance standard for the entire APF, thereby broadening the reach of this work's contributions.

It is concluded that the general objective was achieved, with 96 domains remaining exposed, a residual group that proved largely unresponsive to the successive mitigation actions carried out. Among the contributions, the open-source release of the developed tool and the regulatory outcome that turned the research parameters into a compliance standard for the APF stand out. The main limitation lies in the focus restricted to the sender domain's perspective — not covering the equally relevant behavior of the receiving server — a constraint that may be addressed in future work.

Keywords: E-mail spoofing; SPF; DMARC; cybersecurity; communications security.

ÍNDICE

1. INTRODUÇÃO.....	1
1.1. JUSTIFICATIVA E MOTIVAÇÃO.....	4
1.1.1. Contraineligência no Estado Brasileiro.....	5
1.1.2. Proteção do Conhecimento Sensível.....	7
1.1.3. Proteção de Infraestruturas Críticas.....	8
1.1.4. Segurança Cibernética na Administração Pública Federal.....	9
1.1.5. Phishing e Spoofing.....	13
1.1.6. Motivação.....	14
1.2. OBJETIVO.....	15
1.2.1. Objetivo Geral.....	15
1.2.2. Objetivos Específicos.....	15
1.3. METODOLOGIA DE PESQUISA.....	16
1.4. ESTRUTURA DA DISSERTAÇÃO.....	21
2. FUNDAMENTAÇÃO TEÓRICA.....	23
2.1. A ARQUITETURA DO CORREIO ELETRÔNICO.....	23
2.2. SIMPLE MAIL TRANSFER PROTOCOL (SMTP).....	29
2.3. INTERNET MESSAGE FORMAT (IMF).....	32
2.4. MECANISMOS DE AUTENTICAÇÃO DE REMETENTE.....	34
2.4.1. Extensões SMTP: SPF, DKIM E DMARC.....	39
2.5. ATAQUES DE ENGENHARIA SOCIAL VIA E-MAIL.....	70
2.6. FALSIFICAÇÃO DE ENDEREÇOS DE E-MAIL (E-MAIL SPOOFING).....	72
2.7. TRABALHOS CORRELATOS.....	77
3. MATERIAIS E MÉTODOS.....	86
3.1. CONSTRUÇÃO DO INSTRUMENTO DE PESQUISA: STOPEMAILSPOOFING.....	86
3.1.1. Validação do instrumento e trabalho publicado.....	94
3.1.2. Registro de Software.....	95
3.2. SELEÇÃO DA AMOSTRAGEM.....	95
3.3. COLETA E ANÁLISE DE DADOS.....	97
3.4. AÇÕES VISANDO A MITIGAÇÃO.....	97
4. RESULTADOS E DISCUSSÕES.....	100
4.1. RECOMENDAÇÃO 06/2025 - CTIR Gov.....	100
4.2. RESULTADOS AGREGADOS DA AMOSTRA.....	102
4.2.1. Taxas de Adoção e Conformidade dos Registros SPF, DKIM e DMARC.....	102
4.2.2. Deficiências mais recorrentes nas configurações das extensões de segurança SMTP.....	111
4.2.3. Estado de vulnerabilidade dos órgãos públicos federais brasileiros a ataques de spoofing de e-mail.....	113
4.2.4. Evolução da implementação e da conformidade da configuração dos protocolos SPF, DKIM e DMARC nos domínios da APF ao longo da pesquisa.....	114
4.3. RESULTADOS POR AGRUPAMENTO TEMÁTICO.....	118
4.4. RESPOSTAS RECEBIDAS.....	120
5. CONCLUSÕES.....	122
5.1. RESPOSTAS ÀS QUESTÕES DE PESQUISA.....	122
5.2. ALCANCE DOS OBJETIVOS.....	123

5.2.1. Alcance do Objetivo Geral.....	123
5.2.2. Alcance dos Objetivos Específicos.....	124
5.3. CONTRIBUIÇÕES DA PESQUISA.....	126
5.3.1. Contribuições Acadêmicas.....	126
5.3.2. Contribuições Sociais.....	128
5.4. LIMITAÇÕES DA INVESTIGAÇÃO.....	130
5.5. SUGESTÕES PARA TRABALHOS FUTUROS.....	133
5.5.1. Continuidade da observação e reprodução em outras amostras.....	133
5.5.2. Pesquisa qualitativa junto aos órgãos ainda vulneráveis.....	133
5.5.3. Acesso a mensagens legítimas para auditoria efetiva de DKIM.....	134
5.5.4. Acesso aos relatórios DMARC.....	134
5.5.5. Pesquisa sob a perspectiva do servidor receptor.....	135
5.5.6. Aprimoramento do instrumento de pesquisa (StopEmailSpoofing).....	135
5.5.7. Extensão de navegador.....	136
5.5.8. Registro defensivo de domínios visualmente semelhantes.....	136
REFERÊNCIAS BIBLIOGRÁFICAS.....	138
APÊNDICES.....	151
A- ANÁLISE DO COMPORTAMENTO INDIVIDUAL DOS AGRUPAMENTOS.....	151
A.1. ADMINISTRAÇÃO E ECONOMIA.....	151
A.2. AGRICULTURA E ORGANIZAÇÃO AGRÁRIA.....	153
A.3. PREVIDÊNCIA, ASSISTÊNCIA SOCIAL, TRABALHO E HABITAÇÃO.....	154
A.4. CIÊNCIA, TECNOLOGIA E COMUNICAÇÕES.....	156
A.5. CULTURA E EDUCAÇÃO.....	158
A.6. DEFESA NACIONAL, SEGURANÇA PÚBLICA E RELAÇÕES EXTERIORES.....	160
A.7. DESPORTO, LAZER E DIREITOS DA CIDADANIA.....	162
A.8. ENERGIA E GESTÃO AMBIENTAL.....	165
A.9. INDÚSTRIA, COMÉRCIO E SERVIÇOS.....	166
A.10. LEGISLATIVO, JUDICIÁRIO E ESSENCIAIS À JUSTIÇA.....	169
A.11. SAÚDE E SANEAMENTO.....	170
A.12. TRANSPORTE E URBANISMO.....	172
B- RESPOSTAS RECEBIDAS A PARTIR DOS ALERTAS INDIVIDUAIS.....	175
ANEXOS.....	177
A- CERTIFICADO DE REGISTRO DE SOFTWARE.....	177

LISTA DE ILUSTRAÇÕES

Gráficos 1.1 e 1.2. Número de campanhas únicas de phishing por e-mail observadas em 2023, 2024 e 2025; e número de marcas ou entidades personificadas nas referidas campanhas, respectivamente...	2
Gráficos 1.3 e 1.4. Domínios governamentais explorados em campanhas de phishing, por quantidade de URLs maliciosas relacionadas e por domínio único, respectivamente.....	3
Quadro 1.1. Metodologia de pesquisa adotada nesta dissertação.....	19
Figura 2.1. Esquema ilustrativo da arquitetura técnica do fluxo percorrido por uma mensagem de e-mail.....	28
Figura 2.2. Diagrama conceitual do modelo arquitetural do SMTP.....	29
Figura 2.3. Visão geral do processo de envio de e-mails e das autenticações de remetente.....	38
Figura 2.4. Visão geral da falsificação de remetente.....	38
Figura 2.5. Esquema didático do resultado da falsificação.....	39
Figura 2.6. Registros DNS de um domínio incluindo SPF, DKIM e DMARC.....	41
Figura 2.7. Comparação de cabeçalhos de uma mensagem genuína (esquerda) e falsificada (direita)..	41
Figura 2.8. Fluxograma da verificação SPF.....	46
Figura 2.9. Exemplo de cabeçalho DKIM-Signature.....	49
Figura 2.10. Fluxograma da verificação DKIM.....	51
Figura 2.11. Fluxograma da verificação DMARC.....	62
Figura 2.12. Comparação de cabeçalhos com resultados dos protocolos de autenticação. E-mail aprovado em cima e rejeitado embaixo.....	65
Figura 2.13. Rejeição de mensagem durante sessão SMTP devido a não conformidade encontrada durante a autenticação.....	66
Figura 2.14. Comparação de mensagens renderizadas ao usuário. Genuína à esquerda e falsificada à direita.....	74
Quadro 3.1. Comparação do StopEmailSpoofing com as outras ferramentas mencionadas.....	89
Quadro 3.2. Categorias de vulnerabilidade à falsificação consideradas pela ferramenta.....	90
Figura 3.1. Exemplo de saída da ferramenta com sugestões de mitigação.....	90
Figura 3.2. Exemplo de combinações de mecanismos e tags SPF/DMARC e a situação de vulnerabilidade correspondente consideradas pela ferramenta.....	91
Quadro 3.3. Módulos que compõem a ferramenta.....	92
Figura 3.3. Fluxograma de funcionamento da ferramenta proposta.....	93
Figura 3.4. Captura de tela do frontispício do trabalho publicado. Fonte: RISTI (119).....	94
Figura 3.5. Áreas de atuação utilizadas para detalhar execução de despesas governamentais.....	96
Quadro 3.4. Agrupamento dos órgãos da amostra por área de atuação.....	96
Figura 3.6. Exemplo de mensagem de e-mail enviada aos órgão vulneráveis no primeiro e segundo alertas.....	98
Figura 3.7. Exemplo de mensagem de e-mail enviada no terceiro alerta.....	99
Figura 4.1. Recomendação 06/2025 do CTIR Gov.....	101
Gráfico 4.1. Evolução da taxa de adoção do protocolo SPF ao longo do período de observação.....	103

Gráfico 4.2. Evolução na conformidade dos registros SPF durante o período de observação.....	104
Gráfico 4.3. Evolução na taxa de adoção do protocolo DKIM durante o período de observação.....	106
Gráfico 4.4. Evolução na taxa de adoção do protocolo DMARC durante o período de observação....	107
Gráfico 4.5. Evolução na conformidade dos registros DMARC durante o período de observação.....	108
Gráfico 4.6. Evolução na adoção e conformidade da política DMARC para subdomínios durante o período de observação.....	109
Gráficos 4.7 e 4.8. Ganhos percentuais, absolutos e relativos, respectivamente, na taxa de adoção dos protocolos SPF, DKIM e DMARC durante o período de observação.....	110
Gráfico 4.9. Variação no estado de vulnerabilidade dos domínios da APF no período analisado.....	114
Gráfico 4.10. Evolução da mitigação da vulnerabilidade ao longo da investigação em todos os 281 domínios.....	115
Gráfico 4.11. Ganho percentual na proteção dos órgãos da APF contra spoofing de e-mail durante o período analisado.....	119
Gráfico A.1. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Administração e Economia”.....	151
Gráfico A.2. Variação do estado de vulnerabilidade dos domínios do grupo “Administração e Economia” no período analisado.....	152
Gráfico A.3. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Agricultura e Organização Agrária”.....	153
Gráfico A.4. Variação do estado de vulnerabilidade dos domínios do grupo “Agricultura e Organização Agrária” no período analisado.....	154
Gráfico A.5. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Previdência, Assistência Social, Trabalho e Habitação”.....	155
Gráfico A.6. Variação do estado de vulnerabilidade dos domínios do grupo “Previdência, Assistência Social, Trabalho e Habitação” no período analisado.....	156
Gráfico A.7. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Ciência, Tecnologia e Comunicações”.....	157
Gráfico A.8. Variação do estado de vulnerabilidade dos domínios do grupo “Ciência, Tecnologia e Comunicações” no período analisado.....	158
Gráfico A.9. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Cultura e Educação”.....	159
Gráfico A.10. Variação do estado de vulnerabilidade dos domínios do grupo “Cultura e Educação” no período analisado.....	160
Gráfico A.11. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Defesa Nacional, Segurança Pública e Relações Exteriores”.....	161
Gráfico A.12. Variação do estado de vulnerabilidade dos domínios do grupo “Defesa Nacional, Segurança Pública e Relações Exteriores” no período analisado.....	162
Gráfico A.13. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Desporto, Lazer e Direitos da Cidadania”.....	163
Gráfico A.14. Variação do estado de vulnerabilidade dos domínios do grupo “Desporto, Lazer e Direitos da Cidadania” no período analisado.....	164
Gráfico A.15. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Energia e Gestão Ambiental”.....	165

Gráfico A.16. Variação do estado de vulnerabilidade dos domínios do grupo “Energia e Gestão Ambiental” no período analisado.....	166
Gráfico A.17. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Indústria, Comércio e Serviços”.....	167
Gráfico A.18. Variação do estado de vulnerabilidade dos domínios do grupo “Indústria, Comércio e Serviços” no período analisado.....	168
Gráfico A.19. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Legislativo, Judiciário e Essenciais à Justiça”.....	169
Gráfico A.20. Variação do estado de vulnerabilidade dos domínios do grupo “Legislativo, Judiciário e Essenciais à Justiça” no período analisado.....	170
Gráfico A.21. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Saúde e Saneamento”.....	171
Gráfico A.22. Variação do estado de vulnerabilidade dos domínios do grupo “Saúde e Saneamento” no período analisado.....	172
Gráfico A.23. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Transporte e Urbanismo”.....	173
Gráfico A.24. Variação do estado de vulnerabilidade dos domínios do grupo “Transporte e Urbanismo” no período analisado.....	174
Figura B.1. Resposta de órgão da amostragem a um dos alertas individualizados.....	175
Figura B.2. Resposta de órgão da amostragem a um dos alertas individualizados.....	175
Figura B.3. Resposta de órgão da amostragem a um dos alertas individualizados.....	175
Figura B.4. Resposta de órgão da amostragem a um dos alertas individualizados.....	175
Figura B.5. Resposta de órgão da amostragem a um dos alertas individualizados.....	176
Figura B.6. Resposta de órgão da amostragem a um dos alertas individualizados.....	176
Figura B.7. Resposta de órgão da amostragem a um dos alertas individualizados.....	176
Figura B.8. Resposta de órgão da amostragem a um dos alertas individualizados.....	176
Figura C.1. Certificado de Registro de Programa de Computador no INPI.....	177

LISTA DE TABELAS

Tabela 4.1. Dados coletados referentes aos 281 domínios da APF.....	115
Tabela A.1. Dados coletados referentes aos 23 domínios do grupo “Administração e Economia”.....	151
Tabela A.2. Dados coletados referentes aos 10 domínios do grupo “Agricultura e Organização Agrária”.....	153
Tabela A.3. Dados coletados referentes aos 13 domínios do grupo “Previdência, Assistência Social, Trabalho e Habitação”.....	155
Tabela A.4. Dados coletados referentes aos 16 domínios do grupo “Ciência, Tecnologia e Comunicações”.....	157
Tabela A.5. Dados coletados referentes aos 123 domínios do grupo “Cultura e Educação”.....	159
Tabela A.6. Dados coletados referentes aos 14 domínios do grupo “Defesa Nacional, Segurança Pública e Relações Exteriores”.....	161
Tabela A.7. Dados coletados referentes aos 10 domínios do grupo “Desporto, Lazer e Direitos da Cidadania”.....	163
Tabela A.8. Dados coletados referentes aos 20 domínios do grupo “Energia e Gestão Ambiental”.....	165
Tabela A.9. Dados coletados referentes aos 6 domínios do grupo “Indústria, Comércio e Serviços”.....	167
Tabela A.10. Dados coletados referentes aos 10 domínios do grupo “Legislativo, Judiciário e Essenciais à Justiça”.....	169
Tabela A.11. Dados coletados referentes aos 12 domínios do grupo “Saúde e Saneamento”.....	171
Tabela A.12. Dados coletados referentes aos 24 domínios do grupo “Transporte e Urbanismo”.....	173

LISTA DE NOMENCLATURAS E ABREVIACÕES

ABIN	Agência Brasileira de Inteligência
ADMD	<i>Administrative Management Domain</i> (Domínio de Gerenciamento Administrativo)
aMS	<i>Author Message Store</i> (Armazenamento de Mensagens do Autor)
aMSA	<i>Author Mail Submission Agent</i> (Agente de Submissão de Correio do Autor)
aMUA	<i>Author Message User Agent</i> (Agente de Mensagem de Usuário do Autor)
ANPD	Autoridade Nacional de Proteção de Dados
APF	Administração Pública Federal
API	<i>Application Programming Interface</i> (Interface de Programação de Aplicações)
APWG	<i>Anti-Phishing Working Group</i>
ARC	<i>Authenticated Received Chain</i> (Cadeia de Recebimento Autenticado)
ASCII	<i>American Standard Code for Information Interchange</i>
Bcc	<i>Blind Carbon Copy</i>
BEC	<i>Business Email Compromise</i> (Comprometimento de E-mail Comercial)
BIMI	<i>Brand Indicators for Message Identification</i>
Cc	<i>Carbon Copy</i>
CEO	<i>Chief Executive Officer</i>
CEPESC	Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações
CIDR	<i>Classless Inter-Domain Routing</i>
CLI	<i>Command Line Interface</i> (Interface de Linha de Comando)
CNAME	<i>Canonical Name</i>
CNCiber	Comitê Nacional de Cibersegurança

CPF	Cadastro de Pessoa Física
CR	<i>carriage-return</i>
CRLF	<i>carriage-return/line-feed</i>
CSIRT	<i>Computer Security Incident Response Team</i> (Equipe de Resposta a Incidentes de Segurança Computacional)
CSV	<i>Comma-Separated Values</i> (Valores Separados por Vírgula)
CTIR Gov	Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo
DANE	<i>DNS-based Authentication of Named Entities</i>
DANE-TLSA	<i>DNS-based Authentication of Named Entities with Transport Layer Security Authentication</i>
DKIM	<i>DomainKeys Identified Mail</i>
DMARC	<i>Domain-based Message Authentication, Reporting and Conformance</i>
DNS	<i>Domain Name System</i> (Sistema de Nomes de Domínio)
DNSSEC	<i>Domain Name System Security Extensions</i>
E-Ciber	Estratégia Nacional de Cibersegurança
ENINT	Estratégia Nacional de Inteligência
ENSIC	Estratégia Nacional de Segurança de Infraestruturas Críticas
ETIR	Equipe de Tratamento e Resposta a Incidentes Cibernéticos
EUA	Estados Unidos da América
FQDN	<i>Fully-Qualified Domain Names</i>
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
hMDA	<i>Handling System Oriented Mail Delivery Agent</i> (Agente de Entrega de Correio orientado ao Sistema de Tratamento de Mensagens)
hMSA	<i>Handling System Oriented Mail Submission Agent</i> (Agente de Submissão de Correio orientado ao Sistema de Tratamento de Mensagens)
HTTP	<i>Hypertext Transfer Protocol</i> (Protocolo de Transferência de Hipertexto)

HTTPS	<i>HyperText Transfer Protocol Secure</i>
IANA	<i>Internet Assigned Numbers Authority</i>
IETF	<i>Internet Engineering Task Force</i>
IMAP	<i>Internet Message Access Protocol</i>
IMF	<i>Internet Message Format</i>
INPI	Instituto Nacional da Propriedade Industrial
IP	<i>Internet Protocol</i>
IPv4	<i>Internet Protocol</i> versão 4
IPv6	<i>Internet Protocol</i> versão 6
LAI	Lei de Acesso à Informação
LF	<i>line-feed</i>
LGPD	Lei Geral de Proteção de Dados Pessoais
MDA	<i>Mail Delivery Agent</i> (Agente de Entrega de Correio)
MDN	<i>Message Disposition Notification</i> (notificação de disposição de mensagem ou “recibo de leitura”)
MGI	Ministério da Gestão e da Inovação em Serviços Públicos
MHS	<i>Message Handling System</i> (Sistema de Tratamento de Mensagens)
MS	<i>Message Store</i> (Armazenamento de Mensagens)
MSA	<i>Mail Submission Agent</i> (Agente de Submissão de Correio)
MTA	<i>Mail Transfer Agent</i> (Agente de Transferência de Correio)
MTA-STS	<i>Mail Transfer Agent Strict Transport Security</i>
MUA	<i>Message User Agent</i> (Agente de Mensagem de Usuário)
MX	<i>Mail Exchange</i>
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
NS	<i>Nameserver</i>

Nupitec	Núcleo de Propriedade Intelectual da Universidade de Brasília
ODNI	<i>Office of the Director of National Intelligence of the United States of America</i> (Escritório do Diretor de Inteligência Nacional dos Estados Unidos da América)
OSINT	<i>Open Source Intelligence</i> (Inteligência de Fontes Abertas)
PGP	<i>Pretty Good Privacy</i>
PNCiber	Política Nacional de Cibersegurança
PNI	Política Nacional de Inteligência
PNPC	Programa Nacional de Proteção do Conhecimento Sensível
PNSI	Política Nacional de Segurança da Informação
PNSIC	Política Nacional de Segurança de Infraestruturas Críticas
POP	<i>Post Office Protocol</i>
PPSI	Programa de Privacidade e Segurança da Informação
REGIC	Rede Federal de Gestão de Incidentes Cibernéticos
RFC	<i>Request for Comments</i>
RISTI	Revista Ibérica de Sistemas e Tecnologias de Informação
rMDA	<i>Receiver Mail Delivery Agent</i> (Agente de Entrega de Correio do Receptor)
rMS	<i>Receiver Message Store</i> (Armazenamento de Mensagens do Receptor)
rMUA	<i>Receiver Mail User Agent</i> (Agente de Usuário de Correio do Receptor)
RUA	<i>Reporting URI for Aggregate data</i>
RUF	<i>Reporting Unit Failure</i>
S/MIME	<i>Secure/Multipurpose Internet Mail Extensions</i>
SDID	<i>Signing Domain Identifier</i>
SGD/MGI	Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos
SISBIN	Sistema Brasileiro de Inteligência

SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
SMTP	<i>Simple Mail Transfer Protocol</i> (Protocolo de Transferência de Correio Simples)
SOA	<i>Start of Authority</i>
SPF	<i>Sender Policy Framework</i>
TCP	<i>Transmission Control Protocol</i> (Protocolo de Controle de Transmissão)
TCU	Tribunal de Contas da União
TF-IDF	<i>Term Frequency-Inverse Document Frequency</i>
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TLD	<i>Top-Level Domain</i> (Domínio de Nível Superior)
TLS	<i>Transport Layer Security</i>
UDP	<i>User Datagram Protocol</i> (Protocolo de Datagrama do Usuário)
UnB	Universidade de Brasília
URL	<i>Uniform Resource Locator</i> (Localizador Uniforme de Recursos)

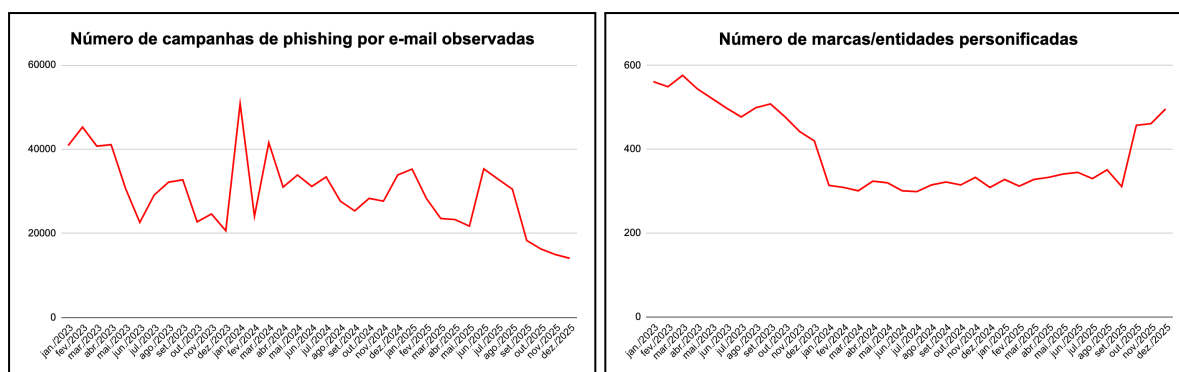
1. INTRODUÇÃO

O e-mail ainda é uma das formas mais comuns de comunicação no mundo digital e o protocolo *Simple Mail Transfer Protocol* (SMTP) tornou-se essencial à sociedade (1). Um endereço de e-mail é necessário para se inscrever em qualquer atividade online, incluindo redes sociais, mensagerias instantâneas e outras formas de presença na Internet. O comércio online também depende do e-mail para confirmações, notificações e outras comunicações pertinentes. O número total de mensagens de e-mail institucionais e pessoais enviadas e recebidas por dia está previsto ultrapassar os 424 bilhões até o final de 2028, período em que o número de usuários de correio eletrônico superará 4,9 bilhões (2).

O uso contínuo e exponencialmente crescente do e-mail também implica risco para os usuários, devido aos ataques facilmente possíveis ao sistema de correio eletrônico. O núcleo de todo o sistema de e-mail depende do protocolo SMTP, criado na década de 1980. No momento do desenvolvimento do SMTP, os ataques de segurança altamente computacionais dos dias atuais não poderiam sequer ter sido considerados, o que acarretou nas brechas de segurança do sistema de e-mail atual (1, 3). Uma vez que o serviço de e-mail impulsiona tanto a comunicação pessoal quanto a profissional, a confiança é o elemento preferencialmente explorado em ciberataques (4). Logo, como uma plataforma central de comunicação em massa, o e-mail se torna o principal alvo de investidas de engenharia social e de ataques de *phishing* (5).

O momento em que os usuários clicam em URLs de *phishing* costuma ser apenas o começo de uma cadeia de ataques muito maior, que resulta em sequestro de contas, acesso e controle não autorizados de sistemas, violação e vazamento de dados, *ransomware* e mais. Os atacantes querem se manter furtivos e despercebidos. Em sequestros de contas, utilizam o *phishing* para roubar credenciais de uma pessoa e se tornam, efetivamente, essa pessoa — pelo menos no que se refere aos sistemas aos quais conseguem acesso (6). Atores maliciosos personificam fontes confiáveis para atrair vítimas a fornecer suas credenciais de login. Com êxito, podem utilizar as credenciais comprometidas para obter acesso a redes institucionais e a recursos protegidos. As técnicas comumente empregadas para roubar credenciais de login incluem: personificar supervisores, colegas de confiança ou pessoal de TI para enviar e-mails direcionados (7).

Os relatórios trimestrais de tendências de atividades de *phishing* do *Anti-Phishing Working Group* (APWG) analisam ataques de *phishing* e outras técnicas de roubo de identidade, com base em dados fornecidos por suas empresas-membro, seus parceiros globais de pesquisa e por submissões recebidas por e-mail. A APWG — que opera como uma coalizão internacional sem fins lucrativos — mede a evolução, a proliferação e a propagação desses métodos. Nos Gráficos 1.1 e 1.2, pode-se observar, respectivamente, a quantidade de campanhas únicas e de entidades personificadas em 2023, 2024 e 2025 (8-19). Nota-se que são mais de 300 entidades personificadas todos os meses em dezenas de milhares de campanhas de *phishing*.



Gráficos 1.1 e 1.2. Número de campanhas únicas de phishing por e-mail observadas em 2023, 2024 e 2025; e número de marcas ou entidades personificadas nas referidas campanhas, respectivamente.

Fonte: Anti-Phishing Working Group (8-19)

As consequências desses ataques podem ser severas, com diversos tipos de informações sensíveis em risco de comprometimento. Dados financeiros, registros médicos, e-mails pessoais e senhas são apenas alguns exemplos de informações valiosas que podem ser obtidas por invasores. Esses ataques frequentemente têm como alvo infraestruturas críticas governamentais e é essencial que indivíduos e organizações adotem medidas de segurança robustas para detectar, prevenir e mitigar o impacto de ataques, protegendo seus ativos e preservando a integridade de seus sistemas (20).

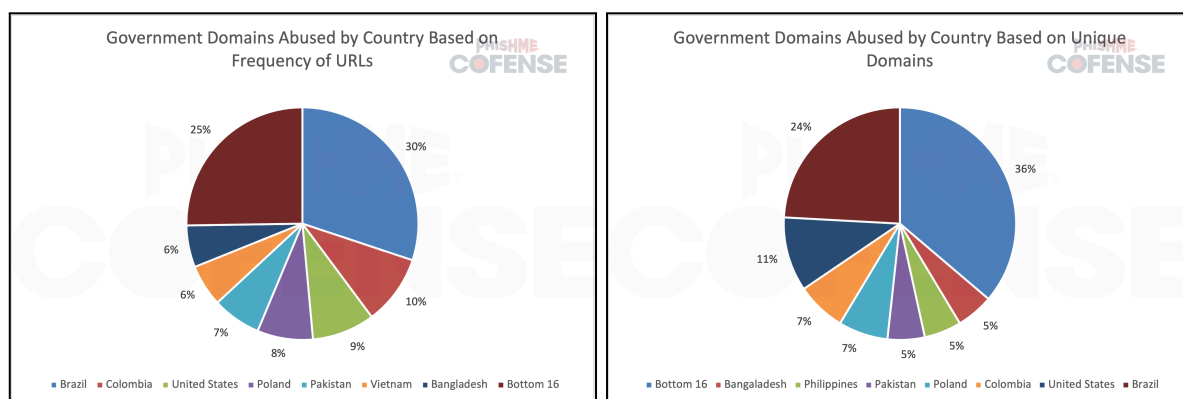
O *Annual Threat Assessment of the U.S. Intelligence Community* de 2025 e 2026 — produzidos pelo *Office of the Director of National Intelligence* (ODNI) —, por exemplo, apresentam uma avaliação coletiva e coordenada das ameaças globais à segurança nacional dos Estados Unidos da América (EUA). Os documentos concentram-se, sob a perspectiva estadunidense, nas ameaças mais diretas e gravosas para o ano subsequente, abrangendo atores estatais e não estatais, fornecendo uma análise das dimensões militares, cibernéticas, econômicas, tecnológicas e de influência que configuram o ambiente de segurança contemporâneo. Ambos os relatórios destacam que uma gama de atores cibernéticos e de inteligência está direcionando suas ações contra infraestruturas críticas de telecomunicações e de mídia e que grupos não estatais são frequentemente habilitados por atores estatais, tanto diretamente quanto indiretamente (21, 22).

Nota-se, portanto, que a gestão de infraestruturas críticas e de serviços essenciais enfrenta novas dificuldades. O fator humano desempenha um papel considerável na segurança dos sistemas destas infraestruturas, e invasores maliciosos podem violar a segurança organizacional por meio de interações humanas, utilizando técnicas de engenharia social (23). A resiliência cibernética passa, portanto, a ser um objetivo a ser alcançado por essas infraestruturas críticas, possibilitando, de forma holística, o alinhamento entre a infraestrutura e o modelo de negócio da organização, trazendo confiança ao sistema, permitindo a prevenção, absorção, recuperação e adaptação após emergências e incidentes (24).

No que diz respeito ainda mais especificamente a ataques direcionados a serviços governamentais, uma publicação recente da Kaspersky (25) destaca que o *phishing* que imita mensagens e portais governamentais, é um clássico, mas que, em 2025, golpistas adicionaram

novos *scripts* ao repertório. No Brasil, por exemplo, os atacantes alvejaram números de CPF por meio da clonagem de portais governamentais. Uma vez que o CPF é a chave mestra para o acesso a serviços estatais, bases de dados nacionais e documentos pessoais, um número comprometido constitui essencialmente um atalho para o roubo de identidade. Como visto, os agentes de ameaça exploram domínios legítimos para fins maliciosos. Infelizmente, os domínios “.gov” não são exceção a esse tipo de abuso. Embora aparentem ser explorados com menor frequência em comparação com outros domínios (26), seu comprometimento oferece maiores riscos às infraestruturas críticas, aos serviços essenciais nacionais e à salvaguarda de conhecimentos sensíveis e informações classificadas.

Num relatório recente publicado pela empresa Cofense (26), foram identificados domínios pertencentes a governos de mais de 20 países sendo explorados como redirecionadores de URLs maliciosas em campanhas de *phishing*. Os sete países mais afetados responderam por 75% de todos os domínios “.gov” abusados. O Brasil, como se pode verificar no Gráfico 1.3, foi o líder absoluto, representando mais do que a soma dos três países seguintes no *ranking*. Entre os domínios “.gov.br” abusados, três domínios específicos foram responsáveis por 65% dos casos de abuso. Quando se considera apenas os domínios únicos — ou seja, ignorando os casos em que um mesmo domínio foi explorado diversas vezes — conforme mostrado no Gráfico 1.4 — o Brasil se mantém em posição de destaque, ainda com ampla diferença em relação aos demais países (26).



Gráficos 1.3 e 1.4. Domínios governamentais explorados em campanhas de phishing, por quantidade de URLs maliciosas relacionadas e por domínio único, respectivamente.

Fonte: Cofense (26).

Desta forma, resta claro que o *phishing* vem se destacando como uma atividade altamente organizada, representando um cibercrime que apresenta ameaças substanciais a indivíduos, empresas e entidades governamentais (27). O *phishing* envolve, muitas vezes, a prática de enviar mensagens falsificadas que personifiquem uma fonte confiável e respeitável (23). É o que se conhece como *spoofing* de e-mail ou domínio.

Neste tipo de falsificação, um nome de domínio semelhante ao de uma instituição legítima é utilizado no endereço do remetente. Esta técnica refere-se, portanto, à situação em que o domínio parece ser de um site bem conhecido pelo alvo. O nome de domínio não deve ser apenas plausível; deve ser reconhecível como familiar, podendo ser idêntico ou assemelhar-se

estritamente ao domínio legítimo personificado (28). É preciso proteger todas as comunicações confiáveis contra ataques de personificação, incluindo domínios falsificados, domínios parecidos e contas legítimas que possam ter sido comprometidas (6).

Neste contexto, o conceito de antispoofting abrange uma ampla gama de protocolos e tecnologias projetados para autenticar os remetentes de e-mails e garantir a integridade da comunicação eletrônica, verificando se os e-mails são genuínos, se realmente vieram do remetente declarado e se não foram alterados durante a transmissão (29). Embora extensões de segurança SMTP como SPF (*Sender Policy Framework*), DKIM (*DomainKeys Identified Mail*) e DMARC (*Domain-based Message Authentication, Reporting and Conformance*) tenham sido desenvolvidas para autenticar a origem das mensagens, muitos domínios ainda carecem de configuração adequada, o que torna os e-mails falsificados mais difíceis de serem detectados e bloqueados (4).

Falsificar um domínio que não adota SPF, DKIM e DMARC resulta em uma taxa de entrega de 60,5%; os domínios com políticas permissivas reduzem a taxa para 47,3%; e aqueles com políticas restritivas reduzem a taxa para 28,4%. Isso confirma os benefícios de publicar registros SPF, DKIM e DMARC. Embora não garanta proteção total (30), o uso desta técnica é considerado adequado para autenticar o remetente de um e-mail e manter a integridade das mensagens enviadas e recebidas (29).

Pesquisadores têm se concentrado em estudar os problemas destas extensões (31). Com centenas de bilhões de e-mails enviados diariamente, a adoção de boas práticas e de padrões modernos de segurança de e-mail pelos provedores é de extrema importância para todos (32). Uma abordagem de defesa pluridimensional — combinando a aplicação de políticas DMARC, a configuração correta de SPF e DKIM, a educação de usuários sobre segurança de e-mail e a filtragem aprimorada de correio eletrônico — precisa ser implementada para combater efetivamente o *spoofing* de domínios (33).

1.1. JUSTIFICATIVA E MOTIVAÇÃO

O avanço tecnológico permeia e impacta qualquer processo desenvolvido na atualidade: as informações circulam com menos intermediação e maior velocidade; os instrumentos tecnológicos e de comunicação são onipresentes graças à interconectividade e à convergência com as plataformas móveis; a infraestrutura tecnológico-informacional está cada vez mais presente em produtos domésticos e industriais; o ambiente virtual permite que conteúdos e aplicativos ampliem alcance e eficiência. Os inegáveis benefícios e facilidades trazidos pela tecnologia são, contudo, acompanhados de vulnerabilidades. Como consequência, o mundo enfrenta o crescimento da espionagem cibernética, inclusive com fins econômicos e científicos, e a automatização e a interconectividade dos sistemas de infraestrutura crítica tornam possíveis sabotagens por meios virtuais. Por outro lado, a disseminação destas ameaças cibernéticas acaba por intensificar as demandas por soluções capazes de elevar o nível de segurança da informação, das comunicações e das infraestruturas críticas (34).

A segurança cibernética é um dos grandes desafios a ser enfrentado pelos governos de diversos países, particularmente no que se refere à garantia do funcionamento de infraestruturas críticas, tais como energia, defesa, transporte, telecomunicações, finanças, entre outros. No setor público brasileiro, não é diferente. Desafios complexos relacionados à segurança cibernética e as rápidas transformações na economia e na sociedade, proporcionadas pelo ambiente digital, impuseram novas ações e estratégias no setor público federal brasileiro, haja vista o número de ataques aos órgãos observados nos últimos anos (24).

1.1.1. Contraineligência no Estado Brasileiro

A Lei nº 12.527, de 18 de novembro de 2011, também conhecida como Lei de Acesso à Informação (LAI) — que dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal — preconiza em seu art. 25 que é dever do Estado controlar o acesso a informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção (35).

Nesta conjuntura de proteção às informações sigilosas produzidas pelo Estado, em 1999, a Lei nº 9.883 instituiu o Sistema Brasileiro de Inteligência (SISBIN), criou a Agência Brasileira de Inteligência (ABIN) como órgão central do referido sistema e estabeleceu as bases normativas para o planejamento, execução, coordenação, supervisão e controle das atividades de inteligência e contraineligência no âmbito da Administração Pública Federal (APF). O objeto central da lei consiste em regular a produção de conhecimentos de interesse nacional para subsidiar o processo decisório, bem como “a proteção de informações sensíveis relativas à soberania, à defesa das instituições democráticas e à segurança da sociedade e do Estado” (36).

A articulação dos dispositivos da supracitada Lei demonstra que os órgãos da APF, ao integrarem o SISBIN ou produzirem conhecimentos de interesse estratégico, assumem o dever jurídico de proteger ativamente seus ativos informacionais contra qualquer forma de acesso não autorizado. A ausência de avaliação prévia e sistemática de vulnerabilidades a tais ameaças compromete, portanto, não apenas a salvaguarda da informação e a proteção de conhecimentos sensíveis, mas também a própria capacidade do Estado de avaliar ameaças à ordem constitucional e de preservar a soberania nacional e o Estado Democrático de Direito.

Em 2016, o Decreto nº 8.793, editado pela Presidência da República, instituiu a Política Nacional de Inteligência (PNI). Trata-se de documento normativo de mais alto nível de orientação para a Atividade de Inteligência no âmbito do SISBIN, conforme estabelecido pela Lei nº 9.883. A PNI estabelece que a Atividade de Inteligência divide-se, fundamentalmente, em dois grandes ramos: inteligência e contraineligência, sendo o segundo — de particular interesse desta dissertação — definido como a “atividade que objetiva prevenir, detectar,

obstruir e neutralizar a Inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado”. Complementarmente, a PNI identifica os ataques cibernéticos como uma das principais ameaças à segurança nacional, destacando a vulnerabilidade dos setores públicos essenciais e reforçando a necessidade de proteção contínua dos conhecimentos sensíveis (37).

Por sua vez, a Estratégia Nacional de Inteligência (ENINT), documento oficial de orientação estratégica do SISBIN, aprovado pelo Decreto presidencial de 15 de dezembro de 2017, estabelece os eixos, desafios, objetivos e diretrizes para o desempenho integrado da Atividade de Inteligência. Seu principal propósito é consolidar conceitos, identificar ameaças e oportunidades no ambiente estratégico e definir ações capazes de fortalecer o SISBIN, de modo a subsidiar o processo decisório do Estado brasileiro com conhecimentos antecipados, precisos e protegidos (34).

A ENINT considera os ataques cibernéticos como sendo uma das principais ameaças que apresentam potencial capacidade de pôr em perigo a segurança nacional e a integridade da sociedade e do Estado brasileiros, definindo-os como “ações deliberadas com o emprego de recursos da tecnologia da informação para interromper, penetrar, adulterar ou destruir redes utilizadas por setores públicos e privados essenciais à sociedade e ao Estado, a exemplo daqueles pertencentes à infraestrutura crítica nacional”. Na mesma linha, o documento conceitua a ameaça da espionagem, que “visa à obtenção de conhecimentos ou dados sensíveis para beneficiar Estados, grupos de países, organizações, facções, grupos de interesse, empresas ou indivíduos” e que, como já mencionado, pode ser perpetrada por meios cibernéticos (34).

No âmbito dos desafios estratégicos da Atividade de Inteligência, a ENINT estabelece o fortalecimento da cultura de proteção do conhecimento e de preservação do sigilo, afirmando textualmente que (34):

“A preservação do sigilo e a proteção [...] do conhecimento sensível são determinantes para o cumprimento dos objetivos da Inteligência. A cultura de proteção, inerente à Atividade de Inteligência, se estende para um campo maior, dentro do qual se incluem os ativos estratégicos nacionais, tanto materiais quanto imateriais, que apoiam o desenvolvimento da sociedade brasileira. O fortalecimento da proteção dos ativos do Estado e da sociedade brasileira é fundamental para que interferências externas não comprometam o interesse nacional”.

Por fim, entre os objetivos estratégicos elencados pela ENINT figura o de criar protocolos conjuntos para a proteção de conhecimentos sensíveis, constando ainda, no mesmo rol, o de aperfeiçoar o processo de gestão de riscos e o de fomentar a cultura de proteção do conhecimento na sociedade (34).

Complementarmente, a Doutrina da Atividade de Inteligência, documento oficial da ABIN publicado em novembro de 2023, divulga que “a Atividade de Inteligência produz conhecimentos e realiza ações visando à redução de vulnerabilidades e à neutralização de ameaças contra a segurança das pessoas e das instituições brasileiras. Também visa proteger

informações, pessoas, áreas, instalações e meios sensíveis”. A contrainteligência é, portanto, o ramo da Atividade de Inteligência que desenvolve ações especializadas voltadas para prevenir, detectar, identificar, avaliar, obstruir e neutralizar ações da Inteligência adversa que constituam ameaça: a interesses do Estado e da sociedade; ao processo decisório; e à salvaguarda de conhecimentos, informações e dados sensíveis, dos meios que as retenham ou em que transitem, de seus detentores e de áreas e instalações (37).

As medidas adotadas pela contrainteligência agrupam-se em dois segmentos: as preventivas, relativas à antecipação e à proteção contra ameaças, e as ativas, relativas à contraposição a ameaças. A contrainteligência preventiva é de especial interesse deste trabalho, sendo o segmento que prevê a adoção de medidas e procedimentos destinados à salvaguarda de conhecimentos, informações e dados sensíveis e de seus detentores, bem como de materiais, áreas, instalações, meios de produção e armazenamento e canais de comunicação que interessem à sociedade e ao Estado proteger. Assim, a contrainteligência preventiva deve atuar em parceria com objetos de interesse adverso, ou seja, potenciais alvos da Inteligência adversa, que podem incluir pessoas, instituições, instalações ou informações. A contrainteligência preventiva é subdividida nas seguintes áreas: proteção do conhecimento sensível, proteção da infraestrutura física e prevenção de ações de interferência na decisão (37).

Destaca-se que, de acordo com o Decreto nº 11.816, de 6 de dezembro de 2023, que prova a Estrutura Regimental da ABIN, compete ao Departamento de Contrainteligência: “[...] III - implementar programas, projetos e ações relativos a: a) proteção de setores estratégicos e infraestruturas críticas, observadas as competências dos demais órgãos; b) proteção de conhecimentos sensíveis” (38).

1.1.2. Proteção do Conhecimento Sensível

A proteção do conhecimento sensível é a vertente da contrainteligência preventiva que estabelece a adoção de medidas e procedimentos destinados a prevenir, detectar e obstruir antagonismos dirigidos aos detentores de conhecimentos e dados sensíveis, sigilosos ou classificados, ao suporte físico que os contém, ao meio que os veicula e aos locais onde se encontram seus detentores, sejam eles pessoas, documentos, materiais, meios de tecnologia da informação e áreas ou instalações (37). Entendem-se por conhecimentos e dados sensíveis aqueles que, devido a sua importância para o desenvolvimento e para a segurança do Estado e da sociedade, necessitam de medidas especiais de proteção. As ações preventivas de proteção do conhecimento incluem sensibilização, orientação e capacitação de instituições estratégicas nacionais para a salvaguarda de ativos de interesse do Estado e da sociedade, promovendo a adoção de comportamentos e medidas de segurança. Ademais, a contrainteligência preventiva pode atuar também na identificação e avaliação das vulnerabilidades nos sistemas de proteção da instituição e apresentar recomendações para redução do risco de incidentes (37).

Neste sentido, a Portaria nº 59, de 26 de julho de 2018, estabeleceu, no âmbito da ABIN, o Programa Nacional de Proteção do Conhecimento Sensível (PNPC), com a finalidade explícita de promover a proteção de conhecimentos sensíveis relativos aos interesses e à segurança do Estado e da sociedade brasileira (39). O documento atribui à ABIN a responsabilidade pela implementação do PNPC no exercício de suas atividades de contrainteligência de Estado, atuando em parceria com instituições nacionais que geram ou detêm conhecimentos sensíveis.

Uma das linhas de ação por meio das quais o PNPC é desenvolvido trata da identificação de vulnerabilidades nos sistemas de proteção das instituições parceiras. Para tanto, o PNPC contempla atividades de sensibilização, realização de fóruns, elaboração de relatórios com apresentação de medidas preventivas e corretivas, além de outras atividades a serem definidas no âmbito das parcerias. No desenvolvimento de suas atividades, o PNPC abrange temas estratégicos relativos à política externa e a informações estratégicas de Estado (39).

1.1.3. Proteção de Infraestruturas Críticas

Outra vertente da contrainteligência preventiva, a proteção de infraestruturas críticas, por sua vez, preconiza a adoção de medidas e procedimentos destinados a prevenir, detectar e obstruir ameaças de qualquer natureza dirigidas às infraestruturas críticas nacionais. São consideradas infraestruturas críticas instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade. A atividade de segurança de infraestruturas críticas objetiva articular, em diversas esferas dos setores público e privado, o desenvolvimento de procedimentos de segurança preventiva de recursos humanos, equipamentos, instalações, serviços, sistemas, informações e de outros recursos que assegurem a manutenção e o funcionamento dos serviços e atividades indispensáveis ao Estado e à sociedade (37).

As infraestruturas críticas de Tecnologia da Informação e Comunicação (TIC) possuem a peculiar característica de poderem fazer parte, com relações de interdependência horizontais, de várias outras infraestruturas críticas, ou seja, a informação gerada por determinada área prioritária de uma infraestrutura crítica de TIC pode ser insumo para outra infraestrutura crítica, evidenciando, desta forma, seu alto grau de acoplamento e interdependência. Isso eleva a necessidade de identificar os ativos de informação essenciais, bem como de tratar os riscos a que estão expostos, pois o impacto causado pela perda ou indisponibilidade desses ativos poderia comprometer toda a cadeia de infraestruturas críticas existente (37).

Dentro deste cenário, o Decreto nº 9.573, de 22 de novembro de 2018, aprovou a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), visando garantir a segurança, a resiliência e a continuidade dos serviços essenciais prestados pelas infraestruturas críticas do País. A norma estabelece que “são princípios da PNSIC: I - a prevenção e a precaução, com base em análise de riscos; II - a integração entre as diferentes esferas do Poder Público, o setor empresarial e os demais segmentos da sociedade; III - a redução de custos para a

sociedade decorrente de investimentos em segurança; e IV - a salvaguarda do interesse da defesa e da segurança nacional”. Ademais, são objetivos da PNSIC, entre outros: “I - a prevenção de eventual interrupção, total ou parcial, das atividades relacionadas às infraestruturas críticas ou, no caso de sua ocorrência, a redução dos impactos dela resultantes; [...] VI - o estabelecimento da prevalência do interesse da defesa e da segurança nacional na proteção, na conservação e na expansão das infraestruturas críticas” (40).

Em 2020, o Decreto nº 10.569, aprovou a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC) como instrumento orientador da PNSIC, com ênfase na prevenção, resiliência e gestão de riscos em setores estratégicos como comunicações, energia, transportes, finanças e águas, integrando esforços do Estado e do setor privado para a salvaguarda da soberania nacional (41). O documento traz, entre outros, os seguintes desafios que reúnem elementos essenciais para que os objetivos na PNSIC sejam alcançados: “c) consolidação da cultura de segurança junto aos órgãos da administração pública, ao setor privado e à sociedade; e) institucionalização da gestão de riscos na administração pública e em entidades privadas”. Elencam-se ainda, como objetivos e iniciativas estratégicas: “4.3. Incentivar a adoção de recursos e procedimentos voltados à segurança cibernética nas infraestruturas críticas; 4.3.1. Estimular os responsáveis pelas infraestruturas críticas a ampliar seus investimentos em recursos de segurança cibernética cada vez mais avançados; e 4.3.2. Orientar as infraestruturas críticas a observarem a Estratégia Nacional de Segurança Cibernética” (41).

1.1.4. Segurança Cibernética na Administração Pública Federal

Adentrando mais especificamente na questão da segurança cibernética estatal, entre 2020 e 2021, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) editou três instruções normativas. A Instrução Normativa nº 1, de 27 de maio de 2020, trata da aprovação e da implementação da Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da APF, direta e indireta, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional. Para os fins do disposto no documento, a segurança da informação abrange: “I - a segurança cibernética; II - a defesa cibernética; III - a segurança física; IV - a proteção de dados organizacionais; e V - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação” (42).

O ato estabelece às referidas instituições da APF a obrigatoriedade de elaboração de uma Política de Segurança da Informação própria, da designação de Gestor de Segurança da Informação, e da instituição de um Comitê de Segurança da Informação e de uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), além da observância de outras referências normativas, como a Estratégia Nacional de Segurança Cibernética (42).

A Instrução Normativa nº 2, de 24 de julho de 2020, por sua vez, alterou a Instrução Normativa nº 1 com o objetivo de aperfeiçoar a Estrutura de Gestão da Segurança da

Informação nos órgãos e entidades da APF, instituindo, de forma obrigatória, as ETIRs para órgãos e entidades que administram suas próprias infraestruturas de rede (43). Finalmente, a Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, estabeleceu os processos obrigatórios de gestão de segurança da informação a serem observados pelos órgãos e entidades da APF, visando estruturar uma governança contínua e alinhada à evolução tecnológica e aos riscos institucionais. Trata-se, portanto, de um marco regulatório destinado a subsidiar o planejamento, a implementação e a manutenção de controles internos de segurança da informação no âmbito do Poder Executivo Federal. Esta última norma define cinco processos de realização obrigatória: I - mapeamento de ativos de informação; II - gestão de riscos de segurança da informação; III - gestão de continuidade de negócios em segurança da informação; IV - gestão de mudanças nos aspectos de segurança da informação; e V - avaliação de conformidade de segurança da informação”. O processo de mapeamento de ativos de informação, em especial, estrutura-se com vistas a subsidiar a identificação de ameaças e vulnerabilidades (44).

Ainda em 2021, o Decreto nº 10.748, instituiu a Rede Federal de Gestão de Incidentes Cibernéticos no âmbito da APF. Trata-se de ato normativo que visa aprimorar a coordenação entre órgãos e entidades para prevenção, tratamento e resposta a incidentes cibernéticos, elevando o nível de resiliência em segurança cibernética dos ativos de informação do Poder Executivo Federal. A participação dos órgãos da administração direta, autárquica e fundacional é obrigatória, enquanto a das empresas públicas e sociedades de economia mista é voluntária mediante adesão formal (45).

O decreto define os objetivos, a composição, as competências e as disposições transitórias da Rede, com ênfase na criação de equipes especializadas e na articulação coordenada pelo GSI/PR, por meio do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov). São objetivos da Rede Federal de Gestão de Incidentes Cibernéticos: I - divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos; II - compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas; III - divulgar informações sobre ataques cibernéticos; IV - promover a cooperação entre os participantes da Rede; e V - promover a celeridade na resposta a incidentes cibernéticos” (45).

Segundo a norma, compete aos órgãos e às entidades da APF direta, autárquica e fundacional comunicar imediatamente o CTIR Gov, por meio de suas ETIRs, sobre a existência de vulnerabilidades ou incidentes de segurança cibernética que impactem ou que possam impactar os serviços prestados ou contratados; e sanar, com urgência, as vulnerabilidades cibernéticas, em especial aquelas identificadas nos alertas e nas recomendações expedidos pelo CTIR Gov (45).

Em 2023, o Decreto nº 11.856 instituiu a Política Nacional de Cibersegurança (PNCiber) e o Comitê Nacional de Cibersegurança (CNCiber), sendo princípios da PNCiber, entre outros: “III - a prevenção de incidentes e de ataques cibernéticos, em particular aqueles dirigidos a infraestruturas críticas nacionais e a serviços essenciais prestados à sociedade; IV - a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos; V - a educação e o desenvolvimento tecnológico em segurança cibernética; VI - a cooperação entre

órgãos e entidades, públicas e privadas, em matéria de segurança cibernética”. Constatam ainda, entre os objetivos da PNCiber: “II - garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações; [...] V - estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos; VI - incrementar a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos” (46).

Na mesma linha, o Decreto nº 12.573, de 4 de agosto de 2025, instituiu a Estratégia Nacional de Cibersegurança (E-Ciber) estruturando-a nos seguintes eixos temáticos: I - proteção e conscientização do cidadão e da sociedade; II - segurança e resiliência dos serviços essenciais e das infraestruturas críticas; III - cooperação e integração entre os órgãos e entidades, públicas e privadas; e IV - soberania nacional e governança. Segundo o diploma, a proteção e a conscientização do cidadão e da sociedade abrangem, entre outras, a promoção da prevenção e do combate aos cibercrimes, às fraudes digitais e a outras ações maliciosas no ciberespaço por meio de atuação multissetorial (47).

O decreto prossegue estabelecendo que a segurança e a resiliência dos serviços essenciais e das infraestruturas críticas têm por objetivo fornecer à sociedade instrumentos efetivos para prevenção e resposta a ciberincidentes, abrangendo, no mínimo, as seguintes ações: I - estímulo às entidades dotadas de competências regulatórias para promover a gestão de riscos e adotar medidas de proteção e resposta a ciberincidentes nos seus setores; VIII - incentivo à realização de exercícios e simulações setoriais e multissetoriais regulares destinados ao aprimoramento da resiliência dos serviços essenciais e das infraestruturas críticas. Dispõe ainda que a soberania nacional e a governança têm por objetivo atender e proteger os interesses da sociedade brasileira no ciberespaço e garantir um ambiente cibernético confiável que assegure o crescimento econômico e tecnológico do País (47).

Datado também de 4 de agosto de 2025, o Decreto nº 12.572 instituiu a Política Nacional de Segurança da Informação (PNSI) e dispôs sobre a governança da segurança da informação no âmbito da APF, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação no País. O texto normativo estabelece princípios, objetivos, competências e instrumentos para a proteção da informação, abrangendo a segurança dos dados, dos ativos de informação, do ambiente físico e eletrônico e do pessoal envolvido no ciclo de vida da informação, definindo responsabilidades para o GSI/PR e para outros órgãos federais (48).

São objetivos da PNSI, entre outros: “I - contribuir para a segurança da informação, observados os direitos e as garantias fundamentais, especialmente em relação: [...] c) à gestão e à proteção adequadas do conhecimento sensível e das informações com restrição de acesso; II - salvaguardar as infraestruturas críticas e os serviços essenciais; III - estimular a gestão de riscos, a proteção e o controle da informação”. Ademais, compete aos órgãos e entidades da APF, em seu âmbito de atuação: I - implementar a PNSI; [...] IV - elaborar, publicar, implementar e revisar regularmente suas políticas de segurança da informação e suas normas

internas de segurança da informação, observados os normativos sobre segurança da informação editados pelo GSI/PR; [...] VI - realizar a avaliação de conformidade com as normas relativas à segurança da informação (48).

Por parte do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), a Portaria nº 852 da Secretaria de Governo Digital (SGD), de 28 de março de 2023, tratou da instituição oficial do Programa de Privacidade e Segurança da Informação (PPSI) no âmbito dos órgãos e entidades da APF direta, autárquica e fundacional que integram o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) (49). Trata-se de ato normativo de caráter infralegal, com o propósito de elevar a maturidade e a resiliência institucionais em matéria de privacidade e segurança da informação no contexto do governo digital brasileiro.

A portaria estabelece os agentes responsáveis pela implementação, monitoramento e melhoria contínua dos controles de privacidade e segurança da informação em cada órgão e entidade da APF direta, autárquica e fundacional integrante do SISP; adota um modelo de governança multicamadas, alinhado aos princípios da primeira das três linhas de defesa previstas na Instrução Normativa nº 3 da Controladoria-Geral da União, de 9 de junho de 2017; e integra competências previstas na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), na PNSI e em normativos relacionados. Na referida disposição normativa, os Gestores de TIC e de Segurança da Informação, juntamente com os proprietários de ativos, gestores do negócio ou de políticas públicas, atuam como a primeira linha de defesa quando se trata de controles de privacidade e segurança da informação (49).

No contexto do PPSI, também foi instituído, pela SGD, o Guia do Framework de Privacidade e Segurança da Informação. Trata-se de um instrumento normativo-orientativo destinado, primordialmente, aos órgãos e entidades da APF, com o propósito de fomentar a implementação de controles integrados de privacidade, proteção de dados pessoais e segurança da informação, em estrita conformidade com a LGPD, a PNSI e outros normativos correlatos emitidos pela Autoridade Nacional de Proteção de Dados (ANPD) e pelo GSI/PR. O guia apresenta uma estruturação de controles inspirada em referências internacionais consolidadas — como CIS Controls v8, NIST Cybersecurity Framework, NIST Privacy Framework, ISO/IEC 29100:2011, ISO/IEC 29151:2017, ABNT NBR ISO/IEC 27701:2019, entre outras —, adaptadas à realidade da gestão pública brasileira (50). Seu escopo abrange desde a estruturação básica da governança até a avaliação da maturidade institucional, por meio de ciclos de diagnóstico, implementação e monitoramento.

O referido guia é o primeiro documento do arcabouço normativo analisado neste trabalho a abordar diretamente a segurança de e-mails e domínios. Seu “Controle 9: Proteções de E-mail e Navegador Web” visa melhorar as proteções e detecções de vetores de ameaças via e-mail e web, pois constituem oportunidades para atacantes manipularem o comportamento humano por meio do engajamento direto, uma vez que conteúdos podem ser criados para atrair ou enganar os usuários para que revelem suas credenciais, forneçam dados sensíveis ou forneçam um canal aberto por onde os atacantes obtenham acesso indevido, aumentando assim o risco para as instituições. A ênfase recai sobre a mitigação de riscos associados a clientes de e-mail e navegadores como vetores de ataque, com destaque para a

implementação dos mecanismos de autenticação de domínios (nomeadamente SPF, DKIM e DMARC), com o objetivo de reduzir a probabilidade de e-mails forjados ou modificados serem enviados personificando o domínio da instituição (50).

Como último documento normativo relacionado ao objeto desta pesquisa, a “Matriz de riscos e controles para serviços de hospedagem Web, e-mail e DNS”, elaborada pelo Tribunal de Contas da União (TCU), teve por objetivo promover a melhoria na gestão de riscos de segurança da informação em organizações públicas federais, estaduais e municipais, inspirando-se na ferramenta “top.nic” do Núcleo de Informação e Coordenação do Ponto BR (NIC.br) e em dados de relatórios internacionais sobre vetores de ataques cibernéticos (51). A obra apresenta uma matriz estruturada de riscos e controles técnicos para os serviços de DNSSEC, HTTPS, TLS, cabeçalhos de segurança HTTP, e-mail (SPF, DKIM, DMARC e DANE) e suporte a IPv6, com descrição sucinta de cada controle, exemplos de riscos associados à sua ausência, critérios normativos, referências de implementação, além de estimativas preliminares de custo e benefício. O TCU classifica a implementação de SPF, DKIM e DMARC como de baixo custo e alto benefício (51).

O documento supracitado menciona que foi realizada uma auditoria pelo TCU com o objetivo específico de promover a melhoria da gestão de riscos de segurança da informação, no contexto dos serviços de hospedagem Web, e-mail e resolução de nomes (*Domain Name System* - DNS) em organizações públicas federais, estaduais e municipais. Mais de 14 mil URLs governamentais, de todas as esferas de governo e Poderes do Brasil, foram coletadas e testadas com apoio da ferramenta “top.nic” e os resultados apresentados no relatório constante do TC 009.585/2023-0 — não encontrado em fontes abertas. No âmbito dos serviços de e-mail, o documento ratifica que, sem a implementação do DMARC, criminosos podem se passar pelo domínio da instituição e enviar e-mails fraudulentos, aumentando as chances de sucesso de ataques de *phishing*. Da mesma forma, enfatiza que a ausência de SPF aumenta o risco de *phishing* e *spoofing* (51).

1.1.5. Phishing e Spoofing

Como visto, os ataques de *phishing* por e-mail estão entre os tipos mais comuns de crimes cibernéticos e constituem um dos principais riscos à segurança digital. Uma grande parte das violações de engenharia social ocorre justamente no setor público (52). Para se antecipar aos ataques de *phishing*, os profissionais de segurança devem analisar as técnicas empregadas pelos atacantes, identificar tendências emergentes e desenvolver contramedidas adequadas. Isso pode, em última análise, reduzir as chances de um ataque bem-sucedido (20). A gravidade do impacto dos crimes cibernéticos originados de e-mails falsificados e as limitações das tecnologias desenvolvidas para mitigá-los exigem uma análise abrangente do fenômeno e a proposição de novas ferramentas (53).

Desde o início dos anos 2000, muitos esforços têm sido feitos para implementar protocolos antispoofing, como SPF, DKIM e DMARC. Infelizmente, a implementação dessas extensões

é voluntária (54) e, apesar de mais de 20 anos de desenvolvimento, sua adoção ainda é considerada baixa. De acordo com análises recentes em larga escala, 50,3% dos domínios possuem registro SPF e apenas 11,5% possuem registro DMARC (53). Essa baixa aceitação compromete seriamente a segurança de todo o ecossistema de e-mail (55).

Algumas pesquisas qualitativas relatam que administradores de e-mail acreditam que os protocolos antispoofting são ineficazes e que o custo supera os benefícios (56), enquanto outras destacam que os desafios de implementação levam a erros de configuração (30). Uma preocupação comum entre os administradores é ver e-mails falsificados passando pelos controles de segurança e, ao mesmo tempo, e-mails legítimos sendo bloqueados.

Os registros SPF e DMARC são intrinsecamente publicizados para consulta, o que significa que, se houver algum grau de vulnerabilidade, qualquer invasor pode identificar um alvo em potencial e explorá-lo em um ataque de *spoofing*. Ignorar as configurações de subdomínio também pode levar a certos tipos de ataques. O resultado é previsível (57). Logo, se é possível proteger e-mails com os protocolos existentes, a questão é: por que esses protocolos não estão sendo usados de forma a alcançar este objetivo (58)?

O primeiro passo para compreender as razões disso é medir regularmente a adoção das extensões (53). Medições de SPF, DKIM e DMARC em escala global são necessárias para compreender melhor o estado atual de adoção (1) e entender como más configurações podem ser corrigidas (53). É fundamental compreender os índices de implantação, corrigir configurações inadequadas e promover a conscientização sobre boas práticas de segurança em e-mails (53). A adoção de SPF, DKIM e DMARC precisa ser acelerada (30).

1.1.6. Motivação

Ante o exposto, em consonância com as lacunas identificadas na literatura e com os objetivos elencados pelo arcabouço normativo examinado, analisar a vulnerabilidade da APF brasileira a ataques de *spoofing* de e-mail e propor ações de mitigação às instituições vulneráveis pode contribuir com a melhoria da segurança, da integridade e da autenticidade das comunicações oficiais do País.

Um e-mail com o remetente forjado e contendo uma URL maliciosa é, na maior parte das vezes, a porta de entrada para um ataque cibernético complexo que, se exitoso contra entes públicos — onde concentra-se a maior parte das infraestruturas críticas e da produção de conhecimentos sensíveis relativos a decisões de interesse nacional — pode desencadear uma série de danos ao Estado brasileiro, como espionagem e sabotagem cibernéticas, vazamento de documentos classificados e comprometimento da confiança estatal tanto no cenário interno quanto externo.

Desta forma, a identificação e a mitigação dessa vulnerabilidade mostram-se imperativas para a proteção da APF e para a preservação da segurança e da soberania nacionais.

1.2. OBJETIVO

1.2.1. Objetivo Geral

O objetivo desta pesquisa é auxiliar na mitigação da vulnerabilidade dos órgãos públicos federais brasileiros a ataques de *spoofing* de e-mail, contribuindo para a resiliência cibernética das infraestruturas críticas e a proteção de conhecimentos sensíveis de interesse do Estado e da sociedade.

1.2.2. Objetivos Específicos

Constituem objetivos específicos deste trabalho:

- Delimitar e caracterizar o universo de domínios pertencentes à Administração Pública Federal brasileira, de modo a estabelecer o escopo institucional da pesquisa e a distinguir aqueles que de fato operam infraestrutura de correio eletrônico e estão, portanto, expostos ao risco de *spoofing* de e-mail;
- Mensurar a taxa de adoção e de conformidade dos mecanismos de autenticação SPF, DKIM e DMARC nos domínios identificados, de forma a classificar objetivamente o nível de vulnerabilidade de cada órgão a ataques de *spoofing* e a compor um retrato fidedigno da postura de segurança de e-mail praticada pela APF;
- Compreender como essa vulnerabilidade se distribui entre os diferentes setores da administração pública, analisando o panorama de exposição por área de atuação governamental e evidenciando eventuais tendências ou disparidades entre esses grupos, sem que seja comprometida a identidade dos órgãos individualmente vulneráveis;
- Contribuir para a correção das fragilidades identificadas, oferecendo aos órgãos vulneráveis um retorno sobre sua situação e subsídios técnicos que orientem a adoção ou o aprimoramento de suas políticas de SPF, DKIM e DMARC; e
- Compreender a dinâmica temporal da resiliência cibernética da APF diante da ameaça em questão, verificando, ao longo de um intervalo de dezoito meses, se as práticas de autenticação de e-mail evoluem, se estagnam ou retrocedem, de modo a inferir em que medida a pesquisa e as ações de mitigação sugeridas aos órgãos produzem efeito mensurável sobre a segurança do ecossistema de e-mail governamental brasileiro.

1.3. METODOLOGIA DE PESQUISA

Kumar (59) define a pesquisa aplicada como aquela em que as técnicas, procedimentos e métodos que formam o corpo da metodologia de pesquisa são aplicados para coletar dados sobre vários aspectos de uma situação, questão, problema ou fenômeno, de modo que as informações coletadas possam ser utilizadas para propósitos como: formulação de políticas; desenvolvimento, modificação e avaliação de programas; aprimoramento da compreensão sobre um fenômeno; estabelecimento de causalidade e consequência; identificação de necessidades; e desenvolvimento de estratégias. Assim, uma vez que o presente estudo não se restringe à construção teórica abstrata, mas busca subsidiar políticas de cibersegurança e estratégias de mitigação para ampliar a resiliência cibernética da APF, apresenta-se aqui uma pesquisa aplicada que visa a geração de conhecimentos práticos e acionáveis por meio da aplicação de técnicas metodológicas a um problema concreto: a vulnerabilidade dos órgãos públicos federais brasileiros a ataques de *spoofing* de e-mail.

Sob a perspectiva da abordagem de pesquisa, o presente estudo enquadra-se no paradigma quantitativo. A pesquisa quantitativa é caracterizada por seguir uma metodologia rígida, estruturada e predeterminada, com o objetivo principal de quantificar a extensão da variação de um fenômeno, enfatizando a mensuração objetiva de variáveis (59). No contexto deste trabalho, essa abordagem evidencia-se pelo foco do estudo em quantificar a magnitude do problema — ou seja, medir com precisão quantos domínios apresentam níveis específicos de vulnerabilidade ao *spoofing* de e-mail ao longo do tempo.

Ainda segundo Kumar (59), uma pesquisa envolve exploração e descrição sistemática, controlada, válida e rigorosa do que não é conhecido, e o estabelecimento de associações e causalidade que permitam a predição precisa de resultados sob um dado conjunto de condições. Também envolve a identificação de lacunas no conhecimento, a validação do que já é conhecido e a identificação de erros e limitações anteriores. A força do que se encontra repousa em grande medida na forma como foi encontrado. Desta forma, a principal função de um desenho de pesquisa é decidir, descrever, justificar e explicar como encontrar-se-ão respostas para as questões de pesquisa. O desenho de pesquisa estabelece os detalhes específicos de uma investigação. Em estudos longitudinais, a população é visitada um número determinado de vezes, em intervalos regulares, geralmente ao longo de um período prolongado, para coletar a informação necessária. Os intervalos podem ser tão curtos quanto uma semana ou tão longos quanto um ano. Independentemente do tamanho do intervalo, o tipo de informação coletada a cada vez é idêntico. A principal vantagem de um estudo longitudinal é permitir ao pesquisador medir o padrão de mudança e obter informações factuais, exigindo coleta em base regular ou contínua, o que aumenta sua precisão (59).

Logo, a coleta mensal — ao longo de 18 meses — dos registros DNS dos domínios dos órgãos públicos federais brasileiros, com fins de verificar o estado de vulnerabilidade da APF frente a ataques de *spoofing* de e-mail, configura um desenho de pesquisa longitudinal, haja vista que a mesma população é examinada repetidamente em intervalos regulares para captar padrões de mudança ao longo do tempo. É importante destacar que estudos longitudinais podem sofrer o efeito de condicionamento. Isso descreve situações em que, se contatados

com frequência, os respondentes começam a saber o que se espera deles e podem responder as perguntas de forma direcionada, sem pensar, ou podem, ainda, perder o interesse na investigação. Essa desvantagem não se aplica à presente pesquisa, uma vez que as coletas são realizadas por meio de registros DNS disponíveis na rede mundial de computadores, e não por intermédio de interação humana. Além disso, intervenções que contatem os órgãos visando a mitigação têm justamente o objetivo de notificá-los sobre o que se espera que eles façam para a correção da vulnerabilidade.

Kumar (59) classifica ainda os desenhos de pesquisa quanto ao período de referência. O período de referência refere-se ao intervalo temporal no qual um estudo explora um fenômeno, situação, evento ou problema. Os estudos são categorizados, sob esta ótica, como retrospectivos, prospectivos ou retrospectivo-prospectivos. O presente estudo é prospectivo, pois a coleta dos registros DNS ocorre exclusivamente a partir do momento presente, estendendo-se por 18 meses, sem a incorporação de dados históricos anteriores ao início da investigação. As alterações observadas nos registros, ocorridas após as ações de mitigação, são mensuradas ao longo do período prospectivo de coleta, o que corresponde exatamente à definição de longitudinalidade prospectiva.

Complementarmente, de acordo com a classificação de Kumar quanto à natureza da investigação, os desenhos de pesquisa dividem-se em experimentais, não experimentais e quase-experimentais, sendo que no delineamento experimental o pesquisador introduz uma intervenção que se assume ser a causa da mudança e aguarda para observar os seus resultados ou efeitos (59). Sob esta ótica, a presente pesquisa caracteriza-se como um estudo experimental, pois, após um período inicial de observação passiva para constatar o estado de vulnerabilidade da APF, o pesquisador introduz ativamente intervenções de mitigação. A partir da introdução dessas ações, a pesquisa continuou a realizar coletas mensais para observar os resultados e avaliar se houve resposta às mitigações propostas na correção da vulnerabilidade.

A construção de um instrumento de pesquisa, por sua vez, envolve a seleção do método de coleta de dados, a definição de requisitos, o pré-teste e a verificação de validade e confiabilidade (59). Essa etapa orienta, portanto, o desenvolvimento e a validação de ferramenta automatizada — constituindo-se, assim, em instrumento quantitativo — para a realização de coletas e verificações mensais de conformidade dos registros DNS de cada órgão, em especial das extensões SPF, DKIM e DMARC, garantindo reprodutibilidade e precisão nas mensurações. A escolha de um método específico de coleta de dados depende do propósito da coleta, do tipo de informação a ser coletada, dos recursos disponíveis, das habilidades do pesquisador no uso desse método e das características da população de estudo (59).

Após construir o instrumento de pesquisa, seleciona-se uma amostra da população de estudo. A amostra é um subconjunto da população, selecionado para a coleta de dados. A qualidade dos resultados depende, em grande medida, da qualidade da amostra. Na presente pesquisa, haja vista tratar-se de população finita, realizou-se uma seleção censitária, ou seja, foram

incluídos todos os nomes de domínio relacionados a cada um dos órgãos da APF, desde que efetivamente utilizados para a troca de mensagens eletrônicas.

Tendo sido definida a amostragem, segue-se com a coleta de dados, processo de reunir as informações necessárias para responder às questões de pesquisa. Os dados podem ser coletados de fontes primárias ou secundárias. Kumar (59) preconiza que fontes primárias são aquelas que se originam de respondentes com o propósito específico para o qual um estudo é realizado, como em entrevistas, observação e o uso de questionários. Todas as outras fontes, onde a informação necessária já está disponível independentemente da existência da pesquisa, são chamadas de fontes secundárias. A ferramenta aqui desenvolvida atua como mero instrumento de consulta, extração e análise de dados, não como geradora primária desses dados. Registros DNS, ao constituírem-se de registros rotineiros mantidos por uma organização, existentes independentemente do estudo e não gerados por “respondentes” com o propósito específico da pesquisa, configuram-se, portanto, como fontes secundárias. A enumeração dos nomes de domínio das instituições públicas federais, por meio de *Open Source Intelligence* (OSINT), também corresponde à definição de coleta de dados secundários extraídos de fontes públicas já existentes.

Após a coleta, os dados devem ser processados e exibidos de forma clara. No processamento quantitativo, isso inclui a tabulação e a aplicação de estatísticas descritivas e inferenciais para quantificar tendências ao longo do tempo, utilizando planilhas eletrônicas e gráficos, por exemplo. A redação do relatório de pesquisa, por sua vez, deve apresentar os achados de forma clara e lógica, com base em evidências, incluindo recomendações práticas. Aqui, enfatiza-se a comunicação dos resultados e das sugestões de mitigação, baseados nos dados longitudinais devidamente tratados, aos órgãos federais em situação de vulnerabilidade.

Em conclusão, essa estrutura metodológica, ancorada no modelo de oito etapas descrito por Kumar (59), contribui para o rigor científico desta pesquisa de natureza aplicada e quantitativa, além de reprodutibilidade e aplicabilidade prática dos achados, alinhando-se aos objetivos da dissertação. A adoção de coletas de OSINT como fonte secundária, combinada ao desenho prospectivo-longitudinal, maximiza o alcance do trabalho e a detecção de padrões temporais de vulnerabilidade, conferindo robustez à investigação e aos objetivos almejados. Espera-se, com isso, que esta abordagem garanta que os achados sobre a vulnerabilidade da APF a ataques de *spoofing* de e-mail não sejam apenas descritivos, mas também acionáveis para o fortalecimento da cibersegurança institucional brasileira.

Desta forma, o problema de pesquisa que norteia esta dissertação é conhecer o estado atual de vulnerabilidade da APF frente a ataques de *spoofing* de e-mail e gerar ações que auxiliem na mitigação desta ameaça. Embora estes ataques representem, sabidamente, uma ameaça significativa à segurança de infraestruturas críticas e conhecimentos sensíveis brasileiros, verifica-se uma lacuna no conhecimento sistemático sobre o nível de vulnerabilidade dos domínios dos órgãos da APF, em especial no que tange à implementação e à conformidade das extensões de segurança (SPF, DKIM e DMARC), bem como à evolução da resiliência cibernética dessas instituições ao longo do tempo, considerando-se as ações propostas para a mitigação. Tem-se como questões de pesquisas subsidiárias ao problema mencionado:

1. Quais são as taxas de adoção e conformidade dos registros SPF, DKIM e DMARC entre os órgãos públicos federais brasileiros?
2. Quais são as deficiências mais recorrentes observadas nas configurações das extensões de segurança SMTP da amostra e quais ações práticas podem ser propostas para mitigar as vulnerabilidades identificadas?
3. Qual é o estado de vulnerabilidade dos órgãos públicos federais brasileiros a ataques de *spoofing*?
4. Como evoluíram a implementação e a conformidade da configuração dos protocolos SPF, DKIM e DMARC nos domínios da APF ao longo de um período de monitoramento de 18 meses, em especial considerando-se as ações de mitigação propostas?

Em conclusão, segundo a metodologia de oito etapas proposta por Kumar (59) — e conforme se resume no Quadro 1.1 —, o presente trabalho é classificado como uma pesquisa quantitativa aplicada, tratando-se de um estudo censitário e prospectivo-longitudinal de natureza experimental, a partir de fontes secundárias de dados.

Quadro 1.1. Metodologia de pesquisa adotada nesta dissertação

Etapas	Objetivo	Aplicação
1) Formulação do problema de pesquisa	Formular um problema de pesquisa é o primeiro e mais importante passo no processo de pesquisa, pois define seu objetivo. Deve deixar claro ao pesquisador e aos leitores o que se pretende investigar.	Conhecer o estado atual de vulnerabilidade da APF frente a ataques de <i>spoofing</i> de e-mail, gerar ações que auxiliem na mitigação desta ameaça e constatar se há evolução na proteção dos órgãos durante o período de investigação.
2) Desenho de pesquisa	A principal função de um desenho de pesquisa é decidir, descrever, justificar e explicar como encontrar-se-ão respostas para as questões de pesquisa. É o desenho de pesquisa que define os detalhes específicos a serem executados durante a investigação.	Prospectivo-longitudinal de natureza experimental: Coleta mensal, durante 18 meses, dos registros DNS dos domínios dos órgãos públicos federais brasileiros e envio de propostas de mitigação, com o objetivo de verificar a variação do estado de vulnerabilidade da APF frente a ataques de <i>spoofing</i> de e-mail ao longo deste período.

3) Construção do instrumento de pesquisa	A maioria dos instrumentos de pesquisa é construída pelos próprios pesquisadores. Existem, no entanto, alguns instrumentos padronizados disponíveis que podem ser utilizados, caso sejam adequados ao estudo. A construção de um instrumento de pesquisa envolve a seleção do método de coleta de dados, a redação de perguntas ou itens, o pré-teste e a verificação da validade e da confiabilidade.	Desenvolvimento e validação de ferramenta automatizada para a realização de coletas e verificações mensais de conformidade dos registros DNS de cada órgão, em especial das extensões SPF, DKIM e DMARC.
4) Definição da amostra	A amostra é um subconjunto da população, selecionado para a coleta de dados. A qualidade dos resultados depende, em grande medida, da qualidade da amostra. Na pesquisa quantitativa, a amostragem visa à representatividade; na qualitativa, à saturação de informação.	Seleção censitária: todos os domínios relacionados a cada um dos órgãos da APF, desde que sejam utilizados para a troca de mensagens eletrônicas.
5) Proposta de pesquisa	A proposta de pesquisa é um documento que serve como um plano detalhado, devendo descrever o que se pretende fazer, como se pretende fazê-lo e por quê.	Este subitem da presente dissertação.
6) Coleta de dados	A coleta de dados é o processo de reunir as informações necessárias para responder às questões de pesquisa. Os dados podem ser coletados de fontes primárias ou secundárias. Ao usar fontes secundárias,	Fontes secundárias: Registros DNS, ao constituírem-se de registros rotineiros mantidos por uma organização, existentes independentemente do estudo e não gerados por “respondentes” com o

	extraem-se informações já disponíveis.	propósito específico da pesquisa, configuram-se como fonte secundária. A enumeração dos nomes de domínio das instituições públicas federais, por meio de OSINT, também corresponde à definição de coleta de dados secundários extraídos de fontes públicas já existentes.
7) Processamento, visualização e análise dos dados	Após a coleta, os dados devem ser processados e exibidos de forma clara. No processamento quantitativo, isso inclui a tabulação e a aplicação de estatísticas descritivas e inferenciais para quantificar tendências ao longo do tempo.	Tabulação em planilha eletrônica e geração de gráficos.
8) Reportar resultados da pesquisa	A redação do relatório de pesquisa é o passo final. O relatório deve apresentar os achados de forma clara e lógica, com base em evidências, incluindo recomendações práticas para solucionar o problema de pesquisa.	Envio de resultados das coletas e sugestões de mitigação aos órgãos em situação de vulnerabilidade; e composição desta dissertação.

1.4. ESTRUTURA DA DISSERTAÇÃO

Esta dissertação está estruturada em cinco capítulos, a partir desta introdução, organizados de modo a garantir uma progressão lógica desde a fundamentação teórica, passando por materiais e métodos utilizados, até chegar aos resultados e conclusões.

No **Capítulo 2**, discorre-se sobre os principais conceitos e o funcionamento das tecnologias envolvidas no problema pesquisado, de modo a fornecer a base conceitual necessária à compreensão das discussões e dos resultados desenvolvidos nos capítulos seguintes. Contém uma visão geral do protocolo SMTP, das extensões de segurança (SPF, DKIM e DMARC)

voltadas à mitigação de ataques de falsificação de endereços de e-mail, e dos fundamentos da engenharia social, das campanhas de *phishing* e dos mecanismos explorados para a falsificação, além de discutir trabalhos correlatos.

O **Capítulo 3** descreve os materiais e os métodos utilizados no trabalho. Em especial, detalha o desenvolvimento do instrumento para a coleta e análise automatizadas dos registros DNS, a periodicidade com que os dados foram coletados e as estratégias utilizadas para a notificação dos órgãos vulneráveis, com fins de mitigação.

No **Capítulo 4**, apresenta-se e discute-se os resultados da pesquisa, incluindo a análise do estado de vulnerabilidade dos órgãos da APF a ataques de *spoofing* de e-mail ao longo do período de monitoramento e da eficácia das ações de mitigação propostas.

O **Capítulo 5** apresenta, por fim, as conclusões gerais do trabalho, destacando suas contribuições, as limitações identificadas e as recomendações para trabalhos futuros.

2. FUNDAMENTAÇÃO TEÓRICA

O presente capítulo, destinado à fundamentação teórica, discorre sobre os principais conceitos e o funcionamento das tecnologias envolvidas no problema pesquisado, de modo a fornecer a base conceitual necessária para a compreensão das discussões desenvolvidas nos capítulos seguintes. Abarca-se uma visão geral sobre a arquitetura de correio eletrônico, o SMTP, o *Internet Message Format* (IMF), as extensões de segurança voltadas à proteção contra ataques de falsificação de endereços de e-mail, além dos fundamentos de engenharia social, campanhas de *phishing* e mecanismos explorados para *spoofing*. Por fim, discute-se trabalhos correlatos.

2.1. A ARQUITETURA DO CORREIO ELETRÔNICO

As mensagens de e-mail constituem a espinha dorsal da comunicação na maioria das organizações. Trata-se de um correio eletrônico baseado em arquivos de texto, mas que passou a também suportar áudios, vídeos, fotos e outros tipos de extensão (60, 61). A eficiência de custo e tempo é a principal razão pela qual muitas pessoas trocaram o correio tradicional pelo e-mail (61). Com o aumento do uso da tecnologia e da Internet, o número de e-mails enviados por dia continua crescendo notavelmente (62).

O e-mail (abreviação de *Electronic Mail*) é um sistema de mensagens que transmite comunicações eletrônicas através de redes de computadores (27, 63) e que se tornou um pilar da comunicação digital, um aplicativo crítico e a base da comunicação na Internet, constituindo uma parte essencial das comunicações diária, especialmente para conversas e transações confidenciais no ambiente corporativo (27, 55, 63, 64, 65, 66, 67, 68). O e-mail tem suas raízes tecnológicas na era pré-Internet, no início da década de 1980 (32). Com o desenvolvimento da Internet, grandes empresas em todo o mundo adotaram servidores de e-mail especializados para processar centralmente suas mensagens (31). O uso frequente desse canal e a importância das informações que ele transmite atraíram cibercriminosos (27). Devido à sua importância nos negócios, o e-mail exige alta segurança (60).

A *Request for Comments* (RFC) 5598, intitulada “*Internet Mail Architecture*”, publicada em julho de 2009, fornece um modelo de referência para compreender os componentes, os atores e as interações do serviço de correio eletrônico na Internet. Trata-se de documento informativo que não define novo protocolo, mas consolida trinta e cinco anos de evolução do serviço, distinguindo camadas lógicas, responsabilidades e identidades, de modo a permitir que diferentes atores utilizem linguagem comum. A arquitetura repousa especialmente sobre duas especificações que permanecem notavelmente estáveis apesar da evolução do serviço (69):

1. ***Simple Mail Transfer Protocol* (SMTP - RFC 5321)**: protocolo responsável pela transferência ponto a ponto de mensagens, transportando comandos de envelope e dados de conteúdo; e

2. **Internet Message Format (IMF - RFC 5322)**: que estabelece a estrutura formal da mensagem propriamente dita, distinguindo cabeçalhos e corpo.

A RFC 5598 classifica os participantes da arquitetura de correio eletrônico em três grandes categorias de atores, cada qual com responsabilidades distintas (69):

1. **Atores de Usuário**: são produtores e consumidores de mensagens. Podem ser pessoas, organizações ou processos automatizados. São quatro os tipos:
 - a. **Author (Autor)**: responsável por criar a mensagem, seu conteúdo e a lista de endereços de destinatários;
 - b. **Recipient (Destinatário)**: consumidor da mensagem entregue. Pode fechar o ciclo de comunicação gerando respostas ou notificações de disposição de mensagem (MDN), também conhecido como recibo de leitura;
 - c. **Return Handler (Controlador de Retorno)**: forma especial de destinatário encarregado de processar notificações geradas pelo *Message Handling System* (MHS) — falhas ou sucessos — enviadas ao endereço de retorno especificado pelo Originador; e
 - d. **Mediator (Mediador)**: recebe, agrega, reformula e redistribui mensagens entre autores e destinatários originais. Exemplos incluem listas de discussão, *aliases* e *gateways*. O Mediador é um ator de usuário pleno que origina nova mensagem, podendo modificar conteúdo ou regular quem participa da troca, embora preserve, na medida do possível, a informação do autor original.
2. **Atores de MHS (Message Handling System)**: realizam a transferência ponta a ponta, em nome do Autor, até os endereços especificados nos comandos RCPT TO originais. São eles:
 - a. **Originator (Originador)**: assegura que a mensagem esteja válida para postagem segundo normas da Internet e políticas locais do *Administrative Management Domain* (ADMD); submete-a ao *Relay*. Opera com “lealdade dupla”: serve ao Autor e representa o operador local do MHS. É responsável por tarefas administrativas pós-submissão, incluindo o envio de notificações de erro;
 - b. **Relay**: executa roteamento e *store-and-forward* no nível de MHS, adicionando informações de rastreamento (*trace*) sem alterar a semântica do envelope ou do conteúdo editorial;
 - c. **Gateway**: híbrido entre Usuário e Relay que conecta serviços de correio heterogêneos. Geralmente recebe mensagens de um *Message*

Transfer Agent (MTA) e as repassa a outro MTA, que pode estar em uma rede diferente ou mesmo em outra organização. O processo de transferência entre ambientes de correio distintos é complexo, pois envolve diversos formatos e protocolos. *Gateways* também podem ser usados para filtrar mensagens de entrada quanto a *spam*, *malware* e outros conteúdos indesejáveis (33); e

- d. **Receiver (Receptor)**: realiza a entrega final ou redireciona para um endereço alternativo; pode aplicar filtragem e políticas antes ou após a entrega.
3. **Atores Administrativos**: A operação independente de diferentes provedores motiva a noção de *Administrative Management Domain* (ADMD), isto é, um domínio administrativo de gerenciamento. Cada ADMD possui políticas próprias de confiabilidade, controle de acesso, responsabilização e avaliação de conteúdo. A RFC 5598 distingue três tipos básicos:
- a. **Edge**: serviços de transferência independentes nas bordas da Internet aberta;
 - b. **Consumer**: frequentemente um tipo de *Edge*, comum em provedores de webmail; e
 - c. **Transit**: provedores de serviços de correio que oferecem agregação, filtragem e valor agregado para *Edge*. A distinção entre *Transit* e *Edge* é relevante porque realça a necessidade de proteção e responsabilização nas fronteiras administrativas.

Além das três categorias de atores, três formas de identidade são utilizadas no correio eletrônico na Internet, todas devendo ser globalmente únicas (69):

1. **Mailbox (Endereço da Caixa de Correio)**: especificada por um endereço de correio eletrônico, por exemplo 'contato@exemplo.gov.br'. Uma *mailbox* é uma entidade conceitual que recebe correio e não necessariamente corresponde ao armazenamento de arquivos em disco. Normalmente, uma *mailbox* é composta por duas partes, sendo um nome de exibição opcional e um "addr-spec" entre colchetes angulares. O nome de exibição (*display-name*) é uma *string* que indica o nome do destinatário e pode ser exibido renderizado ao usuário em uma aplicação de correio. O "addr-spec" é o identificador específico que contém uma *string* localmente interpretada, seguida do caractere arroba ("@"), seguida de um domínio da Internet. A sintaxe completa de uma *mailbox* é, portanto: "Display-name <local-part@domain>".
2. **Message-ID**: *tag* de nível de usuário atribuída pelo Originador. Identifica de forma única uma versão específica da mensagem para fins de *threading*,

detecção de duplicatas e rastreamento. Revisões substanciais do conteúdo editorial devem gerar um novo Message-ID; e

3. **ENVID (*Envelope Identifier*)**: identificador de envelope utilizado para rastreamento de uma única postagem/entrega.

Complementarmente, os sistemas de e-mail são baseados em uma arquitetura cliente-servidor (32). A infraestrutura é composta por agentes de software que interagem no processo de envio e recebimento de mensagens (32, 67). A arquitetura define cinco tipos básicos de funcionalidade, alguns com subfunções especializadas (69):

- **Nível de Usuário:**

1. ***Message User Agent (MUA)***: representante do usuário no serviço de e-mail. Também chamado de Cliente de E-mail, é o sistema ou aplicativo (como Outlook, Thunderbird e Gmail) com o qual o usuário interage diretamente para compor, ler, redigir, enviar, receber e gerenciar mensagens eletrônicas (32, 33, 67, 68 70, 71, 72, 73). É a fonte inicial e o consumidor final das mensagens (68). Divide-se em:
 - a. ***Author MUA (aMUA)***: quando cria a mensagem, realiza a submissão inicial via *Mail Submission Agent (MSA)* e pode arquivar em *Message Store (aMS)*; e
 - b. ***Recipient MUA (rMUA)***: quando processa e exibe a mensagem recebida, gera MDNs e inicia respostas.
2. ***Message Store (MS)***: é onde o MUA utiliza armazenamento de mensagens de longo prazo, podendo estar localizado em um servidor remoto ou na mesma máquina que o MUA (73). É acessado via protocolos como *Post Office Protocol (POP)* ou *Internet Message Access Protocol (IMAP)*.

- **Nível de MHS:**

3. ***Mail Submission Agent (MSA)***: aceita a mensagem submetida pelo aMUA, aplica políticas do ADMD hospedeiro e requisitos das normas da Internet (73). É um programa de servidor que verifica a mensagem quanto a possíveis erros e, em seguida, a transfere, normalmente via SMTP, para o *Mail Transfer Agent (MTA)* de envio (32, 33). A submissão inicial é geralmente distinguida passando primeiro por um MSA, sendo que a porta 587 é geralmente usada para comunicação entre um MUA e um MSA (32, 72). Divide-se em:
 - a. **aMSA**: focado no Autor; e

- b. **hMSA**: focado no MHS.
4. **Message Transfer Agent (MTA)**: realiza um “salto” de retransmissão no nível de aplicação. É um componente de software que utiliza o SMTP para enviar, receber e retransmitir a mensagem entre sistemas e servidores, atuando como um “carteiro” na Internet (70, 73, 67, 68). O MTA funciona de forma semelhante a um roteador IP, pois sua função é tomar decisões de distribuição e mover a mensagem em direção ao destinatário (73). Um MTA recebe e-mails de outro MTA, de um MSA ou de um MUA. Quando a caixa de correio destinatária não é hospedada localmente, a mensagem é retransmitida, ou seja, encaminhada para outro MTA. Cada vez que um MTA recebe uma mensagem de e-mail, ele adiciona um campo “Received” no topo do cabeçalho da mensagem, criando um registro sequencial dos MTAs que a trataram (72), ou seja, adiciona *trace*, mas não altera endereços de envelope nem conteúdo editorial. Para encaminhar o e-mail ao seu destino final, o MTA de saída precisa localizar o *Mail Exchanger* (MX) *Resource Record* correspondente à zona DNS do domínio do destinatário e realizar outra consulta DNS para descobrir o endereço IP do servidor de destino. Em suma, é o responsável pelo processo de receber e-mails e entregá-los a outro MTA ou ao *Mail Delivery Agent* (MDA) (32). A porta 25 é geralmente usada para comunicação entre MTAs ou de um MSA para um MTA (72). Um MTA pode atuar como:
- a. **Boundary MTA**;
 - b. **Outbound MTA**;
 - c. **Inbound MTA**; ou
 - d. **Final MTA**.
5. **Mail Delivery Agent (MDA)**: efetua a transição de responsabilidade do MHS para o ambiente do Destinatário. É o componente de software responsável por entregar a mensagem de e-mail para a caixa de correio local do deste (32, 67, 70, 73). O MDA recebe e armazena a mensagem na caixa de entrada do usuário e realiza a entrega final do e-mail, filtrando e armazenando a mensagem (32, 72). Após a entrega final, o campo “Return-Path” (extraído de MAIL FROM) é adicionado ao envelope para registrar o caminho de retorno caso a mensagem seja respondida (72). O MDA pode aplicar redirecionamentos e políticas específicas do endereço de destino. Divide-se em:
- a. **hMDA**: orientado ao MHS; e
 - b. **rMDA**: orientado ao Destinatário.

O sistema de correio eletrônico utiliza uma arquitetura *store-and-forward*, o que permite que as mensagens sejam recebidas, retransmitidas, entregues e armazenadas em servidores em qualquer ponto do mundo sem exigir que todos os computadores ou usuários estejam online simultaneamente durante a comunicação (33). Do ponto de origem até a entrega, o correio eletrônico segue predominantemente modelo *push*: o ator que detém a mensagem inicia a transferência para o próximo ponto. Após a entrega, o rMUA ou rMS pode receber a mensagem por *push* ou recuperá-la por *pull* (69). Para tanto, o processo de transmissão utiliza dois protocolos: IMAP, para garantir que as mensagens recebidas sejam armazenadas no servidor; e POP, para auxiliar na localização das mensagens na máquina final do destinatário (33). Devido à sua incapacidade de enfileirar mensagens na porta de saída, o SMTP costuma ser combinado com o POP ou IMAP, que são usados nas comunicações entre MUA e MTA para o acesso e recuperação de e-mails armazenados em um servidor (32, 33, 58, 71, 74). Em suma (58, 67):

- **POP (Post Office Protocol)**: permite que os clientes baixem mensagens de um servidor de e-mail para o dispositivo local e normalmente remove as mensagens do servidor após o download; e
- **IMAP (Internet Message Access Protocol)**: permite acessar e-mails diretamente no servidor, mantendo-os sincronizados entre dispositivos.

A Figura 2.1 resume em um esquema ilustrativo a arquitetura técnica do fluxo percorrido por uma mensagem de e-mail. A transição (S) marca a transferência de responsabilidade da postagem do ambiente do Autor para o MHS e (D) do MHS para o ambiente do Destinatário.

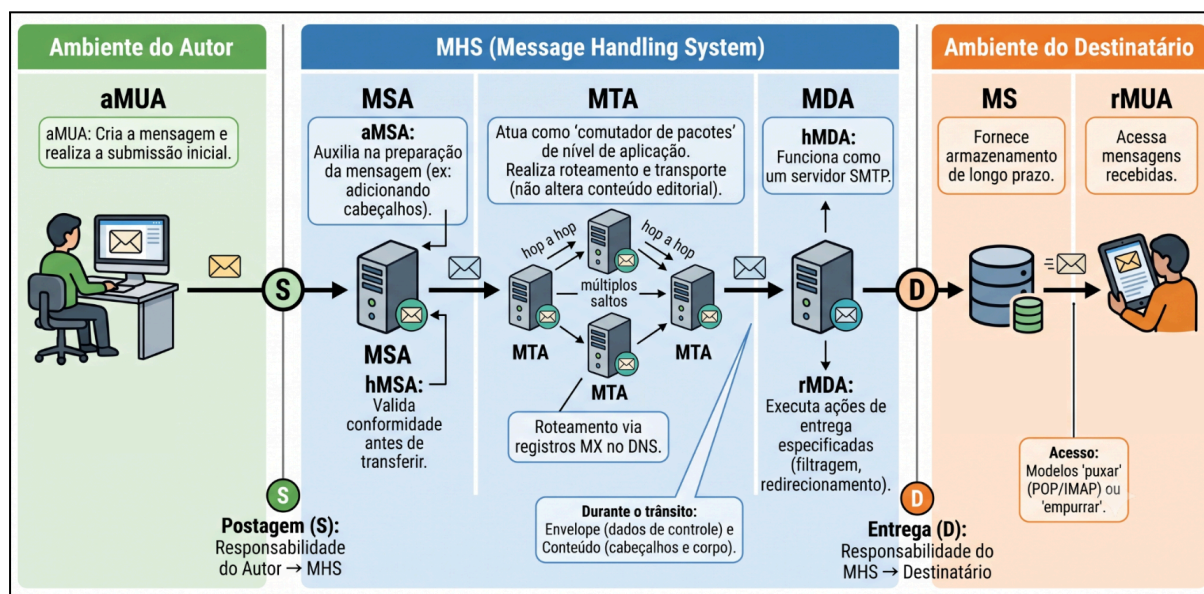


Figura 2.1. Esquema ilustrativo da arquitetura técnica do fluxo percorrido por uma mensagem de e-mail.

2.2. SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

O SMTP, definido na RFC 5321 em 2008, constitui a especificação fundamental para o transporte de correio eletrônico na Internet. A RFC 5321 consolida, atualiza e esclarece várias especificações anteriores, tornando obsoletas partes significativas das RFC 821, RFC 974, RFC 1869 e RFC 2821, além de atualizar a RFC 1123 no que se refere ao transporte de mensagens. O referido documento declara que o objetivo primordial do SMTP é transferir correio de forma confiável e eficiente, independentemente do subsistema de transmissão subjacente, exigindo apenas um canal de dados ordenado e confiável. Embora tenha sido projetado originalmente como protocolo de transporte e entrega, a especificação também fornece informações relevantes para seu uso como protocolo de submissão de mensagens (75).

Com isso, o SMTP tornou-se o protocolo padrão para a transmissão, envio, retransmissão e entrega de correio eletrônico entre dois *hosts* na Internet (1, 5, 32, 33, 54, 58, 62, 73, 76), fornecendo um mecanismo uniforme para trocar mensagens através de uma conexão TCP (5, 58). O protocolo funciona criando um canal de comunicação bidirecional entre o Cliente SMTP e o Servidor SMTP por meio do uso de servidores de e-mail (33, 62). O modelo SMTP pode ser de dois tipos: método ponto a ponto (*end-to-end*) para comunicação entre diferentes organizações ou método armazenar e encaminhar (*store-and-forward*) usado dentro de uma mesma organização (5). O SMTP usa, geralmente, a porta padrão 25 para comunicação entre MTAs (5, 32, 67). A porta 587 pode ser uma alternativa melhor, pois suporta criptografia TLS e é usada para comunicação entre MUA e MTA (5, 32).

O modelo arquitetural do SMTP é ilustrado pela Figura 2.2 por meio de um diagrama conceitual que demonstra a interação entre cliente e servidor (75).

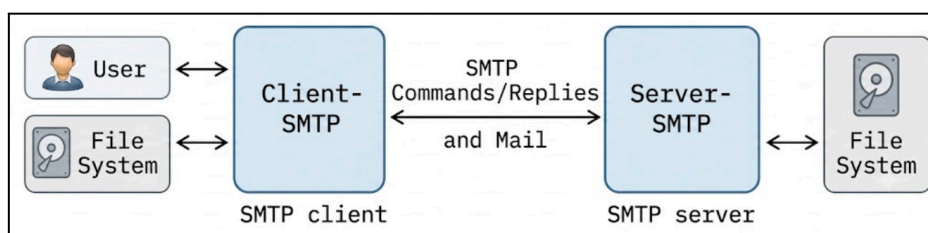


Figura 2.2. Diagrama conceitual do modelo arquitetural do SMTP

Fonte: Adaptado da RFC 5321 (75).

O Cliente SMTP é o ator responsável por iniciar a conexão e transferir mensagens de correio para um ou mais servidores SMTP, ou relatar falhas. O Cliente determina os domínios de destino — localmente ou via DNS — e estabelece um canal de transmissão bidirecional. Implementações totalmente capazes devem suportar enfileiramento, novas tentativas e funções de endereçamento alternativo. Por sua vez, o Servidor SMTP, recebe comandos do Cliente, responde com códigos de resposta e assume responsabilidade formal pela mensagem se emitir um código de sucesso ao final da transmissão dos dados. O protocolo exige que o servidor “DEVE” aceitar a responsabilidade pela entrega ou pelo relato adequado de falhas (75).

Um Servidor SMTP pode atuar como destino final, *relay* ou *gateway*. Um *relay*, como visto na seção anterior, é um servidor SMTP que recebe uma mensagem de um Cliente e a transmite — sem modificações substanciais no conteúdo, exceto adição de informações de rastreamento — para outro Servidor SMTP, para retransmissão ou entrega final. Historicamente, o transporte ocorria diretamente entre *hosts* conectados ao mesmo serviço de transporte; hoje, é comum o uso de servidores de submissão intermediários ou *relays* selecionados via registros MX do DNS. Em outras palavras, a transferência de mensagens pode ocorrer em uma única conexão entre o remetente SMTP original e o destinatário SMTP final, ou em uma série de saltos através de sistemas intermediários. Um *gateway*, como também mencionado anteriormente, diferencia-se dos *relays* por realizar transformações mais profundas na mensagem ao cruzar ambientes de transporte distintos (protocolos ou semânticas diferentes, por exemplo) (75).

O modelo de extensões, introduzido na década de 1990, permite que Cliente e Servidor negociem funcionalidades adicionais, mantendo compatibilidade com implementações legadas. O comando EHLO (*Extended HELLO*) substitui o HELO original e solicita a lista de extensões suportadas. Servidores contemporâneos devem suportar os mecanismos básicos de extensão, incluindo o comando EHLO, mesmo que não implementem extensões específicas. Clientes devem preferir EHLO ao HELO, embora o suporte ao HELO seja obrigatório para compatibilidade. A *Internet Assigned Numbers Authority* (IANA) mantém um registro oficial de extensões de serviço SMTP. Extensões podem alterar propriedades básicas do SMTP (limites mínimos, conjunto de caracteres ASCII etc.), desde que o texto das demais seções seja compreendido nesse contexto (75).

Comandos SMTP são *strings* de caracteres terminadas por <CRLF> (também conhecido como par de caracteres “carriage-return/line-feed”). Estes comandos são *case-insensitive*, exceto *local-part* do endereço da caixa de correio, que deve ser tratado como *case-sensitive*. Os argumentos terminam com <CRLF> e o receptor não age até receber a sequência completa. O conjunto central de comandos inclui EHLO/HELO, MAIL, RCPT, DATA, RSET, NOOP, QUIT, VRFY, EXPN, HELP e AUTH. Alguns destes comandos serão melhor explicados nas seções subsequentes. Toda resposta a um destes comandos consiste em um código de três dígitos seguido de texto (56, 63, 75):

1. O primeiro dígito indica severidade:
 - a. **2yz - Positive Completion:** sucesso; nova requisição pode ser iniciada;
 - b. **3yz - Positive Intermediate:** aceito, mas ação pendente de mais informação;
 - c. **4yz - Transient Negative:** falha temporária; cliente deve tentar novamente; ou
 - d. **5yz - Permanent Negative:** falha permanente; cliente não deve repetir exatamente o mesmo pedido.

2. O segundo dígito categoriza:

- a. **x0z**: sintaxe;
- b. **x1z**: informação;
- c. **x2z**: conexões; e
- d. **x5z**: sistema de correio.

3. O terceiro dígito refina o significado.

Um objeto de correio (*mail object*) é composto por envelope e conteúdo. O envelope é transmitido como unidades de protocolo SMTP (comandos MAIL, RCPT etc.) e inclui o endereço de origem (“reverse-path” ou “originator address”) e um ou mais endereços de destinatário (“forward-paths”). Já o conteúdo é enviado no comando DATA e compreende a seção de cabeçalhos (“header section”) e o corpo (“body”) da mensagem (75), que serão analisados na seção subsequente.

Uma sessão SMTP tem início quando o cliente abre uma conexão TCP e o servidor responde com uma mensagem de saudação (geralmente código 220). Implementações de servidor podem incluir identificação de software e versão após o código 220 para facilitar diagnóstico, mas também podem desabilitar essa informação por razões de segurança. O servidor pode rejeitar formalmente a sessão com 554 na saudação inicial, devendo aguardar QUIT antes de fechar a conexão e responder comandos intermediários com 503. Após a saudação, o cliente normalmente envia o comando EHLO para identificar-se e solicitar a lista de extensões. O comando EHLO confirma que ambas as partes estão no estado inicial (sem transação em andamento e *buffers* limpos). Na sequência, toda transação de correio segue três etapas obrigatórias e na seguinte ordem (31, 33, 58, 68, 75):

1. **MAIL FROM:<reverse-path> [SP <mail-parameters>] <CRLF>**

Este comando informa ao receptor SMTP que uma nova transação de correio está sendo iniciada e que ele deve resetar todas as suas tabelas de estado e *buffers*, incluindo quaisquer destinatários ou dados de correio. O “reverse-path” contém o *mailbox* de origem para relatórios de erro. Se aceito, o servidor retorna 250 OK. Falhas normalmente produzem 550 ou 553;

2. **RCPT TO:<forward-path> [SP <rcpt-parameters>] <CRLF>**

Especifica cada destinatário. O “forward-path” identifica o *recipient* (normalmente *mailbox@domain* entre < >). O servidor retorna 250 OK e armazena o caminho. Se o *recipient* não for entregável, retorna 550; e

3. **DATA <CRLF>**

Inicia a transferência do conteúdo da mensagem. O servidor responde 354 *Intermediate*. Todas as linhas subsequentes até o indicador de fim de dados são consideradas texto da mensagem. O fim é indicado por uma linha

contendo apenas um ponto (“.” ou “\r\n.\r\n”). Ao final bem-sucedido, o servidor processa os *recipients* e dados armazenados e retorna 250 OK. A transação só pode falhar em dois pontos: antes de MAIL FROM ou RCPT TO válidos (códigos 503 ou 554) ou após código 354 se incompleta, sem recursos ou por política de rejeição.

O último comando de uma sessão deve ser QUIT. O cliente deve usá-lo para solicitar o encerramento. O servidor responde 221 e fecha a conexão. QUIT pode ser emitido a qualquer momento e aborta uma transação incompleta (75).

Cumpre destacar, por ser de especial relevância para a compreensão do objeto desta pesquisa, que quando um servidor SMTP recebe uma mensagem para entrega ou processamento posterior, deve inserir informação de rastreamento (“time stamp” ou “Received”) no início do conteúdo da mensagem. A linha “Received” deve conter a cláusula “FROM” contendo o nome do *host* de origem conforme constante em EHLO, somado ao endereço de IP da conexão TCP. Além disso, o cabeçalho “Return-Path” é adicionado pelo MTA/MDA na entrega final, como já explicado na seção anterior. Uma vez identificado lexicalmente o domínio de destino, o cliente SMTP deve realizar consulta DNS para resolver o nome. Apenas FQDNs (*Fully-Qualified Domain Names*) resolvíveis (para MX, A ou AAAA, ou CNAMEs que resolvam para os anteriores) são permitidos em transações SMTP na Internet pública. Nomes locais, *aliases* não qualificados ou *nicknames* não devem ser usados. A consulta tenta primeiro localizar um registro MX. Sistemas SMTP não devem utilizar registros de endereço (A ou AAAA) a menos que estes sejam localizados via MX (75).

A própria RFC 5321 já reconhecia, em 2008, que o SMTP é inerentemente inseguro contra *spoofing* de endereço (75):

“É factível que usuários interajam diretamente com servidores receptores e relays e criem mensagens que enganem destinatários desatentos fazendo-os acreditar que vieram de outro endereço. Construir spoofing indetectável por especialistas é mais difícil, mas não o suficiente para deter atacantes determinados. A segurança real reside apenas em métodos end-to-end envolvendo o corpo da mensagem (assinaturas digitais, PGP, S/MIME). Autenticação em nível de transporte melhora a situação, mas geralmente autentica apenas um servidor para outro, não uma cadeia de relays nem usuários. Esforços para dificultar a alteração de campos From/return-path frustram aplicações legítimas.”

2.3. INTERNET MESSAGE FORMAT (IMF)

Para complementar a compreensão do problema do *spoofing*, faz-se também necessário dissecar a estrutura de uma mensagem de e-mail (77). A RFC 5322, publicada em outubro de 2008, especifica o “Formato de Mensagem da Internet” (*Internet Message Format* – IMF). Trata-se de uma sintaxe para mensagens de texto enviadas entre usuários de computador no âmbito do correio eletrônico. Esta especificação é uma revisão da RFC 2822, que por sua vez sucedeu a RFC 822, atualizando-a para refletir as práticas correntes e incorporando mudanças incrementais especificadas em outras RFCs (78).

Uma mensagem de correio eletrônico compreende envelope e conteúdo. O envelope existe nos comandos do protocolo de transferência (SMTP). O conteúdo, por sua vez, divide-se em cabeçalho e corpo (69). Este conteúdo é composto por linhas formadas por uma série de caracteres. Estas linhas são, cada uma, delimitadas pelo caractere “carriage-return” (CR) seguido imediatamente pelo caractere “line-feed” (LF). O par “carriage-return/line-feed” é usualmente escrito como “CRLF” (78). O cabeçalho é o registro completo da jornada de um e-mail até chegar ao seu destino e inclui informações de identificação, como remetente, destinatário, assunto, data, registros de *timestamp* e as rotas que o e-mail percorreu (63, 70, 79). O corpo contém o conteúdo da mensagem propriamente dito, isto é, o texto ou os dados a serem transmitidos ao destinatário (63).

A seção de cabeçalho carrega a maior parte da informação semântica, enquanto o corpo é uma sequência de linhas de texto que não são interpretadas para os propósitos da RFC 5322. A seção de cabeçalho é uma sequência de linhas de caracteres com sintaxe especial. Cada linha desta seção corresponde a um campo de cabeçalho. O corpo da mensagem é opcional e consiste simplesmente em uma sequência de caracteres que segue a seção de cabeçalho. A seção de cabeçalho e o corpo são separados por uma linha vazia, definida como “uma linha que não contém nada antes do CRLF” (78).

Cada campo de cabeçalho possui uma estrutura uniforme: nome do campo, dois-pontos (‘:’) e corpo do campo, terminado por CRLF. O nome do campo (*field name*) deve ser composto por caracteres US-ASCII imprimíveis, excluindo-se o caractere dois-pontos. O separador de dois-pontos é obrigatório e segue imediatamente o nome do campo, sem espaços entre eles. O corpo do campo (*field body*) pode ser composto por caracteres US-ASCII imprimíveis, espaço e tabulação horizontal, conhecidos coletivamente como caracteres de espaço em branco (78).

Campos de cabeçalho incluem (60, 63, 72, 78, 80, 81):

- **From:** endereço de e-mail do remetente (renderizado e visível ao destinatário como o remetente do e-mail);
- **Subject:** informações sobre o tema ou assunto da mensagem;
- **To:** endereço de e-mail do destinatário principal (visível ao destinatário);
- **Cc (Carbon Copy) e Bcc (Blind Carbon Copy):** incluem outros endereços de e-mail que receberão cópias da mensagem, sendo que os endereços Bcc não são visíveis aos demais destinatários;
- **Date:** mostra a data e hora em que o e-mail foi enviado;
- **Received:** contém informações sobre os servidores de e-mail pelos quais a mensagem passou durante a transmissão;

- **Return-Path:** depois que a mensagem é aceita e armazenada pelo servidor de destino, o endereço de envelope SMTP constante em “MAIL FROM” é gravado no cabeçalho como “Return-Path”. Indica o endereço da caixa postal de retorno caso a mensagem não seja entregue com sucesso (em um e-mail legítimo, normalmente coincide com o campo “From”);
- **Message-ID:** é o identificador único e global da mensagem eletrônica, gerado quando a mensagem é criada, sendo uma combinação de um número exclusivo com o nome de domínio do servidor remetente;
- **Reply-To:** contém o endereço de e-mail que deve ser usado caso o destinatário deseje responder à mensagem recebida;
- **Delivered-To:** contém o endereço de e-mail do destinatário pretendido;
- **X-Received:** indica que o e-mail foi recebido por um servidor SMTP oriundo de outro servidor;
- **Authentication-Results:** mostra o status de autenticidade do servidor de envio, com valores SPF, DKIM e DMARC indicando se o servidor é autêntico para usar o nome do domínio constante no campo “From”; e
- **MIME-Version, Content-Type, Content-Class, Content-Transfer-Encoding:** mostram a codificação do conteúdo para que a mensagem possa ser decodificada corretamente.

O cabeçalho é, portanto, um subconjunto do conteúdo da mensagem (53). Durante o processo de entrega, diferentes componentes da arquitetura adicionam ao cabeçalho detalhes que desempenham um papel essencial no registro da rota e na autenticação do remetente (79). Logo, como cada cabeçalho contém muitas informações e é processado em cada componente da infraestrutura do sistema de correio eletrônico, isso fornece uma pista vital sobre a originalidade da mensagem (72). Se um usuário não legítimo envia um e-mail forjado, alguns dos campos importantes do cabeçalho tendem a estar inconsistentes (81). Contudo, o código-fonte do cabeçalho é de visualização e análise mais complexas do que os campos que o usuário vê renderizados (77).

2.4. MECANISMOS DE AUTENTICAÇÃO DE REMETENTE

O sistema de e-mails atual, construído sobre o protocolo SMTP, foi inicialmente projetado sem considerar aspectos de segurança, pois na época de sua criação, a segurança não desempenhava um papel tão significativo (30, 64, 76, 82). O SMTP original era pouco mais que um mecanismo uniforme para transferir mensagens, não possuindo mecanismos para garantir autenticidade, integridade ou confidencialidade nas mensagens transmitidas (58, 64, 76). A insegurança original do SMTP permite que qualquer usuário envie um e-mail se

passando por outrem (62, 72). Esta é a principal brecha que atacantes exploram para enviar mensagens com endereços de e-mail forjados às vítimas (62). A falta de autenticação no SMTP facilita essa falsificação de e-mails (33, 62, 72).

Desta forma, os serviços de e-mail, por padrão, não são capazes de identificar e bloquear e-mails enganosos com nomes ou endereços de remetentes falsificados (66). A falsificação de remetente pode ser realizada de várias maneiras, sendo as principais: configurar um servidor SMTP próprio; enviar e-mail por meio de servidores de *relay* abertos (que não autenticam o domínio); e usar sites de *fake mailer*, que permitem modificar o campo “From” (60). Com um servidor SMTP operante, o *spoofing* de e-mail pode ser realizado com facilidade, permitindo que o atacante falsifique os campos “From”, “Reply-to” e “Return-Path”. Ao aproveitar brechas nos sistemas de segurança do protocolo, os atacantes conseguem criar mensagens falsificadas quase perfeitas, que parecem originar-se de fontes confiáveis (33).

Em resumo, os sistemas de e-mail dependem da combinação de diversos protocolos (SMTP, POP, IMAP), servidores (MTA, MSA, MDA), provedores e clientes (MUA) para garantir a entrega e o gerenciamento confiável das mensagens eletrônicas (67). Um invasor pode comprometer o SMTP para lançar um ataque de *spoofing* de e-mail; isso não é difícil (33). Os sistemas de e-mail enfrentam desafios significativos de segurança devido à essa facilidade, o que colabora com a ocorrência de *spam*, *phishing* e outras formas de fraude baseadas em e-mail 73. Por essa razão, o SMTP tem sido objeto de inúmeros estudos científicos, e boa parte deles se concentra em mecanismos de segurança para o protocolo (82).

O problema central é que, no processo de comunicação SMTP, as informações de identidade do remetente estão contidas em vários campos de forma complexa e é justamente a inconsistência entre esses campos que fornece a base para ataques de falsificação de e-mail. Os principais campos de identidade incluem (55):

- **Auth username:** o nome de usuário usado no comando AUTH para autenticar o Cliente no Servidor de origem;
- **MAIL FROM:** o remetente no envelope SMTP, usado principalmente para verificação de identidade durante a entrega do e-mail no servidor de destino;
- **From:** o remetente exibido no corpo do e-mail, mostrado ao usuário; e
- **Sender:** identifica o remetente real quando há vários endereços no campo “From”.

Devido a essa deficiência, o SMTP sofreu uma atualização em 1995 para abrir a possibilidade de aprimoramento do protocolo por meio de extensões. Essa versão é chamada de ESMTP (RFC 1869, substituída pelo RFC 5321). Um cliente indica seu suporte ao ESMTP emitindo o comando EHLO em vez de HELO no início da sessão. Se o servidor suportar ESMTP, ele responde com uma lista de extensões compatíveis (58), como já mencionado na seção 2.2. Tecnologias e extensões desenvolvidas ao longo dos anos para autenticação e segurança incluem (1, 30, 32, 64, 68, 71, 72, 73, 76, 83, 84):

- **STARTTLS**: protege mensagens contra interceptadores passivos, assegurando a criptografia entre os saltos individuais de servidores SMTP e autenticando servidores de destino;
- **PGP (Pretty Good Privacy) e S/MIME (Secure/Multipurpose Internet Mail Extensions)**: protocolos de autenticação em nível de usuário que fornecem criptografia e autenticação para mensagens individuais;
- **SenderID**: tecnologia de autenticação baseada em caminho que verifica o endereço IP de origem e examina vários campos relacionados ao remetente no cabeçalho;
- **DNSSEC**: assegura a integridade das respostas DNS. É um conjunto de especificações que fornece meios para autenticar registros DNS, garantindo que os registros TXT de SPF, DKIM e DMARC não tenham sido adulterados;
- **DANE-TLSA**: aproveita as garantias de segurança do DNSSEC para publicar uma descrição do certificado do MTA receptor, garantindo que o certificado apresentado corresponda a essa descrição;
- **MTA-STS (MTA Strict Transport Security)**: introduzido como alternativa ao DNSSEC, instrui o MTA de envio a buscar uma política de segurança via HTTPS;
- **Command Pipelining**: permite que os remetentes enviem múltiplos comandos em lote, eliminando a necessidade de esperar pelas respostas de código de status. Servidores que suportam *pipelining* incluem “PIPELINING” no código de status 250 ao responder ao comando “EHLO” do cliente;
- **SPF (Sender Policy Framework)**: permite que os domínios remetentes mantenham um registro TXT no DNS contendo a lista de endereços IP autorizados a enviar e-mails em nome de seus domínios;
- **DKIM (Domain Keys Identified Mail)**: utiliza uma assinatura criptográfica para garantir que o e-mail realmente se origina de uma fonte autorizada dentro do domínio e que seu conteúdo não foi adulterado;
- **DMARC (Domain-based Message Authentication, Reporting and Conformance)**: fornece uma estrutura de políticas para coordenar os resultados das verificações realizadas por SPF e DKIM e tomar decisões sobre e-mails falsificados ou suspeitos;
- **ARC (Authenticated Received Chain)**: construído sobre o DMARC, visa tratar o problema de falha de autenticação causado por modificações de encaminhadores de e-mail, permitindo que servidores receptores tomem

decisões com base nos resultados de autenticação de encaminhadores anteriores; e

- **BIMI (*Brand Indicators for Message Identification*)**: permite que proprietários de domínio exibam indicadores específicos de logomarca para mensagens autenticadas pelo DMARC.

Os sistemas de correio eletrônico dependem de algumas destas extensões de segurança para autenticar o remetente e decidir como lidar com e-mails suspeitos (56, 74), embora nem todos os provedores as suportem e configurações incorretas sejam comuns (64). A autenticação do remetente em uma troca de e-mails é fundamental para verificar se a mensagem realmente foi originada da fonte declarada (56). A autenticação no processo de transmissão de e-mails envolve quatro etapas importantes e está ilustrada na Figura 2.3 (53, 55):

1. **Autenticação no envio**: ao enviar um e-mail a partir do MUA via SMTP, o remetente precisa inserir seu nome de usuário e senha para autenticação. Nessa etapa, o MTA do remetente deve não apenas verificar a identidade do usuário, mas também garantir que MAIL FROM seja consistente com o “AUTH username”;
2. **Verificação no recebimento**: o MTA do destinatário recebe o e-mail e valida a autenticidade do remetente por meio dos protocolos SPF, DKIM e DMARC;
3. **Renderização da interface do usuário no cliente de e-mail**: fornece aos usuários uma exibição amigável do e-mail. Geralmente renderiza o remetente contido no campo “From” do cabeçalho. A maioria dos clientes de e-mail populares não apresenta os resultados da verificação de autenticidade ao usuário. Alguns formatos de codificação ou caracteres especiais podem induzir o destinatário ao erro, exibindo um endereço falsificado; e
4. **Verificação no encaminhamento de e-mails**: quando um servidor de encaminhamento reenvia automaticamente um e-mail, ele deve verificar o endereço do remetente.

Para maior compreensão da questão da falsificação de e-mails, é necessário explicar brevemente o processo de entrega e autenticação (56). Conforme exibido nas Figuras 2.4 e 2.5, Alice (alice@origem.com.br) envia e-mails legítimos para Bob (bob@destino.com.br). Elliot (atacante) quer enviar um e-mail para Bob se passando por Alice, usando seu respectivo servidor (malicioso.com.br). O MDA no servidor de Bob entrega dois e-mails com o mesmo endereço do remetente (alice@origem.com.br), mas vindos de endereços IP diferentes. Um e-mail é de Alice (originado do endereço IP 1.2.3.4) e o outro de Elliot (originado de 5.6.7.8). Um mecanismo antispoofting eficaz precisa diferenciar a mensagem de Elliot do e-mail legítimo de Alice (56).

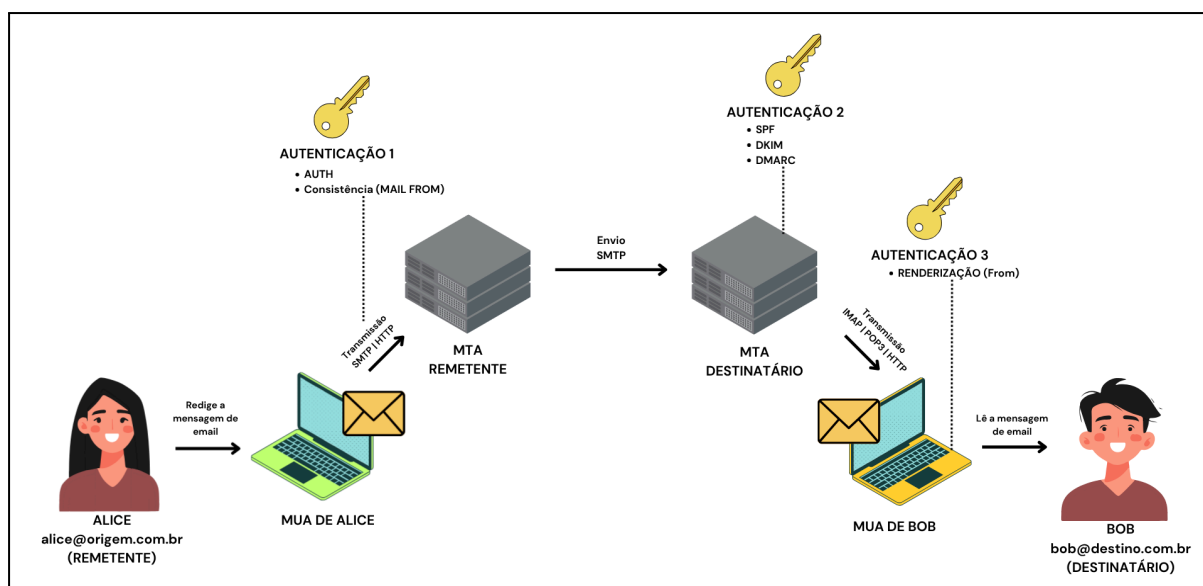


Figura 2.3. Visão geral do processo de envio de e-mails e das autenticações de remetente

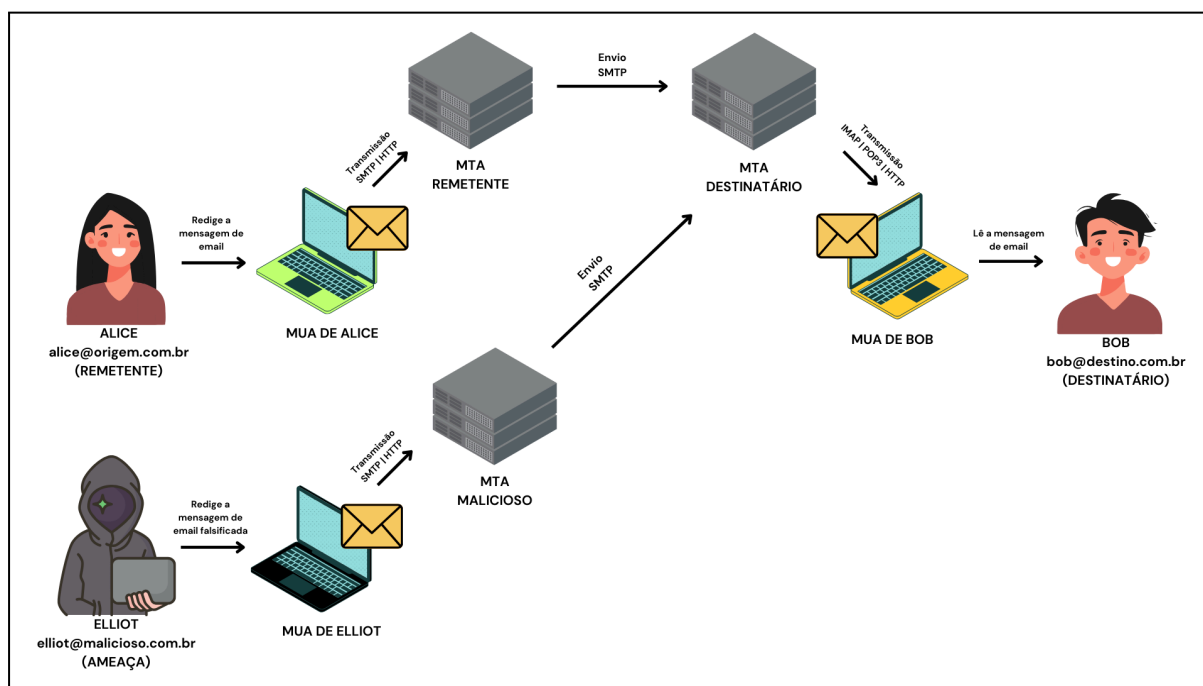


Figura 2.4. Visão geral da falsificação de remetente.

Desta forma, o cabeçalho do e-mail desempenha um papel significativo na avaliação da legitimidade de uma mensagem (31). Quando um servidor destinatário recebe um e-mail, ele pode detectá-lo como sendo genuíno ou falsificado (72). A autenticação de e-mails pode ser validada examinando assinaturas digitais, cabeçalhos de mensagem, registros DNS e outros mecanismos criptográficos (67). Em termos simples, a verificação questiona: o provedor que está enviando esta mensagem está autorizado a enviar e-mails em nome do remetente original (32)?

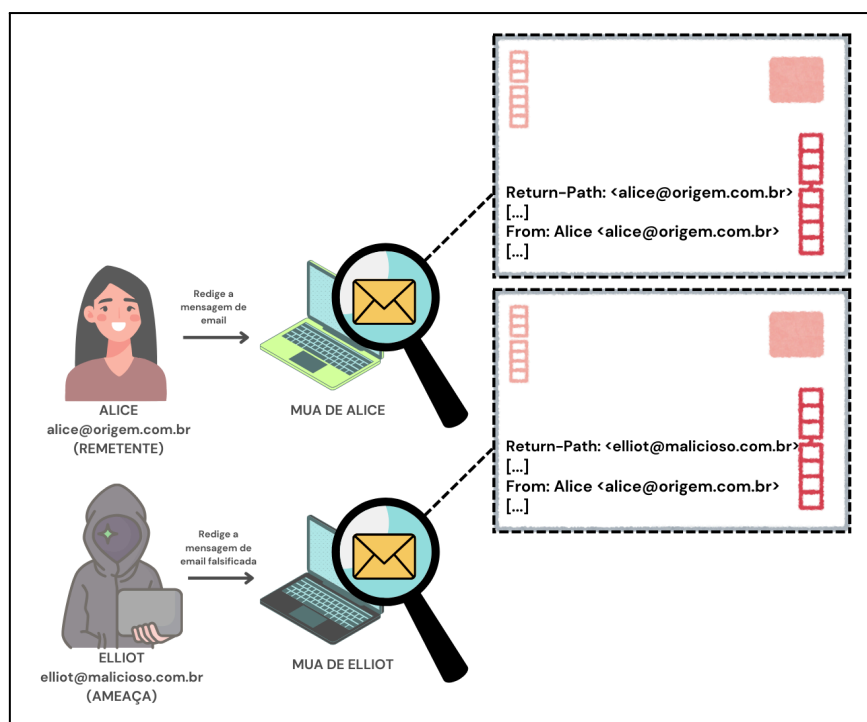


Figura 2.5. Esquema didático do resultado da falsificação.

Apesar das deficiências de segurança originais do SMTP, a introdução das extensões — mais crucialmente os protocolos de autenticação de domínio SPF, DKIM e DMARC — forneceram os mecanismos necessários para verificar a autenticidade do remetente e mitigar o *spoofing* (58, 64, 74). No entanto, a eficácia da segurança de e-mail depende da aplicação consistente dessas políticas por todas as partes envolvidas na complexa cadeia de autenticação de e-mail, pois a inconsistência entre esses elementos também pode criar ameaças à segurança (55).

A autenticidade de um e-mail depende do elo mais fraco da cadeia de autenticação (55). Qualquer falha nessa cadeia, que envolve múltiplos protocolos, funções e serviços, pode quebrar toda a defesa, resultando em danos sem precedentes (55). A escala das implicações de permitir que e-mails falsificados entrem na caixa de entrada, mesmo após terem passado por múltiplas camadas de segurança, é significativa e evidencia vulnerabilidades existentes quando apenas o SMTP é implementado sem camadas adicionais de segurança nos domínios (5).

2.4.1. Extensões SMTP: SPF, DKIM E DMARC

Como apontado na seção anterior, para combater o problema da falsificação de endereços de e-mail, o *Internet Engineering Task Force* (IETF) e a comunidade de correio eletrônico têm proposto e desenvolvido diversos protocolos e extensões ao longo dos anos (3, 30, 31, 53, 55, 57, 62, 73, 74, 76). Essas extensões definem um conjunto de regras que especificam quem tem permissão para enviar e-mails em nome de um domínio e fornecem estratégias para lidar com mensagens falsificadas (85). Os três protocolos principais — SPF, DKIM e DMARC —

se complementam, e a implementação conjunta deles oferece a melhor proteção contra o *spoofing* de e-mail (2, 67, 71).

O SPF é um protocolo de autenticação de domínio baseado em DNS que permite que os domínios emissores especifiquem quais *hosts* estão autorizados a usar o nome de domínio para as identidades constantes em HELO e MAIL FROM (33, 64). As identidades em HELO e MAIL FROM devem ser certificadas pelos registros SPF do domínio remetente para que os MTAs consigam distinguir entre mensagens originadas de fontes permitidas e não permitidas (33). Resumidamente, o SPF foi criado para limitar quais servidores estão autorizados a enviar e-mails em nome de um determinado domínio (86).

O DKIM adiciona uma assinatura criptográfica às mensagens para garantir sua integridade, sendo mais eficaz que o SPF por adotar uma abordagem mais abrangente (64, 86, 87). Com o DKIM, o administrador do domínio remetente publica uma chave criptográfica pública via DNS (64). Ao enviar um e-mail, o MTA originador assina cada mensagem com a chave privada correspondente, e o servidor de correio receptor consulta o DNS para recuperar a chave pública e validar o e-mail recebido (64).

O DMARC foi introduzido devido às falhas identificadas no SPF e no DKIM (64). O DMARC foi, desta forma, construído sobre a arquitetura dos dois protocolos precedentes, resultando em uma segurança superior (87, 88). Ele atua como uma camada adicional, definindo políticas de resposta a falhas de validação SPF e DKIM (impondo alinhamento entre os protocolos), e também gerando relatórios de autenticação, o que aumenta a resiliência contra a personificação de domínios (29, 86, 87). Aliadas a SPF e DKIM, as políticas DMARC permitem que as organizações eliminem quase que completamente o *spoofing* de e-mail (88).

Porém, ainda que a implementação cuidadosa dessas extensões possa mitigar completamente o problema de falsificação de domínios exatos (85), a segurança proposta depende predominantemente da iniciativa dos domínios e provedores em implementar as extensões SPF, DKIM e DMARC (5). O uso correto e rigoroso desses protocolos constitui a base mínima para garantir a autenticidade e integridade das mensagens (58). Para que sejam eficazes, tanto o proprietário do domínio quanto o MTA do destinatário devem implementá-las corretamente, definindo e verificando as regras estabelecidas (85, 89). É fundamental que as organizações adotem protocolos antispoofting para que os filtros sejam mais eficazes, sendo a tecnologia de autenticação de e-mails sempre a primeira linha de defesa (90, 91). Um exemplo de registro DNS contendo a implementação das extensões pode ser encontrado na Figura 2.6.

As organizações devem tomar a iniciativa de melhorar a configuração de SPF, DKIM e DMARC, independentemente de o domínio em si ter ou não a função de enviar e receber e-mails (89). No lado do destinatário, as verificações devem estar habilitadas, e os provedores devem processar a mensagem de acordo com os resultados da verificação retornados (89). Os usuários devem inspecionar o código-fonte do e-mail para verificar se a mensagem passou pelo crivo da autenticidade, antes de acreditar que ele é genuíno (62). Uma comparação entre

os cabeçalhos de uma mensagem genuína e de uma mensagem falsificada é feita na Figura 2.7.

☐ Type	Host	Value	TTL	
☐ A Record	*	185. 	Automatic	
☐ A Record	@	185. 	Automatic	
☐ A Record	www	185. 	Automatic	
☐ TXT Record	@	v=spf1 ip4:185.  -all	Automatic	
☐ TXT Record	_dmarc	v=DMARC1; p=reject; aspf=r; sp=reject	Automatic	
☐ TXT Record	dkim._domainkey	v=DKIM1;k=rsa;t=s;s=email;p=MIIBIjANBgkqhkiG9w0BAQEFA...	Automatic	

Figura 2.6. Registros DNS de um domínio incluindo SPF, DKIM e DMARC

Message headers

Return-Path: <meucorreios@correios.com.br>

X-Original-To: 

Delivered-To: 

Received: from mx1.correios.com.br (mx1.correios.com.br [201.48.198.27]) (using TLSv1.2 with cipher ECDHE-RSA-AES256-SHA384 (256/256 bits)) (No client certificate requested) by mailin047.protonmail.ch (Postfix) with ESMTPS id 4ThJKM4H19z3T for <>; Fri, 23 Feb 2024 18:23:03 +0000 (UTC)

Authentication-Results: mail.protonmail.ch; dmarc=none (p=none dis=none) header.from=correios.com.br

Authentication-Results: mail.protonmail.ch; spf=pass smtp.mailfrom=correios.com.br

Authentication-Results: mail.protonmail.ch; arc=none smtp.remote-ip=201.48.198.27

Authentication-Results: mail.protonmail.ch; dkim=none

Date: Fri, 23 Feb 2024 15:22:55 -0300

To: 

From: <meucorreios@correios.com.br>

Subject: Meu Correios

Message-Id: <rmF82dUrXlfJCDBXnmsyxN6ERTiWNIaLWMLhIhoQ@localhost.localdomain>

X-Mailer: PHPMailer 6.0.1 (https://github.com/PHPMailer/PHPMailer)

MIME-Version: 1.0

Message headers

Return-Path: <'.mom>

X-Original-To: 

Delivered-To: 

Received: from  (unknown [194.110. .70]) by mailin040.protonmail.ch (Postfix) with ESMTP id 4TgjPm2wBzz3q for <>; Thu, 22 Feb 2024 19:09:47 +0000 (UTC)

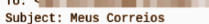
Authentication-Results: mail.protonmail.ch; dmarc=none (p=none dis=none) header.from=correios.com.br

Authentication-Results: mail.protonmail.ch; spf=pass smtp.mailfrom=.mom

Authentication-Results: mail.protonmail.ch; arc=none smtp.remote-ip=194.110. .70

Authentication-Results: mail.protonmail.ch; dkim=none

From: <meucorreios@correios.com.br>

To: <>

Subject: Meus Correios

Date: Thu, 22 Feb 2024 19:09:44 +0000

Content-Type: text/html

Mime-Version: 1.0

Message-Id: <1538085644648.096e3d4e-bc38-4027-b57e-0P2wXI@message-ids..mom>

Figura 2.7. Comparação de cabeçalhos de uma mensagem genuína (esquerda) e falsificada (direita)

Em suma, toda organização que dedica tempo para criar e manter políticas rígidas e eficazes de SPF, DKIM e DMARC contribui significativamente para a segurança de todos os usuários (80). Essa estratégia de combinação tem se mostrado eficiente, pois minimiza a complexidade de implementação para remetentes e destinatários, permitindo que apenas *e-mails* legítimos cheguem à caixa de entrada dos usuários (88). A seguir, pormenoriza-se o funcionamento técnico de cada uma das extensões, como seus resultados são exibidos e suas limitações.

(i) SPF

O *Sender Policy Framework* (SPF) é um padrão e um sistema de validação projetado para detectar e ajudar a prevenir *spoofing* de e-mails ao não permitir que terceiros enviem mensagens em nome de determinado domínio (5, 57, 72, 92), garantindo que apenas endereços IP autorizados originem correspondência em nome desse domínio (54, 73) e possibilitando a identificação de mensagens com endereço de remetente falsificado (65). O

protocolo foi proposto no início dos anos 2000, padronizado em 2014 e é considerado a primeira tentativa de impedir que atores maliciosos enviem e-mails a partir de domínios que não possuem (62, 53). Originalmente definido como protocolo experimental na RFC 4408, foi refinado pela RFC 7208, que especifica a versão 1 e estabelece o mecanismo pelo qual os ADMDs autorizam explicitamente quais *hosts* podem utilizar seus nomes de domínio nas identidades de envio, com base em registros TXT configurados no DNS do remetente (1, 67, 72, 76, 83, 93, 94).

A motivação trazida pela RFC 7208 menciona que os protocolos de correio não impõem restrição alguma sobre o que um *host* emissor pode declarar no comando MAIL FROM ou no domínio informado nos comandos HELO/EHLO, o que abre caminho para diversas formas de falsificação (94). O SPF responde a essa lacuna transferindo ao domínio publicante a responsabilidade pela autorização de uso de sua identidade e oferecendo aos receptores um meio verificável de conferi-la. Não substitui outros mecanismos de autenticação, como o DKIM e o DMARC, mas integra-se a eles, acrescentando uma camada de verificação no nível da infraestrutura de transporte (94).

O protocolo vincula o domínio e o endereço IP do remetente (55) e opera em duas etapas: o domínio remetente publica no DNS o registro SPF com os IPs autorizados; e o servidor do destinatário consulta esse registro para confirmar se o IP do remetente consta da lista (29). A verificação recai sobre o IP do MTA de envio, confrontado com o domínio declarado nos comandos HELO/EHLO ou MAIL FROM durante a transação SMTP (33, 58, 68, 82, 85). O servidor receptor extrai o nome de domínio do remetente a partir desses campos, solicita ao DNS o registro correspondente (89), compara o endereço IP de onde o e-mail realmente chegou com a lista de IPs autorizados (62) e decide se deve aceitar, rejeitar ou sinalizar a mensagem (67), entregando-a quando há correspondência e bloqueando-a ou direcionando-a à pasta de *spam* em caso contrário, conforme políticas predeterminadas (5). O SPF permite ainda que organizações, ao utilizarem o mecanismo “include”, deleguem parte ou toda a política a terceiros, comumente provedores em nuvem (76).

As organizações que desejam evitar a falsificação de e-mails de seus domínios devem criar um registro DNS que contenha as regras SPF, sendo este um registro TXT de um domínio de segundo nível (example.com) ou de um subdomínio (subdomain.example.com) (80). Todo registro começa com a *tag* “v=”, que identifica a versão do protocolo (atualmente v=spf1) (80, 85), seguida de uma ou mais regras conhecidas como mecanismos (80). Registros com múltiplas *strings* devem ser concatenados sem espaços adicionais e mantidos pequenos o bastante para que a resposta DNS caiba em 512 octetos UDP, idealmente abaixo de 450 octetos para compatibilidade com implementações antigas; o uso de *wildcards* é desencorajado e exige replicação cuidadosa dos subdomínios relevantes (94). Os mecanismos SPF mais comuns são (53, 56, 80, 85, 87, 94):

- **ip4 e ip6:** especificam um endereço ou um conjunto de endereços IPv4 (ou IPv6) a serem comparados pela função *check_host*, com suporte à notação CIDR;

- **a e mx**: instruem a função *check_host* a realizar primeiro uma consulta DNS para registros A (ou MX) e comparar os IPs retornados com o endereço IP do remetente;
- **include**: instrui a função *check_host* a incluir a regra SPF de outro domínio na avaliação, o que pode resultar em chamadas recursivas e permite autorizar *hosts* de domínios administrativamente independentes; e
- **all**: sempre corresponde, de modo que seu qualificador resulta na decisão final, sendo frequentemente usado com “-” (Fail) para rejeitar remetentes não autorizados.

Os mecanismos são precedidos por qualificadores que declaram como o receptor deve classificar os e-mails, sendo eles (53, 56, 80, 85, 87):

- **+ (Pass)**: aceitar;
- **- (Fail)**: rejeitar;
- **~ (SoftFail)**: suspeitar; e
- **? (Neutral)**: não tomar nenhuma ação.

Se um mecanismo resulta em correspondência, o valor do qualificador é utilizado (85), sendo o valor permissivo “+” (pass) o padrão quando nenhum é especificado (56, 80, 85). O SPF possui ainda os modificadores “redirect” e “exp”, que devem aparecer preferencialmente ao final do registro. O primeiro verifica as mensagens em relação à política de outro domínio, permitindo consolidar autorizações em um conjunto compartilhado dentro de um mesmo ADMD; o segundo retorna uma explicação personalizada, sujeita a expansão de macros, que pode acompanhar as respostas de rejeição SMTP para mensagens que falharem nas verificações (56, 80, 94).

As duas identidades sobre as quais o protocolo opera são definidas no próprio SMTP. A identidade HELO (ou EHLO) representa o *host* cliente que inicia a sessão, e a identidade MAIL FROM corresponde ao “reverse-path”, ou endereço de remetente do envelope (94). A RFC 7208 recomenda avaliar primeiro a identidade HELO/EHLO, cujos registros costumam referir-se a um único *host* e constituem fonte confiável de status de autorização; obtido resultado conclusivo nessa etapa, evita-se o processamento da identidade MAIL FROM, em geral mais complexo, com economia de consultas DNS. Quando o “reverse-path” é nulo, o SPF define a identidade MAIL FROM como o *mailbox* composto pelo “local-part” “*postmaster*” somado à identidade HELO (94).

A verificação é realizada pela função simbólica *check_host()*, cujo comportamento semântico deve ser reproduzido por qualquer implementação em conformidade com o padrão. Seus argumentos são o endereço IP do Cliente SMTP, o domínio que fornece as informações de autorização e a identidade completa MAIL FROM ou HELO (94). Se o domínio estiver

malformado ou se a consulta retornar NXDOMAIN, a função retorna imediatamente “none”. Consultado o registro TXT, descartam-se aqueles que não iniciem exatamente com “v=spf1”; a ausência de registro válido produz “none” e a existência de mais de um produz “permerror” (94). A avaliação dos termos ocorre da esquerda para a direita, com os mecanismos processados sequencialmente até que um corresponda ou ocorra exceção; os modificadores fornecem informações adicionais sem retornar correspondência direta (94).

A decisão sobre a mensagem é, com isso, feita pela função *check_host()*, que retorna um dos sete resultados possíveis (1, 56, 60, 62, 72, 80, 81, 85, 87, 94), que podem ser assim explicados:

- **pass**: o cliente está autorizado a enviar e-mails com a identidade fornecida. Se o endereço IP de onde o e-mail realmente chegou corresponder ao disposto no registro SPF, o e-mail é considerado autêntico e a verificação é aprovada;
- **fail**: o cliente é absolutamente não autorizado, podendo o software rejeitar o e-mail durante a própria transação SMTP com o código 550 5.7.1, preferencialmente acompanhado da explicação fornecida pelo domínio publicante;
- **softfail**: o domínio acredita que o *host* não é autorizado, mas não faz uma afirmação rígida, sendo tratado entre “fail” e “neutral”, exigindo análise mais rigorosa e podendo ser marcado como *spam* potencial, sem que a mensagem seja rejeitada apenas com base nesse resultado;
- **neutral**: o proprietário do domínio declarou explicitamente que não afirma se o endereço IP está autorizado, o que também ocorre quando nenhum mecanismo corresponde, devendo ser tratado de forma idêntica a “none” para fins de política local;
- **none**: não foi possível extrair um nome de domínio sintaticamente válido ou nenhum registro foi publicado pelo domínio remetente;
- **temperror**: erro transitório, geralmente de DNS, podendo o software aceitar temporariamente a mensagem ou rejeitá-la com o código 451 4.4.3; e
- **permerror**: o registro publicado pelo domínio não pode ser interpretado corretamente, o que exige intervenção do operador DNS e recomenda rejeição com o código 550 5.5.2. Pode decorrer de erros de sintaxe (caracteres ausentes ou uso incorreto de pontuação), da existência de múltiplos registros SPF, de falhas em consultas DNS ou da ultrapassagem do limite de dez consultas provocadas por mecanismos como “a”, “mx” e “include”.

Esses resultados não impõem tratamento normativo obrigatório. Cada receptor define sua política local a partir deles, ponderando o equilíbrio entre falsos positivos e falsos negativos (94). O limite de dez consultas mencionado acima integra um conjunto de restrições

destinadas a evitar carga excessiva sobre o DNS e ataques de negação de serviço. Para o mecanismo “mx”, cada registro consultado não pode gerar mais de dez consultas de endereço adicionais, com descarte dos registros excedentes. As implementações devem ainda limitar as *void lookups* — consultas que retornam resposta positiva com contagem zero ou NXDOMAIN — a no máximo duas, e permitir ao menos vinte segundos de avaliação, findos os quais o resultado deve ser “temperror” (94).

Para que agentes situados adiante na cadeia de entrega, como filtros internos e MUAs, possam avaliar a segurança aparente da mensagem, recomenda-se registrar o resultado da checagem de SPF no cabeçalho por meio de dois campos. O “Received-SPF” é um *trace field* que permite reconstruir a avaliação e inclui o resultado, um comentário explicativo e pares chave-valor padronizados, entre eles “client-ip”, “envelope-from”, “helo”, “mechanism”, “identity”, “receiver” e “problem”. Já o campo “Authentication-Results” destina-se a comunicar o resultado e os detalhes relevantes ao usuário final e será tratado mais minuciosamente adiante. Ambos podem ser empregados em conjunto, desde que as informações sejam consistentes (94).

A principal limitação do protocolo é que o SPF não autentica o cabeçalho “From” definido na RFC 5322, justamente o campo que é exibido ao usuário final pela maioria dos clientes de e-mail (5, 64). Como autoriza apenas as identidades HELO (comando) e MAIL FROM (envelope), nenhuma garantia é oferecida quanto às demais identidades do cabeçalho, de modo que um atacante pode obter resultado “pass” para seu próprio domínio e ainda assim falsificar o nome de exibição ou o endereço “From” apresentado ao destinatário (64, 90, 94). A RFC 7208 registra outras preocupações de segurança, entre elas o *spoofing* de dados de DNS e de IP, a falsificação entre usuários de um mesmo MTA, a exposição de privacidade decorrente de consultas DNS e os riscos de entregar mensagens com resultado “fail” à caixa de entrada, situação em que o receptor admite conteúdo explicitamente não autorizado pelo suposto remetente. Também os mediadores, como listas de discussão e serviços de reenvio, são afetados, pois costumam reescrever o MAIL FROM e provocar falhas de verificação (94).

No plano da implantação, as organizações devem criar registros SPF também para domínios e subdomínios alternativos, evitando que invasores se valham desses domínios secundários para enviar e-mails falsificados (80): um subdomínio sem registro publicado produzirá o resultado “none”, permitindo que a mensagem forjada seja recebida caso a segurança do destinatário não esteja adequadamente configurada (57). A RFC 7208 recomenda “v=spf1 -all” para domínios que não enviam correio e “v=spf1 a -all” para *hosts* individuais envolvidos no processamento de mensagens, além de sugerir a preferência por “ip4” e “ip6” em relação a “a” ou “mx” quando os endereços forem estáveis, de modo a reduzir consultas DNS. Determinações negativas definitivas dependem, aliás, da publicação de registros terminados em “-all” ou outros que redirecionem para registros que assim terminem, exigência que também recomenda transição cuidadosa na alteração de registros, para que o correio legítimo continue a ser aceito durante o período de propagação (94).

Como técnica de autenticação de e-mail, o SPF é uma medida eficaz para bloquear a entrega de mensagens de fontes não autorizadas ou duvidosas e, portanto, reduzir o volume de e-mails indesejados (32), desde que toda organização que opera um servidor legítimo configure seus servidores de recebimento para verificar os registros dos remetentes e mantenha registros DNS precisos de seu próprio domínio (58, 80). A RFC 7208 estabelece, assim, um protocolo maduro, com limites operacionais definidos e orientações detalhadas de implementação, implantação e tratamento de resultados, cuja contribuição para a redução da falsificação de e-mail depende de sua integração a uma estratégia mais ampla de autenticação de mensagens e a políticas locais (94).

A Figura 2.8 traz um fluxograma exemplificando a verificação feita pela extensão SPF a partir do estabelecimento de uma sessão SMTP com vias a entregar uma mensagem de e-mail.

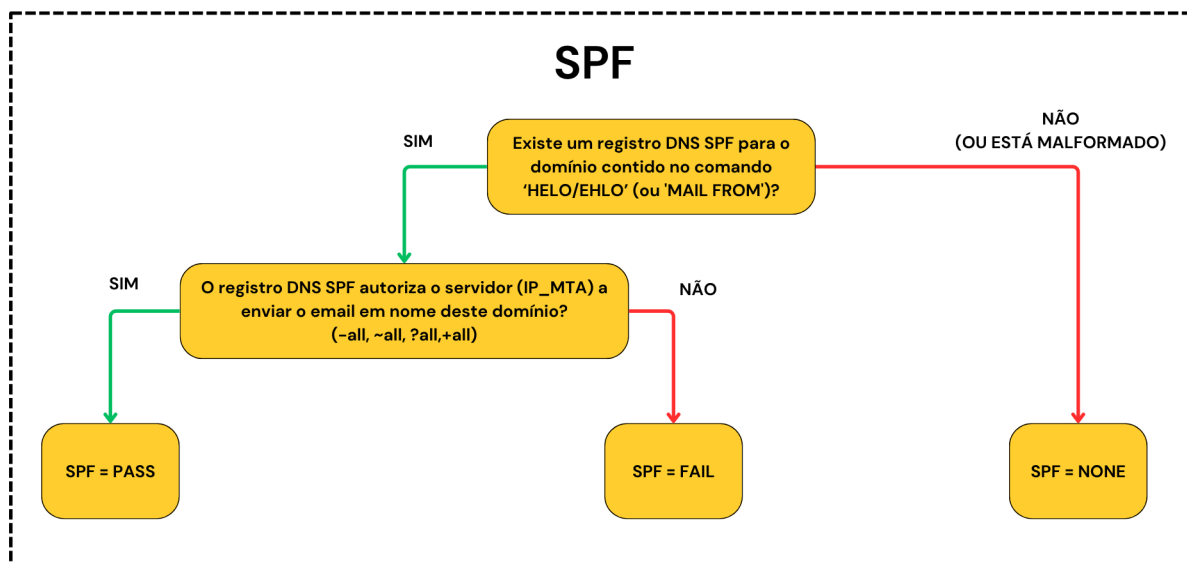


Figura 2.8. Fluxograma da verificação SPF

(ii) DKIM

O *DomainKeys Identified Mail* (DKIM) está contido tanto na RFC 5585 — publicada em julho de 2009 e que descreve a arquitetura e a funcionalidade do serviço — quanto na RFC 6376 — publicada em setembro de 2011, estabelecendo a especificação normativa das assinaturas e tornando obsoletas as RFCs 4871 e 5672. A primeira destas, editada originalmente em 2007, é ainda hoje a versão à qual boa parte da literatura sobre o protocolo remete, o que exige cautela ao se tomarem por vigentes afirmações que já foram superadas pela especificação de 2011 (62, 76, 80, 93).

Situado ao lado do SPF e do DMARC entre os protocolos voltados à contenção da falsificação de remetente, o DKIM distingue-se destes por recorrer a técnicas de criptografia de chave pública e privada para verificar a autenticidade e a integridade das mensagens (33,

72, 73, 84, 86, 92). Nesses termos, o protocolo assume responsabilidade por uma mensagem em trânsito e permite que o servidor receptor verifique se um endereço alegadamente pertencente a determinado domínio está de fato autorizado a enviar mensagens em seu nome (60, 62, 90), autenticando informações de remetente nos cabeçalhos e confirmando a integridade do corpo da mensagem (67, 80, 88). Destaca-se que o DKIM se destina a ser um método de comprovação de autenticidade, e não de fornecimento de prova criptográfica forte sobre autoria ou conteúdo, requisitos para os quais existem tecnologias como o OpenPGP e o S/MIME (95).

Uma pessoa — ou uma organização — possui uma identidade, que pode ser entendida como um conjunto de características que a distinguem de qualquer outra, e a essa abstração pode associar-se um identificador. O DKIM emprega um nome de domínio como identificador para referir-se à identidade de um responsável por uma mensagem de e-mail (96). A RFC 6376 formaliza esse identificador como o *Signing Domain Identifier* (SDID), um único nome de domínio que se refere à identidade que reivindica a responsabilidade pela mensagem ao assiná-la, domínio este transportado na *tag* “d=” do campo “DKIM-Signature” (95). O responsável pode ser a organização do autor, um *relay*, um intermediário no caminho de trânsito da mensagem ou um serviço independente que preste assistência a qualquer deles, e a escolha do SDID cabe a quem assina, pois é ele que estabelece a base para as avaliações posteriores. O proprietário do SDID declara aceitar responsabilidade pela mensagem e pode, por isso, ser responsabilizado por ela (96); é justamente essa declaração que fundamenta, do lado do servidor receptor, a verificação de que um endereço alegadamente vinculado ao domínio está de fato autorizado a assiná-lo, a partir de um usuário autenticado no domínio de origem (60, 62, 90).

A RFC 6376 nomeia três classes de atores relacionados ao DKIM (95):

- **Signatários:** elementos que assinam mensagens em nome de um domínio — MUAs, MSAs, MTAs e outros agentes, como distribuidores de listas —, todos de algum modo envolvidos na inserção da mensagem no sistema, sendo essencial que a mensagem seja assinada antes de deixar o ADMD do signatário;
- **Verificadores:** elementos que verificam assinaturas, o que pode ocorrer em MTAs, MDAs ou MUAs, esperando-se que estejam próximos do usuário final ou de algum outro agente consumidor; e
- **Avaliador de identidade:** elemento que consome a carga útil do protocolo, isto é, o SDID responsável, dedicando-se à avaliação do identificador entregue.

Do lado do signatário, o primeiro passo é determinar se a mensagem deve ser assinada e por quem, decisão que não se resume à posse da chave privada, havendo diversas outras razões pelas quais se pode optar por não assinar; quando a mensagem não pode ser assinada, seu destino é decisão de política local (95). Caso decida-se assinar a mensagem, o signatário

escolhe um SDID, realiza a assinatura digital sobre a mensagem e declara a informação de assinatura por meio de um campo de cabeçalho; o verificador obtém do mesmo campo o nome de domínio e um seletor, recupera a chave pública associada e verifica a assinatura (96).

Tecnicamente, a assinatura aplica-se ao corpo e a determinados campos de cabeçalho selecionados. Calcula-se um *hash* dos campos escolhidos e outro *hash* do corpo, e o signatário emprega a chave privada para codificar criptograficamente essa informação junto a outros parâmetros, depositando o resultado no campo de cabeçalho “DKIM-Signature”. Essa assinatura é criada pelo provedor do remetente com o propósito de convencer o provedor destinatário da autenticidade da mensagem e de protegê-la contra adulteração em trânsito (58). Essa descrição corresponde, na prática, a uma sequência que a literatura costuma detalhar de modo mais operacional (1, 29, 32, 53, 54, 55, 62, 80, 87, 97):

1. Gera-se inicialmente um par de chaves pública e privada para os usuários que enviam mensagens a partir do domínio;
2. A chave pública é então disponibilizada em um registro DNS do tipo TXT sob o repositório de chaves do domínio remetente, identificado pela combinação entre o seletor e o próprio domínio;
3. O servidor de envio calcula, a cada mensagem, os *hashes* criptográficos das partes submetidas à autenticação, isto é, do corpo e dos cabeçalhos selecionados; e
4. A mensagem é, por fim, assinada digitalmente com a chave privada correspondente, sendo o resultado inserido no cabeçalho sob o campo “DKIM-Signature”.

Como se pode depreender do supracitado, o SDID não basta para formular uma consulta ao registro DNS. Um mesmo domínio pode possuir múltiplas chaves e múltiplos signatários, e por isso o DKIM só identifica uma assinatura por intermédio da combinação do SDID com um seletor, especificado na *tag* “s=”. A semântica do seletor, se houver alguma, é estritamente reservada ao signatário e deve ser tratada como cadeia opaca pelas demais partes, pois, se os verificadores passassem a empregá-lo como parte de mecanismo de avaliação, não restaria mecanismo algum para realizar a transição de uma chave antiga, ou comprometida, para uma nova (96). Em suma, a vinculação com o DNS determina que todas as chaves sejam armazenadas em um subdomínio denominado “_domainkey”, formando-se a consulta pela concatenação do seletor, desse rótulo e do domínio, no formato “[seletor]_domainkey.[domínio]”; as cadeias de um registro TXT devem ser concatenadas sem espaçamento interveniente e os registros devem ser únicos para um dado seletor, pois a existência de múltiplos produz resultados indefinidos (95). Quanto à representação, o registro de chave segue a mesma sintaxe das *tags* empregada na assinatura:

- “v=”: indica a versão e deve ser a primeira *tag* do registro;

- “**h**”:
- “**k**”:
- “**n**”:
- “**p**”:
- “**s**”:
- “**t**”:

O campo “DKIM-Signature” — cuja Figura 2.9 é um exemplo —, que armazena a assinatura e todos os dados de obtenção de chave, deve ser tratado como um campo de rastreamento (*trace field*), não devendo ser reordenado e devendo ser inserido no início da mensagem. São obrigatórias sete *tags* (1, 53, 87):

- “**v**”:
- “**a**”:
- “**b**”:
- “**bh**”:
- “**d**”:
- “**h**”:
- “**s**”:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
    d=gmail.com; s=20230601; t=1735164116; x=1735768916; darn=;
    h=to:subject:message-id:date:from:mime-version:from:to:cc:subject
    :date:message-id:reply-to;
    bh=6vlfbb6m3qYLCNXM0D4DAiodD9G0dnSooICl/SWj/XU=;
    b=kjYeL97gfurKpftNB0IcPKdVeUaU92YUf267XikmeuHH9lpMIY7H1ThdKoxkiCT7pe
    YBMRB1fSRWr7S0r4DePSZ98tJNGVGCX4QMrUDbv+6vwiBJfQ5fx8iThGC2UNyOa4kM6u
    tqapYCw8WS6pSqZQa2aeWb7GMJTyH+g7i8bDunmSQo9r2jc6SEaNHJ/4wHgzk/wNByyY
    6t2IKWpk3AVupgd74z1nQoflbrbYvdCm3G5IdebnZBVZkrNX7WocPGxFyIbjV11rkaCl
    mGGqGxe5V/SjqP+XPg7KYbf1maJKyuiAr3t1TnyDceqLKxHXDyceuJsXSfFXVuGbUJP9
    VUvw==
```

Figura 2.9. Exemplo de cabeçalho DKIM-Signature

O campo “From” deve obrigatoriamente ser assinado, e não se devem assinar campos passíveis de modificação ou remoção legítima em trânsito, como o “Return-Path”. Três

estratégias são apresentadas: (a) assinar todos os campos existentes não repetíveis; (b) assinar apenas os campos que provavelmente serão exibidos ou afetarão o processamento; ou (c) assinar apenas os campos bem conhecidos — com a advertência de que verificadores podem tratar campos não assinados com extremo ceticismo, aconselhando-se ativamente assinar “Date”, “Subject”, “Reply-To”, “Sender” e os campos MIME. O propósito declarado dessas escolhas é afixar um identificador de modo simultaneamente robusto contra as alterações normais de trânsito e resistente a formas de ataque por reenvio, incluindo-se no *hash* os campos que constituem o núcleo do conteúdo — de sorte que qualquer reenvio precise mantê-los — e excluindo-se aqueles que ocorrem repetidamente ou são modificados em trânsito. Este ponto merece atenção acerca da literatura secundária sobre o protocolo: a afirmação, frequente, de que a inclusão do campo “From” na assinatura seria opcional (33, 80) correspondia à especificação anterior, não à RFC vigente, que a torna obrigatória e determina falha permanente na sua ausência.

Do lado do verificador, a especificação aconselha que a checagem ocorra em tempo hábil, sendo o momento mais oportuno durante a aceitação pelo MTA de borda ou logo em seguida, e desencoraja expressamente adiá-la até o acesso pelo usuário final, uma vez que o signatário pode remover ou revogar a chave a qualquer momento. A validação do campo “DKIM-Signature” deve ser meticulosa, qualquer inconsistência ou valor inesperado obriga a ignorá-lo por completo e a retornar falha permanente por erro de sintaxe (95). A omissão de qualquer *tag* obrigatória, a incompatibilidade de versão e a ausência do campo “From” conduzem igualmente a falha permanente. A obtenção da chave emprega o método da *tag* “q=”, o domínio da *tag* “d=” e o seletor da *tag* “s=” — o servidor receptor consulta, assim, o registro do domínio remetente sob o seletor indicado para obter a chave pública correspondente (5, 31, 54, 62, 64, 80, 87). Os resultados possíveis são:

- **Aprovação;**
- **Falha temporária:** devido a ausência de resposta; e
- **Falha permanente:** devido a inexistência do registro, registro malformado, algoritmo de *hash* não listado, chave revogada por dado vazio e chave inadequada aos tipos declarados.

A verificação propriamente dita consiste em (5, 31, 54, 62, 64, 80, 87):

1. Preparar a versão “canonizada” da mensagem, calcular os hashes e, antes de compará-los, conferir se o algoritmo indicado pela *tag* “a=” está entre os aceitos e se o prazo eventualmente informado pela *tag* “x=” não foi ultrapassado; e
2. Conferir o *hash* do corpo contra a *tag* “bh=” e verificar a assinatura da *tag* “b=” mediante a chave pública recuperada via DNS, sendo a divergência em qualquer etapa causa de falha.

Coincidindo os valores de *hash* e confirmando-se a assinatura, considera-se que a mensagem não foi modificada em trânsito e que efetivamente se origina do domínio alegado (62, 81, 97), o que corresponde à aprovação no teste do protocolo e garante, nessa medida, a integridade e a autenticidade da mensagem (5, 67, 73). Verificada a assinatura com sucesso, informação de reputação é empregada para avaliar o signatário e depois repassada ao sistema de filtragem.

A comunicação dos resultados pode ser feita como o verificador julgar adequado, sendo comum acrescentar um campo de cabeçalho antes de repassar a mensagem, para o que o campo “Authentication-Results” pode ser empregado; adverte-se que filtros de MUA devem confirmar que tal campo foi acrescentado pelo domínio verificador apropriado, de modo a não serem influenciados por campos falsos inseridos por atacantes. Quanto à política local, os módulos que consomem a saída do DKIM não devem determinar a aceitabilidade da mensagem apenas pela ausência de assinatura ou por assinatura não verificável, pois tal rejeição causaria problemas graves de interoperabilidade. Verificada a assinatura, se o SDID difere do endereço do campo “From”, o sistema deve empenhar-se para que o SDID efetivo fique claro ao leitor (95).

A Figura 2.10 traz um fluxograma exemplificando a verificação feita pela extensão DKIM.

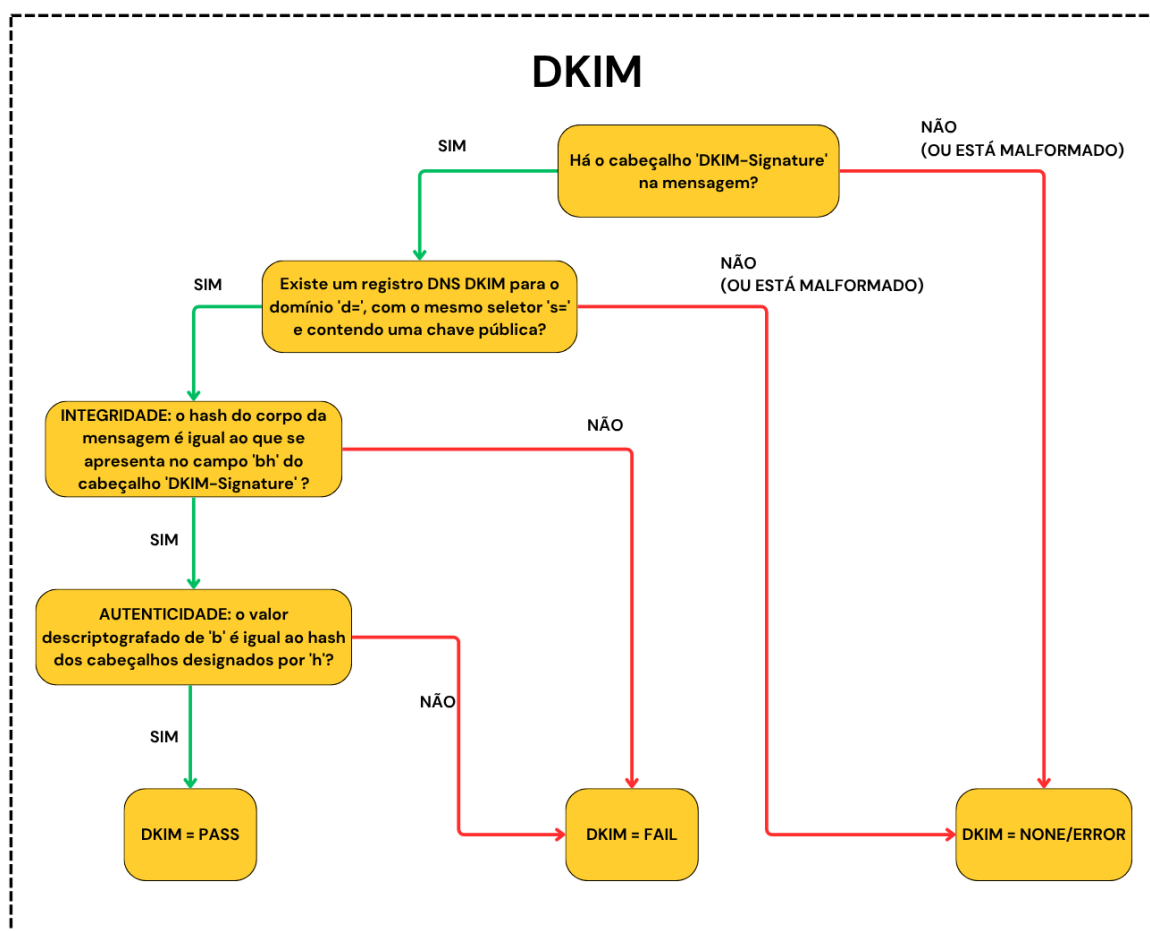


Figura 2.10. Fluxograma da verificação DKIM

Comparando-se DKIM e SPF, nota-se que os dois protocolos operam de forma independente e sobre partes distintas da mensagem. O SPF atua no envelope SMTP, verificando

HELO/EHLO ou MAIL FROM, ao passo que o DKIM atua sobre o conteúdo da mensagem propriamente dito (80). Dessa diferença decorre uma vantagem operacional ao DKIM. Por apoiar-se em uma autenticação criptográfica que viaja com a própria mensagem, e não em uma verificação amarrada ao endereço IP do último salto, o DKIM tende a resistir melhor ao encaminhamento de e-mails, permanecendo válido em cenários nos quais o SPF, dependente da origem de rede, falha (5, 55, 67). O DKIM depende, ademais, de um requisito elementar e recorrente na literatura, isto é, que as organizações efetivamente configurem seus servidores para gerar e verificar assinaturas válidas em cada mensagem e mantenham registros de chave precisos e atualizados no DNS, sem o que o protocolo, ainda que corretamente especificado, não produz o efeito de responsabilização a que se propõe (80).

(iii) DMARC

O *Domain-based Message Authentication, Reporting, and Conformance* (DMARC) foi rascunhado em 2011 e consolidado normativamente na RFC 7489, publicada em março de 2015 (53, 62, 73, 93, 98). Tratava-se, então, de submissão independente, de categoria informacional, que não integrava a trilha de padrões da Internet. Esse estatuto foi substancialmente alterado recentemente, em maio de 2026, quando a IETF publicou simultaneamente três documentos que tornam obsoleta a RFC 7489: a RFC 9989, que trata do núcleo do protocolo; a RFC 9990, dedicada aos relatórios agregados; e a RFC 9991, voltada aos relatórios de falha (99, 100, 101). A atualização não foi apenas de conteúdo, mas de posição hierárquica, uma vez que a RFC 9989 registra que a RFC 7489 não resultara de nenhum fluxo de trabalho da IETF, tendo sido publicada como informativa, ao passo que os três novos documentos integram o *Internet Standards Track*, representam o consenso da comunidade da IETF e foram aprovados pelo *Internet Engineering Steering Group*. Converteu-se, assim, um conjunto de práticas consolidadas por convergência de mercado em especificação normativa formal e com requisitos de conformidade expressos.

Cumprе esclarecer, entretanto, que o presente trabalho foi construído majoritariamente antes da publicação destas novas RFCs. Tanto o instrumento de pesquisa (que será apresentado na seção 3.1) quanto 15 das 18 coletas de registros DNS (descritas no item 3.3) foram desenvolvidos antes da publicação e, portanto, levaram em consideração as especificações outrora vigentes na RFC 7489.

Apesar da atualização mencionada, o diagnóstico que motiva o protocolo permanece essencialmente o mesmo nas duas gerações normativas, isto é, mensagens abusivas que empregam de modo não autorizado e enganoso um nome de domínio no campo de cabeçalho “From”, domínio que costuma pertencer à organização que o destinatário conhece e considera confiável. O SPF e o DKIM já ofereciam autenticação em nível de domínio e permitiam que receptores cooperativos detectassem mensagens autorizadas a usar determinado domínio, mas nenhum dos dois se vinculava diretamente ao domínio exibido no campo “From” — precisamente aquele que o usuário final observa —, e não havia mecanismo único,

amplamente aceito, para comunicar políticas de tratamento específicas de cada domínio nem para solicitar relatórios sobre autenticação e disposição das mensagens recebidas.

A literatura registra esse diagnóstico ao afirmar que o DMARC foi projetado para corrigir a brecha deixada pelo SPF e pelo DKIM, que permitia a circulação de mensagens com o “From” falsificado ainda que os testes de validação fossem aprovados (33, 53, 64, 71, 73, 80, 88). Além disso, originadores que haviam implementado autenticação tinham dificuldade em avaliar a eficácia de sua própria configuração, e o uso de falhas de autenticação como critério de filtragem tipicamente não prosperava; a solução que se desenhou ao longo do tempo foram acordos bilaterais entre remetentes e receptores, com meios privados de comunicar políticas e receber relatórios, os quais funcionavam mas exigiam coordenação manual significativa e não escalavam para uso geral na Internet (98, 99).

O DMARC alavanca esses dois protocolos preexistentes, ao permitir que o proprietário de um domínio publique, em registro TXT do DNS, as políticas de autenticação aplicáveis ao seu domínio (quanto autor) e solicite tratamento específico para as mensagens que falharem nas verificações — desenho descrito na literatura como protocolo interdependente (31, 33, 62, 74, 77, 87, 88), que opera em conjunto com SPF e DKIM para detectar o *spoofing* e oferecer ao servidor receptor um meio de agir quando a mensagem for considerada suspeita (62, 87).

O desenho básico pode ser descrito em quatro movimentos (98):

1. O proprietário do domínio publica asserções de política via DNS;
2. O receptor compara o endereço “From” com os resultados de SPF e DKIM, quando presentes, e com a política DMARC no DNS;
3. O receptor usa esses resultados para decidir como tratar a mensagem; e
4. O receptor envia relatórios ao proprietário do domínio ou a quem este designar.

É importante notar que o DMARC não produz nem estimula privilégio elevado de entrega para mensagens autenticadas; trata-se de mecanismo de distribuição de políticas que possibilita tratamento progressivamente mais rigoroso das mensagens que falham nas verificações, indo da inação à alteração da entrega e, no limite, à rejeição (98). Uma aprovação DMARC indica apenas que o uso do domínio de autoria naquela mensagem foi validado como autorizado pelo proprietário, e tal autorização não carrega qualquer asserção de valor, explícita ou implícita, sobre o conteúdo da mensagem ou sobre o próprio proprietário, de modo que uma aprovação, por si só, não garante que a entrega na caixa de entrada do destinatário seja segura ou desejável (99).

Em suma, os objetivos de alto nível do protocolo são (98, 99):

- Permitir que proprietários de domínio expressem o tratamento preferido para falhas de autenticação em mensagens que se apresentem como tendo autoria em seu domínio;
- Permitir que proprietários de domínio verifiquem sua própria implantação de autenticação;
- Minimizar a complexidade de implementação tanto para originadores quanto para receptores, bem como o impacto sobre o tratamento e a entrega de mensagens legítimas;
- Reduzir a quantidade de correio falsificado entregue com sucesso; e
- Operar em escala de Internet.

Esse último ponto é tratado como questão de primeira ordem para sistemas que necessitem operar em ambiente tão amplamente implantado quanto o correio SMTP, razão pela qual o protocolo procura evitar a necessidade de terceiros ou de acordos prévios entre remetentes e destinatários, preservando os aspectos positivos da infraestrutura vigente; embora não introduza remetentes terceirizados no fluxo de tratamento, tampouco os exclui, permanecendo tais terceiros livres para prestar serviços em conjunto com o protocolo (98, 99). É essa combinação de propósitos que sustenta a caracterização do DMARC como mecanismo escalável que reúne SPF e DKIM em uma solução mais completa de autenticação de e-mail (29, 32, 90).

Quanto ao *antiphishing*, o mecanismo foi desenhado para impedir que agentes maliciosos enviem correio que alegue provir de remetentes legítimos, particularmente de remetentes de correio transacional, cujo desvio mais comum é a indução do usuário a fornecer informações sensíveis mediante a simulação do serviço legítimo que as requisitaria (98, 99). Limitações, porém, são reconhecidas de imediato nas RFCs. O mecanismo só combate diretamente formas específicas de falsificação de domínio exato; e não pretende resolver todos os problemas relacionados a correio falsificado ou fraudulento, não tratando, em particular, do uso de nomes de domínio visualmente similares — os chamados domínios primos (ou *typosquatting*). Esse reconhecimento merece ser confrontado com a afirmação, recorrente na literatura, de que as políticas DMARC permitiriam às organizações eliminar completamente o *spoofing* de e-mail (88). A supressão é integral apenas no que diz respeito à falsificação do domínio exato. Também ficam fora do escopo do DMARC, ajudando a explicar por que o protocolo, ainda que corretamente implantado, não elimina categorias inteiras de fraude por correio eletrônico (98, 99):

- Tratamento diferenciado entre mensagens não autenticadas e mensagens que falham na autenticação;
- Avaliação de qualquer campo que não o “From”;
- Existência de múltiplos formatos de relatório;

- Publicação de política por meio distinto do DNS;
- Relatório ou a avaliação de endereço IP que não o do último salto (último MTA antes da entrega);
- Ataques ao campo “From” conhecidos como ataques de nome de exibição (ou de renderização);
- Autenticação de entidades que não sejam domínios, uma vez que o protocolo se constrói sobre SPF e DKIM, que autenticam apenas domínios; e
- Análise de conteúdo.

Passando a uma análise mais técnica do DMARC, os “identificadores autenticados” são definidos como identificadores em nível de domínio validados por tecnologia de autenticação suportada. O DKIM fornece identificador no conteúdo da *tag* “d=” do cabeçalho “DKIM-Signature” validado; o SPF pode autenticar tanto o domínio do comando HELO/EHLO quanto o do comando MAIL FROM, mas o DMARC utiliza exclusivamente o resultado da autenticação SPF da identidade MAIL FROM, remetendo à seção 2.4 da RFC 7208 para os casos em que esse comando apresenta caminho nulo, hipótese em que, como já mencionado anteriormente, a identidade é composta pela parte local “*postmaster*” somada à identidade HELO (98, 99).

O domínio de autoria é definido como o nome de domínio do autor aparente, extraído do campo “From”. Trata-se de campo obrigatório e, portanto, garantidamente presente em mensagens conformes, o qual a maioria dos agentes de usuário de correio exibe como originador da mensagem, renderizando seu conteúdo para o usuário final (98, 99). Por ser o campo que os usuários empregam para identificar a origem da mensagem, ele é alvo preferencial de exploração, e é dessa constatação que decorre a avaliação de que o DMARC é a primeira e única tecnologia amplamente implantada capaz de tornar confiável justamente o domínio que os usuários visualizam renderizado em seus clientes de correio (90).

O DMARC pressupõe o que se chama de necessidade de alinhamento, que decorre de uma constatação sobre o DKIM. Uma mensagem pode portar assinatura válida de qualquer domínio, inclusive de um domínio utilizado por agente malicioso, de modo que a mera presença de uma assinatura válida não permite inferir autenticidade do domínio do autor; não existe mecanismo pelo qual um proprietário possa declarar lista de domínios de terceiros autorizados a assinar em seu nome, de sorte que apenas um identificador autenticado por DKIM que esteja alinhado com o domínio de autoria pode validar seu uso autorizado (98, 99). Raciocínio simétrico aplica-se ao SPF, ou seja, qualquer proprietário, inclusive um agente malicioso, pode publicar registro SPF para seu próprio domínio e obter aprovação nessa verificação, o que torna o alinhamento igualmente necessário nesse caso.

Uma mensagem satisfaz as verificações do DMARC se ao menos um dos mecanismos de autenticação suportados (SPF ou DKIM) produzir resultado de aprovação com base em identificador alinhado; se ambas as tentativas falharem, o DMARC é considerado reprovado

(31, 33, 55, 65, 68, 88, 93). Esse desenho confere robustez a cenários como o do e-mail encaminhado, em que o SPF pode falhar enquanto o DKIM sobrevive ao encaminhamento, resultando ainda assim em aprovação (71).

O referido alinhamento entre domínios pode ser total ou parcial (56, 85, 93). Cada tecnologia subjacente pode operar em modo “estrito” ou “relaxado”, escolha expressa pelo proprietário nas *tags* “adkim” e “aspf”. No alinhamento relaxado, domínio de autoria e identificador autenticado devem compartilhar apenas o mesmo domínio organizacional (aprovando subdomínios); no estrito, devem ser idênticos (não incluindo, portanto, subdomínios). Para o DKIM, a RFC ilustra com o caso de assinatura validada com “d=example.com” e endereço “From” “alerts@news.example.com”, ou seja, os identificadores se alinham em modo relaxado, mas o teste falharia em modo estrito. Para o SPF, o exemplo equivalente é o de mensagem aprovada com “MAIL FROM” “cbg.bounces.example.com” e endereço “From” “payments@example.com”, que resultaria positivo apenas em modo relaxado (98, 99). A especificação vigente explicita que o proprietário pode optar por não submeter um dos mecanismos subjacentes à avaliação do DMARC — bastando não publicar registro SPF ou enviar mensagens sem assinatura DKIM —, embora se recomende que ambos sejam utilizados como base (98, 99).

O resultado da avaliação de alinhamento admite três estados. Se um ou ambos identificadores autenticados estiverem alinhados com o domínio de autoria, a mensagem é aprovada; se não existirem identificadores autenticados, ou se nenhum estiver alinhado, é reprovada; e se uma ou mais consultas de DNS necessárias à validação não se completarem por erro temporário ou permanente, a mensagem não pode ser considerada aprovada nem reprovada, não podendo a política ser aplicada e ficando as demais decisões a critério do receptor (99). Estes estados correspondem aos códigos de resultado registrados junto à IANA (98):

- **pass**: aprovação;
- **fail**: rejeição devido a existência de registro de política sem identificador alinhado;
- **none**: inexistência de registro para o domínio de autoria;
- **permerror**: erro irrecuperável, como registro sintaticamente incorreto; e
- **temperror**: erro provavelmente transitório, como indisponibilidade momentânea de servidor DNS.

À semelhança do SPF e do DKIM, o DMARC publica suas informações e políticas em registros DNS do tipo TXT (32, 54, 80) armazenados sob o rótulo “_dmarc”. O proprietário de “example.com”, por exemplo, publica as políticas em “_dmarc.example.com”, e o receptor que deseje consultá-las emite consulta TXT para esse mesmo nome (5, 54, 64, 80, 85, 98, 99). A escolha do DNS é justificada pela natureza paramétrica e simples da consulta e pelo reaproveitamento de infraestrutura de operação, administração e gerenciamento já consolidada. Como um registro TXT pode ser composto por vários objetos de cadeia de

caracteres, as RFCs determinam que o módulo de avaliação concatene essas cadeias na ordem em que aparecem, tratando o resultado como cadeia única.

Os registros seguem a sintaxe de *tag* e valor definida para registros de chave baseados em DNS no DKIM, e a IANA mantém um registro de *tags* conhecidas — apenas estas *tags*, ou aquelas incorporadas por extensões posteriores, devem ser processadas, devendo as desconhecidas serem ignoradas (5, 32, 53, 56, 80, 85, 89, 93, 98, 99). Essa regra permite acrescentar novas *tags* sem gerar nova versão do protocolo, ao passo que a alteração de *tags* existentes exige mudança de versão; erros de sintaxe no restante do registro devem levar ao descarte em favor de valores padrão, quando existentes, ou ao descarte puro e simples. São *tags* DMARC consolidadas tanto pela RFC 7489 quanto pela nova RFC 9989:

- **v:** identifica a versão, é obrigatória, deve ser a primeira da lista e admite exclusivamente o valor “DMARC1”, sensível a maiúsculas e minúsculas; ausência ou valor diverso implica o descarte de todo o registro;
- **p:** expressa a política de avaliação do proprietário do domínio, aplicando-se ao domínio consultado e a seus subdomínios salvo política de subdomínio (“sp”) explícita; seus três valores possuem significados distintos:
 - **none:** o proprietário não requer ação específica quanto à entrega, correspondendo ao modo de monitoramento. Permanecer neste modo pode representar risco de segurança elevado, ao levar o receptor a aceitar e-mails falsificados;
 - **quarantine:** o proprietário deseja que as mensagens suspeitas sejam tratadas com cautela adicional, admitindo que possam ser válidas ainda que a falha suscite preocupação; e
 - **reject:** toda falha é considerada indicação clara de uso inválido do domínio, sendo a rejeição preferencialmente feita durante a própria transação SMTP.
- **sp:** define a política aplicável aos subdomínios (apenas aos existentes) do domínio organizacional, com sintaxe idêntica à de “p”. Na ausência de “sp” e de “np”, a política de “p” aplica-se aos subdomínios. A *tag* “sp” é ignorada quando publicada em registros DNS de um subdomínios;
- **adkim e aspf:** indicam, respectivamente, se o proprietário exige modo estrito ou relaxado de alinhamento para DKIM e SPF, admitindo os valores “r” (relaxado) e “s” (estrito), sendo “r” o padrão em ambas;
- **rua:** indica os endereços para os quais os relatórios agregados devem ser enviados;
- **ruf:** indica os endereços para relatórios de falha específicos por mensagem;

- **fo**: reúne as opções de geração de relatórios de falha, é opcional, tem valor padrão “0” e admite lista separada por dois-pontos, com exclusividade mútua entre “0” e “1”. Seu conteúdo é ignorado se “ruf” não estiver também especificada, e os geradores de relatório podem aderir ou não às opções solicitadas:
 - **0**: solicita relatório quando todos os mecanismos subjacentes deixam de produzir resultado alinhado de aprovação;
 - **1**: solicita relatório quando quando qualquer um dos mecanismos subjacentes deixam de produzir resultado alinhado de aprovação;
 - **d**: solicita relatório de falha de DKIM quando a mensagem porta assinatura reprovada, independentemente de alinhamento; e
 - **s**: solicita relatório de falha de SPF quando a mensagem falhou nessa avaliação, também independentemente de alinhamento.

Três *tags* são inteiramente novas na RFC 9989 (99):

- **np**: estabelece a política de avaliação para subdomínios inexistentes, na sua ausência, aplica-se “sp” — quando presente — ou “p”;
- **psd**: sinaliza se o domínio é de sufixo público, admitindo:
 - **y**: incluída por operadores de sufixo público para indicar essa condição, informação usada na determinação do domínio organizacional e da política;
 - **n**: indica registro publicado para domínio que não é sufixo público mas é organizacional para si e seus subdomínios; e
 - **u**: indica indefinição, cabendo ao mecanismo de descoberta decidir.
- **t**: define o modo de teste:
 - **n**: sinaliza se as políticas declaradas em “p”, “sp” e “np” devem ser efetivamente aplicadas, sem afetar a geração de relatórios nem qualquer política de valor “none”; e
 - **y**: solicita que não sejam aplicadas as políticas propriamente ditas, mas eventuais regras de tratamento especial do receptor, como reescrita de “From”, esperando o proprietário que a política aplicada seja um nível abaixo da declarada, ou seja, quarentena comportando-se como “none” e rejeição como quarentena.

Três *tags* que constavam da RFC 7489 (98) foram removidas na especificação vigente (99) e mantidas no registro da IANA apenas com estatuto histórico:

- **pct**: que solicitava a aplicação da política a determinado percentual das mensagens;
- **rf**: que especificava o formato dos relatórios de falha; e
- **ri**: que especificava o intervalo de tempo entre relatórios agregados.

A justificativa para a remoção de “pct” é que a *tag* admitia todos os inteiros de 0 a 100, com a intenção de permitir migração gradual de “none” para “quarantine” ou de “quarantine” para “reject”, mas a experiência operacional demonstrou que raramente era aplicada de forma acurada, salvo nos valores extremos; o valor padrão, “100”, era de fácil implementação, enquanto o valor “0” assumiu significado não pretendido, sendo empregado por intermediários e provedores de caixas postais como sinalização para desviar do tratamento padrão, usualmente reescrevendo o “From” para evitar falhas a jusante — uso que permitia aos proprietários, ao comparar relatórios anteriores e posteriores à mudança, inferir quanto de seu tráfego transitava por intermediários que não reescreviam aquele campo, informação útil à decisão sobre migrar do monitoramento para a imposição. Não fazendo sentido manter uma *tag* com apenas dois valores efetivamente empregados, optou-se por preservar essa funcionalidade introduzindo a *tag* “t”, cujos valores “y” e “n” são análogos, respectivamente, aos antigos valores 0 e 100 de “pct” (99).

Movendo a análise do protocolo para a óptica do receptor, o domínio presente no campo “From” é extraído como o domínio a ser avaliado. Para ser processada, a mensagem precisa conter exatamente um domínio no “From”; mensagens com múltiplos campos “From” ou sem qualquer campo “From” são rejeitadas por vedação da própria RFC 5322, e mensagens cujo “From” contenha domínios com sintaxe incorreta são ignoradas. Quando um único campo “From” apresenta sintaticamente múltiplos valores válidos, o procedimento consiste em aplicar a verificação a cada domínio encontrado e adotar a política mais restritiva entre as que falharem (98, 99).

A RFC 9989 estabelece as ações que o receptor deve executar para chegar a uma política aplicável a uma mensagem individual, esclarecendo que as etapas de verificação de DKIM, SPF e de descoberta da política DMARC podem ser realizadas em paralelo, enquanto as etapas de alinhamento e de aplicação da referida política dependem das anteriores. Em suma, o processo pode ser sintetizado da seguinte maneira (3, 62, 98, 99):

1. Extrai-se o domínio do campo “From”;
2. Consulta-se o DNS deste domínio em busca do registro de política DMARC, prosseguindo apenas se algum for encontrado;
3. Realizam-se as verificações de DKIM, cujos resultados devem obrigatoriamente incluir o valor de “d=” de cada assinatura examinada;

4. Realizam-se as verificações de SPF, cujos resultados devem incluir o domínio empregado (geralmente o contido em “Return-Path”);
5. Conduzem-se as verificações de alinhamento, considerando-se aprovada a mensagem com um ou mais identificadores alinhados; e
6. Aplica-se, por fim, a política definida pelo proprietário do domínio.

Vale mencionar que havendo erro temporário em um ou ambos os mecanismos sem que nenhum aprove, o receptor não pode concluir falha permanente nem aplicar a política, embora possa reportar o erro quando apropriado — o tratamento de erro permanente de DNS permanece à discricionariedade do receptor.

Quanto à disposição das mensagens, o tratamento final de qualquer mensagem é sempre matéria de política local do servidor destinatário, e o receptor pode optar por rejeitar ou colocar em quarentena uma mensagem mesmo que ela seja aprovada na verificação, uma vez que o mecanismo não informa se um fluxo de mensagens é bom, apenas se ele é atribuível a um domínio — sendo os receptores encorajados a manter tecnologias antiabuso para enfrentar campanhas que utilizem domínios com DMARC corretamente configurado. Quando o receptor decide não honrar a política publicada, recomenda-se, no mínimo, a inserção do cabeçalho “Authentication-Results” (que será discutido na próxima seção), e que a ocorrência e a razão do desvio sejam comunicadas ao proprietário por meio do recurso de sobreposição de política dos relatórios agregados (98, 99).

A produção destes relatórios é um componente estruturante do protocolo e visa oferecer aos proprietários visibilidade sobre como os receptores implementam e impõem o mecanismo. A adoção da geração de relatórios é apontada como condição crítica para estabelecer e manter implantações precisas de autenticação, pois é quando os proprietários enxergam o efeito de suas políticas (98, 100). Vale registrar, contudo, que a RFC 9989 é explícita quanto à natureza não obrigatória dessa colaboração do lado do receptor. A organização receptora não tem obrigação de enviar os relatórios solicitados, embora se recomende que envie ao menos os relatórios agregados (99) — nuance que reforça o caráter deliberadamente permissivo do desenho do protocolo mesmo após sua recente elevação ao status de padrão formal da Internet.

Os receptores reportam nos relatórios agregados apenas as ações de rejeição ou quarentena decorrentes da política DMARC, e não as decorrentes de política local, pois a exposição de informações sobre políticas locais permitiria a adversários obter subsídios sobre a eficácia de suas campanhas. Os relatórios agregados são desenhados para oferecer visão precisa sobre resultados de autenticação, sobre ações corretivas necessárias e sobre o efeito da política nos fluxos processados pelos receptores. A justificativa é de ordem decisória: quando os proprietários sabem quais mensagens legítimas estão enviando, quais resultados de autenticação essas mensagens obtêm e quais mensagens forjadas os receptores estão recebendo, podem decidir melhor sobre as políticas necessárias e os passos para habilitá-las; e quando as políticas são bem definidas e seus efeitos compreendidos, os receptores podem

agir sobre elas com maior confiança (98, 100). É essa a via pela qual os administradores identificam maneiras de melhorar a autenticidade de suas mensagens, aprimorar as configurações de SPF e DKIM e coibir os e-mails falsificados que abusam de seus domínios (87).

O conteúdo de um relatório agregado inclui: a política descoberta e aplicada, quando houver; a disposição realizada; o identificador avaliado por SPF e por DKIM e os respectivos resultados; indicação de alinhamento para ambos os mecanismos; dados de cada subdomínio separados dos do domínio organizacional, mesmo sem política explícita de subdomínio; os domínios remetente e receptor; a política solicitada e a efetivamente aplicada, quando distintas; o número de autenticações bem-sucedidas; e a contagem de mensagens computada sobre todas as recebidas, ainda que sua entrega venha a ser bloqueada por outros agentes de filtragem (98, 100).

Complementarmente, os relatórios de falha, também designados relatórios forenses, cumprem propósito duplo, isto é, de um lado, auxiliam o proprietário a determinar a causa de falhas que aparecem apenas de forma estatística nos relatórios agregados; de outro, permitem identificar e enfrentar rapidamente mensagens que envolvam abuso direto do domínio. A primeira finalidade é diagnóstica e volta-se ao remetente legítimo; a segunda é investigativa e volta-se ao adversário — distinção que separa um problema de configuração de um incidente e que confere valor operacional ao mecanismo (98, 101). São normalmente gerados e enviados quase imediatamente após a detecção da falha, ao contrário do ciclo dos relatórios agregados, e oferecem maior granularidade sobre a mensagem específica. Recomenda-se que incluam a maior quantidade possível de campos de cabeçalho e de corpo da mensagem problemática, de forma compatível com as políticas de privacidade da parte relatora (101).

A avaliação conjunta da literatura e das RFCs permite concluir, antes de tudo, que o DMARC é uma camada de decisão, não de autenticação, limitando-se a exigir que a prova produzida por SPF ou DKIM se refira ao domínio que o usuário efetivamente vê — ou seja o campo “From” — e a instruir o receptor sobre como reagir quando as informações desses protocolos não coincidem ou não estão alinhadas com o “From” (29, 82). A elevação ao *Standards Track* em 2026 não altera essa natureza; antes a formaliza, ao articular com maior precisão os mesmos mecanismos preexistentes, ao reforçar o vínculo entre autenticação e identificador efetivamente exibido ao usuário e ao instituir com maior rigor um canal de retroalimentação que permite ao proprietário do domínio conhecer e corrigir sua própria postura de autenticação antes de assumir os riscos da imposição.

A granularidade das *tags* implica que a mera presença de um registro diz pouco sobre a proteção efetiva. Política em “none”, modo de teste ativado pela *tag* “t”, ausência de “sp” ou “np” combinada com delegação de subdomínios, e ausência de endereços de relatório configuram, cada qual a seu modo, situações em que o registro existe sem produzir o efeito pretendido — daí a observação de que a ausência de políticas rigorosas facilita a chegada de mensagens falsificadas à caixa de entrada do usuário final, pois nenhuma instrução de rejeição é dada ao receptor (91). O desenho permanece deliberadamente permissivo do lado do destinatário, pois a maior parte das ações é expressa em termos de recomendação, e a

disposição final é sempre matéria de política local, de modo que a eficácia observada depende tanto da publicação correta por parte dos proprietários quanto da adesão dos receptores. É por isso que se sustenta ser fundamental que as organizações tanto configurem seus servidores para verificar e aplicar os registros DMARC do correio de entrada, quanto mantenham registros precisos em seu DNS ao se tratar do correio de saída — tendo por objetivo final a adoção de políticas mais rigorosas, como quarentena ou rejeição — (53, 80, 89).

A Figura 2.11 traz um fluxograma exemplificando a verificação feita pela extensão DMARC.

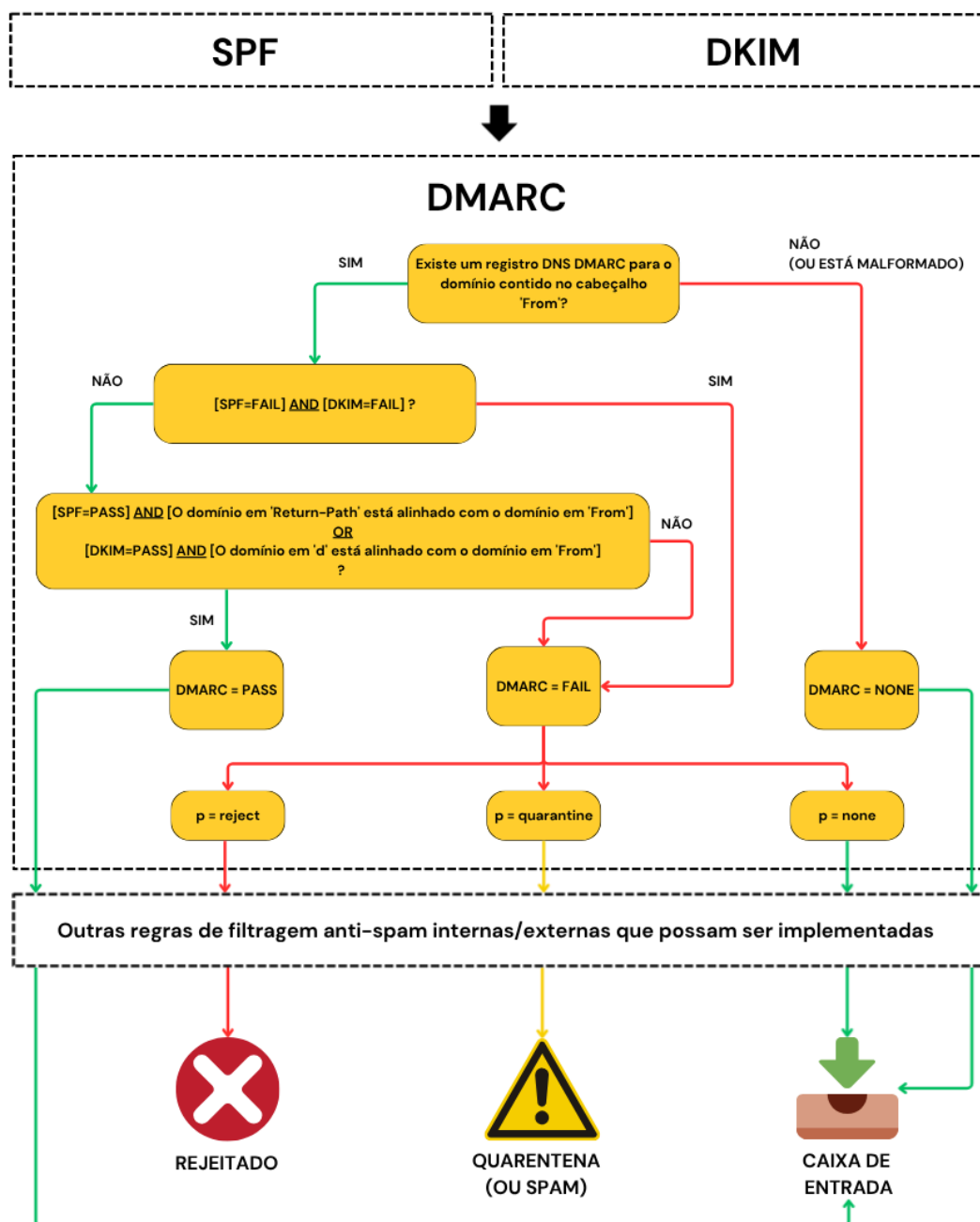


Figura 2.11. Fluxograma da verificação DMARC

(iv) AUTHENTICATION-RESULTS

Por sua vez, as RFCs 8601 e 7372 compõem, em conjunto, o arcabouço normativo responsável por padronizar a forma como os resultados da autenticação de mensagens de e-mail — a partir das extensões de segurança — são comunicados aos diferentes agentes envolvidos no fluxo de correio eletrônico. Trata-se de dois documentos complementares, na medida em que atuam em momentos distintos desse fluxo. A RFC 8601, publicada em maio de 2019, ocupa-se do registro dos resultados de autenticação já obtidos, incorporando-os à própria mensagem por meio do campo de cabeçalho “Authentication-Results”, destinado ao consumo de MUAs e filtros situados a jusante da entrega (102); já a RFC 7372, publicada em setembro de 2014, ocupa-se de um estágio anterior, definindo códigos de status aprimorados capazes de comunicar, ainda durante a sessão SMTP, que uma mensagem está sendo rejeitada ou postergada especificamente em razão de falha em algum desses mesmos mecanismos de autenticação (103). Compreendidas em conjunto, as duas especificações fornecem tanto o vocabulário quanto a sintaxe empregados pelos protocolos de autenticação de remetente — notadamente SPF, DKIM e DMARC — para expressar seus veredictos de forma interoperável.

A RFC 8601 substituiu integralmente a especificação anterior, a RFC 7601, incorporando o registro de novos atributos associados ao DKIM e orientações voltadas ao correio eletrônico internacionalizado (102). Um de seus objetivos é servir como ponto de convergência para os resultados de diferentes esquemas de autenticação, evitando a proliferação de campos de cabeçalho exclusivos para cada novo mecanismo criado — tal como ocorria anteriormente com o cabeçalho “Received-SPF”, específico do SPF, e com o extinto “DomainKey-Status”, associado ao obsoleto DomainKeys (102). O documento é explícito, contudo, quanto a não prescrever como esses dados devem ser efetivamente empregados nas decisões de filtragem, por entender que tal escolha pertence ao domínio e à política local de cada implementação (102).

A validade prática do campo “Authentication-Results” depende inteiramente do contexto de confiança em que ele circula, motivo pelo qual a especificação dedica atenção considerável ao conceito de ADMD e à fronteira de confiança que o delimita, caracterizada como a linha divisória entre entidades internas, providas pela infraestrutura do ADMD, e entidades externas a essa autoridade administrativa (102). Como o cabeçalho normalmente não carrega, por si só, qualquer mecanismo de integridade, sua presença deve ser tratada como confiável apenas dentro do domínio que efetivamente o gerou, exigindo-se que qualquer instância alegando pertencer ao próprio ADMD seja removida no momento em que a mensagem ingressa nesse domínio (102). O processamento das mensagens dentro de um ADMD costuma envolver diferentes papéis funcionais — MSA, MTA de borda, MTAs intermediários e MDA —, sendo a verificação de autenticação tipicamente realizada no MTA de borda ou de entrega (MDA), embora a especificação reconheça a possibilidade de ela ocorrer também em um MTA intermediário (102).

Quanto aos códigos de resultado possíveis em “Authentication-Results” (102):

- **none**: indica ausência de assinatura, autenticação ou tentativa de verificação;
- **pass**: indica êxito;
- **fail**: indica tentativa sem sucesso;
- **neutral**: empregado sobretudo no DKIM, designa assinaturas com erro de sintaxe ou não processáveis por outra razão;
- **policy**: designa os casos em que um mecanismo de política local complementa ou substitui o resultado originalmente produzido, como no exemplo de uma assinatura DKIM tecnicamente válida rejeitada por não abranger o campo “Subject” entre os cabeçalhos assinados;
- **softfail**: específico de falhas de SPF;
- **temperror**: compartilhado pela maioria dos métodos, distinguindo falhas transitórias, passíveis de resultado distinto em nova tentativa; e
- **permerror**: compartilhado pela maioria dos métodos, distinguindo falhas permanentes, para as quais uma nova tentativa dificilmente produzirá resultado diferente.

Já as quatro categorias chamadas de “ptype” distinguem-se pela origem da informação avaliada (102):

- **body**: refere-se ao corpo da mensagem;
- **header**: refere-se a informações extraídas do próprio cabeçalho;
- **policy**: de propriedade e valor de escolha arbitrária do ADMD; e
- **smtp**: referente a comandos de sessão, cujo nome é convertido para letras minúsculas e despojado de espaços, de modo que MAIL FROM se torna mailfrom, por exemplo.

Um contraste entre cabeçalhos “Authentication-Results” com resultado positivo e negativo, respectivamente, é exibido na Figura 2.12.

No que diz respeito às obrigações de implementação, o cabeçalho deve ser sempre inserido no topo da mensagem, sendo vedado acrescentar um novo resultado a uma instância já existente do campo (102). Recomenda-se, ainda, que sistemas que tratem determinados resultados de falha não recuperável (“permerror”) como justificativa para rejeição o façam preferencialmente por meio de resposta de rejeição no próprio nível de sessão SMTP, evitando que a mensagem avance até a entrega e gere, internamente, uma notificação de status direcionada a um remetente possivelmente forjado (102). É justamente nesse ponto — a formalização de uma resposta de rejeição no nível de sessão SMTP, motivada por falha de

autenticação — que a RFC 7372 intervém, definindo os códigos de status aprimorados necessários para que essa recomendação seja expressa de forma padronizada.

```
Authentication-Results: mail.██████████;
    dkim=pass header.d=gmail.com header.s=20230601 header.b=kjYeL97g;
    spf=pass (mail.██████████: domain of ██████████@gmail.com designates 209.85.208.51 as permitted sender)
    smtp.mailfrom=██████████@gmail.com;
    dmarc=pass (policy=none) header.from=gmail.com

Authentication-Results: mail.██████████.ink;
    dkim=none;
    spf=pass (mail.██████████: domain of 'any@██████████.pro' designates 185.██████████.16 as permitted sender)
    smtp.mailfrom='any@██████████.pro';
    dmarc=fail reason="SPF not aligned (relaxed), No valid DKIM" header.from=██████████.ink (policy=reject)
```

Figura 2.12. Comparação de cabeçalhos com resultados dos protocolos de autenticação.
E-mail aprovado em cima e rejeitado embaixo.

A RFC 7372 parte da constatação de que o conjunto de códigos de status aprimorados então vigente, instituído pela RFC 3463 e organizado em registro próprio pela RFC 5248, carecia de um código específico para indicar que a rejeição ou o adiamento de uma mensagem decorria de política local relacionada ao DKIM ou ao SPF, bem como à uma verificação reversa de DNS (103).

Antes de definir os códigos propriamente ditos, a RFC 7372 estabelece que uma assinatura DKIM é considerada aprovada quando o algoritmo básico de verificação definido na RFC 6376 é bem-sucedido, e aceitável quando, além de aprovada, satisfaz também os requisitos definidos localmente pelo operador, como a exigência de que determinados cabeçalhos estejam incluídos no conteúdo assinado (103). A partir dessa distinção, registra-se o código X.7.20, associado ao código básico 550, aplicável quando a mensagem não contém nenhuma assinatura aprovada; o código X.7.21, também associado ao código básico 550, utilizado quando existem assinaturas aprovadas, mas nenhuma satisfaz os critérios adicionais locais; e o código X.7.22, descrito como caso particular do anterior, aplicável quando nenhuma das assinaturas aprovadas contém identificador correspondente ao endereço indicado no campo “From” (103).

Quanto ao SPF, registra-se o código X.7.23, associado ao código básico 550, empregado quando a verificação produz resultado “fail” em desacordo com a política local; e o código X.7.24, associado aos códigos básicos 451 ou 550, destinado a situações de erro na avaliação do SPF (103). Complementarmente, institui-se o código X.7.25, associado ao código básico 550, aplicável quando o endereço IP de um cliente falha em verificação de DNS reverso exigida pela política local; e o código X.7.26, também associado ao código básico 550, previsto para os casos em que uma mensagem falha em mais de uma verificação de autenticação, sem que os mecanismos especificamente responsáveis sejam individualizados (103).

Em razão da própria natureza do protocolo SMTP, apenas um código de status pode ser retornado para uma dada troca entre cliente e servidor, ainda que a rejeição decorra de diversas razões simultâneas; por conseguinte, recomenda-se que, quando mais de uma verificação resultar em falha que justifique a rejeição, o servidor utilize o código

correspondente à falha de múltiplos métodos em vez de reportar apenas o primeiro método falho, sobretudo porque, em certos casos, um dos métodos é esperado sempre falhar, de modo que informá-lo especificamente não traria informação útil ao remetente (103). Um exemplo de rejeição de uma mensagem durante a sessão SMTP é exibido na Figura 2.13.

```
=== Trying [REDACTED]..google.com:25...
=== Connected to [REDACTED].google.com.
<- 220 mx.google.com ESMTP c19-20020a544t [REDACTED]
-> EHLO spftrap.com
<- 250-mx.google.com at your service, [REDACTED]
<- 250-SIZE 157286400
<- 250-8BITMIME
<- 250-STARTTLS
<- 250-ENHANCEDSTATUSCODES
<- 250-PIPELINING
<- 250-CHUNKING
<- 250 SMTPUTF8
-> MAIL FROM:<no_r[REDACTED]>
<- 250 2.1.0 OK c1
-> RCPT TO:<admin@[REDACTED]>
<- 250 2.1.5 OK c1
-> DATA
<- 354 Go ahead c[REDACTED]
-> Date: Wed, 24 May 2023 00:28:36 +0800
-> To: admin@[REDACTED]
-> From: no_reply@[REDACTED]
-> Subject: [REDACTED]
-> Message-ID: [REDACTED]
-> X-Mailer: [REDACTED]
-> [REDACTED]
-> [REDACTED]
-> [REDACTED]
** 550-5.7.26 Unauthenticated email from [REDACTED] is not accepted due to
** 550-5.7.26 domain's DMARC policy. Please contact the administrator of
** 550-5.7.26 spftrap.com domain if this was a legitimate mail. Please visit
** 550-5.7.26 https://support.google.com/mail/answer/2451690 to learn about the
** 550 5.7.26 DMARC initiative. [REDACTED]
-> QUIT
<- 221 2.0.0 closing connection [REDACTED]
=== Connection closed with remote host.
```

Figura 2.13. Rejeição de mensagem durante sessão SMTP devido a não conformidade encontrada durante a autenticação.

Fonte: Zhang et al. (89) em https://github.com/sunknighteric/Measurement_for_SPF_and_DMARC_2023

Do ponto de vista da segurança, a RFC 7372 pondera que o uso desses códigos revela aspectos da política local de autenticação adotada por um operador, informação que pode ser útil a agentes interessados em contorná-la para entregar mensagens indesejadas; por essa razão, esclarece-se que não existe obrigação de utilização desses códigos, podendo um operador que prefira não expor tais critérios continuar a empregar um código genérico, como 5.7.7, 5.7.1 ou 5.7.0 (103).

As considerações de segurança da RFC 8601, por sua vez, tratam de um risco distinto, relacionado não à exposição de política local, mas à própria integridade do campo “Authentication-Results”. Um agente malicioso pode inserir uma instância falsa do cabeçalho utilizando o domínio do ADMD receptor, de modo a simular autenticação bem-sucedida, risco que se torna concreto sempre que o MTA responsável pela filtragem inicial não estiver em conformidade com as obrigações de remoção descritas na especificação (102). Como mitigação, recomenda-se que a interpretação do campo não seja habilitada por padrão, sugerindo-se a assinatura criptográfica do próprio cabeçalho via DKIM, a interrogação do

MTA que supostamente o adicionou, a verificação da cadeia de cabeçalhos “Received” ou o deslocamento dos dados de autenticação para um canal de metadados independente (102).

Esta RFC adverte, também, que a presença de um resultado “pass” não torna a mensagem automaticamente confiável, uma vez que mensagens indesejadas podem satisfazer diversos métodos simultaneamente, como no caso de *spam* assinado com DKIM pelo próprio remetente malicioso (102). O documento chama atenção, por fim, para o fenômeno do *backscatter*, para o cenário de comprometimento de *hosts* internos, em que um MUA ou MTA legítimo, uma vez comprometido, poderia gerar mensagens com cabeçalho “From” forjado acompanhado de um “Authentication-Results” igualmente forjado, e para a possibilidade de campos excessivamente extensos ou malformados serem empregados como vetor de ataque contra o próprio código de análise sintática (102).

(v) LIMITAÇÕES DAS EXTENSÕES

Apesar da coexistência dos protocolos de segurança SPF, DKIM e DMARC ao longo dos últimos quinze anos, ataques de *spoofing* ainda podem ser bem-sucedidos devido à inconsistência entre as entidades protegidas, à baixa adoção e à má configuração desses mecanismos (5, 55, 91).

O sistema de e-mail só pode prevenir ataques de falsificação quando todos os protocolos estiverem bem aplicados. Nessa estrutura baseada em cadeia, a falha de qualquer elo pode invalidar toda a autenticação (55). A segurança total dos sistemas de e-mail depende da aplicação consistente das mesmas tecnologias de autenticação tanto pelo servidor remetente quanto pelo servidor destinatário, o que frequentemente não ocorre (82, 104). Mesmo grandes organizações enfrentam dificuldades para configurar e manter seus sistemas de e-mail seguros (82).

A autenticação baseada em domínio apresenta certas limitações também em seu controle de granularidade ampla e não pode assegurar a autenticidade dos indivíduos dentro de um mesmo domínio, sendo insuficiente em casos em que atacantes utilizam contas legítimas comprometidas (73). Devido ao fato do SPF ser baseado em endereços IP, se e-mails falsificados forem enviados a partir do mesmo IP de um determinado provedor, podem passar na verificação de SPF e consequentemente de DMARC, especialmente porque muitos clientes incorporam o registro SPF do provedor em suas próprias configurações, podendo outros domínios hospedados no mesmo provedor realizar a falsificação (5, 68). Além disso, o SPF exige que todos os servidores de e-mail autorizados sejam listados nos registros DNS, o que é desafiador para infraestruturas complexas (87).

Um problema de *design* no DKIM permite que um invasor omita o cabeçalho de assinatura, levando o destinatário a presumir que o domínio não implementa o protocolo, burlando a verificação (1). A ausência de uma assinatura DKIM é ambígua, pois pode significar que o

remetente não implementa o protocolo ou que um invasor está falsificando o domínio ou adulterando a mensagem (58).

Além disso, uma regra de SPF ou DMARC mal configurada é tão perigosa quanto a ausência de regras, pois a avaliação não leva a uma decisão correta (56, 85, 92). Configurações incorretas ou ausentes de SPF e DMARC podem colocar uma organização em risco de ter seu domínio falsificado para a realização de ataques de *phishing* enquanto passa uma falsa sensação de segurança (29, 89).

O *spoofing* de e-mail também é possível explorando as discrepâncias entre os quatro componentes de autenticação do remetente — SPF, DKIM, DMARC e DNS (3, 33, 55). Um atacante pode forjar domínios ambíguos para fazer o componente de autenticação crer que está verificando o domínio legítimo, enquanto o componente DNS consulta o domínio do atacante para obter registros de política (71). Como o DMARC lida apenas com falsificação de domínios exatos, ele não consegue solucionar o problema da proliferação de “domínios primos” (*cousin domains*) ou domínios *typosquatting* (53, 105). Um atacante pode registrar um domínio semelhante, publicar seus próprios registros SPF, DKIM e DMARC válidos, contornando as verificações e fazendo com que o e-mail seja classificado como genuíno (62, 53).

As defesas técnicas existentes incluem soluções baseadas em *blacklists*, que sofrem com problemas de latência, e soluções baseadas em aprendizado de máquina (79). Atualmente, ferramentas como *dnstwist*¹ podem ajudar organizações a identificar variações de domínios primos (*cousin domains*) e *typosquatting* para descobrir quais já estão registrados, permitindo registrar domínios defensivamente (53). Contudo, mesmo que o registro defensivo possa mitigar ataques, esses domínios ainda precisam ter seus protocolos SPF e DMARC registrados para serem protegidos contra falsificação (85).

Outros ataques possíveis são (57, 68, 74, 85):

- **Forward MTA Attack:** o atacante configura um serviço de encaminhamento de e-mails em uma conta intermediária, que adiciona uma assinatura DKIM válida à mensagem falsificada, fazendo com que ela passe pelos mecanismos de autenticação;
- **Shared MTA Attack:** o atacante e o usuário personificado possuem contas no mesmo domínio, permitindo que o invasor envie mensagens forjadas, pois compartilha o mesmo IP e registros SPF/DKIM da vítima;
- **SMTP smuggling:** é executado embutindo comandos SMTP no corpo do e-mail, permitindo que invasores enviem múltiplos e-mails em uma única sessão SMTP — sendo o primeiro legítimo e os demais forjados — burlando SPF e DMARC e possibilitando a personificação de qualquer remetente dentro do mesmo domínio; e

¹ <https://github.com/elceef/dnstwist>

- **Ataque dos múltiplos nomes de exibição:** o atacante envia uma mensagem cuidadosamente forjada que especifica múltiplas informações de endereços de e-mail durante a fase de envio. Além disso, a introdução de símbolos especiais (como os caracteres # ou ;) no campo “From” também pode contornar os métodos de detecção de segurança.

A despeito destas falhas técnicas, um dos principais problemas das extensões SPF, DKIM e DMARC vem de sua baixa adoção (54, 91). A adoção dessas extensões é voluntária, o que torna sua taxa de implementação relativamente baixa e insatisfatória (5, 91). A autenticação do remetente acaba dependendo do trabalho opcional dos provedores de serviço (74). A aplicação dos mecanismos aumentou a complexidade para os implementadores de e-mail (64) e a falta de controle sobre servidores de e-mail e servidores DNS, aliada a dependência de serviços em nuvem — onde blocos de IP são compartilhados —, tornam a implantação mais custosa e problemática (62, 76).

Os benefícios que um usuário de domínio obtém ao usar os protocolos antispoofting são considerados indiretos, pois eles previnem apenas o abuso do domínio como servidor remetente e não protegem diretamente o domínio e seus usuários de receberem e-mails falsificados. A percepção de dificuldade na implantação desses protocolos e o receio de bloquear ou rejeitar um e-mail autêntico também contribuem para a baixa taxa de adoção (62).

As configurações também não são, na maior parte das vezes, restritivas o suficiente para captar ataques mais sofisticados, pois as empresas evitam o risco de perder e-mails legítimos devido a falsos positivos (77). O equilíbrio entre taxa de falso positivo e taxa de falso negativo é decisivo, mas os falsos positivos são mais problemáticos, pois podem bloquear mensagens legítimas antes da entrega (53). Devido ao receio de bloquear e-mails autênticos, a maioria dos provedores de e-mail configura uma política DMARC relaxada, o que resulta na entrega da mensagem na caixa de entrada mesmo se ela falhar nos testes SPF e/ou DKIM (62). Provedores tendem a priorizar a entrega sobre a segurança, entregando e-mails reprovados se a política DMARC do domínio não for “reject” (30) e permitindo que seus domínios sejam falsificados.

Portanto, apesar dos esforços substanciais para mitigar o *spoofing*, a falha em evitar ataques se deve principalmente à baixa adoção e à configuração incorreta ou excessivamente permissiva desses mecanismos (62, 80, 92). A eficácia plena depende de uma implementação rigorosa e da colaboração ampla entre remetentes e destinatários em aplicar políticas restritivas (54, 71, 97). É essencial que a implementação de mecanismos de segurança seja obrigatória, funcionando como um fator coercitivo para que os remetentes configurem corretamente SPF, DKIM e DMARC (5). É igualmente fundamental que as pesquisas se concentrem em: aprimorar as técnicas de detecção, avançar nos mecanismos de autenticação de usuários e explorar medidas proativas, combinando tecnologia, educação e conscientização (20) na luta contra a falsificação de endereços de remetente.

2.5. ATAQUES DE ENGENHARIA SOCIAL VIA E-MAIL

Como já mencionado, o e-mail tornou-se uma ferramenta indispensável devido à sua eficiência, rapidez e versatilidade na comunicação para fins pessoais e profissionais (70, 74, 86, 106, 107, 108). Entretanto, transformou-se também em uma ameaça crítica à segurança, por ser um dos canais mais vulneráveis a ataques cibernéticos, especialmente os de engenharia social (31, 70, 82, 86, 91).

Em uma era dominada por interações digitais, os ataques evoluíram para explorar não apenas vulnerabilidades tecnológicas, mas também características humanas (109). A engenharia social é a arte de persuadir usuários para que revelem informações sensíveis (110). Trata-se de uma forma de engano ou manipulação que permite a um invasor explorar sua vítima para obter acesso a informações confidenciais (23, 110, 111, 112). Essa técnica utiliza táticas enganosas para levar pessoas a violarem medidas de segurança, explorando a tendência humana à confiança (97, 111).

Os ataques de engenharia social podem ser orquestrados por indivíduos com ou sem expertise cibernética. Muitos dos golpes bem-sucedidos são de baixa complexidade tecnológica, embora o subterfúgio exija atacantes com algum nível de conhecimento técnico (27, 112). Os autores de fraudes que se valem de engenharia social utilizam princípios de persuasão para alcançar seus objetivos (112). Esses princípios são utilizados em 88% dos ataques de engenharia social e se baseiam em seis categorias principais (82, 112):

1. **Autoridade:** tendência a obedecer pessoas em posições de autoridade;
2. **Simpatia (*Liking*):** tendência a dizer “sim” a pedidos de pessoas conhecidas ou simpáticas;
3. **Escassez:** tendência a atribuir maior valor a itens e oportunidades quando sua disponibilidade é limitada;
4. **Consistência:** tendência a agir de maneira coerente com decisões e comportamentos passados;
5. **Comportamento de Manada (*Social Proof*):** propensão a considerar um comportamento correto na medida em que outras pessoas o adotam; e
6. **Reciprocidade:** sentimento de dever em retribuir favores recebidos.

Os ataques cognitivos, que exploram essas vulnerabilidades, geralmente consistem na inserção de frases específicas — por exemplo, no corpo de um e-mail — para exercer persuasão sobre o destinatário (82). Outros fatores psicológicos explorados incluem: recompensa, apelando à ganância; urgência, explorando o fator tempo para induzir reações impulsivas; e confiança, explorando vínculos pessoais (29, 82).

Atores maliciosos enviam e-mails que induzem o indivíduo a agir, seja fornecendo informações pessoais ou abrindo links e arquivos maliciosos que oferecem um ponto de entrada para o ataque (112). Para tanto, é essencial conquistar a confiança da vítima (84). Os atacantes buscam maximizar a superfície de ataque e minimizar a detecção, geralmente personificando alguma pessoa ou instituição na qual o alvo confia, dependendo exclusivamente de técnicas de manipulação para estabelecer essa confiança e convencer a vítima a realizar a ação desejada (105). Os seres humanos representam o elo mais fraco da segurança da informação, o que oferece uma oportunidade significativa para os fraudadores, pois as organizações frequentemente dependem das pessoas como primeira linha de defesa (77, 112). Os ataques de engenharia social exploram emoções humanas, tornando essa dependência do usuário uma defesa frágil (112).

A engenharia social é empregada em e-mails de *phishing* (112). O *phishing* explora precipuamente usuários da Internet (20, 86, 110) valendo-se da credulidade e das limitações cognitivas dos usuários, fazendo da pessoa a abordagem mais econômica e gerando algumas das maiores taxas de sucesso entre os ciberataques (73, 77, 83). Este ataque é atualmente uma das ameaças cibernéticas mais problemáticas (20, 86). A falta de conhecimento e conscientização dos usuários sobre as táticas de engenharia social e a negligência humana na verificação da legitimidade de mensagens são causas principais do sucesso desses ataques (105, 110, 112).

O *phishing* é uma tentativa maliciosa de cibercriminosos de roubar informações pessoais, sendo um ataque cibernético que geralmente se inicia com um e-mail ou outra comunicação fraudulenta (33, 83). Trata-se de uma prática enganosa em computação, onde os atacantes enviam e-mails enganosos, se passando por entidades legítimas, a fim de induzir os destinatários a revelarem informações privadas (27). É o ato de obter informações confidenciais, como nome de usuário, senha ou dados de cartão de crédito, fingindo ser uma fonte autorizada, sendo um dos métodos mais antigos e fáceis de roubo de informações e identidade (52). A primeira ocorrência conhecida de *phishing* foi registrada em 1995, quando *hackers* se passaram por funcionários da empresa *America Online* (73, 84).

Os ataques de *phishing* podem ser subdivididos em algumas categorias, sendo o *phishing* por e-mail o tipo mais comum, no qual os atacantes enviam e-mails genéricos falsos em larga escala fingindo ser correspondências oficiais de fontes confiáveis (2, 113, 114). O *spear phishing* é uma forma direcionada e sofisticada de *phishing* em que os atacantes utilizam informações pessoais das vítimas para iniciar o ataque, personalizando as mensagens para um indivíduo, equipe ou organização específica (2, 70, 83, 114). Este tipo de ataque é considerado até dez vezes mais eficaz do que campanhas genéricas de larga escala (73, 83, 114). O *whaling* é um *spear phishing* altamente direcionado que têm como alvo indivíduos de alto perfil, como executivos, altos funcionários do governo ou oficiais com acesso a informações sensíveis (23, 67, 70, 84, 111). Por fim, o *Business Email Compromise* (BEC), também conhecido como “fraude do CEO”, é uma forma especializada e sofisticada de fraude por e-mail com fins financeiros, onde um atacante se passa por um funcionário ou executivo

da organização, usando contas de e-mail falsas ou comprometidas, e tenta induzir a vítima a fazer transações financeiras (33, 115, 116, 117).

O custo do *phishing* — considerando perda de receita, vazamento de dados, custos de mitigação e sanções regulatórias — é alto demais para deixar o canal de e-mail desprotegido (90). O impacto de um clique indevido pode ser grande, desde o comprometimento da própria conta associada ao usuário até mesmo de toda a rede corporativa, pelo escalonamento de privilégios (106). O *phishing* não se resume a perdas financeiras, pois também implica em riscos à reputação organizacional, quebra de confiança de clientes e investidores, perda de propriedade intelectual, penalidades regulatórias e interrupções nas operações (27, 83). Além disso, o *phishing* é frequentemente usado para sustentar outras ações maliciosas, como *ransomware*, extorsão e espionagem cibernética (2, 84, 106).

O *phishing*, em especial o *spear phishing*, continua sendo uma ameaça persistente e crescente, apesar dos esforços substanciais da indústria e da academia para combatê-lo. Devido às suas altas taxas de sucesso e baixo custo de execução, o *phishing* evoluiu para uma das principais estratégias de ciberataque (73). Os ataques têm gerado sérias ameaças relacionadas à obtenção de informações sensíveis, seguindo como uma grande ameaça no mundo da cibersegurança (118). A gravidade dos danos financeiros e a preferência crescente dos atacantes em erros humanos exigem uma mudança de paradigma nas estratégias defensivas (116).

2.6. FALSIFICAÇÃO DE ENDEREÇOS DE E-MAIL (*E-MAIL SPOOFING*)

Como visto, a luta contra fraudes por e-mail parece interminável (79). O sistema de e-mail é o campo de batalha central contra ataques de *phishing* e engenharia social e os provedores de e-mail continuam enfrentando desafios importantes para autenticar e-mails recebidos (54). Na vida digital cotidiana, o correio eletrônico é um dos sistemas de comunicação mais utilizados, apresentando um ponto de entrada comum para ciberataques (4).

O e-mail oferece facilidades para o envio de mensagens digitais e torna a comunicação mais simples. No entanto, essa comodidade também intensifica o uso indevido do e-mail, uma vez que, como comprovado nas seções passadas, é tecnicamente possível alterar a identidade do remetente para fazer com que a mensagem pareça ter sido enviada a partir de um endereço legítimo. Essa atividade é comumente conhecida como *spoofing* de e-mail (63). Trata-se de um ataque no qual um ator malicioso envia um e-mail com o endereço de remetente adulterado para parecer que foi originado de uma fonte confiável (5, 30, 52, 56, 60, 62, 63, 65, 67, 68, 70, 72, 77, 84, 97, 104, 106). A segurança e a confiabilidade do correio eletrônico são seriamente comprometidas por esse tipo de falsificação. Por meio dessa técnica, usuários ilegítimos podem alterar cabeçalhos, forjar identidades de remetentes e, por fim, enganar os destinatários (81) levando a diversos riscos, como violação de dados, danos à reputação e até prejuízos financeiros (29). Estima-se que 6,4 bilhões de e-mails falsificados circulem diariamente (1, 53).

Os cibercriminosos exploram oportunidades para falsificar e-mails e obter informações e credenciais valiosas (107). Os atacantes têm se tornado mais habilidosos em falsificações que pareçam idênticas ao esperado, incluindo logotipos e imagens dentro dos e-mails de *phishing*, para torná-los mais convincentes. O *spoofing* também desempenha um papel central na credibilidade de mensagens fraudulentas (86). Na verdade, esse método é mais elaborado e eficaz do que e-mails de *phishing* tradicionais, pois as mensagens se assemelham significativamente às enviadas pelas entidades verdadeiras (31). Ao se passar por uma entidade confiável como remetente, o invasor tem mais chances de ganhar a confiança da vítima e levá-la a responder às suas solicitações, sendo geralmente uma tentativa de enganar o usuário para alcançar objetivos maliciosos como, por exemplo, solicitar que ele faça uma declaração prejudicial, baixe softwares maliciosos ou revele informações sensíveis como senhas e outras credenciais (29, 54, 56, 63, 67, 72). Esses ataques frequentemente personificam pessoas influentes ou superiores hierárquicos, induzindo o destinatário a executar ações específicas, resultando em comprometimento de dados (29). A maior parte dos e-mails de *spear phishing* utiliza *spoofing* (66).

Logo, campanhas de *phishing*, *spam* e distribuição de *malware* são alguns exemplos de ataques que dependem do *spoofing* de e-mail (30, 31, 56, 87). Os ataques de personificação atingem facilmente canais de comunicação para alcançar seus objetivos, deixando as vítimas arcando com as consequências (27). Apesar dos enormes esforços realizados para mitigar essa técnica, ela ainda constitui um dos ciberataques mais bem-sucedidos e é responsável por danos significativos. Por exemplo, em 2018, a falsificação de e-mails custou mais de 1,2 bilhão de dólares às vítimas nos EUA (85).

Objetivos comuns para utilização de *e-mail spoofing* são (62):

- Ocultar a identidade real do remetente;
- Obter informações importantes e sensíveis de indivíduos e organizações;
- Fingir ser uma organização genuína e confiável para obter acesso a informações privadas;
- Fingir ser um remetente genuíno e confiável, como alguém que o destinatário já conhece, para coletar informações pessoais;
- Burlar listas de bloqueio e filtros de *spam*;
- Prejudicar a reputação do remetente original;
- Cometer ataques de roubo de identidade; e
- Disseminar e instalar vários tipos de *malwares* ocultos em arquivos anexados a e-mails forjados.

O *spoofing* de e-mail ocorre em dois tipos. O primeiro consiste em comprometer servidores de e-mail legítimos e utilizá-los para enviar e-mails falsificados às vítimas, especificando um endereço “Reply-to” diferente, ou fornecendo uma URL de *phishing* no corpo da mensagem. O segundo tipo é o *spoofing* de domínio, no qual os atacantes alteram outros cabeçalhos da mensagem para enviar e-mails em nome de domínios legítimos (29, 56, 85). O presente trabalho se concentra neste segundo tipo de falsificação.

Na maioria dos e-mails falsificados, o nome de domínio é apenas similar ao verdadeiro, uma prática chamada de *typosquatting* e que pode passar despercebida (109). Os invasores podem aplicar *typosquatting* para adquirir domínios parecidos com o domínio alvo e fazer o endereço do remetente ser semelhante — mas não idêntico — ao que querem falsificar. Esse tipo de endereço remetente é um forte indicador de *phishing* e tem sido usado para detectar e-mails maliciosos (54). O termo “registro defensivo” refere-se ao processo de registrar nomes de domínio com diferentes TLDs (*Top Level Domain*) e variações gramaticais para proteger marcas e organizações contra ataques como *typosquatting* (85).

Contudo, esta técnica de falsificação não é a mais preocupante, uma vez que, embora nem sempre facilmente detectável, há diferença visual entre os domínios. A maioria das ameaças mais severas de e-mail pode ser rastreada até uma única causa comum: a falta de autenticação no protocolo SMTP (72). Devido às limitações de segurança do SMTP que foram exaustivamente tratadas nas seções anteriores, o atacante pode utilizar o método de *spoofing* de domínio para falsificar um endereço de remetente visualmente idêntico e a um baixo custo (74). Na Figura 2.14, observa-se uma comparação entre mensagens, uma genuína e outra falsificada, renderizadas ao usuário com um endereço de remetente visualmente idêntico. Uma das causas fundamentais desse problema é a fragilidade da autenticação no sistema de envio de e-mails, que permite que qualquer pessoa envie mensagens em nome de um determinado domínio sem autorização (86).



Figura 2.14. Comparação de mensagens renderizadas ao usuário. Genuína à esquerda e falsificada à direita.

É amplamente sabido que este tipo de falsificação de e-mail é possível apenas pelo fato de que todo o sistema de e-mail funciona sobre o SMTP, que não fornece originalmente nenhum mecanismo para autenticar o remetente do e-mail (3). Os protocolos de segurança de e-mail enfrentam desafios desde sua origem (31). Infelizmente, os projetistas do SMTP nunca previram esse tipo de uso fraudulento e não incorporaram nenhum mecanismo de segurança ou autenticação em seu *design* original (31, 53, 54, 71, 92). O cerne dos ataques de *phishing* está justamente na falha de autenticidade. A autenticidade abrange dois aspectos críticos: a imutabilidade do conteúdo durante a transmissão da mensagem e a verificação da identidade do remetente. Nem sempre os destinatários conseguem verificar de forma confiável se um endereço aparentemente legítimo realmente pertence à organização que afirma representar (73).

O *design* do SMTP inclui múltiplas “identidades” no tratamento de mensagens. Como analisado anteriormente, tanto o comando MAIL FROM (no envelope SMTP) quanto o cabeçalho “From” (no cabeçalho do e-mail) identificam o remetente do e-mail, mas possuem significados diferentes em uma conversação SMTP. O primeiro representa o usuário que transmitiu a mensagem e normalmente não é exibido ao destinatário. O segundo representa o usuário que compôs a mensagem e é visível para o destinatário. Além disso, o SMTP introduz várias outras identidades de remetente, como o comando HELO e os cabeçalhos “Sender” e “Resent-From”. Nada no *design* do protocolo impõe consistência entre essas identidades (31, 33, 71).

É relativamente fácil falsificar mensagens (63, 93). O requisito principal é possuir um servidor SMTP e uma aplicação para enviar mensagens. No momento de compor o e-mail, o atacante altera alguns dos campos encontrados dentro do cabeçalho da mensagem, como “From”, “Reply-to” ou “Return-Path” (62, 63). Isso ocorre porque essas são as partes mais reconhecíveis e visíveis ao destinatário e podem ser adulteradas para fazê-lo acreditar que o e-mail vem de uma fonte confiável (53). Quando qualquer usuário recebe essa mensagem de e-mail modificada, presumirá que ela veio do endereço forjado e não de sua origem real. Pelo campo “Reply-to” o servidor de e-mail receptor passa a saber para onde enviar uma resposta, e isso pode ser modificado para uma caixa de correio que esteja sob o controle do atacante, diferente do endereço do remetente personificado (62, 63).

E-mails falsificados deveriam ser detectados antes de serem transmitidos ao destino (108), mas não o são. O servidor de e-mail remetente ou mesmo o protocolo SMTP não conseguem detectar que o e-mail é forjado. Torna-se completamente responsabilidade do servidor receptor verificar os endereços e determinar se a mensagem é de um remetente genuíno ou não (62, 63).

Atacantes podem configurar um servidor SMTP próprio ou usar servidores SMTP comprometidos que permitem conexões sem necessidade de autenticação (33). No primeiro caso, os invasores geralmente exploram o SMTP configurando seus próprios servidores para enviar mensagens falsas (54, 71) o que exige habilidade em infraestrutura de redes, além de ser necessário que o endereço de IP do servidor e o domínio real atrelado a ele tenham boa reputação. Desta forma, um atacante pode enviar e-mails arbitrários à vítima

(victim@victim.com) diretamente de seu servidor (attack.com), falsificando o endereço do remetente no cabeçalho “From” com um domínio legítimo (admin@legitimate.com) (71). No segundo caso, esses e-mails podem ser retransmitidos por servidores SMTP abertos, que aceitam e repassam qualquer mensagem sem autenticar o remetente (84). Se um serviço de e-mail não for configurado corretamente, um invasor pode utilizar o endereço IP do domínio, configurado como um *relay* aberto, para enviar e-mails forjados (33). O protocolo SMTP não exige que os servidores de transferência de correio realizem autenticação, pressupondo que todo e-mail recebido seja legítimo (32). O uso de um servidor confiável é um método frequentemente utilizado para maximizar as chances de ultrapassar filtros de segurança, pois reduz as chances das mensagens serem marcadas como *spam* ou maliciosas (109). Destaca-se que alguns sites como <https://emkei.cz/> (um originador gratuito de e-mails com cabeçalhos forjáveis) também podem ser usados para enviar mensagens falsas de forma tecnicamente simples (70).

Um ataque de falsificação de remetente é considerado bem-sucedido se (55):

- Na autenticação de envio, o invasor puder modificar livremente identificadores como “AUTH username”, “MAIL FROM” e “From”;
- Na verificação de recebimento, o servidor MTA do destinatário retornar “none/pass”, mesmo que o domínio falsificado tenha políticas de SPF, DKIM e DMARC;
- No encaminhamento, o servidor encaminhador atribuir uma validação de segurança à mensagem;
- Na renderização da interface, o endereço exibido ao destinatário for inconsistente com o real.

A ameaça crescente do *spoofing* tornou-se uma preocupação central entre os usuários de diversos sistemas (29). À medida que a falsificação de e-mails se torna mais prevalente, é essencial proteger ativos contra roubo de identidade. O e-mail deve ser protegido da mesma forma que qualquer outra rede ou aplicação, já que é por meio dele que grande parte dos *malwares* invade os computadores (107). Os mais disseminados e onipresentes ataques via e-mail são justamente os de *spoofing* (92), que têm se mostrado um vetor de ataque extremamente eficaz, mesmo quando usado contra especialistas, haja vista o crescimento drástico de casos bem-sucedidos de BEC implementados com a utilização desta técnica. Existem boas soluções para lidar com o problema. Cada uma delas o aborda por um ângulo diferente e, quando utilizadas em conjunto, formam uma defesa em camadas sólida contra falsificação de e-mails (77).

É nesse ponto que a implementação de tecnologias antispoofing desempenha um papel crucial — ao sinalizar e-mails suspeitos e alertar o usuário, ou rejeitá-los antes mesmo de chegarem à caixa de entrada (53). Estudos acadêmicos recomendam aprimorar os mecanismos de autenticação e criptografia em navegadores e clientes de e-mail como forma

de criar uma linha de defesa mais robusta contra este tipo de ataque. Entre as medidas sugeridas estão: uso de um único nome de domínio pelas organizações, evitando confundir os usuários com múltiplos domínios ou endereços IP; adoção das extensões de segurança do SMTP (SPF, DKIM, DMARC e outras) pelos clientes de e-mail, para autenticar mensagens recebidas; e o uso de indicadores de segurança que alertem o usuário quando e-mails não verificados chegam à caixa de entrada (83).

Em certas áreas, uma aplicação legal obrigatória pode permitir uma adoção mais rápida e reduzir o risco de falsificação de e-mails. Por exemplo, uma diretiva obrigatória foi publicada pelo *Department of Homeland Security*, estabelecendo que todos os domínios oficiais dos EUA (.gov) deveriam usar DMARC com a política “p=reject” a partir de 16 de outubro de 2018. Existe também um equivalente britânico à diretiva e uma recomendação para que a União Europeia (UE) use DMARC em domínios administrativos. Domínios de classificação mais alta, que geralmente são operados por organizações maiores, parecem levar o problema de segurança da falsificação mais a sério do que organizações menores. Deve-se observar que domínios conhecidos provavelmente são mais suscetíveis a serem falsificados do que domínios desconhecidos (1).

Desta forma, resta claro que a implementação de medidas robustas de antispoofting ajuda a prevenir ataques (29). As organizações precisam gerenciar seus domínios e aplicar as medidas de segurança (88). A ampla literatura sobre detecção de e-mails falsificados pode ser dividida em duas grandes vertentes: (a) a análise da implementação e dos desafios de adoção dos protocolos antispoofting; e (b) o estudo das limitações e lacunas técnicas desses protocolos, propondo técnicas aprimoradas de detecção (53). Este trabalho se enquadra na primeira vertente.

2.7. TRABALHOS CORRELATOS

Aqui são apresentados, em ordem cronológica, os trabalhos correlatos ao presente estudo. Optou-se por considerar as pesquisas realizadas a partir de 2011, ano em que o protocolo DMARC foi criado (embora tenha sido publicado oficialmente apenas em 2015). Este recorte temporal se justifica pelo fato de que a proteção efetiva dos domínios contra a falsificação de remetente só se tornou possível após a criação dessa extensão e sua respectiva coexistência com SPF e DKIM, motivo pelo qual avaliações anteriores fogem ao interesse desta investigação.

Kumar, Hanumanthappa e Kumar (72) abordaram a ausência de mecanismos que alertem o verdadeiro proprietário do endereço falsificado. A contribuição central consistiu em propor uma técnica capaz de detectar quando um e-mail é enviado utilizando indevidamente o endereço de um usuário e, em seguida, informar este usuário automaticamente sobre o incidente. Essa abordagem permite que a vítima personificada tome medidas imediatas de contenção e segurança.

Gupta et al. (60) investigaram como diferentes clientes de e-mail se comportam ao receber mensagens com remetente falsificado e, a partir disso, desenvolveram um mecanismo de detecção capaz de identificar o *spoofing* por meio da análise detalhada dos cabeçalhos de autenticação. A principal contribuição está na criação de um algoritmo que utiliza campos de cabeçalho para distinguir e-mails legítimos de e-mails forjados, demonstrando sua eficácia por meio de experimentos com um *dataset* controlado.

Durumeric et al. (76) forneceram a primeira análise global abrangente sobre a adoção e a eficácia das principais extensões de segurança do protocolo SMTP — STARTTLS, SPF, DKIM e DMARC — avaliando tanto a configuração de servidores quanto o tráfego real observado ao longo de um ano. O estudo revelou um cenário de segurança desigual, no qual grandes provedores aplicam boas práticas avançadas, mas a grande maioria dos servidores ainda apresenta configurações frágeis ou inexistentes. O trabalho demonstrou como políticas permissivas permitem ataques como *TLS downgrade* e falsificação de registros MX, trazendo evidências concretas de exploração em diversos países.

Foster et al. (58) avaliaram o nível de segurança oferecido pelos principais mecanismos e extensões de proteção do ecossistema de e-mail — TLS, SPF e DKIM — identificando em que medida eles são implementados e aplicados por provedores globais. Os autores demonstraram, por meio de medições empíricas em larga escala, que embora haja avanços importantes na adoção de TLS e mecanismos de autenticação, falhas críticas persistem, especialmente a ausência de verificação de certificados, a baixa aplicação de SPF e a adoção limitada de DKIM.

Iyer et al. (104) introduziram uma abordagem para detecção de e-mails falsificados utilizando técnicas de forense de memória, ampliando as capacidades tradicionais de análise voltadas apenas para cabeçalhos, protocolos e *logs* de servidores. A contribuição principal foi demonstrar que a análise periódica da memória volátil do cliente pode identificar tanto o recebimento quanto a interação do usuário com e-mails falsificados, garantindo assim a não repudição e fornecendo evidências para investigações de crimes cibernéticos. Ao registrar automaticamente artefatos de *spoofing* em arquivos de *log* destinados a investigadores, o estudo apresenta um método, complementar às práticas existentes, capaz de fortalecer significativamente a detecção pós-ataque.

Opazo, Whitteker e Shing (77) propuseram uma solução complementar aos mecanismos tradicionais de autenticação de e-mail, capaz de detectar discrepâncias em cabeçalhos que podem indicar *spoofing*, sem depender exclusivamente de configurações rígidas no lado do servidor. A principal contribuição consistiu na introdução de uma aplicação “sentinela” no lado do cliente que analisa o código-fonte dos cabeçalhos, alerta o usuário sobre possíveis falsificações, registra incidentes e reforça políticas internas de segurança.

Hu e Wang (30, 54) investigaram como os provedores de e-mail lidam com mensagens falsificadas e avaliaram a eficácia de seus mecanismos de detecção, bloqueio e alerta ao usuário frente a ataques de *spear phishing*. Os autores demonstraram que, embora a maioria dos provedores implemente protocolos de autenticação como SPF, DKIM e DMARC, ainda

há condições em que e-mails forjados chegam à caixa de entrada, muitas vezes sem qualquer aviso — especialmente em aplicativos móveis — e com interfaces que reforçam a falsa legitimidade da mensagem. Ao combinar medições técnicas com testes de comportamento de usuários, o estudo evidenciou lacunas tanto na infraestrutura de defesa quanto na comunicação visual com o usuário final, oferecendo recomendações para aprimorar protocolos, interfaces e práticas de segurança visando reduzir a eficácia dos ataques baseados em *spoofing* e engenharia social.

Pongchanchai et al. (108) desenvolveram um mecanismo preventivo capaz de detectar, ainda no momento do envio, e-mails que utilizam *display names* falsificados para facilitar ataques de *phishing* e *spoofing*. A contribuição principal consistiu em implementar e validar uma solução integrada ao MSA, que verifica a autenticidade do nome exibido antes que a mensagem seja encaminhada ao destinatário. Essa abordagem permite a atuação na origem do problema — no ponto de submissão da mensagem — reduzindo significativamente a propagação de *spam* e e-mails falsificados. Os resultados demonstram que o método é eficaz na identificação de falsificações e, embora haja algum impacto no tempo de transmissão, o oferece uma solução prática para reforçar a segurança do ecossistema de e-mail, mitigando ataques baseados em *display name*.

Raulot (86) estudou a eficácia dos filtros de *spam* na detecção de e-mails de *phishing* para identificar técnicas capazes de burlar esses mecanismos de defesa. A contribuição principal foi demonstrar empiricamente que, ao seguir estritamente padrões e protocolos de autenticação — como SPF, DKIM e DMARC — atacantes podem enviar e-mails maliciosos, mas devidamente autenticados, a partir de domínios recém-registrados e, com isso, evitar a detecção dos filtros.

Nanaware, Mohite e Patil (88) pesquisaram de que forma soluções especializadas podem fortalecer a segurança de domínios organizacionais ao oferecer visibilidade ampliada e ferramentas eficazes para detecção e prevenção de ataques de e-mail *spoofing*. A contribuição principal foi demonstrar que, além dos protocolos fundamentais — STARTTLS, SPF, DKIM e especialmente DMARC —, as organizações necessitam de plataformas capazes de interpretar relatórios RUA e RUF, fornecer análises detalhadas e permitir respostas rápidas a abusos.

Ajina e Kumar (5) investigaram como os principais provedores de e-mail lidam com ataques de *spoofing* e avaliaram a eficácia das camadas de segurança e dos protocolos de autenticação, como SPF, DKIM, DMARC e ARC. Os autores combinaram análises técnicas, experimentos e observações para revelar sob quais condições e-mails falsificados conseguem ultrapassar mecanismos de defesa e alcançar a caixa de entrada — muitas vezes devido a falhas de configuração, limitações dos protocolos ou interfaces enganosas que reforçam uma falsa sensação de segurança.

Giorgi, Saracino e Martinelli (66) desenvolveram um mecanismo de verificação de autoria capaz de identificar ataques de e-mail *spoofing* com base no estilo de escrita, ampliando a proteção além dos mecanismos tradicionais de autenticação baseados em infraestrutura. A

principal contribuição consistiu em introduzir uma verificação de autoria *end-to-end*, que analisa não apenas o padrão de escrita do remetente, mas também as interações específicas entre remetente e destinatário.

Chen, Paxson e Jiang (71) expuseram como inconsistências internas entre componentes de Servidores e Clientes de e-mail podem ser exploradas para comprometer mecanismos de autenticação e violar a integridade dos sistemas de e-mail. A contribuição principal foi a identificação de 18 novas técnicas de evasão capazes de permitir a falsificação de assinaturas DKIM, a personificação de remetentes e o *bypass* de verificações de autenticação adotadas por grandes provedores. Ao testar tais explorações em múltiplos serviços e MUAs amplamente utilizados e demonstrar sua vulnerabilidade generalizada, o estudo revelou falhas sistêmicas que desafiam a confiabilidade das tecnologias mais comuns de autenticação.

Kambourakis, Gil e Sanchez (32) avaliaram, em larga escala, o nível de adoção dos principais padrões contemporâneos de segurança de e-mail pelos provedores — especialmente no tráfego SMTP de entrada e saída — por meio da ferramenta MECSA, desenvolvida para medir automaticamente o estado de segurança desses serviços. A contribuição principal do trabalho consistiu em disponibilizar a primeira análise longitudinal abrangente, baseada em mais de 7 mil avaliações ao longo de 15 meses, revelando avanços significativos na adoção de STARTTLS e SPF, mas também lacunas em DKIM, DMARC, MTA-STS e DNSSEC.

Maroofi, Korczyński e Duda (85) mediram a adoção dos protocolos SPF e DMARC entre domínios de alto perfil e avaliaram sistematicamente como a ausência ou a má configuração das regras possibilita o envio de e-mails falsificados. A principal contribuição residiu em fornecer uma análise detalhada — incluindo o “TOP500 domínios globais”, sites bancários e domínios registrados defensivamente — revelando que configurações incorretas são amplamente disseminadas, inclusive entre grandes empresas, e reforçando o entendimento de que essas falhas permitem que mensagens forjadas passem pelas verificações dos provedores. O estudo também avançou ao investigar, pela primeira vez, o papel dos subdomínios como vetor de abuso em *spoofing* e ao demonstrar que erros de sintaxe em SPF podem quebrar todo o modelo de confiança da autenticação por e-mail. Além disso, o trabalho contribuiu diretamente para a mitigação do problema ao envolver Equipes de Resposta a Incidentes de Segurança Computacional (CSIRTs) na correção de configurações errôneas.

Sustina, Fadlil e Riadi (63) demonstraram como a análise de cabeçalhos pode ser empregada como técnica de investigação forense para detectar e-mails falsificados, estabelecendo critérios simples e objetivos para identificar inconsistências estruturais em mensagens. A principal contribuição está em apresentar um método direto, acessível e de baixo custo que utiliza apenas a comparação de campos essenciais do cabeçalho — “From”, “Message-ID”, “Date” e “Received” — para diferenciar e-mails legítimos de mensagens manipuladas.

Shen et al. (55) investigaram como a cadeia de autenticação de e-mail pode ser comprometida por novas técnicas de ataque capazes de contornar mecanismos — como SPF, DKIM, DMARC e alertas de interface — revelando fragilidades estruturais do ecossistema. A principal contribuição da pesquisa foi a identificação de ataques inéditos, incluindo o ataque

conjunto do tipo “coquetel”, que permite a criação de e-mails falsificados altamente convincentes capazes de atravessar defesas de provedores renomados. Além disso, o estudo apresentou uma análise em larga escala demonstrando que 30 serviços de e-mail e 23 clientes permanecem vulneráveis, ao mesmo tempo em que propôs medidas de mitigação.

Maroofi, Korczynski e Hölzel (56) analisaram em escala global a adoção e a correta configuração dos mecanismos de autenticação SPF e DMARC, identificando falhas que facilitam o *spoofing* de domínio e possibilitam o envio bem-sucedido de mensagens forjadas. A contribuição principal consistiu em: (1) realizar uma das maiores medições já conduzidas, abrangendo 236 milhões de domínios; (2) desenvolver um algoritmo inovador capaz de identificar domínios registrados defensivamente e detectar configurações incorretas de SPF por meio da emulação da função *check_host()*; e (3) formular modelos de ameaça envolvendo *spoofing* de subdomínios, acompanhados de uma metodologia prática para mitigação baseada em boas práticas de configuração e análise de *logs* DNS. Além disso, o estudo demonstrou a eficácia de intervenções diretas ao apresentar os impactos de notificações enviadas a CSIRTs, oferecendo evidências de como ações coordenadas podem reduzir superfícies de ataque e melhorar significativamente a autenticação de e-mail.

Deccio et al. (65) avaliaram, em grande escala, como os servidores de e-mail realmente implementam e aplicam os mecanismos de autenticação SPF, DKIM e DMARC, analisando seu comportamento tanto diante de remetentes válidos quanto inválidos. A principal contribuição foi revelar que uma parcela significativa dos servidores adota validação SPF e que mais da metade implementa o trio completo de protocolos, embora com nuances e inconsistências na aderência às determinações das RFCs.

Tatang, Zettl e Holz (1) analisaram, de forma longitudinal e em larga escala, o estado de adoção, configuração e segurança dos principais mecanismos de autenticação de e-mail baseados em DNS — SPF, DKIM e DMARC — identificando tendências, falhas e impactos na segurança dos domínios. Os autores forneceram uma avaliação sobre esses mecanismos, confirmando crescimento significativo na adoção, mas também revelando que erros de configuração persistem, que o uso combinado das três tecnologias ainda é raro e que vulnerabilidades estruturais — como chaves DKIM fracas ou duplicadas — continuam presentes. O estudo ofereceu evidências de que, apesar dos avanços, a segurança global do e-mail permanece limitada pela adoção insuficiente e pela má configuração dos protocolos.

Yu et al. (74) estudaram o processo de transmissão de e-mails para identificar novas formas de ataques capazes de contornar mecanismos de autenticação e proteção amplamente adotados, como SPF, DMARC e funcionalidades de segurança dos MUAs. A principal contribuição do trabalho foi a descoberta de vetores de *bypass* inéditos, validados por experimentos em larga escala com provedores populares, evidenciando vulnerabilidades ainda presentes no ecossistema de e-mail. Além disso, o estudo demonstrou que a mitigação eficaz desses ataques exige uma postura padronizada de segurança entre todos os provedores, cobrindo cada nó da cadeia de entrega.

Marzuki, Hanif e Hariyadi (61) avaliaram a eficácia dos mecanismos de autenticação de e-mail (DKIM e SPF), bem como das ferramentas de filtragem antispam e antivírus, na prevenção de *spam*, *spoofing* e disseminação de *malware* por e-mail. A contribuição principal foi a implementação e análise de um sistema completo de proteção baseado na metodologia NDLC, demonstrando, por meio de simulações e testes, como DKIM e SPF atuam de maneira complementar para autenticação e controle de remetentes, enquanto soluções como SpamAssassin, ClamAV e Amavisd-New reforçam a defesa contra conteúdo malicioso.

Chauhan e Shah (3) avaliaram se os mecanismos modernos de segurança — SPF, DKIM, DMARC e demais extensões — são realmente capazes de impedir o *spoofing* de e-mail no ecossistema contemporâneo, considerando o estado das tecnologias até o final de 2022. A contribuição principal consistiu em testar empiricamente a afirmação de que, apesar de avanços importantes, o SMTP permanece intrinsecamente vulnerável, possibilitando que atacantes continuem falsificando remetentes mesmo frente à adoção crescente de protocolos antispooofing.

D'Angelone (53) desenvolveu uma ferramenta para medir, em larga escala, a adoção e a qualidade da implementação dos protocolos SPF e DMARC, superando limitações metodológicas presentes em pesquisas anteriores. A principal contribuição foi justamente a criação de um *domain crawler* capaz de analisar mais de 1,4 milhão de domínios e revelar, com precisão, padrões de conformidade — como a baixa adesão de domínios governamentais dos EUA à política DMARC obrigatória, por exemplo. O estudo também demonstrou, por meio de análise estatística, que a adoção dos protocolos está aumentando de forma significativa, enquanto as más configurações diminuem..

Jalda, Nanda e Pitchai (107) avaliaram diferentes abordagens de aprendizado de máquina para detecção de e-mail *spoofing* e demonstraram que um modelo baseado em *stacking* oferece desempenho superior em precisão e velocidade quando comparado a outros algoritmos tradicionais. A principal contribuição consistiu em propor uma arquitetura específica de *stacking* para identificar e-mails falsificados.

Li et al. (79) desenvolveram um método para detecção de e-mail *spoofing*, superando as limitações das abordagens tradicionais baseadas em *blacklists*, análise de conteúdo e mecanismos de autenticação, como SPF e DKIM. Os autores apresentaram o *SpoofingGuard*, um framework que utiliza aprendizado de representações em grafos para analisar caminhos de entrega presentes nos cabeçalhos dos e-mails — capturando, assim, características estruturais reais da infraestrutura de envio e recepção que, ao contrário dos cabeçalhos, não podem ser facilmente manipuladas por atacantes.

Zhang et al. (57) avaliaram a qualidade da implementação de SPF e DMARC em larga escala — incluindo uma análise específica de subdomínios — e demonstraram como falhas nessas configurações deixam domínios vulneráveis ao envio de e-mails falsificados. A principal contribuição foi revelar que, apesar do crescimento na adoção, a grande maioria dos domínios e subdomínios permanece inadequadamente configurada, permitindo a exploração em ataques de *spoofing*. Além disso, o estudo avançou ao propor novas metodologias de avaliação de

segurança, medidas práticas de mitigação e o sistema SMAEDS, uma solução proativa baseada em macros SPF capaz de detectar e bloquear e-mails anômalos antes que atinjam o usuário final.

Blechschtmidt e Stock (64) avaliaram o nível de segurança do ecossistema de e-mail, investigando a adoção, correta configuração e eficácia de mecanismos essenciais de proteção, como TLS, SPF, DKIM, DMARC, DANE e MTA-STS. Os autores ofereceram uma visão integrada sobre o estado da confidencialidade e integridade no e-mail, revelando vulnerabilidades persistentes — como certificados inválidos amplamente aceitos, baixa aplicação de autenticação de remetente e falta de validação de padrões críticos — que permitem interceptação e abuso por atacantes. O estudo demonstrou que, apesar de avanços graduais, a infraestrutura de e-mail ainda permanece suscetível a ataques sistêmicos.

Chauhan e Shah (62) examinaram as deficiências de segurança herdadas do SMTP e avaliaram a eficácia dos protocolos desenvolvidos para mitigar essas vulnerabilidades, como SPF, DKIM, DMARC, TLS e extensões relacionadas. A contribuição principal foi oferecer uma visão de como cada protocolo atua na proteção do ecossistema de e-mail, destacando seus potenciais, limitações e o grau de mitigação que realmente proporcionam diante de ameaças modernas; além de mapear lacunas remanescentes e comparar as contramedidas disponíveis.

Zhang et al. (89) mediram o nível de adoção dos protocolos SPF e DMARC entre os domínios mais populares da Internet, avaliando tanto a capacidade de envio quanto de recebimento de e-mails. A principal contribuição consistiu em revelar, com dados atualizados de 2023, que apesar do crescimento no uso desses protocolos, há também um aumento preocupante de registros inválidos e uma parcela significativa de servidores receptores — cerca de 27% — incapazes de validar SPF e DMARC corretamente.

Ragheb, Elmedany e Sharif (87) compararam a eficácia dos mecanismos de autenticação SPF e DKIM na proteção contra ameaças de falsificação e personificação de e-mail. A principal contribuição foi demonstrar, por meio de análise empírica, que embora ambos ofereçam camadas importantes de defesa, o DKIM apresenta desempenho superior por validar a integridade e a autenticidade do conteúdo da mensagem, indo além das capacidades do SPF.

Shukla, Misra e Varshney (92) objetivaram aprimorar métodos de detecção de e-mails falsificados utilizando técnicas de forense de memória e aprendizado de máquina, superando limitações identificadas em trabalhos anteriores. Os autores introduziram duas melhorias inovadoras: um módulo rápido e eficiente de validação de URLs — reduzindo significativamente o tempo de análise — e um modelo de aprendizado de máquina que incorpora campos modernos de cabeçalho (como BIMi e X-FraudScore) aos principais mecanismos de autenticação (SPF, DKIM, DMARC e ARC).

Hureau et al. (93) investigaram lacunas de entendimento, implementação e comportamento operacional do DMARC que impediriam sua adoção mais ampla. Os autores revelaram, por meio de metodologias de medição, que profissionais, ferramentas e proprietários de domínio

frequentemente interpretam ou configuram o DMARC de forma equivocada, resultando em comportamentos inesperados e riscos severos. Além disso, o estudo introduziu um *parser* de registros DMARC, uma metodologia de coleta de dados e uma análise do cenário de domínios, oferecendo bases técnicas e conceituais para melhorar o entendimento e a implementação do DMARC.

Sethuraman et al. (33) analisaram o ecossistema de correio eletrônico e seus mecanismos de segurança, identificando como vulnerabilidades em SMTP, cabeçalhos de e-mail, protocolos de autenticação e baixas taxas de adoção de medidas de proteção permitem a realização bem-sucedida de ataques de *spoofing* e *phishing*. O trabalho combinou experimentos com provedores de e-mail renomados — evidenciando que muitos ainda apresentam falhas exploráveis — com uma análise do papel dos fatores humanos na detecção de mensagens falsificadas e do uso de e-mail como canal de comando e controle por *malwares*. Além disso, sistematizaram e propuseram diversas estratégias de mitigação contra o *spoofing*.

Samonte et al. (29) analisaram o estado das técnicas antispoofing aplicadas ao *e-commerce* e propuseram formas mais robustas e acessíveis de integrar autenticação de e-mail às práticas de marketing digital das empresas. Sua principal contribuição consistiu em revisar de forma abrangente os mecanismos existentes — como SPF, DKIM e DMARC — identificando suas limitações no contexto do comércio eletrônico, bem como sugerir novas direções para fortalecer a segurança das comunicações entre empresas e clientes.

Ma et al. (31) analisaram as vulnerabilidades presentes no *Delegation Mechanism* dos protocolos de e-mail e demonstraram como a ausência de validação do campo “Sender” permite que atacantes contornem mecanismos de autenticação como DKIM e DMARC, enviando e-mails altamente convincentes. As principais contribuições foram: (1) revelar que provedores populares aceitam e entregam mensagens com “Sender” falsificado; (2) demonstrar que metade dos destinatários não consegue perceber a falsificação; (3) propor novos vetores de ataque capazes de passar por todas as extensões de segurança existentes; e (4) apresentar um esquema de validação e recomendações de design para mitigar essas falhas.

Li et al. (73) analisaram as limitações das estratégias atuais de combate ao *phishing* e, especialmente, ao *spear phishing*, destacando a dificuldade persistente de verificar com segurança a autenticidade do remetente. A contribuição principal foi a proposição de um novo esquema de assinatura digital, que automatiza o uso de chaves públicas e privadas geradas por sessão, tornando o processo transparente para o usuário e superando as barreiras tradicionais de custo e complexidade das assinaturas digitais.

Anitha et al. (4) desenvolveram e demonstraram um sistema capaz de detectar e-mails falsificados combinando análise de conteúdo baseada em aprendizado de máquina com validação de autenticação de domínio via SPF e DMARC. Os autores criaram uma solução híbrida que avalia simultaneamente a origem e o conteúdo das mensagens — algo ausente em muitas abordagens tradicionais — utilizando TF-IDF e *Random Forest* para classificação, além de integração segura via Gmail API e OAuth 2.0.

Wang et al. (68) realizaram a primeira avaliação do impacto do *SMTP smuggling*, identificando a magnitude da vulnerabilidade em serviços públicos e privados de e-mail, softwares de código aberto e *gateways* de segurança. A principal contribuição revelou, com base em medições empíricas e metodologias éticas inovadoras, que a vulnerabilidade é amplamente explorável mesmo após sua divulgação pública, possibilitando *spoofing* de domínios altamente confiáveis e *bypass* de mecanismos como SPF e DMARC.

Azkia, Soleha e Nariswari (86) avaliaram experimentalmente a eficácia dos protocolos SPF, DKIM e DMARC na prevenção de ataques de *phishing* e na detecção de remetentes falsificados. Os autores demonstraram, por meio de simulações em ambiente controlado, que a integração desses três mecanismos de autenticação oferece uma defesa significativamente robusta contra *spoofing*. O trabalho fornece evidências práticas de que a adoção combinada desses protocolos melhora a filtragem de e-mails falsificados, reduz riscos para organizações e usuários finais e representa uma solução viável e acessível para aumentar a segurança do ecossistema de e-mail.

Garcia, Nunes e Souza Neto (106) apresentaram e validaram a metodologia Q.U.A.S.E. como um framework prático, simples e de baixo custo para auxiliar usuários finais a identificar sinais de *phishing* em e-mails. Sua principal contribuição foi oferecer um modelo de avaliação baseado em apenas cinco elementos, permitindo que qualquer usuário — independentemente de experiência técnica — realize análises rápidas e eficazes de mensagens suspeitas.

Mane et al. (81) desenvolveram um mecanismo de detecção de e-mail *spoofing* capaz de identificar inconsistências nos cabeçalhos de e-mail em nível de servidor, combinando práticas modernas de segurança cibernética com técnicas de inteligência artificial. A principal contribuição consistiu em demonstrar que anomalias em campos essenciais dos cabeçalhos — como endereço IP, remetente e parâmetros de entrega — podem ser usadas como indicadores de falsificação, permitindo que sistemas de e-mail rejeitem mensagens maliciosas antes que alcancem o usuário final.

3. MATERIAIS E MÉTODOS

Este capítulo apresenta os materiais e procedimentos metodológicos empregados para o alcance dos objetivos delineados nesta pesquisa. Inicialmente, descreve-se o processo de concepção e desenvolvimento da ferramenta *StopEmailSpoofing*, instrumento criado para automatizar a coleta de registros DNS e a avaliação das taxas de adoção e conformidade dos protocolos SPF, DKIM e DMARC pelos domínios analisados. Em seguida, expõe-se o critério adotado para a seleção da amostragem, correspondente à totalidade dos domínios vinculados aos órgãos da APF que operam correio eletrônico, bem como o agrupamento desses órgãos por área de atuação, escolha feita para preservar o anonimato das instituições vulneráveis. Na sequência, detalham-se os procedimentos de coleta e de análise dos dados, conduzidos mensalmente ao longo de dezoito meses, e, por fim, as ações de mitigação propostas ao longo do período. Busca-se, com isso, oferecer uma descrição transparente e reprodutível do percurso metodológico que fundamenta os resultados apresentados no capítulo subsequente.

3.1. CONSTRUÇÃO DO INSTRUMENTO DE PESQUISA: *STOPEMAILSPOOFING*

Para viabilizar os objetivos de: (a) coletar os registros DNS dos domínios dos órgãos da APF; (b) constatar a adoção e a conformidade das regras SPF, DKIM e DMARC; e (c) classificar a vulnerabilidade de cada domínio; faz-se necessária a utilização de ferramenta que automatize e facilite este processo.

Diversas ferramentas para detecção de vulnerabilidades relacionadas à falsificação de endereços de e-mail já foram propostas ao longo dos anos. A solução *MXToolbox SuperTool*², por exemplo, é um utilitário de avaliação de serviços de e-mail e DNS, integrando múltiplas funcionalidades de verificação em uma interface web. O sistema aceita um domínio, um endereço IP ou um *hostname* como entrada, mantendo um histórico cronológico dos resultados para referência futura (119). Entretanto, existem limitações que comprometem sua eficácia no contexto desta pesquisa. A ferramenta não oferece código-fonte aberto, não permite automatização para análise em massa de múltiplos domínios e não integra todas as verificações em uma única interface, o que obriga o usuário a recorrer a consultas fragmentadas e manuais. Mais gravemente, o *MXToolbox SuperTool* falha em informar explicitamente se o domínio analisado é ou não vulnerável a *spoofing* de e-mail, não realiza classificação de níveis ou tipos de vulnerabilidade, tampouco cobre todas as combinações possíveis entre registros SPF, DKIM e DMARC que poderiam gerar cenários de risco. Acrescenta-se a isso a ausência de suporte a subdomínios e a impossibilidade de exportação em formato tabular (CSV ou similar), o que inviabiliza análises escaláveis e auditorias em larga escala.

² <https://mxtoolbox.com/SuperTool.aspx>

D’Angelone (53) propôs uma ferramenta de medição em larga escala para avaliar a adoção dos protocolos SPF e DMARC. O sistema opera por meio de um *crawler* de domínios que coleta os dados necessários por meio de APIs comerciais ou de arquivos CSV. A ferramenta executa consultas DNS automatizadas para verificar a presença, a configuração e as políticas dos registros SPF e DMARC, normalizando os resultados e identificando erros de configuração. Os dados são processados e armazenados em formato tabular, permitindo geração de gráficos, análises comparativas e reprodução experimental (119). Contudo, embora o trabalho de D’Angelone mencione que a ferramenta é de código aberto, não foi possível encontrá-lo em fontes abertas. Mais criticamente, a solução não oferece suporte a subdomínios, ignora a verificação de DKIM, não avalia os parâmetros “aspf” e “sp” do DMARC e, sobretudo, não informa ao usuário se o domínio é ou não vulnerável ao *spoofing* de e-mail, tampouco realiza a classificação de níveis ou tipos de vulnerabilidade. A ferramenta também não fornece instruções personalizadas para correção de más configurações (53).

A *Global Cyber Alliance*, organização sem fins lucrativos internacional dedicada à redução de riscos cibernéticos e à promoção de um ambiente digital mais seguro, desenvolveu recursos para fortalecer a autenticação de e-mail e a proteção de domínios, destacando-se o *DMARC Guide*³ e o *Domain Security Scanner*⁴. O *DMARC Guide* é um guia prático e interativo que orienta organizações na análise, criação e implementação de políticas de SPF, DKIM e DMARC. Complementarmente, o *Domain Security Scanner* é uma solução de código aberto que realiza varreduras automatizadas — individuais ou em massa — dos registros DNS, fornecendo recomendações, suporte a CLI e API, e integração via caixa de correio. Os principais problemas da ferramenta consistem em não oferecer suporte a subdomínios e falhar na verificação de parâmetros críticos do DMARC, como “aspf” e “sp”. A solução também não informa explicitamente ao usuário se o domínio é ou não vulnerável a *spoofing* de e-mail, não realiza qualquer classificação de níveis ou tipos de vulnerabilidade e não cobre todas as combinações possíveis entre os registros SPF, DKIM e DMARC que poderiam gerar cenários de risco.

Uma excelente solução nacional, elaborada pelo NIC.br, é o Teste TOP E-mail, que verifica, a partir do domínio informado, se o serviço de e-mail atende aos principais padrões técnicos modernos da Internet. Ao final, o usuário recebe um relatório com percentual de conformidade às melhores práticas, além de resultados detalhados por categoria e subteste, sendo possível utilizar esse relatório para melhorar as configurações. Contudo, o [NIC.br](https://nic.br) não disponibiliza o código-fonte e a ferramenta não aceita automação para análise de múltiplos domínios, tampouco oferece suporte a subdomínios. Ademais, deixa de verificar parâmetros importantes do protocolo DMARC (“aspf” e “sp”), não realiza a classificação de níveis ou tipos de vulnerabilidade e falha em cobrir todas as combinações possíveis entre os registros SPF e DMARC. Por fim, a impossibilidade de exportar resultados em formato tabular representa outra limitação relevante para análises em volume.

³ <https://dmarcguide.globalcyberalliance.org/>

⁴ <https://github.com/GlobalCyberAlliance/domain-security-scanner>

A ferramenta de maior destaque para os objetivos da presente pesquisa é o *Spoofy*⁵. Desenvolvida em 2023 e disponibilizada em código-aberto por Matthew Keeley, é uma evolução das soluções *SpoofCheckSelfTest*⁶ (2015) e *SpoofCheck*⁷ (2016) da empresa *Bishop Fox* e oferece um diagnóstico automatizado da vulnerabilidade de domínios a *spoofing* de e-mail através da análise das configurações SPF e DMARC. O sistema executa consultas DNS autoritativas e implementa um algoritmo de decisão para determinar a suscetibilidade dos domínios à falsificação. Os resultados são processados por meio de uma tabela de combinações entre SPF e DMARC. Todavia, a referida tabela foi construída a partir de testes empíricos que consistiram no envio de mensagens falsificadas (utilizando a ferramenta *EmailSpoofTest.com*⁸) e na observação do comportamento de serviços como *Gmail*, *ProtonMail* e *Microsoft 365* ao receberem estas mensagens. Esta abordagem apresenta algumas limitações metodológicas. Considerando-se o objetivo de detectar a vulnerabilidade em domínios (e não em MTAs/MUAs), as medidas efetivas para reduzir a exposição a ataques de *spoofing* baseiam-se unicamente na configuração correta das extensões SMTP (SPF, DKIM e DMARC) no DNS do domínio. Realizar um diagnóstico com base no comportamento específico de determinados MTAs/MUAs pode levar a uma falsa conclusão quanto à segurança. Isso porque a vítima das mensagens falsificadas pode utilizar qualquer outro MTA/MUA que não tenha sido contemplado nos testes. É válido lembrar que as decisões de autenticação de cada MTA/MUA podem diferir das orientações configuradas nas extensões SMTP e ser complementadas, ou mesmo sobrepostas, por mecanismos de filtragem antispam (119).

Na mesma linha, a partir da abordagem escolhida, o *Spoofy* agrupa os estados de vulnerabilidade em 8 categorias, sendo algumas dessas classificadas como “*Mailbox Dependant*”. Repisa-se que não se pode depender do comportamento do MTA/MUA para a avaliação da vulnerabilidade intrínseca a um nome de domínio. Logo, uma ferramenta com o objetivo de avaliar a vulnerabilidade de um domínio à falsificação deveria concentrar-se unicamente nas configurações declaradas no DNS por meio das extensões SMTP, sem requerer resultados obtidos a partir da interpretação de MTAs/MUAs específicos. Somente assim seria possível fornecer uma avaliação alinhada às reais possibilidades de intervenção dos administradores de domínio. Por fim, a tabela de combinações do *Spoofy* não considera todas as combinações possíveis entre “all”, “aspf”, “p” e “sp” (119). São as más configurações combinadas destes quatro itens que acarretam os diversos tipos de vulnerabilidade de *spoofing* de e-mail, logo, todas as combinações possíveis precisam ser levadas em consideração.

Frente ao exposto, com o objetivo de oferecer aos administradores de domínios uma ferramenta capaz de automatizar a detecção de vulnerabilidades e sugerir correções às inconsistências de maneira precisa, este autor propôs a solução *StopEmailSpoofing*⁹ (119). Trata-se de um aprimoramento das soluções já existentes por, em uma única ferramenta: (a)

⁵ <https://github.com/MattKeeley/Spoofy>

⁶ <https://github.com/BishopFox/SpoofcheckSelfTest>

⁷ <https://web.archive.org/web/20220211170519/https://github.com/BishopFox/spoofcheck>

⁸ <https://emailspooftest.com/>

⁹ <https://github.com/vlsc0/stopemailspoofing>

cobrir todas as possibilidades de combinação entre “all”, “aspf”, “p” e “sp” que podem influenciar na suscetibilidade de um domínio principal, bem como de seus subdomínios, à falsificação de e-mail; (b) informar ao usuário a situação e o tipo de vulnerabilidade que o domínio se encontra frente à ameaça; (c) oferecer sugestões imediatas e precisas de mitigação personalizadas para cada domínio avaliado; (d) verificar a possível adoção de DKIM; (e) permitir a automatização para comportar a coleta e a análise de diversos domínios simultaneamente; (f) retornar resultados em formato tabular; e (g) ser de código aberto. Uma comparação entre o instrumento apresentado e as ferramentas similares mencionadas está apresentada no Quadro 3.1.

Quadro 3.1. Comparação do *StopEmailSpoofing* com as outras ferramentas mencionadas

		MXToolbox SuperTool	D’Angelone	DMARC Guide / Domain Security Scanner	Test TOP E-mail	Spoofy	StopEmail Spoofing
Código-fonte disponível?		✗	✗	✓	✗	✓	✓
Aceita automatização para análise de diversos domínios?		✗	✓	✓	✗	✓	✓
Checagens integradas em uma única interface?		✗	✓	✓	✓	✓	✓
Checa se os domínios têm registro MX?		✓	✗	✓	✓	✗	✓
Checa se são subdomínios ou domínios principais?		✓	✗	✗	✗	✓	✓
Checagem da existência e da conformidade de SPF?		✓	✓	✓	✓	✓	✓
DMARC	Checa "p"?	✓	✓	✓	✓	✓	✓
	Checa "aspf"?	✓	✗	✗	✗	✓	✓
	Checa "sp"?	✓	✗	✗	✗	✓	✓
Tentativa de checagem de DKIM?		✓	✗	✓	✓	✓	✓
Informa ao usuário se o domínio é ou não vulnerável a <i>spoofing</i> de e-mail?		✗	✗	✗	✓	✓	✓
Faz classificação de níveis ou tipos de vulnerabilidade?		✗	✗	✗	✗	✓	✓
Cobre todas as combinações possíveis entre os registros que poderiam levar à situação de vulnerabilidade?		✗	✗	✗	✗	✗	✓

Funciona para subdomínios?	✗	✗	✗	✗	✓	✓
Oferece instruções personalizadas para conformidade ou mitigação?	✓	✗	✓	✓	✗	✓
Permite saída em formato tabular (.csv ou similares), facilitando análise de grande quantidade de dados?	✗	✓	✓	✗	✓	✓

Ao utilizar o *StopEmailSpoofing*, os usuários podem escolher enviar um único domínio ou uma lista deles para a avaliação. Por meio de consultas DNS, além de verificar se os domínios fornecidos são domínios principais ou subdomínios e obter registros SOA (*Start of Authority*), NS (*Nameserver*) e MX (*Mail Exchange*), a ferramenta coleta os registros SPF e DMARC e, considerando a configuração combinada desses registros (especialmente entre “all”, “aspf”, “p” e “sp”), realiza conclusões quanto à suscetibilidade dos domínios analisados às categorias de vulnerabilidade à falsificação de e-mail dispostas no Quadro 3.2. Por fim, a partir da conclusão quanto à vulnerabilidade do domínio, a ferramenta aponta ações detalhadas de mitigação, como exemplificado na Figura 3.1, para que o administrador possa sanar o problema e ampliar a segurança da autenticação (119).

Quadro 3.2. Categorias de vulnerabilidade à falsificação consideradas pela ferramenta

Categoria	Explicação
1	A falsificação do domínio principal e de subdomínios é possível.
2	Apenas a falsificação do domínio principal é possível.
3	Apenas a falsificação de subdomínios é possível.
4	Condição desconhecida (possivelmente vulnerável devido a erro de sintaxe nos registros).
5	A falsificação não é possível.

Fonte: CANDIDO et al. (119)

```

Spoofing:
[*] Spoofability: Organizational domain spoofing and subdomain spoofing are possible.

For additional security it is recommended:
SPF All Mechanism: Keep it the way it is.
DMARC Policy (p=): Replace it by "p=reject" or "p=quarantine".
DMARC ASPF (aspf=): Add "aspf=s" or "aspf=r".
DMARC Subdomain Policy (sp=): Add "sp=reject" or "sp=quarantine".
DMARC PCT: Consider adding pct=100.
DKIM: Make sure to have DKIM record set up.
BIMI: Consider setting up a BIMI record.

Results saved in results.csv

```

Figura 3.1. Exemplo de saída da ferramenta com sugestões de mitigação

Fonte: CANDIDO et al. (119)

As conclusões sobre o estado de vulnerabilidade e as sugestões de mitigação são feitas a partir do que se dispõe em uma tabela¹⁰ que relaciona todas as 295 combinações possíveis entre o mecanismo “all” do registro SPF e as tags “aspf”, “p” e “sp” do registro DMARC, tanto para domínio principal quanto para os subdomínios, conforme mostrado na Figura 3.2 (119). Para testes e validações empíricas do preconizado na referida tabela, dois domínios foram adquiridos: um para atuar como remetente e outro como destinatário. As extensões SMTP do domínio remetente foram alteradas no DNS conforme cada caso analisado. O domínio destinatário foi vinculado a um servidor de e-mails *mailcow*¹¹ com a solução antispam *Rspamd*¹² embutida, o que permitiu o controle dos mecanismos de autenticação e a checagem do processamento das mensagens (por meio do cabeçalho “Authentication-Results”) (119). Conferências foram realizadas, quando necessário, utilizando as diversas ferramentas similares elencadas anteriormente.

Progressivamente, o *StopEmailSpoofing* também coleta registros de DKIM e BIML. Ressalta-se que, para a coleta de DKIM, é necessário conhecer o seletor “s=” utilizado no registro, o que somente seria possível com acesso a uma mensagem de e-mail legítima enviada a partir do domínio analisado, uma vez que este seletor não é exibido publicamente nos registros DNS. Desta forma, a ferramenta utiliza uma lista de 100 seletores comuns para realizar as consultas e tentar identificar a presença de DKIM. Portanto, a conclusão da ferramenta refere-se a ter ou não encontrado o registro DKIM e, em caso negativo, sugerir que o administrador se certifique de ter configurado a extensão, uma vez que não é possível afirmar com certeza que ela não foi adotada (119).

ALL	P	ASPF	SP	DOMAIN TYPE	RESULT	SPOOFABILITY
~all	none	No aspf=	quarantine	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
				SUBDOMAIN	QUARANTINE	
~all	none	No aspf=	reject	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
				SUBDOMAIN	REJECT	
~all	none	r	No sp=	ORG. DOMAIN	INBOX	Organizational domain spoofing and subdomain spoofing are possible.
				SUBDOMAIN	INBOX	
~all	none	r	none	ORG. DOMAIN	INBOX	Organizational domain spoofing and subdomain spoofing are possible.
				SUBDOMAIN	INBOX	
~all	none	r	quarantine	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
				SUBDOMAIN	QUARANTINE	
~all	none	r	reject	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
				SUBDOMAIN	REJECT	
~all	none	s	No sp=	ORG. DOMAIN	INBOX	Organizational domain spoofing and subdomain spoofing are possible.
				SUBDOMAIN	INBOX	
~all	none	s	none	ORG. DOMAIN	INBOX	Organizational domain spoofing and subdomain spoofing are possible.
				SUBDOMAIN	INBOX	
~all	none	s	quarantine	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
				SUBDOMAIN	QUARANTINE	
~all	none	s	reject	ORG. DOMAIN	INBOX	Only organizational domain spoofing is possible.
				SUBDOMAIN	REJECT	
~all	quarantine	No aspf=	No sp=	ORG. DOMAIN	QUARANTINE	Spoofing is not possible.
				SUBDOMAIN	QUARANTINE	

Figura 3.2. Exemplo de combinações de mecanismos e tags SPF/DMARC e a situação de vulnerabilidade correspondente consideradas pela ferramenta

Fonte: CANDIDO et al. (119)

A solução ainda verifica se o servidor de e-mail do domínio adota uma política de *catch-all*. *Catch-all* é uma configuração que permite ao servidor receber mensagens enviadas para endereços de e-mail inexistentes no domínio. Em vez de rejeitar ou devolver as mensagens enviadas para endereços errados, o servidor redireciona todas elas para uma conta de e-mail

¹⁰ https://github.com/v1sc0/stopemailspoofing/blob/main/ULTIMATE_TABLE.xlsx

¹¹ <https://mailcow.email/>

¹² <https://rspamd.com/>

designada como *catch-all*. Isso pode ser útil para reduzir a enumeração e a validação de endereços de e-mail por parte de atacantes, uma vez que a resposta do servidor SMTP não permitirá que confirmem a existência de endereços coletados e que, provavelmente, se tornariam alvos em uma campanha de *phishing* (119).

Todos os resultados das avaliações feitas pela ferramenta são apresentados na interface textual via terminal (stdout) e salvos em formato CSV, permitindo a integração com outras aplicações de tratamento e análise de dados. A ferramenta foi desenvolvida em Go (*Golang*), por ser uma linguagem de programação que oferece vantagens quanto à utilização, alteração e acréscimo de módulos. Uma descrição dos módulos desenvolvidos para a aplicação e um fluxograma do seu funcionamento podem ser encontrados no Quadro 3.3 e na Figura 3.3, respectivamente (119).

Quadro 3.3. Módulos que compõem a ferramenta

Módulo	Descrição
dns.go	Classifica o nome informado como domínio ou subdomínio usando a biblioteca “publicsuffix”. Em seguida, “ObterSOARecord” consulta o registro SOA do domínio; se o registro for encontrado, armazena o nome do nameserver e procura seu endereço IP. Já “ObterMXRecords” busca registros MX para listar os servidores de e-mail associados.
catchall.go	Usa a biblioteca “AfterShip/email-verifier” para verificar se um domínio aceita e-mails de qualquer endereço. A função “NovoCatchAllVerifier” cria um verificador com checagem SMTP habilitada. O método “VerificarCatchAll” verifica se o domínio possui registro MX; em caso afirmativo, realiza uma verificação SMTP para determinar se a caixa é <i>catch-all</i> e, então, preenche a estrutura “CatchAllResult”.
dkim.go	Define a estrutura “DKIMResult” e a lista de 100 seletores comuns usados por diversos provedores. A função “VerificarDKIM” recebe uma lista de domínios, valida o nome de cada domínio e, para cada seletor padrão, monta uma consulta do tipo “seletor._domainkey.<domínio>”; se encontrar um registro TXT contendo uma chave DKIM, marca o resultado como “SIM” e armazena o registro. Caso nenhum seletor retorne resposta positiva, indica que o DKIM não foi encontrado.
bimi.go	Define a estrutura “BIMI” com campos para o domínio, o servidor DNS e informações extraídas do registro BIMI. O construtor “NovoBIMI” consulta “default._bimi.<domínio>” via DNS, salvando o registro textual se este contiver “v=BIMI” e extraíndo a versão, a localização do logotipo e a autoridade por meio das funções “ExtrairVersao”, “ExtrairLocalizacao” e “ExtrairAutoridade”. Caso o registro não exista, o campo “BIMIRecord” é definido como “BIMI não encontrado”.
spf.go	A estrutura “SPF” inclui o domínio, o registro SPF e as informações derivadas. “NovoSPF” chama “ObterSPFRecord”, que procura, nos registros TXT, um início com “v=spf1”; se encontrado, armazena o registro. Depois, “ObterMecanismoAll” identifica o mecanismo “all”;

Módulo	Descrição
	“ContarConsultasDNS” analisa recursivamente as diretivas “include” e “redirect”, bem como os mecanismos “a”, “mx”, “ptr” e “exists”, para contar quantas consultas DNS o SPF realiza. Se esse número exceder 10, “TooManyDNSQueries” é marcado como verdadeiro.
dmARC.go	A estrutura “DMARC” guarda o domínio, servidor DNS e campos extraídos. “NovoDMARC” chama “ObterDMARCRecord” para consultar “_dmarc.<domínio>”; se o domínio for um subdomínio sem registro DMARC, tenta o domínio organizacional (eTLD+1). Após localizar um registro contendo “DMARC1”, a estrutura extrai a política “p=”, o percentual “pct=”, o alinhamento SPF “aspf=”, a política para subdomínios “sp=” e os endereços para relatórios forenses e agregados.
spoofing.go	Define a estrutura de “Spoofing” para combinar as informações de SPF e DMARC. A função “CheckSpoofing” verifica várias combinações dessas configurações para determinar se é possível falsificar o domínio. Ela usa a supracitada tabela de condições para identificar cenários em que o <i>spoofing</i> não é possível, é possível apenas para o domínio organizacional, é possível apenas para subdomínios, ou é totalmente possível. Retorna uma mensagem explicativa que indica o nível de vulnerabilidade.
suggestion.go	Oferece recomendações de segurança. A função “Suggestion” avalia o mecanismo “all” do SPF e as opções DMARC (“p”, “aspf” e “sp”). Dependendo dos valores, sugere manter, corrigir ou adicionar configurações.

Fonte: Adaptado de CANDIDO et al. (119)

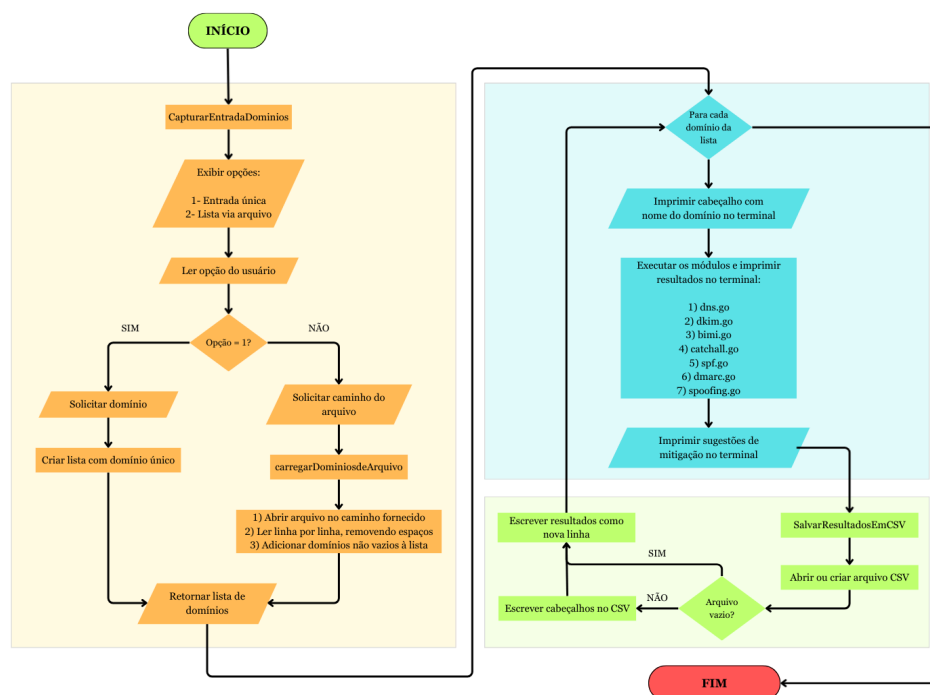


Figura 3.3. Fluxograma de funcionamento da ferramenta proposta

Fonte: CANDIDO et al. (119)

3.1.1. Validação do instrumento e trabalho publicado

Realizou-se, em dezembro de 2024, um estudo de caso com uma amostragem composta pelos domínios das instituições públicas de ensino superior brasileiras a fim de validar a eficiência e a confiabilidade da ferramenta desenvolvida.

Este grupo específico de instituições foi escolhido por constituir uma área da administração pública que desenvolve pesquisas, tecnologias e conhecimentos sensíveis, sendo flagrante a importância da mitigação das vulnerabilidades de falsificação de endereços de e-mail para combater campanhas de *phishing* que possam comprometer esta produção.

Uma lista das instituições de ensino superior brasileiras foi obtida a partir do website do Ministério da Educação¹³. A lista foi filtrada para incluir apenas as instituições públicas, resultando num universo de 345 instituições. Os nomes de domínio destas instituições foram coletados por meio de técnicas de OSINT. Por fim, a lista final com os 345 domínios foi submetida à ferramenta *StopEmailSpoofing* (119).

Para apresentar a ferramenta à comunidade acadêmica, uma nova coleta foi executada nesta amostragem em agosto de 2025 e, a partir desta atualização, elaborou-se o artigo “StopEmailSpoofing: uma solução para detecção de vulnerabilidade de domínios à ataques de falsificação de e-mail” que foi submetido à Revista Ibérica de Sistemas e Tecnologias de Informação (RISTI) em 14 de setembro de 2025. A RISTI aceitou o artigo em 16 de novembro do mesmo ano e publicou-o entre as páginas 57 e 73 de sua edição de nº 60 (dez. 2025). O artigo está disponível em: <https://scielo.pt/pdf/risti/n60/2183-0126-risti-60-57.pdf> (DOI: 10.17013/risti.60.57-73) e a Figura 3.4 traz uma representação de sua página inaugural.

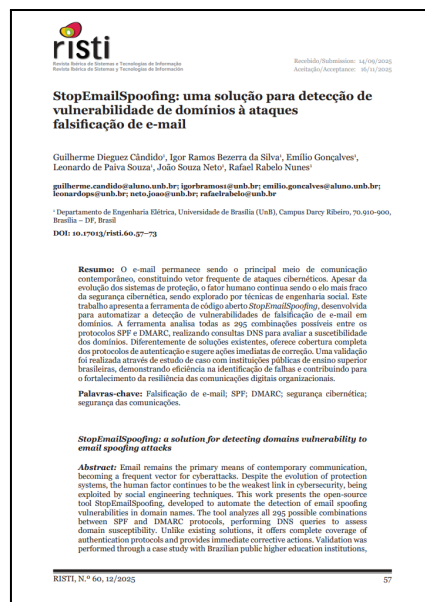


Figura 3.4. Captura de tela do frontispício do trabalho publicado.
Fonte: RISTI (119).

3.1.2. Registro de Software

Concluídos o desenvolvimento e os testes de validação, a ferramenta *StopEmailSpoofing* foi, com o auxílio do Núcleo de Propriedade Intelectual (Nupitec) da Universidade de Brasília (UnB), registrada junto ao Instituto Nacional da Propriedade Industrial (INPI). A Diretoria de Patentes, Programas de Computador e Topografias de Circuitos do INPI expediu, em 9 de dezembro de 2025, o Certificado de Registro de Programa de Computador (constante do Anexo A) sob o Processo nº BR512025006327-0, de titularidade da Fundação Universidade de Brasília. Classificando-o como PD01 – Segurança e Proteção de Dados na categoria TC04-SERV/REDES (Serviços, Redes, Estações e Material de Telecomunicações), o certificado garante ao software proteção legal pelo prazo de 50 anos, a contar de 1º de janeiro do ano subsequente à data de publicação, em conformidade com o § 2º do art. 2º da Lei nº 9.609, de 19 de fevereiro de 1998.

Conforme já mencionado, o código-fonte encontra-se disponível publicamente em <https://github.com/v1sc0/stopemailspoofing>, garantindo auditoria e reprodutibilidade à pesquisa.

3.2. SELEÇÃO DA AMOSTRAGEM

Na presente pesquisa, haja vista tratar-se de população finita, realizou-se uma seleção censitária, ou seja, foram incluídos todos os nomes de domínio relacionados a cada um dos órgãos da APF, desde que utilizados para a troca de mensagens eletrônicas.

Para identificar os órgãos que compõem a APF, recorreu-se à página oficial do governo da República Federativa do Brasil¹⁴, na qual constavam 331 órgãos federais pertencentes aos Poderes Executivo, Legislativo e Judiciário. A partir desta lista, coletou-se, por intermédio de técnicas de Inteligência de Fontes Abertas (OSINT), os nomes de domínio utilizados por cada órgão.

Constatou-se, na sequência, ainda por OSINT, que alguns órgãos não possuíam domínios próprios ou, ainda que possuindo, não os utilizavam para comunicações de correio eletrônico, — por não terem servidores MX registrados em seu DNS ou por utilizarem o domínio de um órgão superior para este tipo de comunicação, por exemplo. Desta forma, estes órgãos foram removidos da amostra por não atenderem aos requisitos necessários à consecução dos objetivos deste trabalho, restando 281 órgãos na amostragem final.

Optou-se por agrupar estes 281 órgãos por áreas de atuação, para que a publicização dos resultados da pesquisa não revelasse vulnerabilidades individuais que pudessem impactar a reputação dos órgãos ou divulgar diretamente a possíveis adversários quais órgãos encontram-se vulneráveis a serem explorados em ataques de *spoofing* de e-mail durante campanhas de *phishing*.

¹⁴ <https://www.gov.br/pt-br/orgaos>

As áreas de atuação foram escolhidas de acordo com a classificação utilizada no Portal da Transparência do Governo Federal¹⁵ para detalhar a execução de despesas governamentais, conforme se observa na Figura 3.5. Adaptou-se esta lista, agrupando algumas áreas de atuação que contavam com poucos órgãos, mais uma vez, a fim de não expô-los a ataques direcionados. Ao final, os 281 órgãos foram distribuídos em 12 grupos, conforme exibido no Quadro 3.4.

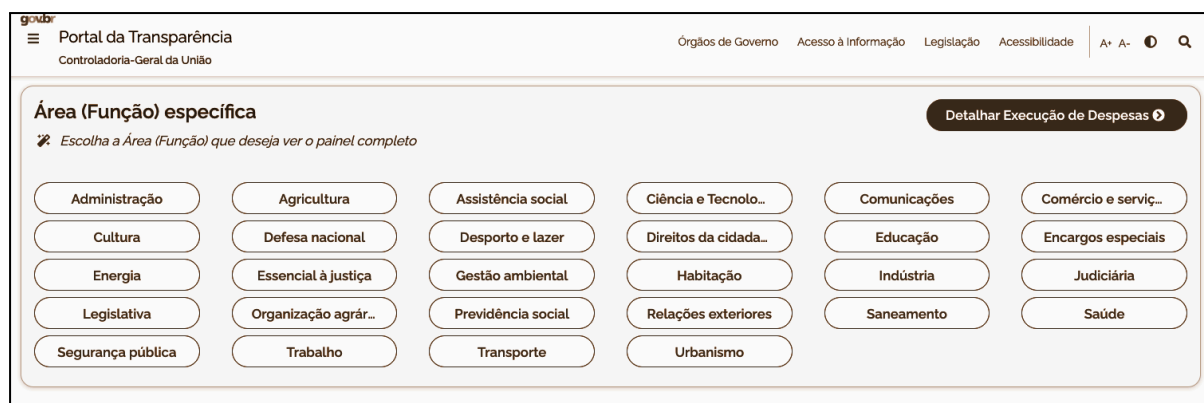


Figura 3.5. Áreas de atuação utilizadas para detalhar execução de despesas governamentais

Fonte: <https://portaldatransparencia.gov.br/funcoes>

Quadro 3.4. Agrupamento dos órgãos da amostra por área de atuação

Área de Atuação	Quantidade de órgãos no grupo
Administração e Economia	23
Agricultura e Organização Agrária	10
Previdência, Assistência Social, Trabalho e Habitação	13
Ciência, Tecnologia e Comunicações	16
Cultura e Educação	123
Defesa nacional, Segurança pública e Relações Exteriores	14
Desporto, Lazer e Direitos da Cidadania	10
Energia e Gestão Ambiental	20
Indústria, Comércio e Serviços	6
Legislativo, Judiciário e Essenciais à Justiça	10
Saúde e Saneamento	12
Transporte e Urbanismo	24

Ressalta-se que os referidos grupos foram formados apenas para fins de exibição dos resultados, tendo todas as coletas, análises e ações de mitigação sido feitas individualmente junto a cada órgão.

¹⁵ <https://portaldatransparencia.gov.br/funcoes>

3.3. COLETA E ANÁLISE DE DADOS

De posse da lista composta pelos 281 domínios vinculados a cada órgão, iniciou-se as coletas dos registros DNS — e consequentemente das configurações de SPF, DKIM e DMARC — por meio da ferramenta *StopEmailSpoofing*. Ao todo foram feitas 18 coletas mensais, executadas entre os dias 10 e 15 de cada mês, começando em fevereiro de 2025 e findando em julho de 2026. Os dados, exportados a partir da ferramenta em formato “.csv”, alimentaram uma planilha eletrônica para tabulação e com vias a acompanhar o estado de vulnerabilidade dos órgãos e a eficácia das ações de mitigação propostas ao longo do período. Metodologicamente, estabeleceu-se que a presença de qualquer um dos quatro cenários de vulnerabilidade, quais sejam “Completamente Vulnerável”, “Apenas Subdomínios Vulneráveis”, “Apenas Domínio Principal Vulnerável” ou “Erro de Sintaxe”, classifica um domínio como vulnerável, independentemente das gradações de severidade entre eles.

3.4. AÇÕES VISANDO A MITIGAÇÃO

As cinco primeiras coletas, de fevereiro a junho de 2025, foram feitas sem qualquer proposta de mitigação por parte deste pesquisador. O objetivo foi o de realizar uma observação passiva, constatar o estado de vulnerabilidade da APF frente à vulnerabilidade de *spoofing* de e-mail e obter indícios de que o problema não estava recebendo a devida atenção, uma vez que, se verdadeira a hipótese, pouca alteração seria percebida nestes primeiros cinco meses.

Em seguida, os resultados da coleta de junho de 2025 foram apresentados ao PNPC da ABIN. O referido Programa, por sua vez, produziu e difundiu, no início do mês subsequente, relatórios para órgãos do SISBIN que estavam em situação de vulnerabilidade e convidou-os para uma palestra de conscientização sobre a ameaça. A palestra ocorreu presencialmente em Brasília/DF no dia 18 de julho 2025, tendo sido proferida por este autor. Nesta apresentação, estiveram presentes representantes do CTIR Gov, situação que possibilitou — com intermediação do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC) da ABIN — ações de mitigação mais abrangentes, notadamente a atualização e republicação, em agosto de 2025, da Recomendação 06/2025 por parte do CTIR Gov, que será discutida no Item 4.1 do capítulo subsequente.

Após as intervenções realizadas por intermédio do PNPC, acompanhou-se os resultados por meio das coletas mensais durante um período de 6 meses, isto é, de julho de 2025 a dezembro de 2025. A partir dos resultados obtidos na coleta de dezembro de 2025, iniciou-se uma nova etapa das ações de mitigação. Este ciclo consistiu no envio de mensagens de e-mail direcionadas para alertar individualmente cada um dos órgãos que apresentava algum nível de vulnerabilidade frente à ameaça analisada. Essas mensagens consistiram em: (a) uma apresentação dos objetivos da pesquisa; (b) uma explicação sobre a vulnerabilidade de *spoofing* de e-mails; (c) a situação em que o domínio se encontrava; e (d) as ações imediatas requeridas para sanar o problema.

As mensagens foram endereçadas para contas de e-mail coletadas com OSINT. Priorizou-se o contato com endereços relacionados a ETIRs, CSIRTs, “abuse” e outras equipes designadas como responsáveis pela segurança da informação de acordo com o disposto em seus websites. Quando existente, também contatou-se os endereços de e-mail constantes nas tags “rua” e “ruf” do registro DMARC. Nos casos em que nenhuma conta específica foi encontrada, as mensagens foram enviadas para endereços relacionados a protocolo, contato, ouvidoria ou comunicação.

O primeiro envio ocorreu entre os dias 15 e 20 de dezembro de 2025 e os resultados foram observados pelos próximos três meses (janeiro a março de 2026). O segundo, entre 31 de março e 02 de abril de 2026 e os resultados observados na coleta do mês de abril. Ambos os envios foram compostos por mensagens de e-mail com o conteúdo exibido na Figura 3.6.



Figura 3.6. Exemplo de mensagem de e-mail enviada aos órgão vulneráveis no primeiro e segundo alertas

Por fim, entre os dias 22 e 24 de abril de 2026, um terceiro e último alerta foi enviado aos órgãos que ainda se encontravam vulneráveis à ameaça. Desta vez, o texto foi composto por um lembrete sobre a Recomendação 06/2025 publicada pelo CTIR Gov a respeito da vulnerabilidade em questão e sobre a obrigatoriedade dos órgãos em saná-la de acordo com o disposto no Decreto nº 10.748, além de, mais uma vez, informar a condição específica do domínio e as ações imediatas requeridas para sanar o problema. Os resultados foram observados por mais três meses, ou seja, de maio até o final da investigação, em julho de 2026. Um exemplo do texto deste terceiro alerta pode ser encontrado no Figura 3.7.

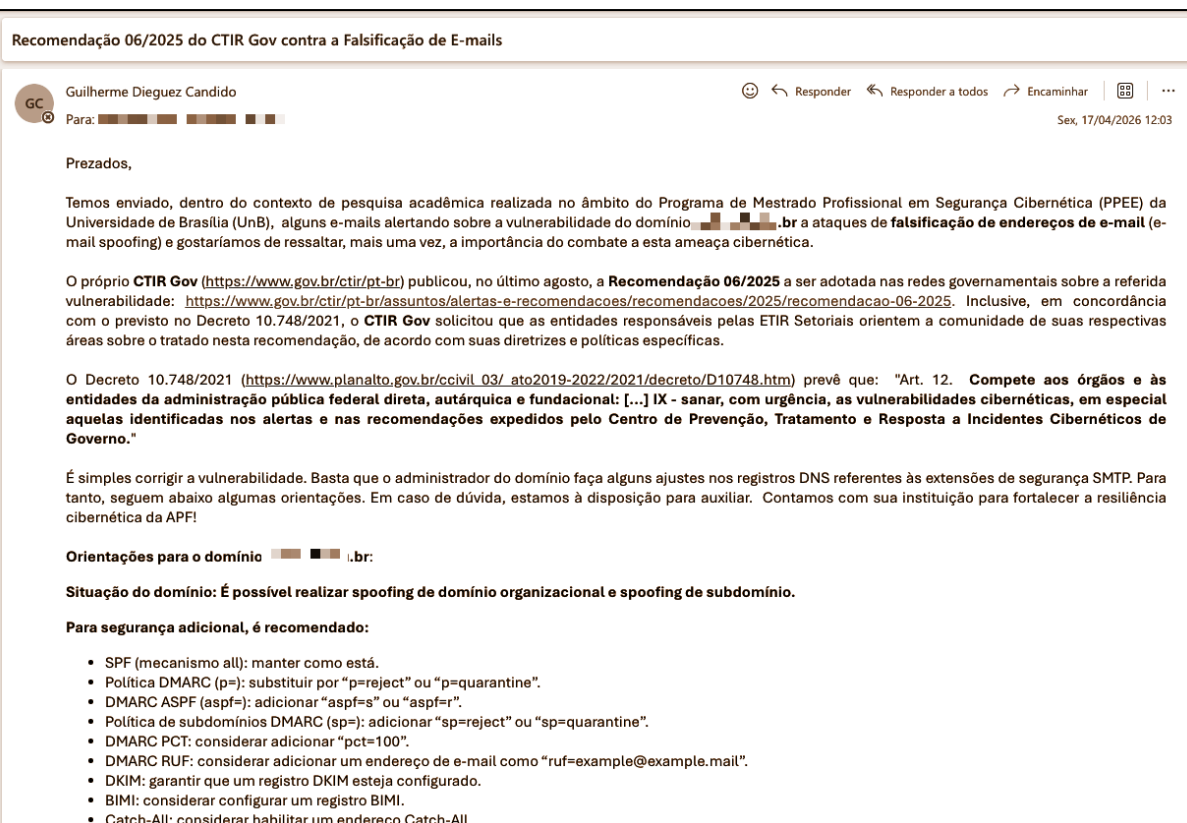


Figura 3.7. Exemplo de mensagem de e-mail enviada no terceiro alerta.

4. RESULTADOS E DISCUSSÕES

Este capítulo se dedica a apresentar e discutir os resultados obtidos ao longo da investigação considerando seu objetivo geral, isto é, auxiliar na mitigação da vulnerabilidade dos órgãos públicos federais brasileiros a ataques de *spoofing* de e-mail. Além de descrever a evolução quantitativa da amostra, busca-se compreender em que medida as diferentes intervenções empregadas induziram mudanças efetivas no comportamento dos órgãos da APF frente à ameaça em questão.

4.1. RECOMENDAÇÃO 06/2025 - CTIR Gov

Como mencionado no item 3.4, os dados obtidos na coleta de junho de 2025 serviram para uma intervenção a nível estratégico na APF e este é o primeiro resultado desta pesquisa que merece destaque.

Apresentados os referidos resultados parciais ao PNPC da ABIN, a constatação da situação de vulnerabilidade governamental por parte deste órgão culminou na realização, em Brasília/DF, de uma palestra presencial a órgãos componentes do SISBIN. A palestra foi proferida por este autor em 18 de julho de 2025, e teve o propósito de alertar e sensibilizar os representantes destes órgãos acerca da gravidade da falsificação de endereços de e-mail. O efeito desta ação foi ampliado pela presença de atores regulatórios, entre os quais se destacam representantes do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov). Este contato institucional, viabilizado com intermédio do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC) da ABIN, permitiu que os achados desta pesquisa balizassem uma ação de intervenção de amplo alcance no ecossistema digital público brasileiro. Trata-se da atualização e republicação, em 13 de agosto de 2025, da Recomendação nº 06/2025 pelo CTIR Gov (<https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/recomendacoes/2025/recomendacao-06-2025>). Conforme explicitado no item 3 do documento: “A presente recomendação foi elaborada em conjunto com a Agência Brasileira de Inteligência (ABIN), que identificou oportunidades de aprimoramento na configuração desse serviço em determinados entes da REGIC, motivando a elaboração deste documento para reforçar a adoção das melhores práticas de segurança”.

O teor técnico do documento, que pode ser verificado integralmente na Figura 4.1, prescreve, de forma detalhada, as boas práticas para a implementação conjunta das extensões SPF, DKIM e DMARC na Rede Federal de Gestão de Incidentes Cibernéticos (REGIC). A diretriz avançou ao estabelecer critérios técnicos rígidos de conformidade, para além da mera adoção dos protocolos, tais como o uso de chaves criptográficas robustas para o DKIM e de políticas restritivas no DMARC, desaconselhando explicitamente o modo de mero monitoramento (p=none) em favor das políticas de quarentena (p=quarantine) ou rejeição (p=reject). Ademais, a recomendação abordou o alinhamento da *tag* de domínio principal (p=) com a de

subdomínios (sp=), abordando, como se verá mais à frente, uma das vulnerabilidades residuais mais recorrentes identificadas na amostragem deste estudo.

Por fim, em estrita concordância com o Decreto Federal nº 10.748/2021, o CTIR Gov instrumentalizou a recomendação ao compelir as Equipes de Tratamento e Resposta a Incidentes Cibernéticos (ETIRs) setoriais a orientarem e fiscalizarem suas respectivas comunidades, convertendo a provocação feita a partir desta pesquisa em um padrão de conformidade técnica e normativa obrigatório para toda a APF, uma vez que, como preconiza o referido Decreto em seu Art. 12, “Compete aos órgãos e às entidades da administração pública federal direta, autárquica e fundacional: [...] IX - sanar, com urgência, as vulnerabilidades cibernéticas, em especial aquelas identificadas nos alertas e nas recomendações expedidos pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.”

Desta forma, o envolvimento do órgão responsável pela resposta a incidentes cibernéticos governamentais (CTIR Gov) transformou as evidências empíricas desta pesquisa em um vetor para a formulação de recomendações normativas de segurança sobre o tema, superando o isolamento comum entre achados acadêmicos e práticas regulatórias.

CTIR Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo

O que você procura?

RECOMENDAÇÃO 06/2025

Marcadores de autenticidade (SPF, DKIM e DMARC)

Publicado em 14/03/2025 14h36 | Atualizado em 13/08/2025 10h42

Compartilhe: [f](#) [X](#) [in](#) [v](#) [p](#)

. [TL;P;CLEAR]

1. O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) alerta sobre os riscos vinculados a configuração incorreta (que não segue as boas práticas de segurança) dos servidores de domínio relacionadas à autenticação de e-mail para os usuários dos sistemas governamentais e órgãos da Rede Federal de Gestão de Incidentes Cibernéticos (REGIC);

2. Nesse sentido, listamos algumas recomendações importantes a serem adotadas nas redes governamentais:

- Habilitar o SPF no DNS do domínio, especificando quais IPs/servidores podem enviar e-mails no nome da instituição;
- Usar -all (hardfail) ou -all (softfail) no final do registro para rejeitar ou marcar como suspeitos os envios não autorizados;
- Configurar o DKIM no servidor de e-mails, ativando a assinatura digital de cabeçalhos;
- Usar chaves de 1024 ou 2048 bits, preferencialmente com o algoritmo SHA-256;
- Implemente DMARC em sinergia com SPF e DKIM — ele depende dos dois para funcionar corretamente;
- Definir uma política (p=reject, p=quarantine, p=none), dependendo do grau de rigidez desejado:
 - p=reject: rejeita mensagens que falham a autenticação.
 - p=quarantine: envia para spam.
 - p=none: apenas monitora.
- Sugere-se utilizar p=reject ou p=quarantine (evitar o uso de p=none). Adicionalmente é importante forçar que sp=reject/quarantine siga a política adotada por p= (p= é aplicada ao domínio principal e sp= para os subdomínios);

3. A presente recomendação foi elaborada em conjunto com a Agência Brasileira de Inteligência (ABIN), que identificou oportunidades de aprimoramento na configuração desse serviço em determinados entes da REGIC, motivando a elaboração deste documento para reforçar a adoção das melhores práticas de segurança.

4. Em concordância com o previsto no Decreto 10.748/2021, o CTIR Gov solicita que as entidades responsáveis pelas ETIR Setoriais orientem a comunidade de suas respectivas áreas sobre o tratado nesta recomendação, de acordo com suas diretrizes e políticas específicas.

Figura 4.1. Recomendação 06/2025 do CTIR Gov
Fonte: CTIR Gov.

4.2. RESULTADOS AGREGADOS DA AMOSTRA

De início, cumpre lembrar que, metodologicamente, os 5.058 registros DNS coletados não serão expostos individualmente. Optou-se por analisar os dados coletados ao longo dos 18 meses de investigação agrupando os 281 órgãos da amostra por áreas de atuação. Isso se deu, como já explicado no item 3.2 desta dissertação, para que a publicização dos resultados da pesquisa não revelasse vulnerabilidades individuais que pudessem impactar a reputação dos órgãos ou divulgasse diretamente a possíveis adversários quais órgãos se encontram vulneráveis a serem explorados em ataques de *spoofing* de e-mail. Essa opção metodológica não compromete, contudo, a reprodutibilidade da pesquisa, uma vez que qualquer interessado pode replicar as coletas aqui discutidas, em período de referência prospectivo, ao seguir integralmente os procedimentos descritos no capítulo 3.

Antes de uma análise pormenorizada dos doze agrupamentos por área de atuação, faz-se necessário discutir o comportamento da amostra como um todo, uma vez que é nesse panorama que se evidencia o efeito agregado das ações de mitigação propostas na APF ao longo dos dezoito meses de pesquisa.

4.2.1. Taxas de Adoção e Conformidade dos Registros SPF, DKIM e DMARC

Examina-se aqui, para cada um dos três protocolos de autenticação de remetente, tanto a taxa de adoção — entendida como a mera presença de um registro publicado no DNS do domínio — quanto o grau de conformidade das configurações adotadas, ou seja, o quão permissivas ou restritivas são as configurações em relação a remetentes possivelmente falsificados, uma vez que a simples existência do registro não é suficiente para caracterizar proteção efetiva contra a falsificação de e-mails.

(i) SPF

Ao contrastar os resultados da primeira coleta, realizada em fevereiro de 2025, com a última, em julho de 2026 — após a exposição da amostra ao conjunto cumulativo de iniciativas de mitigação conduzidas durante a pesquisa—, a análise da amostra geral, composta por todos os 281 domínios, permite observar uma discreta evolução no que diz respeito à extensão SPF.

Tratando-se especificamente da taxa de adoção, isto é, da mera existência de um registro SPF publicado no DNS de cada domínio — independentemente da conformidade da configuração —, verificou-se que a ampla maioria da amostra já adotava esse mecanismo mesmo antes de qualquer intervenção. Em fevereiro de 2025, 96,4% dos domínios já possuíam registro SPF. Ao final da investigação, essa taxa evoluiu para 97,5%. Ainda que a variação absoluta seja modesta, representa uma queda relativa de quase um terço no conjunto de órgãos que, no início da pesquisa, não dispunham deste registro. Os dados podem ser observados no Gráfico 4.1.

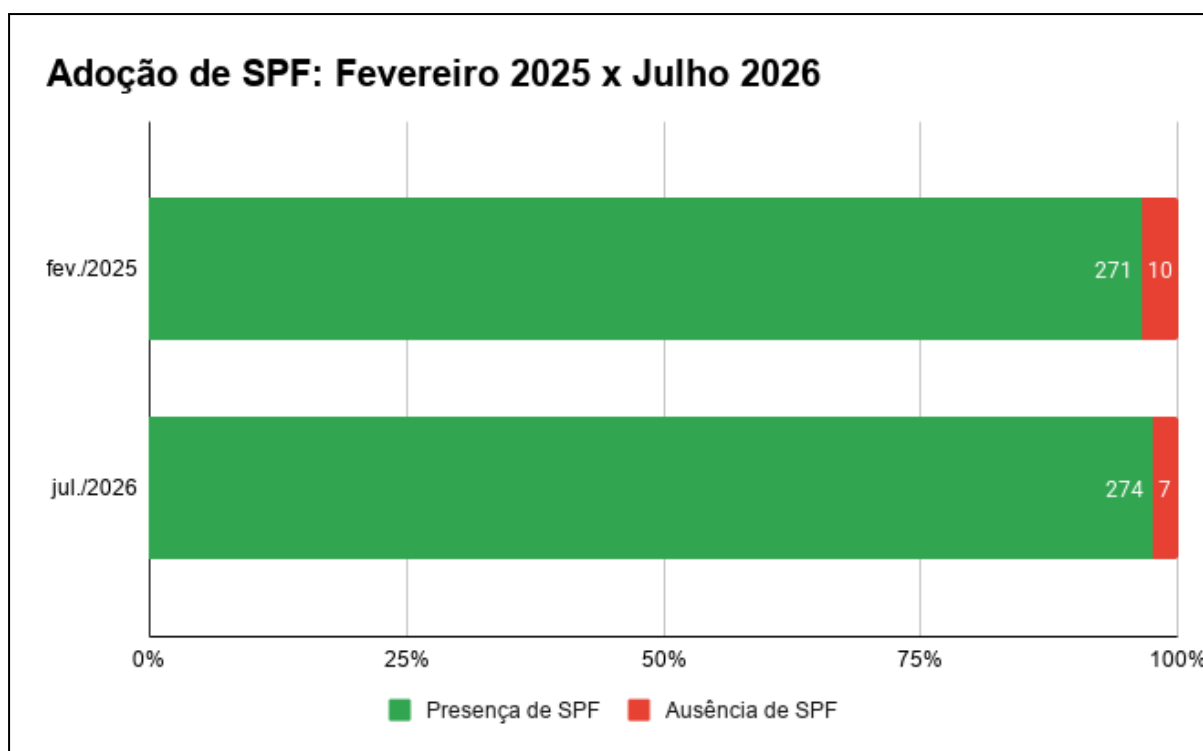


Gráfico 4.1. Evolução da taxa de adoção do protocolo SPF ao longo do período de observação.

Este comportamento é coerente com o que a literatura já indicava a respeito desta extensão. Por ser o mais antigo e o de mais simples implementação dos três mecanismos de autenticação de remetente, o SPF tende a apresentar uma taxa de adoção mais elevada. A persistência de uma fração residual de domínios sem registro de SPF, mesmo após as ações de mitigação, sugere que esse pequeno grupo talvez corresponda a órgãos com menor maturidade em gestão de TI ou em Segurança da Informação.

Considerando apenas os domínios que possuem SPF, a distribuição dos qualificadores empregados junto ao mecanismo “all” registrou uma tendência de enrijecimento das políticas SPF ao longo do período de observação. Em fevereiro de 2025, 174 domínios (64,2%) adotavam o qualificador restritivo “-all” (Fail), 94 (34,7%) utilizavam o qualificador permissivo “~all” (SoftFail), 2 (0,7%) publicavam um registro SPF sem qualquer mecanismo “all” e 1 (0,4%) utilizava o qualificador “?all” (Neutral). Nenhum domínio utilizava o qualificador “+all” (Pass), que autoriza explicitamente qualquer servidor a enviar e-mails em nome do domínio; tampouco se constatava o problema de excesso de requisições DNS. Em julho de 2026, após todas as ações de mitigação propostas, os domínios com “-all” passaram a 186 (67,9%), enquanto os que utilizavam “~all” recuaram para 84 (30,7%). As categorias de ausência de “all” e “?all” permaneceram estáveis, com 2 (0,7%) e 1 (0,4%) domínios, respectivamente — o que sugere tratar-se de órgãos refratários às sucessivas intervenções feitas durante a pesquisa.

Surgiu, ainda, um único domínio classificado em “muitas requisições”, que passou a publicar, a partir de junho de 2025, dois registros SPF distintos simultaneamente, condição que a RFC 7208 trata como erro fatal e que persistiu sem correção até o final da pesquisa. Um segundo

domínio, adotante de “~all”, manteve-se, ao longo das 18 coletas realizadas, com uma contagem de consultas DNS entre 11 e 14, decorrente da expansão recursiva das cadeias de autorização de dois provedores incluídos em seu registro SPF. Um terceiro caso, surgido apenas a partir de março de 2026, envolveu um domínio que adotava “-all” mas que continha um mecanismo de inclusão do próprio registro apontando para si, gerando um *loop* que impossibilita a resolução DNS, situação que também permaneceu inalterada até o fim da pesquisa. Em conjunto, esses achados indicam que a mitigação da falsificação de e-mails não se resume à adoção do protocolo, exigindo também acompanhamento técnico contínuo, sob pena de os próprios ajustes introduzirem novas falhas.

A comparação numérica, e não apenas percentual, permite qualificar melhor o progresso. O crescimento de 12 domínios na categoria “-all” (de 174 para 186) é superior ao número de domínios que passaram a adotar SPF pela primeira vez no período — apenas 3, o que indica que a maior parte do ganho não decorreu simplesmente da entrada de novas adesões ao protocolo, mas de uma reconfiguração de domínios que já contavam com SPF — mas configurado de forma permissiva — e que responderam às orientações recebidas, promovendo o ajuste de suas políticas SPF para o nível de rigor recomendado. O avanço discutido pode ser observado no Gráfico 4.2.

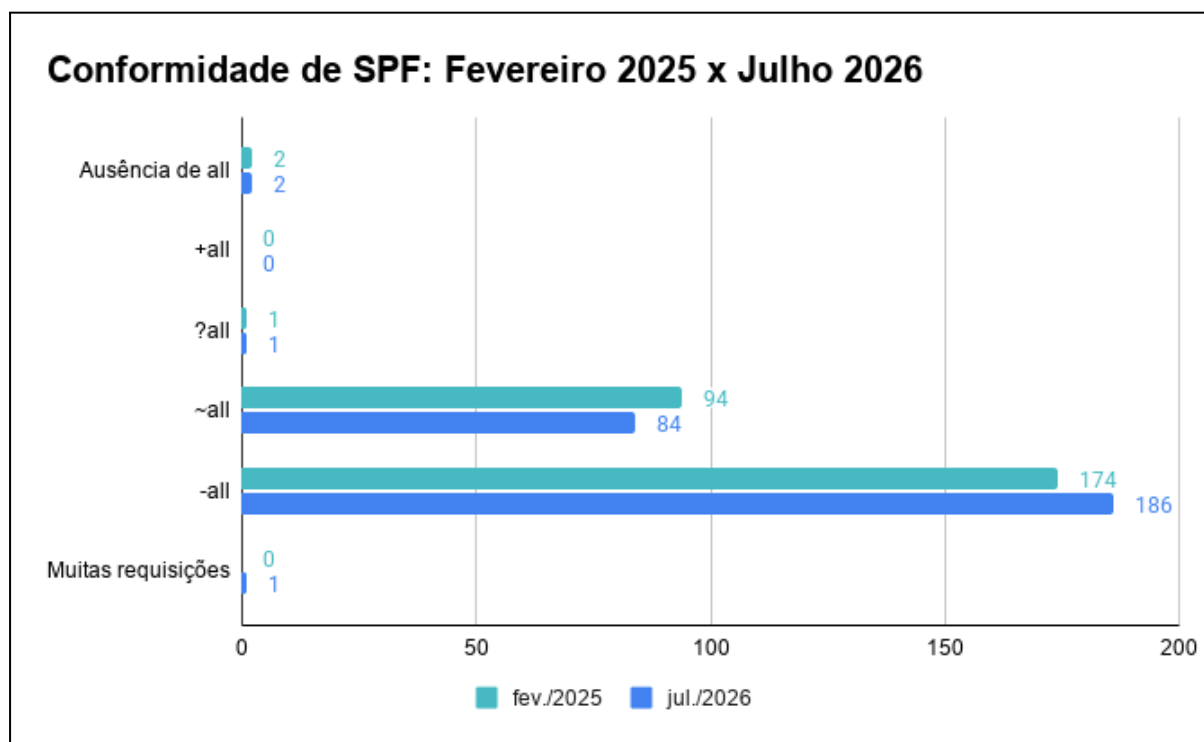


Gráfico 4.2. Evolução na conformidade dos registros SPF durante o período de observação.

Em síntese, os resultados sugerem que a amostra geral, tomada da perspectiva da extensão SPF, apresentou uma evolução positiva, apesar de modesta em termos absolutos, ao longo dos dezoito meses e das ações de mitigação conduzidas.

(ii) DKIM

Como já mencionado na fundamentação teórica desta dissertação, há uma limitação importante na leitura dos resultados de DKIM. Como a chave pública é cadastrada em um registro TXT localizado em um subdomínio identificado pelo seletor “[seletor]._domainkey.[domínio]” e esse seletor é definido livremente por cada organização — ao contrário do DMARC, cujo registro está sempre em “_dmarc”, ou do SPF, publicado diretamente no domínio —, a verificação da adoção do protocolo via OSINT depende de testar seletores comumente utilizados pelo mercado. Isso significa que a categoria “DKIM não encontrado” deve ser interpretada como ausência de evidência de DKIM sob os 100 seletores testados pela ferramenta *StopEmailSpoofing*, e não necessariamente como uma prova definitiva de que o mecanismo não está implementado. Isso também explica por que, diferentemente do SPF e do DMARC, não se produziu um indicador de conformidade nesta seção. Sem acesso a uma mensagem privada efetivamente assinada, não é possível auditar remotamente a validade criptográfica da assinatura, restando à pesquisa apenas um mero indicador de adoção.

Feita esta ressalva metodológica, os números revelam que o DKIM partiu, entre os três protocolos, do patamar de adoção mais baixo da amostra geral. Em fevereiro de 2025, apenas 55,5% (156) dos 281 domínios apresentavam registro DKIM localizável. Esse resultado é coerente com a natureza do protocolo. Enquanto o SPF exige apenas a publicação de uma lista de servidores autorizados e o DMARC depende essencialmente da configuração de uma política declarativa, o DKIM pressupõe a geração e a gestão de um par de chaves criptográficas e a integração do processo de assinatura ao fluxo de envio de e-mails do MTA, o que representa uma barreira técnica e operacional consideravelmente maior e, portanto, uma adoção mais lenta e complexa.

Ao longo do período de observação, contudo, a proporção de domínios com DKIM identificável cresceu, alcançando 64,8% (182) em julho de 2026. O avanço de 9,3 pontos percentuais é superior ao observado no SPF no mesmo intervalo. Esse resultado também é compatível com o conteúdo das mensagens de alerta enviadas aos órgãos, que traziam ao DKIM uma orientação pouco detalhada — devido à complexidade de implementação — restrita a “garantir que um registro DKIM esteja configurado”. A evolução pode ser observada no Gráfico 4.3.

Mesmo com esse avanço, o DKIM permanece, ao final do período analisado, como o protocolo com a maior lacuna de adoção — mais de um terço da amostra geral segue sem registro identificável. Repisando, os registros podem existir, embora não tenham sido localizados por OSINT. A análise dos resultados indica que a complexidade de implementação de cada mecanismo é, na prática, o principal fator explicativo dos níveis de adesão e conformidade observados na amostra.

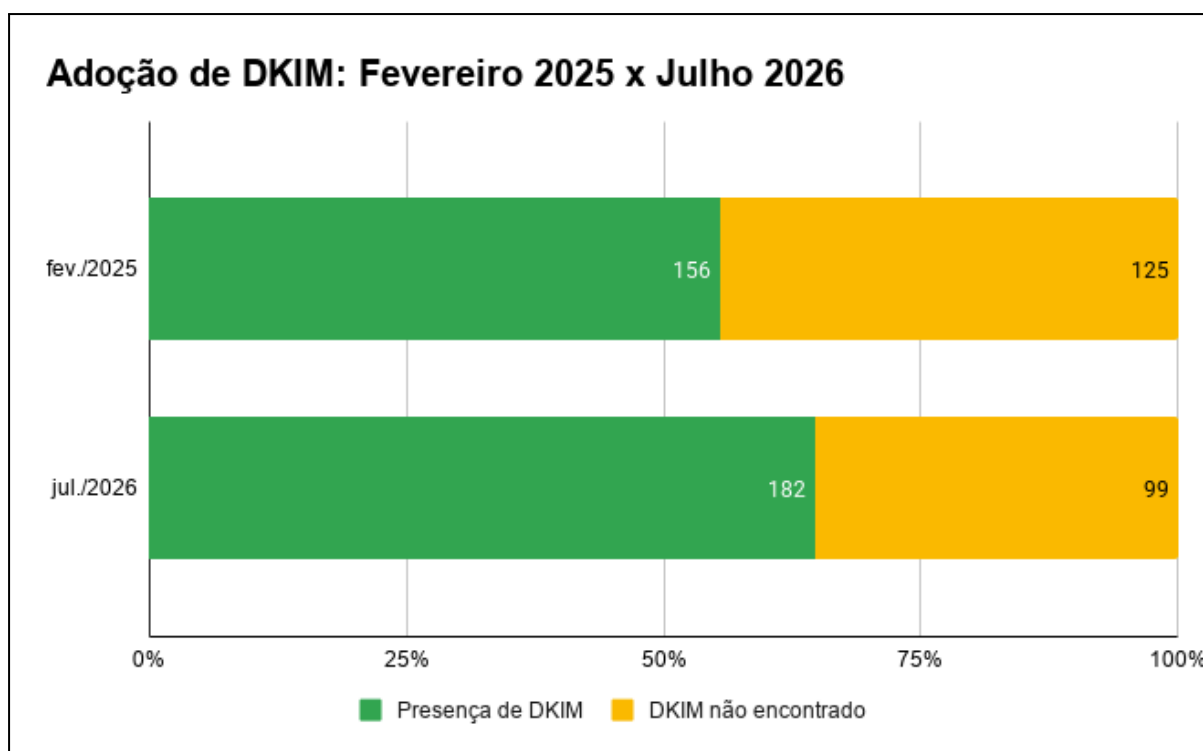


Gráfico 4.3. Evolução na taxa de adoção do protocolo DKIM durante o período de observação.

(iii) DMARC

Diferentemente do que se observou para o SPF, cuja adoção já se encontrava consolidada na amostra desde o início do período de observação passiva, o DMARC apresentou, na coleta de fevereiro de 2025, um quadro de adesão mais incipiente. Apenas 208 dos 281 domínios da amostra (74,0%) publicavam algum registro DMARC, restando 73 domínios (26,0%) completamente desprotegidos por essa camada, que é essencial para que os demais protocolos também sejam efetivos. Esse patamar inicial mais baixo é coerente com o que a fundamentação teórica já indicava sobre o protocolo. Por ser o mais recente dos três mecanismos de autenticação de remetente e por depender da arquitetura prévia de SPF e DKIM para operar de forma eficaz, o DMARC tende a apresentar uma curva de adoção mais lenta do que a de seus protocolos subjacentes.

Ao final do período de observação, contudo, o número de domínios com DMARC saltou para 256 (91,1%), restando apenas 25 domínios (8,9%) sem o registro — um ganho líquido de 48 novos adotantes ao longo dos dezoito meses de pesquisa. Esse avanço de 17,1 pontos percentuais é consideravelmente mais expressivo do que a variação observada para SPF e DKIM no mesmo intervalo, sugerindo que a combinação das ações de mitigação teve, sobre esse indicador específico, um efeito mais acentuado. A evolução da adoção da extensão DMARC pelos domínios da APF pode ser observada no Gráfico 4.4.

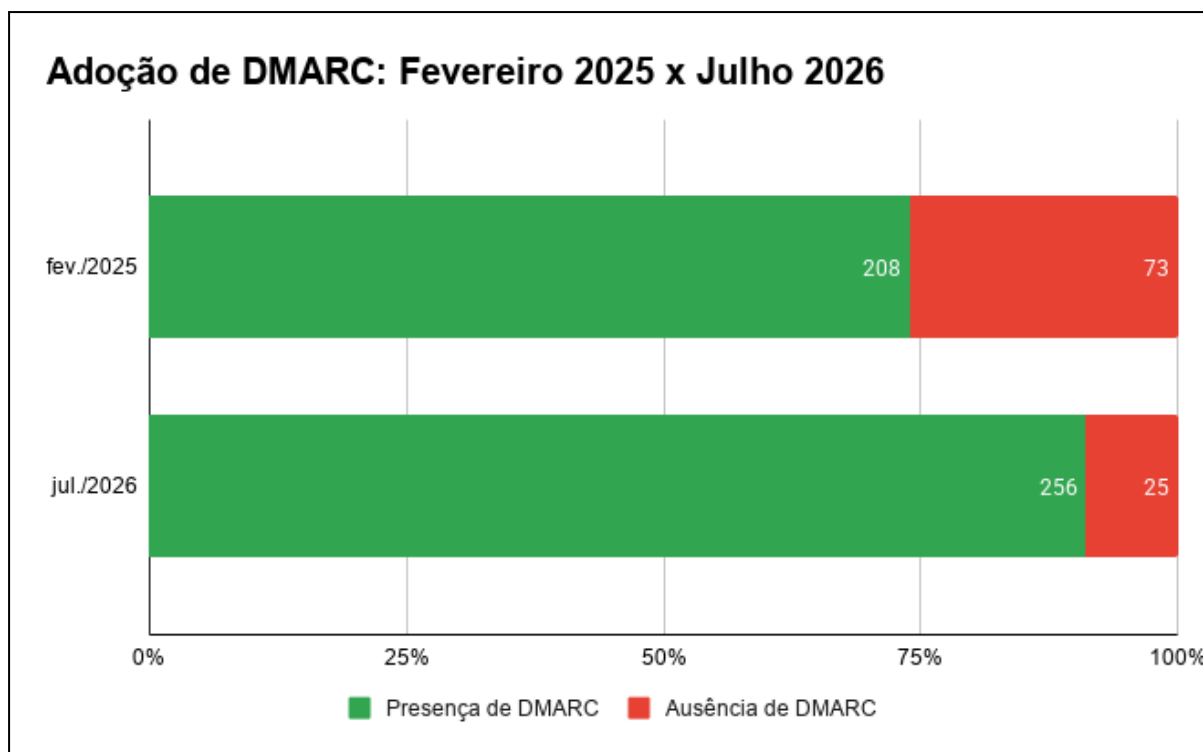


Gráfico 4.4. Evolução na taxa de adoção do protocolo DMARC durante o período de observação.

A análise da conformidade, isto é, no caso do DMARC o grau de rigidez da política (“p=”) efetivamente adotada pelos domínios que adotam o protocolo, destaca uma mudança qualitativa ainda mais importante do que a simples adoção. Em fevereiro de 2025, a distribuição das políticas encontrava-se assim: 91 domínios (43,8%) utilizavam a política “p=none” — modo de monitoramento que não impõe impede a entrega de e-mails falsificados, desaconselhado por criar uma falsa sensação de proteção —, outros 91 (43,8%) já adotavam “p=quarantine” e apenas 24 (11,5%) haviam avançado até a política mais rigorosa, “p=reject”. Complementarmente, um domínio (0,5%) apresentava erro de sintaxe e outro (0,5%) publicava registro sem a *tag* “p=” definida, totalizando dois registros tecnicamente malformados, o que também equivale, na prática, à ausência de proteção efetiva. Em julho de 2026, este cenário se inverteu. A política “p=none” recuou para 54 domínios (21,1%), “p=quarantine” tornou-se majoritária, respondendo por 150 domínios (58,6%), e “p=reject” mais do que dobrou, chegando a 52 domínios (20,3%). Não menos importante, as categorias de erro de sintaxe e de ausência da *tag* “p=” deixaram de aparecer na coleta final, indicando que os dois registros malformados identificados no início foram corrigidos ao longo do período de atuação desta pesquisa.

O crescimento conjunto de “p=quarantine” e “p=reject”, políticas que efetivamente protegem o domínio, somou 87 ocorrências e esse valor coincide com a soma dos resultados de três movimentos distintos. Nota-se que 48 domínios passaram a adotar DMARC pela primeira vez no período, 2 domínios malformados foram corrigidos e 37 domínios migraram da política “p=none” para uma política de fato restritiva. Essa correspondência exata reforça a hipótese de que a orientação recebida pelos órgãos — que recomendava a novos adotantes já configurarem diretamente “p=reject” ou “p=quarantine” — foi seguida, e de que uma parcela

relevante dos domínios que já possuíam DMARC, mas o mantinham em modo de monitoramento, também correspondeu aos ajustes propostos. Vale notar, ainda, que desse total de 87 domínios que passaram a adotar políticas restritivas, a maioria optou pela política intermediária “p=quarantine”, e não diretamente pela mais rigorosa “p=reject”. Este padrão também é compatível com o que a revisão da literatura apontou sobre a cautela dos administradores em adotar políticas de rejeição total, dado o receio de bloquear indevidamente mensagens legítimas, dando preferência à entregabilidade em detrimento da segurança. Os dados aqui mencionados podem ser analisados no Gráfico 4.5.

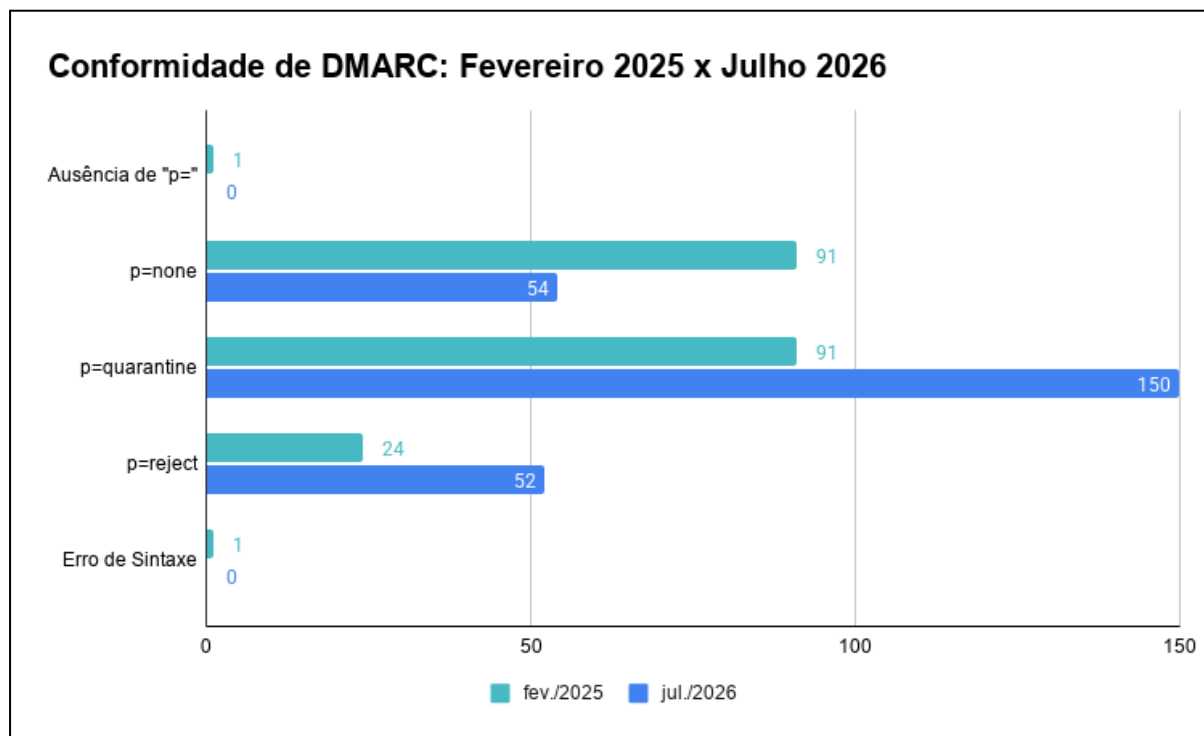


Gráfico 4.5. Evolução na conformidade dos registros DMARC durante o período de observação.

A política DMARC para subdomínios merece uma análise à parte, uma vez que a *tag* “sp=” não é obrigatória no registro. Quando omitida, a política aplicável aos subdomínios simplesmente herda o valor definido em “p=” para o domínio principal. Essa característica exige cautela na leitura dos dados, pois a ausência da *tag* “sp=” não equivale, por si só, a uma vulnerabilidade decorrente dessa omissão; ela apenas indica que essa política decorrerá do que foi definido na política do domínio organizacional.

Considerando apenas os domínios que efetivamente possuem DMARC, em fevereiro de 2025, 145 domínios (69,7% dos 208 com DMARC) não definiam explicitamente a *tag* “sp=”, restando à política do domínio principal a proteção dos respectivos subdomínios; 39 (18,8%) definiam “sp=none”, 18 (8,7%) “sp=quarantine” e apenas 6 (2,9%) chegavam a “sp=reject”. Em julho de 2026, a ausência de “sp=” recuou, em termos percentuais, para 62,1% (159 dos 256 domínios com DMARC); “sp=none” caiu para 11,3% (29 domínios); “sp=quarantine” avançou para 16,4% (42 domínios); e “sp=reject” mais que quadruplicou sua participação absoluta, saltando de 6 para 26 domínios (10,2%). Nota-se aqui um resultado que, à primeira vista, parece contraditório. Embora o percentual de domínios sem “sp=” tenha caído de

69,7% para 62,1%, o número absoluto de domínios nessa condição, na verdade, cresceu de 145 para 159. Isso se explica pelo aumento do número de adotantes de DMARC no período de observação (de 208 em fevereiro de 2025 para 256 em julho de 2026). Os dados estão disponíveis no Gráfico 4.6.

A maioria do ganho observado concentrou-se em políticas mais restritivas, sugerindo que, tanto entre os domínios que passaram a declarar “sp=” pela primeira vez quanto entre os que já o faziam de forma branda, a tendência predominante foi a adoção de políticas de maior rigor. Esse ponto é particularmente relevante porque o risco de falsificação foi avaliado separadamente para o domínio organizacional e para os subdomínios, sendo o segundo cenário frequentemente o mais negligenciado pelos administradores — muitos órgãos possuem dezenas de subdomínios de uso esporádico ou legado, que tendem a escapar da atenção dedicada ao domínio principal e, com isso, continuam sendo vetores viáveis para ataques de *spoofing*.

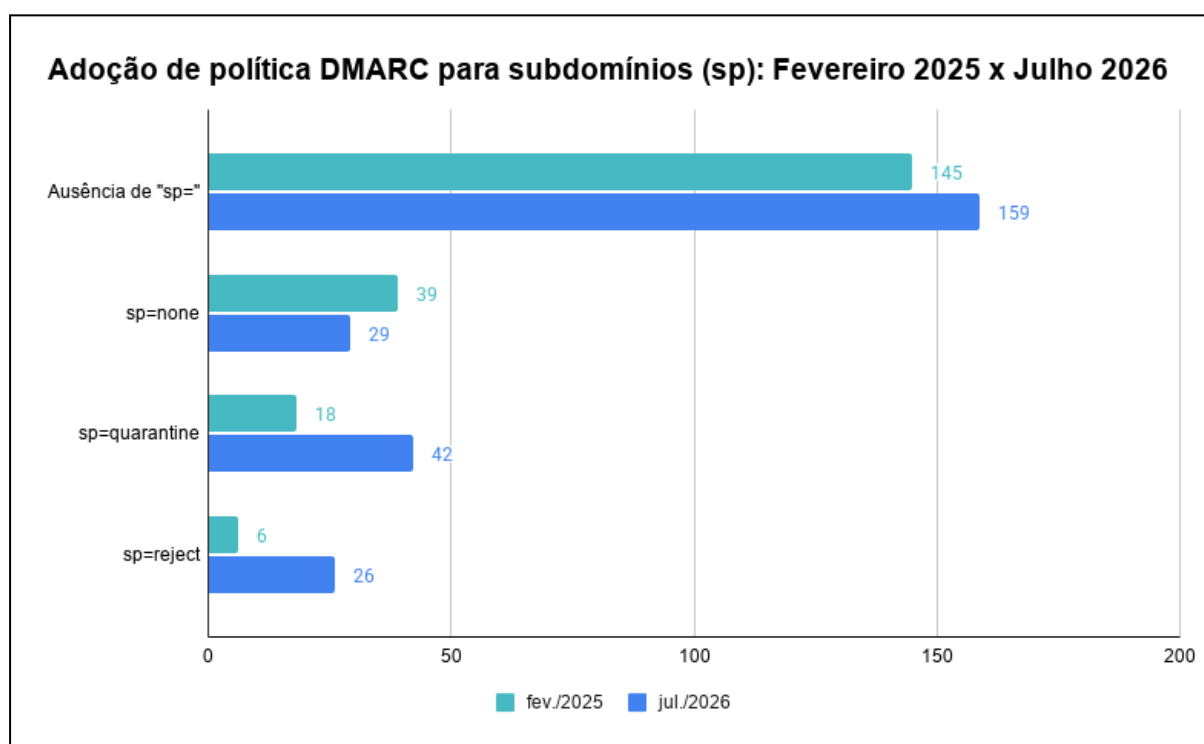


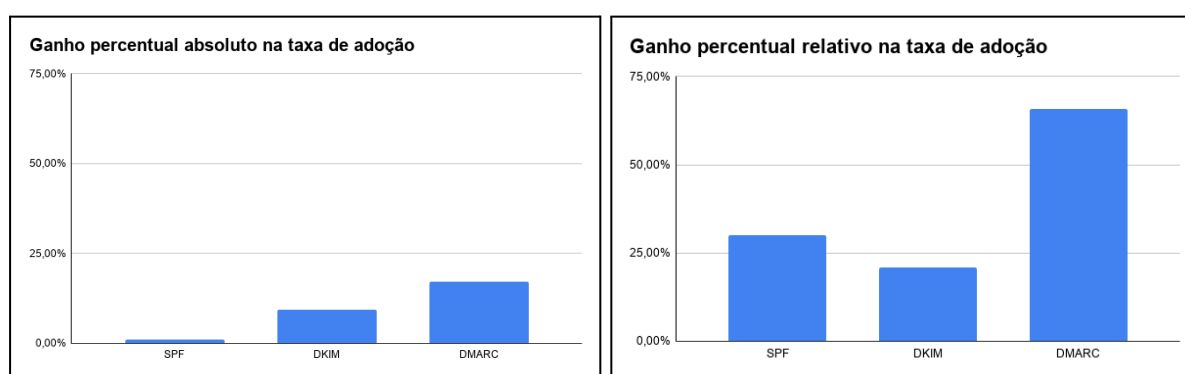
Gráfico 4.6. Evolução na adoção e conformidade da política DMARC para subdomínios durante o período de observação.

Em resumo, a queda de 7,6 pontos percentuais na ausência de “sp=” explícito, somada ao crescimento simultâneo de “quarantine” e, sobretudo, de “reject”, sugere que essa dimensão da configuração de DMARC também respondeu positivamente às orientações enviadas ao longo da pesquisa. O ritmo dessa resposta, contudo, parece mais lento do que o observado para a política “p=” do domínio organizacional, o que é esperado, dado que a proteção de subdomínios tende a ser tratada como uma camada secundária de segurança, implementada somente após a consolidação da política principal.

Ainda em relação ao DMARC, é possível constatar um amadurecimento secundário dos registros. Os endereços de relatórios agregados “rua” passaram de 179 para 223 domínios, e os de relatórios forenses “ruf” de 100 para 121; a declaração explícita de “pct=100” subiu de 61 para 96; e o alinhamento estrito de SPF (“aspf=s”) subiu de 18 para 38. Uma vez que estas *tags* também constavam das sugestões de melhoria enviadas aos órgãos, este é mais um resultado que indica eficiência nas intervenções realizadas durante a pesquisa.

Em conclusão, o protocolo SPF apresentou-se praticamente saturado desde a primeira coleta, com 271 domínios (96,4%) publicando registro em fevereiro de 2025 e 274 (97,5%) em julho de 2026. O DMARC partiu de 208 domínios (74,0%) e alcançou 256 (91,1%) ao final do período. O DKIM, por sua vez, passou de 156 (55,5%) para 182 (64,8%). Complementarmente, vale mencionar que a adoção do protocolo BIMl permaneceu residual, passando de um para três domínios. A ausência de registro, portanto, deixou de ser um problema relevante para o SPF e permaneceu apenas residual para o DMARC. Com relação ao DKIM, em virtude da limitação técnica já discutida, não é possível afirmar categoricamente que os outros 35,2% não possuem registro. Sobre a conformidade, também observou-se a redução da permissividade das configurações adotadas, com o enrijecimento dos qualificadores SPF e, sobretudo, das políticas DMARC — cuja distribuição migrou majoritariamente de “p=none” para “p=quarantine” e “p=reject” —, indicando que as ações de mitigação surtiram efeito tanto sobre a adesão inicial aos protocolos quanto sobre a qualidade das configurações já existentes.

O Gráfico 4.7 resume o ganho percentual absoluto na taxa de adoção de cada um dos três protocolos durante o período de observação, isto é, o quanto a taxa de adoção evoluiu considerando toda a amostra (281 domínios). Por sua vez, o Gráfico 4.8 sintetiza o ganho percentual relativo na taxa de adoção, considerando apenas os domínios sem as extensões de segurança configuradas no início da investigação, uma vez que a evolução só era possível nesse conjunto.



Gráficos 4.7 e 4.8. Ganhos percentuais, absolutos e relativos, respectivamente, na taxa de adoção dos protocolos SPF, DKIM e DMARC durante o período de observação.

4.2.2. Deficiências mais recorrentes nas configurações das extensões de segurança SMTP

A seção anterior trouxe uma análise da evolução das taxas de adoção e de conformidade dos registros SPF, DKIM e DMARC nos domínios da Administração Pública Federal; cabe agora, em consonância com a metodologia de pesquisa proposta, identificar quais falhas de configuração se mostraram mais recorrentes e difíceis de sanitizar.

Partindo da perspectiva dos 76 domínios remanescentes na categoria “Completamente Vulnerável” ao final da pesquisa, verifica-se que nenhum deles possui política DMARC rígida. Desse total, 24 (31,6%) não publicam qualquer registro DMARC e os 52 restantes (68,4%) mantêm o registro com a política permissiva “p=none”. Da mesma amostra, 73 dos 76 (96,1%) já possuíam registro SPF válido, dos quais 40 (52,6%) adotavam o qualificador restritivo “-all”. Mesmo com SPF configurado de forma rígida, a ausência de uma política DMARC coercitiva faz com que o servidor destinatário não reaja a um remetente não autorizado, permanecendo possível a falsificação tanto no domínio organizacional quanto nos subdomínios.

Esse resultado é consistente com o que já era apontado na literatura sobre a política “p=none”. Por não impor qualquer restrição, esta política confere uma falsa sensação de proteção. Uma combinação de SPF e DMARC insuficientemente rígida produz o mesmo efeito prático da ausência desses registros, já que, em ambos os casos, a avaliação do servidor destinatário não resulta em bloqueio efetivo. Como o DMARC recebe os resultados de SPF e DKIM e os traduz em ações concretas, sua ausência ou permissividade anula o efeito dos demais protocolos.

O padrão descrito acima não ocorreu apenas na última coleta, mas se repetiu mês a mês desde o início do período de observação. Em fevereiro de 2025, dos 164 domínios então classificados como completamente vulneráveis, 73 não possuíam registro DMARC e 90 possuíam configurado como “p=none”, restando apenas um caso de registro malformatado sem a *tag* “p=” definida. A repetição desse padrão antes e depois das ações de mitigação, indica que a ausência ou permissividade do DMARC não é apenas um problema pontual, mas o principal fator por trás da exposição da APF à falsificação de e-mails.

Uma segunda deficiência recorrente está na política de subdomínios do DMARC. Durante todo o período de observação, um número que oscilou entre 15 a 18 domínios declarava a *tag* “sp=none” e, portanto, contraía a vulnerabilidade apenas em seus subdomínios, apesar de a política do domínio organizacional ser restritiva. Esse achado difere da simples omissão da *tag* “sp=”, discutida anteriormente, pois quando ela é apenas omitida, o subdomínio herda a política do domínio principal e, caso este esteja protegido, os subdomínios também o são; aqui, a vulnerabilidade decorre da política do subdomínio ter sido explicitamente definida como mais branda que a do domínio principal. O resultado também é consistente com o apontado na fundamentação teórica, segundo a qual os subdomínios são um vetor frequentemente negligenciado, sobretudo nos órgãos que mantêm diversos subdomínios de uso esporádico ou legado.

O caso inverso é o da vulnerabilidade limitada ao domínio organizacional. Nele, a política “p=” está definida como “none”, mas a *tag* “sp=” é definida como “quarantine” ou “reject”, isto é, os subdomínios ficam imunes à falsificação, mas o domínio principal fica exposto. Apesar de este caso ter sido constatado em apenas dois domínios ao final da investigação, a situação manteve-se inalterada durante quase todo o período de investigação. Isso mostra que a granularidade das *tags* de DMARC permite proteger uma camada do domínio e, ao mesmo tempo, deixar outra vulnerável, e que a avaliação de um registro não pode se limitar à sua presença, devendo levar em conta cada *tag* individualmente.

Outras deficiências de menor alcance, mas de persistência relevante, merecem destaque. Ao final da pesquisa, a ausência do registro SPF persistiu em 7 domínios (2,5%), e o qualificador “~all” estava presente em 84 (29,9%) — isoladamente, essa condição não determina a vulnerabilidade do domínio, mas reduz a margem de segurança caso a camada de DMARC também falhe.

Registra-se, ainda, dois pequenos grupos de falhas técnicas no SPF. Em um caso, já mencionado no item 4.2.1, o registro SPF aparenta simplicidade, contendo dois mecanismos “include”, mas a expansão recursiva das cadeias de autorização dos dois provedores elevou, em todas as 18 coletas realizadas, o número de consultas DNS para valores entre 11 e 14, sempre acima do limite de dez previsto na RFC 7208, sem que isso tenha chegado a provocar erro de processamento. Em outro caso, também já mencionado anteriormente, um mecanismo de inclusão do registro SPF aponta para o próprio domínio, criando um *loop* de resolução de DNS; essa condição surgiu na coleta de março de 2026 e permaneceu inalterada até o fim da pesquisa, em julho de 2026.

Dois domínios, por sua vez, permaneceram classificados com erro de sintaxe durante todo o período de observação, de fevereiro de 2025 a julho de 2026, sem que a falha tenha sido corrigida em nenhuma das 18 coletas. No primeiro, a causa é a publicação simultânea de dois registros SPF distintos no mesmo domínio, condição que a RFC 7208 trata como erro fatal; até maio de 2025 este mesmo domínio figurava como completamente vulnerável, migrando para a condição de erro de sintaxe apenas a partir de junho de 2025, quando o segundo registro SPF passou a existir. No segundo, a falha está no registro DMARC, que, apesar de conter política de quarentena, alinhamento e política de subdomínio corretamente definidos, contém um espaço em branco indevido entre a *tag* “p=” e o ponto e vírgula (;) seguinte, o que é suficiente para inviabilizar a leitura do registro pelos servidores destinatários. Em ambos os casos, o erro de sintaxe equivale, na prática, à ausência de proteção.

O DKIM não integra diretamente esta análise, pois a verificação remota de conformidade por OSINT está sujeita à limitação metodológica já discutida; ainda assim, sua possível lacuna de adoção, presente em 35,2% da amostra, permanece como fator agravante, por reduzir as vias alternativas de autenticação DMARC disponíveis quando o alinhamento SPF falha.

Em síntese, a ausência ou permissividade da política DMARC “p=” é a deficiência mais determinante, suficiente para explicar a totalidade dos casos remanescentes de vulnerabilidade completa da amostra. A explícita não rigidez da política de subdomínios

“sp=” ocupa o segundo lugar, restrita a uma parcela menor de domínios, mas presente de forma persistente e uniforme em todas as coletas. Ainda que de menor alcance, parte das demais deficiências residuais — a ausência de registro SPF, o registro SPF duplicado, a expansão recursiva de consultas DNS acima do limite regulamentar, o *loop* de resolução e os erros de sintaxe no registro DMARC — não sofreu qualquer alteração ao longo das ações de mitigação, persistindo praticamente inalterada ao longo de todo o período de observação. Isso reforça que a mitigação da falsificação de e-mails não se resume à mera adoção de protocolos, exigindo também entendimento técnico completo das extensões e monitoramento contínuo.

4.2.3. Estado de vulnerabilidade dos órgãos públicos federais brasileiros a ataques de *spoofing* de e-mail

Nesta seção, contrasta-se o estado geral de vulnerabilidade da APF à *spoofing* de e-mail encontrado no primeiro mês de observação (fevereiro de 2025) com o último (julho de 2026), após todas as ações de mitigação propostas durante a pesquisa.

Convém recordar que o critério de classificação de vulnerabilidade não avalia cada extensão isoladamente, mas sim a combinação entre o mecanismo “all” do SPF e as *tags* “p=”, “aspf=” e “sp=” do DMARC. Das 295 combinações previstas, 187 resultam em algum grau de falsificação e apenas 108 são protetivas. Logo, o cenário é mais propenso à permissividade do que à proteção, e a condição “não vulnerável” só é alcançada mediante um conjunto deliberado e minucioso de configurações. Como estabelecido na seção 3.3, um domínio foi considerado vulnerável sempre que se enquadrava em qualquer um dos quatro cenários de vulnerabilidade, quais sejam: “Completamente Vulnerável”, “Apenas Subdomínios Vulneráveis”, “Apenas Domínio Principal Vulnerável” ou “Erro de Sintaxe”. A categoria “Não Vulnerável”, por sua vez, representa exclusivamente os domínios que não apresentaram nenhuma dessas fragilidades.

Na primeira coleta realizada, em fevereiro de 2025, o estado de vulnerabilidade encontrado mostrava que, dos 281 domínios da amostra, apenas 99 (35,2%) apresentavam configurações que tornavam a falsificação impraticável, enquanto 182 (64,8%) encontravam-se vulneráveis em algum grau. Destes, 164 (58,4%) estavam completamente vulneráveis, isto é, sujeitos à falsificação tanto do domínio organizacional quanto dos subdomínios; 15 (5,3%) eram vulneráveis apenas no âmbito dos subdomínios; 1 (0,4%) apenas no domínio organizacional; e outros 2 (0,7%) apresentavam erros de sintaxe nos registros, restando também desprotegidos. Este quadro inicial mostrou que, antes de qualquer ação de mitigação, a maioria dos órgãos da APF estava vulnerável a ataques de *spoofing* de e-mail, sendo que a maior parte encontrava-se na categoria mais crítica de vulnerabilidade, cenário alarmante numa amostra composta por entes relacionados a infraestruturas críticas e produção de conhecimentos sensíveis.

Ao final do período de atuação desta pesquisa, em julho de 2026, o estado de vulnerabilidade havia se invertido. Observou-se que, dos 281 domínios da amostra, 185 (65,8%) apresentavam configurações que tornavam a falsificação impraticável, enquanto 96 (34,2%) permaneciam vulneráveis em alguma medida. Destes, 76 (27,0%) encontravam-se completamente vulneráveis, 16 (5,7%) vulneráveis apenas no âmbito dos subdomínios; 2 (0,7%) apenas no domínio organizacional e outros 2 (0,7%) permaneceram com erro de sintaxe.

Em termos comparativos, como indica o Gráfico 4.9, o efeito conjunto das ações de mitigação executadas elevou o percentual de domínios protegidos de 35,23% para 65,84%, uma variação positiva de 30,61 pontos percentuais, consequentemente reduzindo a proporção de domínios vulneráveis de 64,77% para 34,16% no intervalo de dezoito meses. Este resultado valida o objetivo geral desta pesquisa ao demonstrar empiricamente que foi possível contribuir com a resiliência cibernética da APF frente a ataques de *spoofing* de e-mail por meio de intervenções contínuas de mitigação.

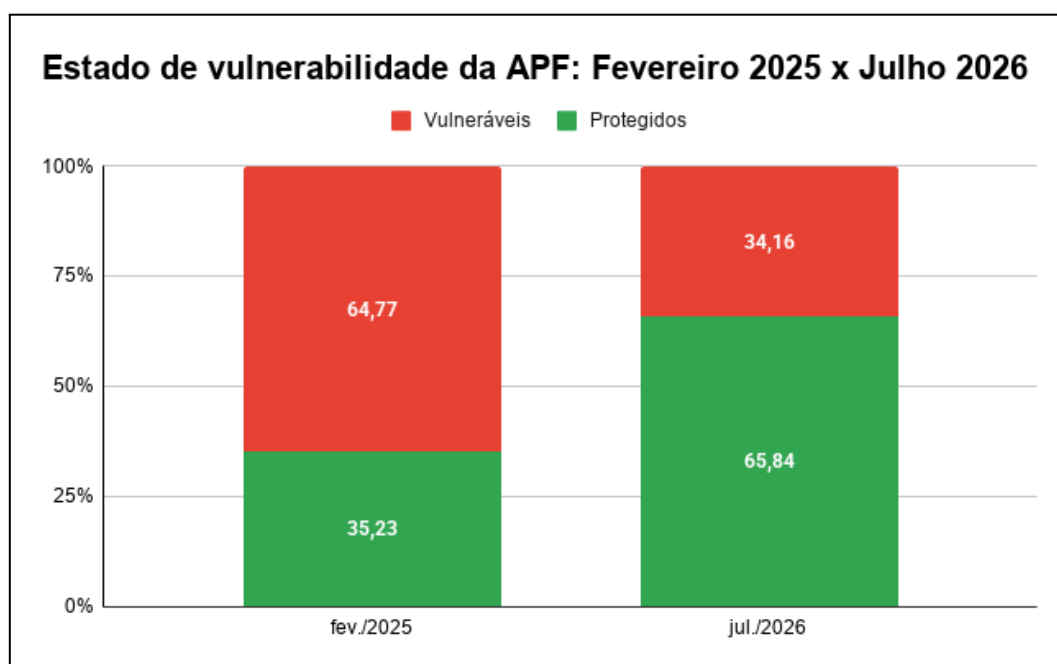


Gráfico 4.9. Variação no estado de vulnerabilidade dos domínios da APF no período analisado.

4.2.4. Evolução da implementação e da conformidade da configuração dos protocolos SPF, DKIM e DMARC nos domínios da APF ao longo da pesquisa

Nesta seção, procede-se uma análise mais detalhada da evolução de toda a amostra, considerada mês a mês, levando em consideração os efeitos de cada ação de mitigação realizada.

O Gráfico 4.10 e a Tabela 4.1 apresentam os dados agregados, coletados ao longo dos dezoito meses de observação, referentes a todos os 281 domínios que compõem a amostra, e permitem a visualização da evolução temporal da mitigação da vulnerabilidade na amostra.

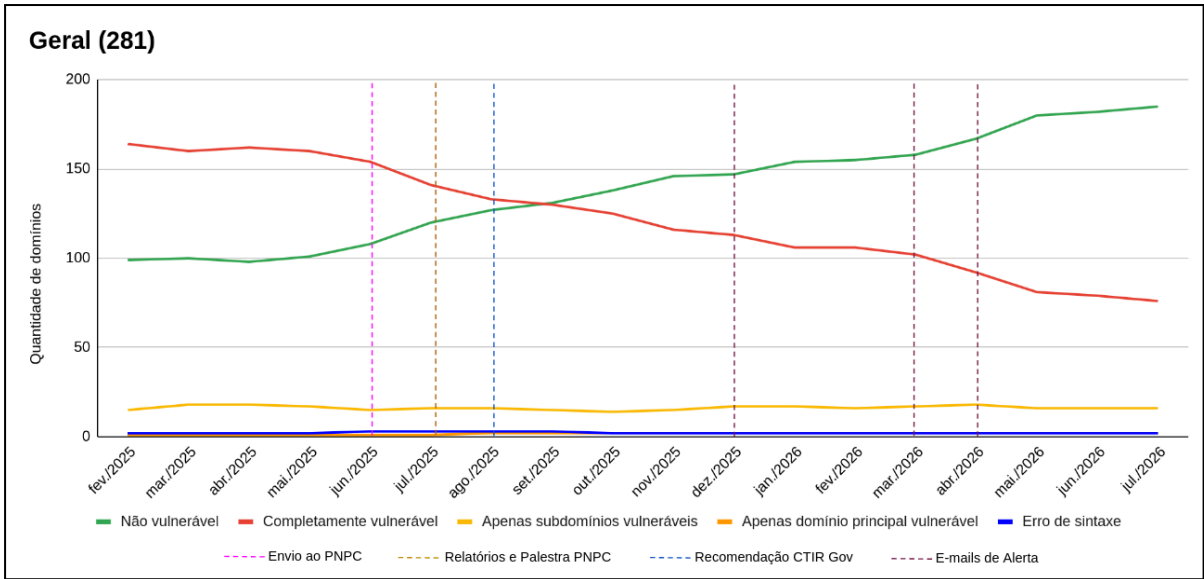


Gráfico 4.10. Evolução da mitigação da vulnerabilidade ao longo da investigação em todos os 281 domínios.

Tabela 4.1. Dados coletados referentes aos 281 domínios da APE.

	Não Vulneráveis	Vulneráveis			
		Completamente Vulneráveis	Apenas Subdomínios	Apenas Domínio Principal	Erro de Sintaxe
fev./2025	99	164	15	1	2
mar./2025	100	160	18	1	2
abr./2025	98	162	18	1	2
mai./2025	101	160	17	1	2
jun./2025	108	154	15	1	3
jul./2025	120	141	16	1	3
ago./2025	127	133	16	2	3
set./2025	131	130	15	2	3
out./2025	138	125	14	2	2
nov./2025	146	116	15	2	2
dez./2025	147	113	17	2	2
jan./2026	154	106	17	2	2
fev./2026	155	106	16	2	2

mar./2026	158	102	17	2	2
abr./2026	167	92	18	2	2
mai./2026	180	81	16	2	2
jun./2026	182	79	16	2	2
jul./2026	185	76	16	2	2

Como já mencionado na seção anterior, no início da coleta (fevereiro de 2025), o cenário da APF era predominantemente vulnerável. Dos 281 domínios analisados, 182 (64,77%) encontravam-se em alguma condição de exposição, ao passo que apenas 99 (35,23%) estavam plenamente protegidos. Esse quadro manteve-se praticamente estável ao longo dos cinco primeiros meses de observação passiva, entre fevereiro e junho de 2025, período em que, conforme descrito na metodologia, nenhuma ação de mitigação foi proposta, justamente para aferir o comportamento natural da amostra na ausência de intervenções externas.

De fato, entre fevereiro e maio de 2025, o número de domínios não vulneráveis oscilou muito discretamente, entre 98 e 101, o que reforça a hipótese de que a vulnerabilidade não tenderia a ser corrigida espontaneamente pelos órgãos e que a inércia institucional poderia prolongar o problema caso nenhuma ação fosse tomada.

A despeito de uma tímida evolução espontânea em junho de 2025, o primeiro sinal de inflexão surgiu exatamente na coleta de julho — mês que sucedeu o repasse dos dados de junho ao PNPC da ABIN —, quando o número de domínios não vulneráveis saltou de 108 para 120, um acréscimo de 12 unidades, o maior até então registrado na série. Esse resultado sugere que a comunicação institucional realizada por intermédio do PNPC, ainda que majoritariamente dirigida aos órgãos do SISBIN, produziu um efeito de mitigação mensurável e praticamente imediato sobre a amostra geral.

O movimento de queda da vulnerabilidade prosseguiu de forma consistente nos meses subsequentes — agosto (127), setembro (131), outubro (138) e novembro (146) —, período que sucede à realização da palestra de conscientização, em julho, e abrange a publicação da Recomendação 06/2025 do CTIR Gov, em agosto, cujos efeitos cumulativos sustentaram notável ritmo de mitigação.

Este ritmo, contudo, arrefeceu visivelmente entre novembro e dezembro de 2025, quando a quantidade de domínios não vulneráveis praticamente estagnou, passando de 146 a 147. Esta estagnação indica que o efeito das ações institucionais de caráter mais amplo já havia se esgotado, uma vez que os órgãos que permaneciam em condições de vulnerabilidade pareciam menos sensíveis a comunicações de natureza coletiva e gerencial. Foi justamente neste momento que se iniciou o segundo ciclo de ações de mitigação, agora de caráter direto e individualizado para cada um dos órgãos vulneráveis, com o envio do primeiro alerta por e-mail (feito entre os dias 15 e 20 de dezembro de 2025). O efeito dessa mudança de estratégia já se manifestou na coleta de janeiro de 2026, quando o número de domínios protegidos voltou a crescer de forma expressiva, passando de 147 para 154.

Novamente, observou-se um período de relativa acomodação entre fevereiro e março de 2026 (155 e 158 domínios não vulneráveis, respectivamente), seguido por um novo salto após o segundo alerta individualizado por e-mail, enviado entre 31 de março e 2 de abril de 2026. A coleta de abril registrou 167 domínios protegidos, um incremento de 9 unidades em relação ao mês anterior.

O efeito mais relevante de toda a série, entretanto, foi verificado após o terceiro e último alerta individualizado, enviado entre os dias 22 e 24 de abril de 2026, que se diferenciou dos anteriores por incorporar um apelo de natureza normativa, mencionando expressamente a obrigatoriedade da observância das recomendações do CTIR Gov, de acordo com o previsto no Decreto nº 10.748/2021, e reforçando a existência da Recomendação 06/2025 sobre a vulnerabilidade de *spoofing* de e-mail. Na coleta de maio, o número de domínios não vulneráveis avançou de 167 para 180, um ganho de 13 domínios em um único mês, o maior de toda a pesquisa.

Nos dois últimos meses de observação, junho e julho de 2026, a curva voltou a se estabilizar, com incrementos mais modestos (182 e 185 domínios não vulneráveis, respectivamente), o que é compatível com o efeito tardio observado após ações de mitigação anteriores, além da expectativa de que os órgãos remanescentes representem os casos de maior resistência à correção — por limitações técnicas, de governança interna ou de priorização — e não meramente por desconhecimento do problema.

Chama a atenção, ainda, o comportamento praticamente inerte das três categorias de vulnerabilidade parcial ao longo de todo o período observado. Os domínios classificados como “Apenas Subdomínios Vulneráveis” oscilaram sempre entre 14 e 18 unidades, os classificados como “Apenas Domínio Principal Vulnerável” mantiveram-se entre 1 e 2, e os com “Erro de Sintaxe” entre 2 e 3, sem qualquer tendência de resposta associada às ações de mitigação. Isso indica que praticamente a totalidade da melhoria observada na amostra decorreu da conversão de domínios “Completamente Vulneráveis” em “Não Vulneráveis” ao passo que as vulnerabilidades parciais se mostraram mais persistentes e menos responsivas ao conjunto de ações adotadas, permanecendo como um resíduo mais difícil de tratar por meio de conscientização.

Quando o período é segmentado de acordo com as janelas de observabilidade de cada ação de mitigação, os incrementos, em termos percentuais, ficam assim distribuídos: 6,8 pontos após o relato ao PNPC e a palestra de conscientização (junho a agosto de 2025); 7,1 pontos no intervalo associado à Recomendação 06/2025 do CTIR Gov (agosto a dezembro de 2025); 3,9 pontos após a primeira notificação por e-mail (dezembro de 2025 a março de 2026); 3,2 pontos no mês seguinte à segunda notificação (março a abril de 2026); e 6,4 pontos após a terceira notificação, com apelo normativo (abril a julho de 2026). Os dois maiores saltos mensais isolados de toda a série ocorrem em julho de 2025 (+4,3) e em maio de 2026 (+4,7), isto é, exatamente nas primeiras coletas após o acionamento do PNPC e o alerta que invocou o Decreto nº 10.748/2021 e a Recomendação 06/2025. Isso poderia indicar, caso não houvesse sobreposição temporal do efeito das medidas de intervenção propostas, que a articulação institucional por meio de comunidades de inteligência e o apelo à obrigatoriedade

normativa surtem mais efeito do que notificações meramente técnicas. Essa possível relação poderia ser objeto de uma investigação futura.

Por fim, uma análise individualizada, domínio a domínio, traz achados que os dados agregados não revelam. Dos 182 domínios inicialmente vulneráveis, 91 nunca deixaram essa condição em nenhuma das 18 coletas realizadas, permanecendo vulneráveis do primeiro ao último mês sem qualquer alteração de estado. Os demais 91 domínios alcançaram, em algum momento da série, a condição de proteção; destes, porém, apenas 89 mantiveram-se corrigidos até o final da pesquisa, enquanto os outros 2 regrediram à vulnerabilidade, terminando a pesquisa no mesmo estado em que a iniciaram, apesar da correção temporária. Olhando para toda a amostra, e não apenas para o subconjunto inicialmente vulnerável, 26 domínios apresentaram ao menos um episódio de retorno à condição vulnerável após alcançarem a proteção. Estas constatações permitem afirmar que existe uma instabilidade nas configurações DNS e que a proteção contra a falsificação de endereços de e-mail exige manutenção e monitoramento contínuos, não apenas intervenções pontuais.

4.3. RESULTADOS POR AGRUPAMENTO TEMÁTICO

Cabe agora examinar os resultados de forma comparativa, a fim de identificar quais segmentos da APF mais se beneficiaram do conjunto de ações de mitigação empregadas nesta pesquisa e, por outro lado, quais se mostraram mais refratários a elas. Conforme ilustra o Gráfico 4.11, o ganho percentual de proteção variou entre os agrupamentos, oscilando de 20,00 a 66,66 pontos percentuais, em contraste com a variação consolidada de 30,61 pontos percentuais na amostra geral. Essa dispersão, de mais de 46 pontos percentuais entre o melhor e o pior desempenho relativo, indica que, embora o efeito das ações de mitigação tenha sido positivo em absolutamente todos os agrupamentos sem exceção, sua magnitude não foi homogênea.

Os três maiores ganhos percentuais couberam aos grupos “Indústria, Comércio e Serviços” (66,66 pontos), “Saúde e Saneamento” (58,33 pontos) e “Agricultura e Organização Agrária” (50,00 pontos). Estes resultados, contudo, exigem leituras distintas. O primeiro caso deve ser interpretado com cautela adicional, uma vez que se trata do menor agrupamento da amostra, com apenas 6 órgãos. Nesse contexto, a correção de um único domínio já corresponde a mais de 16 pontos percentuais de variação, de modo que o resultado, embora real, é mais volátil do que os demais. O caso de “Saúde e Saneamento”, por sua vez, é o que melhor representa uma resposta genuína e distribuída ao longo do tempo. Esse segmento reagiu de forma identificável a praticamente todas as ações de mitigação, incluindo uma resposta particularmente acentuada ao terceiro alerta por e-mail, o que também resultou na completa eliminação de vulnerabilidades parciais. Já o resultado de “Agricultura e Organização Agrária”, apesar de expressivo em magnitude, decorreu majoritariamente de dois movimentos espontâneos concentrados em março e junho de 2025 — anteriores ao início de qualquer ação de mitigação da pesquisa —, o que relativiza a atribuição desse ganho às intervenções aqui propostas.

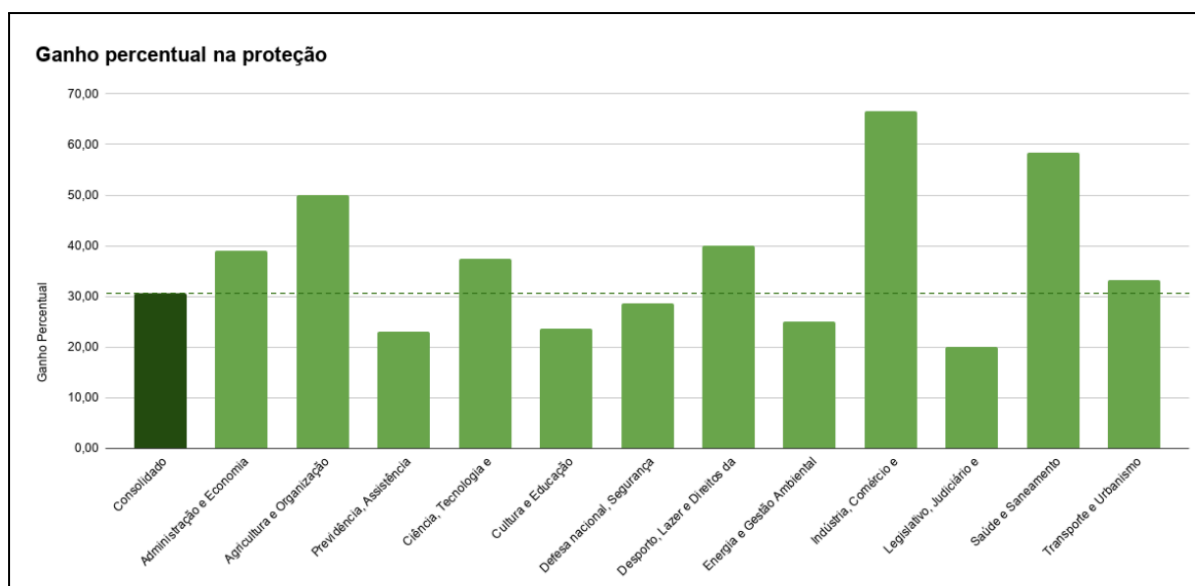


Gráfico 4.11. Ganho percentual na proteção dos órgãos da APF contra spoofing de e-mail durante o período analisado.

No extremo oposto, os menores ganhos percentuais foram registrados em “Legislativo, Judiciário e Essenciais à Justiça” (20,00 pontos), “Previdência, Assistência Social, Trabalho e Habitação” (23,08 pontos) e “Cultura e Educação” (23,57 pontos) — este último, o maior agrupamento da amostra, reunindo 123 dos 281 domínios analisados, o que representa aproximadamente 44% do total. O desempenho abaixo da média deste agrupamento específico é particularmente relevante para a compreensão do resultado geral da pesquisa. Por representar quase metade da amostra em termos numéricos, a trajetória do grupo “Cultura e Educação” exerce um peso desproporcional sobre a curva consolidada. Em outras palavras, o resultado agregado da amostra reflete, no caso em tela, o comportamento do maior bloco que a compõe.

Situando-se em posição intermediária, abaixo da média geral, estão ainda os agrupamentos de “Energia e Gestão Ambiental” (25,00 pontos) e de “Defesa Nacional, Segurança Pública e Relações Exteriores” (28,57 pontos). O primeiro merece destaque, ainda que seu ganho percentual seja modesto. Trata-se do único agrupamento que elimina por completo a categoria “Completamente Vulnerável”, ou seja, o cenário de maior severidade. Esse caso ilustra um ponto metodológico importante para a discussão dos resultados aqui analisados. O ganho percentual de proteção, por si só, pode não evidenciar integralmente a qualidade da melhoria obtida, uma vez que partir de uma condição inicial já relativamente favorável, como é o caso do grupo “Energia e Gestão Ambiental” (45% de vulnerabilidade em fevereiro de 2025, a mais baixa entre todos os agrupamentos) naturalmente comprime a margem de ganho percentual disponível, mesmo quando o resultado qualitativo — a erradicação da vulnerabilidade mais crítica, por exemplo — é um dos mais expressivos de toda a pesquisa.

Acima da média geral, em posição intermediária, situam-se “Transporte e Urbanismo” (33,33 pontos), “Ciência, Tecnologia e Comunicações” (37,50 pontos), “Administração e Economia” (39,13 pontos) e “Desporto, Lazer e Direitos da Cidadania” (40,00 pontos). Ao todo, sete dos doze agrupamentos superaram o ganho médio da amostra geral, ao passo que cinco ficaram

abaixo dele, entre eles o agrupamento mais numeroso da amostra, o que reforça a leitura de que a melhoria consolidada, embora real, esconde uma heterogeneidade entre os diferentes segmentos da APF. Contudo, repisa-se, todos os segmentos tiveram aumento na proteção durante o período observado.

Quanto à natureza das ações de mitigação, observa-se também uma divisão relevante entre os agrupamentos. Alguns grupos — como “Transporte e Urbanismo”, “Ciência, Tecnologia e Comunicações” e, em menor medida, “Saúde e Saneamento” — concentraram a maior parte de seu progresso já nas ações institucionais de 2025 (o repasse ao PNPC, a palestra de conscientização e a Recomendação 06/2025 do CTIR Gov), mostrando-se posteriormente refratários às comunicações individualizadas por e-mail, inclusive ao terceiro alerta (de caráter normativo). Em contraposição, outros agrupamentos — como “Cultura e Educação”, “Energia e Gestão Ambiental”, “Administração e Economia” e “Desporto, Lazer e Direitos da Cidadania” — tiveram no terceiro alerta seu principal ponto de inflexão. Essa distinção sugere que a eficácia entre comunicação institucional, comunicação individualizada técnica e comunicação individualizada com apelo normativo não é uniforme, variando provavelmente em função de características próprias de cada setor — como a maturidade da governança de segurança da informação, a estrutura de *compliance* normativo ou o grau de centralização da gestão de TI —, aspectos que extrapolam o escopo desta pesquisa, mas que se apresentam como possíveis direções para investigações futuras.

Por fim, um padrão identificado já na análise da amostra geral confirma-se, com poucas exceções, também no nível dos agrupamentos. Ao final do período de observação, oito dos doze agrupamentos ainda apresentavam ao menos um domínio residual classificado em alguma das categorias de vulnerabilidade parcial, muitas vezes inalterado desde sua primeira ocorrência na série histórica. Apenas quatro agrupamentos encerraram a pesquisa com um perfil de vulnerabilidade residual restrito à categoria “Completamente Vulnerável”, sem qualquer caso remanescente de vulnerabilidade parcial. Esse achado reforça a hipótese de que as vulnerabilidades parciais representam um problema mais difícil de equacionar por meio de comunicação e conscientização, possivelmente por refletirem arranjos técnicos mais sofisticados do que propriamente desconhecimento do risco.

O Apêndice A aprofunda a discussão dos resultados ao examinar o comportamento individual de cada um dos doze grupos de área de atuação.

4.4. RESPOSTAS RECEBIDAS

Complementarmente à análise quantitativa da evolução do estado de vulnerabilidade apresentada nas seções anteriores, cabe registrar que os três ciclos de alerta individualizado por e-mail geraram, em diversos casos, retorno direto por parte dos órgãos notificados, o que permite qualificar, ainda que de forma ilustrativa, o nível de engajamento institucional da APF diante da comunicação direcionada. As respostas recebidas variaram desde manifestações de agradecimento e encaminhamento interno da demanda às equipes técnicas

responsáveis, passando por relatos concretos de correção, até um interessante caso em que a instituição condicionou qualquer alteração em seus registros DNS à verificação prévia da autenticidade da comunicação e da identificação do pesquisador, evidenciando a existência de protocolos internos de segurança mais rigorosos frente a solicitações externas.

Uma seleção dessas trocas de mensagens, consideradas representativas da contribuição social desta pesquisa e da diversidade de posturas institucionais observadas ao longo do processo de notificação, encontra-se reproduzida, com a devida anonimização das partes envolvidas, entres as figuras B.1 e B.8 constantes do Apêndice B desta dissertação.

5. CONCLUSÕES

O problema de pesquisa que norteou esta dissertação foi conhecer o estado de vulnerabilidade da Administração Pública Federal brasileira frente a ataques de *spoofing* de e-mail, gerar ações que auxiliassem na mitigação dessa ameaça e constatar se as referidas intervenções contribuíram para a evolução do quadro de proteção das instituições. Logo, a escolha por um desenho prospectivo-longitudinal, com dezoito coletas mensais — realizadas entre fevereiro de 2025 e julho de 2026 — sobre a totalidade dos domínios da APF que operam correio eletrônico, impôs à investigação um compromisso que não se esgotava no mero diagnóstico. Não bastava descrever a exposição; era necessário verificar se ela se alterava e em que medida essa alteração respondia ao que a própria pesquisa propunha. Cabe, portanto, examinar se o percurso descrito nos capítulos anteriores efetivamente entregou aquilo a que se propôs.

5.1. RESPOSTAS ÀS QUESTÕES DE PESQUISA

A primeira questão de pesquisa desta dissertação indagava quais seriam as taxas de adoção e de conformidade dos registros SPF, DKIM e DMARC entre os órgãos públicos federais brasileiros. Na primeira coleta, a taxa de adoção do SPF já se encontrava praticamente saturada, com 271 dos 281 domínios (96,4%) publicando registro, ao passo que o DMARC alcançava 208 domínios (74,0%) e o DKIM identificável limitava-se a 156 (55,5%). Ao final do período de observação, esses valores haviam evoluído para 274 (97,5%), 256 (91,1%) e 182 (64,8%), respectivamente. No que diz respeito à conformidade, entre os domínios com SPF, o qualificador restritivo “-all” passou de 174 (64,2%) para 186 (67,9%), enquanto “~all” recuou de 94 (34,7%) para 84 (30,7%). No DMARC, a política permissiva “p=none” caiu de 91 domínios (43,8%) para 54 (21,1%), enquanto “p=quarantine” tornou-se majoritária ao passar de 91 (43,8%) para 150 (58,6%) e “p=reject” ampliou sua participação de 24 (11,5%) para 52 (20,3%). A questão fica respondida, portanto, com a ressalva metodológica de que a adoção do DKIM só pôde ser aferida por meio de uma lista de cem seletores comuns, o que impede afirmar categoricamente que os 35,2% restantes não o tenham implementado — limitação que, embora não invalide o achado, delimita seu alcance.

A segunda questão dizia respeito às deficiências mais recorrentes nas configurações das extensões de segurança SMTP e às ações práticas capazes de mitigá-las. A ausência ou a permissividade da política DMARC “p=” foi a deficiência mais determinante, suficiente para explicar, ao final da pesquisa, a totalidade dos casos remanescentes de vulnerabilidade completa da amostra. A explícita não rigidez da política de subdomínios “sp=” ocupou o segundo lugar, restrita a uma parcela menor de domínios, mas presente de forma persistente e praticamente uniforme em todas as coletas. Ainda que de menor alcance, parte das demais deficiências residuais — ausência de registro SPF, registro SPF duplicado, expansão recursiva de consultas DNS acima do limite regulamentar, *loop* de resolução e erros de sintaxe no registro DMARC — não sofreu qualquer alteração ao longo das ações de mitigação, persistindo praticamente inalterada durante todo o período de observação. Isso

reforça que a mitigação da falsificação de e-mails não se resume à mera adoção de protocolos, exigindo também entendimento técnico completo das extensões e monitoramento contínuo. Quanto às ações práticas, tema que será retomado adiante, a resposta foi construída sobre ações de conscientização e comunicação institucional coletiva, e ações de alerta diretas e individualizadas.

A terceira questão buscava determinar o estado de vulnerabilidade dos órgãos públicos federais brasileiros a ataques de *spoofing*. Em fevereiro de 2025, apenas 99 domínios (35,2%) apresentavam configurações que tornavam a falsificação impraticável, enquanto 182 (64,8%) encontravam-se expostos em algum grau — sendo 164 (58,4%) na condição mais crítica, sujeitos à falsificação tanto do domínio organizacional quanto de seus subdomínios, 15 (5,3%) vulneráveis apenas nos subdomínios, um (0,4%) apenas no domínio organizacional e dois (0,7%) com erros de sintaxe que equivalem, na prática, à desproteção. Em julho de 2026, o quadro havia se invertido: 185 domínios (65,8%) protegidos contra 96 (34,2%) ainda vulneráveis, dos quais 76 (27,0%) completamente vulneráveis. Portanto, o estado inicial era o de uma APF majoritariamente exposta; o estado final é o de uma Administração majoritariamente protegida, ainda que com um resíduo relevante.

A quarta questão, por fim, interrogava como teriam evoluído a implementação e a conformidade dos protocolos ao longo dos dezoito meses, considerando-se as ações de mitigação propostas. A resposta encontra-se na segmentação da série temporal em janelas de observabilidade para cada intervenção. As cinco primeiras coletas, deliberadamente conduzidas sem qualquer ação, confirmaram a hipótese de que o problema não recebia a devida atenção. Além de estagnação, registraram-se episódios de agravamento espontâneo em alguns agrupamentos. A partir do repasse dos resultados ao PNPC e da palestra de conscientização, verificou-se ganho de 6,8 pontos percentuais; 7,1 pontos no intervalo associado à Recomendação 06/2025 do CTIR Gov; 3,9 pontos após o primeiro alerta individualizado por e-mail; 3,2 pontos após o segundo; e 6,4 pontos após o terceiro, este último acrescido de apelo normativo. Os dois maiores saltos mensais isolados de toda a série ocorreram precisamente nas primeiras coletas após o acionamento do PNPC, em julho de 2025, e após o alerta individualizado que invocou o Decreto nº 10.748/2021 e a Recomendação 06/2025, em maio de 2026. A evolução, portanto, não foi apenas positiva, foi temporalmente relacionada às intervenções, o que sustenta a atribuição causal, ainda que se reconheça a impossibilidade de isolá-la por completo de fatores externos ao estudo.

5.2. ALCANCE DOS OBJETIVOS

5.2.1. Alcance do Objetivo Geral

O objetivo geral deste trabalho era auxiliar na mitigação da vulnerabilidade dos órgãos públicos federais brasileiros a ataques de *spoofing* de e-mail, ampliando a resiliência cibernética das infraestruturas críticas e a proteção de conhecimentos sensíveis de interesse do Estado e da sociedade. A verificação de seu alcance pode ser constatada pelo percentual

de domínios protegidos, que passou de 35,23% para 65,84% ao longo dos dezoito meses, uma variação positiva de 30,61 pontos percentuais, com a correspondente redução da proporção de domínios vulneráveis de 64,77% para 34,16%. A inversão do quadro é acompanhada de relação temporal entre os incrementos observados e as janelas de efeito das intervenções conduzidas, e é reforçada pela constatação de que, no período de observação passiva, em que nenhuma ação foi tomada, a amostra permaneceu praticamente estável.

Cabe, contudo, uma análise dos limites desse resultado. O objetivo não era — de forma audaciosa — erradicar a vulnerabilidade, mas auxiliar na mitigação, o que mostrou-se adequado ao que se pôde efetivamente entregar. Ao término da investigação, 96 domínios permaneciam expostos, dos quais 76 na condição mais grave. Trata-se, com boa probabilidade, do conjunto de casos menos sensíveis à conscientização — resistentes às ações institucionais e às três rodadas de alerta, incluindo o próprio argumento de obrigatoriedade normativa —, cuja correção depende de fatores que extrapolam o alcance de uma pesquisa acadêmica, como a maturidade da governança de tecnologia da informação, a disponibilidade de pessoal técnico e a prioridade institucional atribuída ao tema. Reconhecido esse resíduo, o objetivo geral pode ser considerado atingido. A vulnerabilidade foi amplamente mitigada e a resiliência cibernética da APF frente à falsificação de endereços de e-mail evoluiu de forma mensurável. Além disso, o instrumento produzido ao longo do percurso permanece disponível para que essa ampliação prossiga mesmo com o encerramento da presente investigação.

5.2.2. Alcance dos Objetivos Específicos

O primeiro objetivo específico consistia em delimitar e caracterizar o universo de domínios pertencentes à APF, distinguindo aqueles que efetivamente operam infraestrutura de correio eletrônico. Partiu-se da relação oficial de 331 órgãos federais dos três Poderes, e a verificação por fontes abertas conduziu à exclusão dos que não possuíam domínio próprio, não registravam servidores MX ou utilizavam o domínio de um órgão superior para troca de mensagens eletrônicas, restando 281 domínios efetivamente expostos ao risco. Esses domínios foram ainda distribuídos em doze agrupamentos por área de atuação, com base na classificação empregada pelo Portal da Transparência do governo federal. O objetivo foi alcançado, e o recorte resultante confere validade ao caráter censitário do estudo, uma vez que a amostra passou a corresponder à população efetivamente vulnerável, e não ao conjunto formal de órgãos.

O segundo objetivo previa mensurar a adoção e a conformidade dos três mecanismos de autenticação (SPF, DKIM e DMARC) e classificar objetivamente o nível de vulnerabilidade de cada órgão. Seu alcance dependia da existência de um instrumento capaz de realizar essa mensuração de forma automatizada, reproduzível e não dependente do comportamento de MTAs ou MUAs específicos, requisito que as soluções correlatas examinadas na fundamentação teórica não atendiam. Desenvolveu-se, para isso, a ferramenta *StopEmailSpoofing*, estruturada em torno de uma tabela que relaciona as 295 combinações

possíveis entre o mecanismo “all” do SPF e as *tags* “p”, “aspf” e “sp” do DMARC, das quais 187 resultam em algum grau de exposição e apenas 108 são protetivas. A ferramenta foi validada empiricamente em ambiente controlado, teve seu código-fonte disponibilizado à comunidade, foi objeto de artigo publicado na Revista Ibérica de Sistemas e Tecnologias de Informação e obteve registro junto ao INPI. Das dezoito coletas resultaram 5.058 registros, e o objetivo foi alcançado tanto no plano da mensuração quanto no da classificação, com a limitação já apontada quanto ao DKIM.

O terceiro objetivo referia-se à compreensão de como a vulnerabilidade se distribui entre os setores da administração, sem comprometer a identidade dos órgãos individualmente expostos. A opção por reportar os resultados de forma agrupada atendeu simultaneamente ao propósito analítico e à cautela de não converter esta dissertação em um “cardápio de alvos” disponível aos atacantes. Os maiores ganhos couberam aos grupos “Indústria, Comércio e Serviços”, “Saúde e Saneamento” e “Agricultura e Organização Agrária”, embora cada um exija leitura própria. Os menores ganhos ocorreram em “Legislativo, Judiciário e Essenciais à Justiça”, “Previdência, Assistência Social, Trabalho e Habitação” e “Cultura e Educação”, este último reunindo 123 dos 281 domínios e, por isso, exercendo peso desproporcional sobre a curva consolidada. Registrou-se, ainda, que “Energia e Gestão Ambiental”, apesar de um ganho percentual modesto, foi o único agrupamento a eliminar integralmente a categoria de maior severidade, o que evidencia os limites do ganho percentual como métrica isolada de qualidade. Todos os doze grupos apresentaram progresso. Dez deles passaram, ao longo do período, de uma maioria vulnerável a uma maioria protegida. Os outros dois já se encontravam em situação melhor no início da investigação e aumentaram ainda mais sua proteção.

O quarto objetivo vinculava a pesquisa à devolução dos achados aos órgãos vulneráveis, com o fornecimento de subsídios técnicos para correção. Esse compromisso foi cumprido em duas camadas. Na camada institucional, os resultados parciais foram apresentados ao Programa Nacional de Proteção do Conhecimento Sensível da ABIN, o que resultou na difusão de relatórios aos órgãos do SISBIN e em uma palestra presencial em julho de 2025. Esta última, pela presença de representantes do CTIR Gov, desdobrou-se na atualização e republicação da Recomendação nº 06/2025, elaborada em conjunto com a ABIN, que prescreveu boas práticas de implementação conjunta de SPF, DKIM e DMARC na REGIC, desaconselhou explicitamente o modo de monitoramento “p=none” e tratou do alinhamento entre as *tags* “p” e “sp” — precisamente as primeira e segunda deficiências mais recorrentes identificadas nesta pesquisa. Ao vincular-se ao Decreto nº 10.748/2021, a recomendação converteu os parâmetros analíticos aqui construídos em padrão de conformidade obrigatório para a APF. Na camada individualizada, três rodadas de alertas foram enviadas, com prioridade a ETIRs, CSIRTs e contas de *abuse*, contendo a situação específica de cada domínio e as ações requeridas para saná-la. O objetivo foi, assim, superado em relação ao que se havia proposto originalmente, uma vez que a devolutiva não se limitou aos órgãos da amostra, alcançando o ecossistema normativo que os regula.

O quinto objetivo dizia respeito à compreensão da dinâmica temporal da resiliência cibernética da APF e à inferência do efeito mensurável das ações propostas. Os dados sustentam três constatações. A primeira é que a vulnerabilidade não se corrige espontaneamente e pode, inclusive, agravar-se na ausência de intervenção, como se observou durante a fase de observação passiva. A segunda é que praticamente toda a melhoria decorreu da conversão de domínios completamente vulneráveis em não vulneráveis — categoria que recuou de 164 para 76, uma redução de 53,7% —, enquanto as vulnerabilidades parciais permaneceram inertes, oscilando em faixas estreitas ao longo de toda a série, sem tendência de queda associada a qualquer das ações. A terceira é que a eficácia dos diferentes tipos de comunicação não é uniforme entre os setores. Alguns agrupamentos responderam sobretudo às ações institucionais de 2025 e mostraram-se refratários às comunicações individualizadas, ao passo que outros tiveram no terceiro alerta, de apelo normativo, seu principal ponto de inflexão. O objetivo foi alcançado, e sua resposta é a que apresenta maior potencial de aproveitamento para futuras políticas de cibersegurança, ao indicar que a conscientização técnica e o argumento de conformidade normativa atuam sobre públicos parcialmente distintos, porém complementares.

5.3. CONTRIBUIÇÕES DA PESQUISA

5.3.1. Contribuições Acadêmicas

A primeira contribuição desta dissertação é de natureza instrumental. As soluções examinadas na revisão — *MXToolbox SuperTool*, a proposta de D'Angelone (53), o *DMARC Guide* e o *Domain Security Scanner* da Global Cyber Alliance, o Teste TOP E-mail do NIC.br e o *Spoofy* — apresentavam, em conjunto, um mesmo padrão de lacunas: ausência de suporte a subdomínios, omissão de parâmetros determinantes do DMARC, inexistência de classificação de níveis ou tipos de vulnerabilidade e cobertura incompleta das combinações entre registros capazes de gerar exposição. O *StopEmailSpoofing* foi concebido para preencher simultaneamente essas lacunas em uma única ferramenta.

A essa contribuição soma-se um deslocamento conceitual que merece registro. A tabela de combinações do *Spoofy*, referência mais próxima do que aqui se propôs, foi construída a partir da observação do comportamento de MUAs específicos ao receberem mensagens falsificadas, o que levou à existência de categorias dependentes da caixa postal do destinatário. Esta pesquisa sustentou que a vulnerabilidade ao *spoofing*, quando se trata da perspectiva dos nomes de domínio, deve ser tratada como propriedade declarada no DNS e não como resultado observado em provedores receptores particulares, uma vez que a vítima potencial pode utilizar qualquer servidor ou cliente não contemplado nos testes e que decisões de autenticação podem ser complementadas ou sobrepostas por filtros antispam. Ao desacoplar o diagnóstico do comportamento de terceiros, a avaliação passa a alinhar-se exatamente ao que está sob controle do administrador do domínio, que é quem pode intervir. A validação empírica da ferramenta proposta — conduzida em ambiente controlado com dois domínios adquiridos e um servidor próprio, o que permitiu inspecionar o cabeçalho

“Authentication-Results” de cada mensagem — oferece à comunidade um procedimento replicável de verificação.

Decorre daí uma terceira contribuição, de natureza classificatória. A tipologia em cinco categorias — não vulnerável, completamente vulnerável, vulnerável apenas no domínio organizacional, vulnerável apenas nos subdomínios e condição indeterminada por erro de sintaxe — introduz granularidade que a literatura revisada não oferecia e, sobretudo, trata explicitamente a camada de subdomínios, historicamente negligenciada tanto pelas ferramentas quanto pelos administradores.

No plano da evidência empírica, a contribuição reside no desenho longitudinal. As medições de adoção de SPF, DKIM e DMARC disponíveis na literatura são majoritariamente transversais, produzindo retratos temporais que permitem estimar a cobertura, mas não distinguir estagnação de evolução, nem identificar reversões. As dezoito coletas mensais realizadas sobre a totalidade dos domínios de correio da APF, das quais resultaram 5.058 registros, oferecem uma série temporal censitária que sustenta afirmações de outra ordem. Entre elas, a de que a vulnerabilidade não se corrige espontaneamente e pode agravar-se na ausência de intervenção, constatação corroborada pelos episódios observados durante a fase de observação passiva e pelos casos de erro de sintaxe que permaneceram inalterados por todo o período.

A pesquisa contribui, ainda, com um achado que qualifica a forma como a literatura costuma medir o problema. A adoção dos protocolos, tomada isoladamente, é indicador insuficiente de proteção. Entre os 76 domínios que permaneceram completamente vulneráveis ao final do período, 73 já dispunham de registro SPF válido e 40 adotavam inclusive seu qualificador mais restritivo, sem que isso lhes conferisse qualquer proteção efetiva, pois nenhum deles possuía política DMARC coercitiva. A ausência ou a permissividade da tag “p=” mostrou-se suficiente para explicar a totalidade dos casos remanescentes de exposição completa, o que estabelece uma hierarquia causal entre as deficiências e recomenda que futuras medições em larga escala privilegiem a conformidade combinada em vez da mera contagem de registros publicados.

Contribuição de natureza distinta, e possivelmente de maior interesse para além do campo técnico, é a que se refere à eficácia das diferentes intervenções para indução de mudança. Ao segmentar a série pelas janelas de efeito de cada intervenção, observou-se que a comunicação institucional, a comunicação individualizada de conteúdo técnico e a comunicação individualizada com apelo normativo não produzem resultados equivalentes, nem atuam de forma uniforme sobre os diferentes setores. Os dois maiores incrementos mensais de toda a série ocorreram nas coletas imediatamente posteriores ao acionamento do Programa Nacional de Proteção do Conhecimento Sensível e ao alerta que invocou o Decreto nº 10.748/2021 e a Recomendação 06/2025, ao passo que alguns agrupamentos concentraram seu progresso nas ações institucionais e mostraram-se refratários às notificações diretas, enquanto outros só reagiram ao argumento de obrigatoriedade. Trata-se de contribuição à literatura sobre segurança da informação em organizações, que frequentemente aborda a conscientização como categoria unitária.

Complementa esse achado a constatação de que as vulnerabilidades reagem de forma assimétrica às ações de mitigação. Praticamente toda a melhoria observada decorreu da conversão de domínios completamente vulneráveis em não vulneráveis, categoria que recuou de 164 para 76 ocorrências, enquanto as condições de vulnerabilidade parcial permaneceram inertes ao longo de toda a série, sem tendência associada a qualquer das intervenções. A hipótese que daí se extrai — a de que a exposição parcial reflete arranjos técnicos deliberados, e não desconhecimento do risco, sendo por isso menos sensível a conscientização — abre uma frente de investigação que esta dissertação identifica, mas não consegue esgotar.

Por fim, o percurso aqui descrito propõe um modelo de pesquisa aplicada de ciclo fechado, no qual diagnóstico, devolutiva e remensuração se aplicam numa mesma população, tornando a intervenção parte do objeto e não apenas um desdobramento. Esse modelo é diretamente transponível a outros recortes, como entes estaduais e municipais, setores ou administrações públicas de outros países, e sua reprodutibilidade está assegurada pela publicação do código-fonte e pela validação prévia do instrumento, submetida ao escrutínio de pares por meio do artigo publicado na Revista Ibérica de Sistemas e Tecnologias de Informação a partir do estudo de caso conduzido com os domínios das instituições públicas de ensino superior brasileiras. O registro do programa junto ao Instituto Nacional da Propriedade Industrial, sob titularidade da Fundação Universidade de Brasília, consolida institucionalmente esse produto e o mantém disponível como infraestrutura de pesquisa para além desta dissertação.

5.3.2. Contribuições Sociais

A contribuição social mais direta desta pesquisa é a redução mensurável da exposição de órgãos públicos federais brasileiros à falsificação de endereços de correio eletrônico. Entre fevereiro de 2025 e julho de 2026, o número de domínios com configurações que tornam a falsificação impraticável passou de 99 para 185, e a categoria de maior severidade recuou de 164 para 76 ocorrências. São 86 domínios institucionais que deixaram de poder ser explorados como remetentes falsos em campanhas de *phishing*. Convém destacar quem é o beneficiário desse resultado. A vítima de uma mensagem que se apresenta como originária de um órgão público não é apenas o próprio órgão — que tem sua identidade roubada —, mas também quem a recebe, isto é, o cidadão que responde a uma suposta notificação, a empresa que atende a uma suposta solicitação de dados, o servidor de outra instituição que abre um anexo aparentemente oficial. A correção de cada domínio protege, portanto, um conjunto de destinatários que nunca terá conhecimento da medida nem participação nela, e é nessa assimetria que reside boa parte do valor deste trabalho.

Essa proteção incide sobre um universo institucional com características particulares. A amostra reúne órgãos responsáveis por infraestruturas críticas e pela produção de conhecimentos sensíveis relacionados a decisões de interesse nacional. Como discutido na fundamentação teórica, uma mensagem falsificada contendo endereço malicioso é frequentemente o vetor inicial de ataques complexos, cujos desdobramentos, quando

bem-sucedidos contra entes públicos, podem incluir espionagem e sabotagem cibernéticas, vazamento de documentos classificados e comprometimento da confiança depositada no Estado, tanto internamente quanto perante outros países. Ao atuar na porta de entrada, a pesquisa contribui para a preservação de bens que vão além da segurança da informação em sentido estrito.

O desdobramento de maior alcance e permanência, contudo, é de natureza normativa. A apresentação dos resultados parciais ao Programa Nacional de Proteção do Conhecimento Sensível conduziu à difusão de relatórios aos órgãos do Sistema Brasileiro de Inteligência em situação de vulnerabilidade e a uma palestra de conscientização realizada em Brasília, cuja composição de público permitiu o contato interinstitucional que resultou na atualização e republicação da Recomendação nº 06/2025 pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, elaborada em conjunto com a Agência Brasileira de Inteligência. O documento prescreve boas práticas de implementação conjunta das extensões SPF, DKIM e DMARC e estabelece critérios de conformidade que vão além da mera adoção. Ao vincular-se ao Decreto nº 10.748/2021, que impõe aos órgãos federais o dever de sanar com urgência as vulnerabilidades apontadas nas recomendações do CTIR Gov, e ao compelir as equipes setoriais de tratamento de incidentes a orientar e fiscalizar suas comunidades, a recomendação converteu os parâmetros analíticos aqui construídos em padrão obrigatório de conformidade. O efeito dessa conversão alcança órgãos que sequer integraram a amostra e espera-se que permaneça produzindo consequências após o encerramento das coletas, representando a superação do isolamento habitual entre resultados acadêmicos e práticas regulatórias.

A pesquisa também deixou disponível, gratuitamente e em código aberto, um instrumento que qualquer administrador de domínio pode empregar para diagnosticar sua própria situação e obter orientação para correção. Não se trata apenas de dar publicidade a um resultado, mas de transferir capacidade. Enquanto as soluções existentes exigem consultas fragmentadas, não informam explicitamente se o domínio é vulnerável, ignoram subdomínios ou não permitem análise em volume, a ferramenta aqui desenvolvida fornece um diagnóstico conclusivo, com sugestões personalizadas de mitigação e saída em formato tabular que viabiliza auditorias em larga escala. Esse recurso está acessível a órgãos estaduais e municipais, a organizações privadas, ao terceiro setor e a instituições de ensino, que enfrentam a mesma ameaça sem dispor, em muitos casos, de equipes especializadas ou de orçamento para soluções comerciais.

O conteúdo das comunicações enviadas aos órgãos merece registro próprio como contribuição social. As mensagens não se limitaram a apontar a existência de um problema, mas descreveram a ameaça, informaram a condição específica em que cada domínio se encontrava e indicaram as ações imediatas necessárias para saná-la. A escolha por notificar diretamente cada órgão vulnerável, em vez de apenas relatar o panorama agregado, transformou a pesquisa em uma prestação de serviço à administração pública, com custo praticamente nulo para o Estado e resultado verificável tanto nos registros públicos de cada

domínio quanto nas respostas recebidas oriundas de diversos órgãos agradecendo pela contribuição.

Merece igual destaque a decisão de não identificar individualmente os órgãos vulneráveis, reportando os resultados por área de atuação. Publicar a relação nominal teria conferido à dissertação um caráter demonstrativo mais imediato, mas equivaleria a produzir um roteiro de alvos disponível a qualquer interessado, inclusive aos adversários contra os quais a pesquisa pretendia proteger. A opção adotada, que preserva a reprodutibilidade sem entregar a exposição alheia, oferece um precedente de divulgação responsável para investigações acadêmicas que lidam com vulnerabilidades de entidades públicas, campo em que o dever de informar e o dever de não expor entram em conflito com relativa frequência.

Por fim, a pesquisa oferece às políticas públicas de cibersegurança algo de que costumam carecer: uma linha de base e um método de aferição. A Política Nacional de Cibersegurança, a Estratégia Nacional de Cibersegurança, a Política Nacional de Segurança da Informação e a Estratégia Nacional de Segurança de Infraestruturas Críticas estabelecem objetivos de resiliência, prevenção e gestão de riscos sem que existam, na maioria das vezes, indicadores que permitam verificar se tais objetivos estão sendo alcançados. O procedimento aqui descrito converte alguns desses objetivos em métrica observável, coletável, a baixo custo e sem depender da autodeclaração dos órgãos avaliados.

5.4. LIMITAÇÕES DA INVESTIGAÇÃO

A prestação de contas iniciada nas seções anteriores só se completa com o reconhecimento dos limites dentro dos quais os achados aqui apresentados são válidos. Alguns destes limites decorrem de decisões metodológicas deliberadas, já justificadas nos capítulos precedentes; outros são impostos pela natureza do objeto ou pelas condições concretas em que a pesquisa se desenvolveu. Em ambos os casos, explicitá-los é condição para que os resultados sejam devidamente interpretados.

A limitação de maior alcance diz respeito ao próprio recorte do objeto. Esta pesquisa avaliou a vulnerabilidade intrínseca de nomes de domínio, conforme declarada publicamente no DNS por meio das extensões SPF, DKIM e DMARC. Essa escolha foi deliberada e constituiu, inclusive, o principal argumento para aprimorar a ferramenta desenvolvida frente às soluções existentes, uma vez que diagnósticos baseados no comportamento de servidores e clientes específicos podem levar a conclusões equivocadas sobre a segurança de um domínio. A contrapartida é que o estudo não afere o que efetivamente ocorre quando uma mensagem falsificada chega a um destinatário real. As decisões de autenticação de cada MTA ou MUA podem divergir das políticas declaradas, ser complementadas por filtros antispam, mecanismos de reputação ou heurísticas proprietárias, e até sobrepor-se a elas. Um domínio classificado como não vulnerável pelos critérios aqui adotados pode, desta forma, ter mensagens falsificadas entregues por um receptor mal configurado. O que se mediu, portanto, foi a exposição que está sob o controle direto do administrador do domínio, não o desfecho

final de um ataque, que também envolve a exposição sob responsabilidade do administrador do servidor receptor das mensagens falsificadas.

Na mesma linha, o estudo tratou exclusivamente da falsificação do domínio exato. Permanecem fora do escopo os vetores de personificação que não dependem da configuração das extensões SMTP do domínio legítimo, entre eles os domínios visualmente semelhantes (*typosquatting*), os registros homográficos, a manipulação do nome de exibição no MUA e o uso de contas legítimas previamente comprometidas. Um órgão que tenha alcançado a condição de não vulnerável, nos termos desta pesquisa, continua exposto a campanhas de *phishing* construídas com base nesses outros mecanismos, de modo que os resultados não devem ser lidos como uma medida da segurança completa do correio eletrônico institucional, mas apenas de uma de suas dimensões.

A verificação do DKIM foi objeto de uma restrição técnica, como reforçado diversas vezes. Como o seletor é definido livremente por cada organização e não é publicado de forma indexável no DNS, sua identificação remota depende do teste com seletores de uso comum. A categoria “DKIM não encontrado” deve, por isso, ser lida como ausência de evidência nos seletores testados, e não como afirmação de que o mecanismo não foi implementado. Dessa restrição decorre uma segunda. Sem acesso a uma mensagem privada efetivamente assinada, não foi possível auditar a validade criptográfica das assinaturas, razão pela qual o DKIM figurou nesta dissertação apenas como indicador de adoção, sem indicadores de conformidade correspondentes, e não integrou o critério de classificação do estado de vulnerabilidade.

A delimitação da amostra também comporta ressalvas. A enumeração dos domínios foi conduzida por meio de técnicas de OSINT, a partir da relação oficial de órgãos federais, procedimento que não garante exaustividade. Domínios secundários, de campanhas ou projetos específicos podem ter escapado à identificação. Além disso, a lista foi fixada no início do período de coleta e mantida inalterada ao longo dos dezoito meses, condição necessária à comparabilidade da série longitudinal, mas que introduz defasagem em relação a eventuais reestruturações administrativas, criações, extinções ou fusões de órgãos ocorridas no intervalo. Órgãos excluídos por não operarem correio eletrônico próprio no momento inicial permaneceram fora da amostra ainda que possam ter passado a operá-lo posteriormente.

Quanto à atribuição causal, trata-se de um estudo sem grupo de controle. A associação entre as ações de mitigação e as variações observadas apoia-se na coincidência entre os incrementos e as janelas de efeito arbitradas para cada intervenção, o que sustenta a inferência, mas não a demonstra experimentalmente. Não é possível descartar a influência de outros fatores como auditorias, migrações de provedor de correio, incidentes de segurança noticiados no período ou iniciativas de outros atores que atuem sobre o mesmo público. A própria série evidencia essa limitação. O agrupamento “Agricultura e Organização Agrária” concentrou a maior parte de sua melhoria em movimentos ocorridos em março e junho de 2025, anteriores a qualquer ação de mitigação da pesquisa. Cabe registrar que a ausência de grupo de controle não foi acidental. Manter deliberadamente, sem notificação, um conjunto

de órgãos sabidamente vulneráveis, com o propósito de dispor de um grupo de controle, seria incompatível com a natureza aplicada deste trabalho e com o objetivo de proteção da APF.

Some-se a isso o fato de que as ações de mitigação foram cumulativas e parcialmente sobrepostas, o que impede isolar a contribuição individual de cada uma. A Recomendação 06/2025 do CTIR Gov alcançou toda a Rede Federal de Gestão de Incidentes Cibernéticos, incluindo órgãos que também recebiam os alertas individualizados, e permaneceu vigente durante todo o período restante. Os incrementos atribuídos às notificações posteriores incorporam, portanto, um efeito tardio das intervenções anteriores que não pôde ser descontado. A granularidade mensal das coletas, realizadas entre os dias 10 e 15 de cada mês, acrescenta imprecisão adicional, pois alterações efetuadas e revertidas dentro do mesmo intervalo não foram capturadas, e a alocação de uma correção a determinada ação dependeu da janela de observação previamente estabelecida.

A pesquisa observou o efeito das intervenções nos registros DNS, mas não o percurso interno que as levou a esse resultado. Não se sabe se as mensagens chegaram efetivamente aos responsáveis técnicos, se foram lidas, por quem foram encaminhadas ou quais obstáculos institucionais mediarão a decisão de corrigir ou não a configuração. Os endereços de destino foram obtidos também por fontes abertas e, na ausência de contas vinculadas a ETIRs, CSIRTs ou equipes de segurança, recorreu-se a canais de protocolo, ouvidoria ou comunicação, de modo que parte da ausência de resposta pode refletir falha de entrega ou de encaminhamento interno, e não recusa ou desatenção. Pela mesma razão, as hipóteses levantadas para explicar a resposta desigual entre setores permanecem como conjecturas não testadas, já que o desenho quantitativo adotado, apoiado exclusivamente em fontes secundárias, não gerou dados qualitativos suficientes para examiná-las.

O agrupamento dos órgãos por área de atuação, adotado para preservar a identidade das instituições vulneráveis, também produziu uma limitação analítica. Ao renunciar à identificação individual, a pesquisa abriu mão de correlacionar o estado de vulnerabilidade com variáveis institucionais, como porte, orçamento, natureza jurídica ou existência formal de equipe de resposta a incidentes. Os grupos resultantes têm ainda dimensões bastante desiguais, variando de 6 a 123 órgãos, o que compromete a comparabilidade direta entre si. Nos agrupamentos menores, a correção de um único domínio desloca o indicador em mais de 16 pontos percentuais, enquanto o maior deles, que reúne cerca de 44% da amostra, exerce peso desproporcional sobre a curva consolidada.

Por fim, há limitações quanto ao alcance temporal e à generalização dos achados. O recorte de dezoito meses encerrou-se em julho de 2026, três coletas após o último alerta, um intervalo possivelmente insuficiente para captar efeitos tardios desta intervenção. Tampouco há como afirmar que os ganhos consolidados se sustentarão, uma vez que a própria série registrou episódios de agravamento espontâneo e de reversão de configurações, o que sugere que a manutenção da proteção depende de monitoramento contínuo, e não de um ato único de correção. Os resultados referem-se, ademais, à Administração Pública Federal brasileira em um período determinado, não se estendendo automaticamente a entes estaduais e municipais, a organizações privadas ou a outros contextos nacionais. Cabe registrar, ainda, que parte da

eficácia das ações institucionais decorreu do acesso do pesquisador a estruturas que viabilizaram o acesso ao Programa Nacional de Proteção do Conhecimento Sensível e, por meio dele, ao CTIR Gov — condição que amplia o alcance do que se pôde realizar, mas que talvez não estaria disponível a outros investigadores, o que relativiza a reprodutibilidade da pesquisa, ainda que a dimensão de coleta e classificação permaneça integralmente replicável por meio da ferramenta e dos procedimentos descritos no Capítulo 3.

5.5. SUGESTÕES PARA TRABALHOS FUTUROS

5.5.1. Continuidade da observação e reprodução em outras amostras

O encerramento da coleta em julho de 2026 corresponde a uma exigência de prazo, não a um esgotamento do objeto. A primeira sugestão para trabalhos futuros, por isso, é a extensão da própria série temporal. Os ganhos consolidados foram medidos poucos meses após a última intervenção e a série registrou alguns episódios de agravamento espontâneo e de reversão das configurações, o que levanta dúvidas quanto à perpetuidade do resultado obtido. Um acompanhamento prolongado, conduzido por mais dois ou três anos, com a mesma periodicidade e o mesmo instrumento, permitiria verificar se a proteção alcançada se sustenta, se decai na ausência de novos estímulos ou se prossegue por inércia institucional, oferecendo, assim, uma estimativa do intervalo em que a conscientização precisa ser renovada para que o patamar alcançado não regreda.

A replicação do método em outros recortes constitui outra frente de atuação de baixa complexidade e alto retorno prático. Estados, municípios, sociedades de economia mista, entidades do terceiro setor e até administrações públicas de outros países são universos aos quais o mesmo procedimento pode ser aplicado. O estudo de caso conduzido com instituições públicas federais de ensino superior, que serviu à validação do instrumento, indica a viabilidade dessa sugestão. Comparações internacionais teriam interesse adicional, ao permitirem contrastar arranjos regulatórios distintos.

5.5.2. Pesquisa qualitativa junto aos órgãos ainda vulneráveis

Os agrupamentos setoriais responderam de modo desigual às três naturezas de comunicação empregadas, e as razões dessa assimetria foram aventadas apenas como hipóteses — maturidade da governança de segurança da informação, estrutura de conformidade normativa, grau de centralização da gestão de tecnologia da informação, falta de priorização — que o desenho quantitativo adotado não pôde testar. Uma investigação de natureza qualitativa, baseada em entrevistas com gestores de segurança da informação, integrantes de equipes de tratamento de incidentes e responsáveis por infraestruturas de correio eletrônico, permitiria compreender o que separa o recebimento de um alerta de vulnerabilidade da alteração efetiva de um registro DNS. Interessaria particularmente o conjunto dos 76 domínios que permaneceram completamente vulneráveis ao final do período, insensíveis a todas as ações

de mitigação. Saber se essa resistência decorre de ausência de pessoal técnico, de dependência contratual, de desconhecimento persistente, de falha na chegada do alerta ao destinatário adequado ou de decisão deliberada de não priorizar o tema é uma condição essencial para planejar intervenções futuras.

Outra proposta seria a investigação específica das vulnerabilidades parciais, uma vez que as condições de vulnerabilidade restritas a subdomínios, ao domínio organizacional ou decorrentes de erro de sintaxe permaneceram praticamente inertes durante os dezoito meses, sem responder efetivamente a nenhuma das ações. A hipótese levantada de que essas configurações refletem arranjos técnicos deliberados, em vez de desconhecimento do risco, merece verificação direta. Casos como o do domínio cujo registro SPF expande recursivamente para um número de consultas acima do limite, o do mecanismo de inclusão que aponta para o próprio domínio criando um *loop* de resolução DNS, ou o do registro DMARC inviabilizado por um espaço em branco indevido, sugerem que existe uma classe de falhas que a conscientização não resolve porque não decorre de falta de informação, e sim de complexidade operacional, dependência de provedores externos ou ausência de verificação após a alteração.

5.5.3. Acesso a mensagens legítimas para auditoria efetiva de DKIM

A limitação relacionada ao DKIM é a que oferece aprimoramento mais evidente. A verificação realizada por meio de cem seletores comuns produziu um indicador de adoção, mas não de conformidade, e não permitiu afirmar categoricamente a ausência do mecanismo. Um estudo conduzido em cooperação com os órgãos, mediante consentimento para o recebimento de uma mensagem privada legítima de cada domínio, permitiria identificar o seletor efetivamente empregado, além de auditar a assinatura — algoritmo, comprimento da chave, política de rotação e alinhamento com o domínio remetente — e os demais campos de cabeçalho envolvidos.

5.5.4. Acesso aos relatórios DMARC

A mesma cooperação mencionada no item anterior poderia abrir acesso aos relatórios agregados do DMARC, enviados automaticamente para os endereços declarados na *tag* “rua” e inacessíveis por fontes abertas. Trabalhar com esses relatórios permitiria medir o volume real de tentativas de falsificação dirigidas a domínios governamentais, uma dimensão que esta pesquisa não pôde alcançar e que transformaria a avaliação de risco potencial em uma avaliação de ameaça efetivamente materializada.

Adicionalmente, os dados de notificação mantidos pelo CTIR Gov, se cruzados com a série de conformidade aqui produzida, permitiriam estimar em que medida a correção das configurações se traduziu em redução de incidentes de *phishing* com personificação institucional. Esse cruzamento converteria a métrica de exposição em métrica de risco,

fortalecendo o argumento a favor do investimento em autenticação de correio eletrônico e oferecendo aos gestores públicos elementos de decisão que a mera constatação de vulnerabilidade não fornece.

5.5.5. Pesquisa sob a perspectiva do servidor receptor

O problema do *spoofing* de e-mail, como já mencionado diversas vezes, possui duas dimensões: a proteção da identidade do domínio remetente contra falsificação e a verificação dessa identidade pelo servidor destinatário. Dentro deste contexto, uma limitação bastante importante, apontada desde o Capítulo 3, diz respeito à impossibilidade de auditar o comportamento do servidor destinatário por meio de técnicas puramente passivas. Um estudo do lado receptor, agora tratando os órgãos da APF quanto destinatários — verificando se e como seus servidores e clientes de correio efetivamente acatam as políticas declaradas pelos domínios — abordaria a principal restrição de escopo assumida nesta dissertação e permitiria estimar a distância entre a proteção esperada e a proteção efetiva.

Uma ampliação nesse sentido poderia consistir na tentativa de enviar uma mensagem de e-mail aos órgãos da APF, falsificando um domínio remetente — de propriedade do pesquisador, por razões éticas —, com as políticas mais restritivas possíveis aplicadas em seu DNS. A ideia seria, a exemplo do que fizeram Zhang et al. (89), enviar a mensagem diretamente ao servidor MX de cada domínio avaliado, estabelecendo uma sessão SMTP completa e verificando se a mensagem é recusada ainda durante a transação, por meio de um código de rejeição explícito nas fases de RCPT TO ou DATA.

5.5.6. Aprimoramento do instrumento de pesquisa (*StopEmailSpoofing*)

A ferramenta *StopEmailSpoofing* apresenta oportunidades para a expansão de funcionalidades. A segurança do correio eletrônico não se limita à autenticação do remetente. Mecanismos como DNSSEC, STARTTLS, MTA-STS e ARC compõem camadas complementares cuja verificação por fontes abertas é viável, mas que atualmente carecem de medição sistemática no ecossistema cibernético público brasileiro. A incorporação de checagens de DNSSEC permitiria avaliar se a cadeia de confiança dos próprios registros consultados pela ferramenta está protegida contra adulteração, o que reforçaria a validade das conclusões emitidas sobre SPF, DKIM e DMARC. Do mesmo modo, a verificação de STARTTLS e de MTA-STS revelaria uma dimensão da segurança do correio eletrônico distinta da falsificação de remetente, mas igualmente relevante, isto é, a proteção da mensagem em trânsito contra interceptação e *downgrade* de criptografia. E a checagem de ARC, por sua vez, permitiria avaliar a preservação dos resultados de autenticação em cenários de reencaminhamento, situação recorrente em órgãos públicos que utilizam listas de distribuição ou intermediários e na qual o alinhamento de SPF e DKIM tende a se romper.

Merece registro também a possibilidade de inclusão da verificação de suscetibilidade dos domínios a SMTP *smuggling*, técnica relativamente recente que explora interpretações divergentes de delimitadores de mensagem entre diferentes implementações de servidores para contornar as próprias proteções de SPF, DKIM e DMARC, e cuja identificação remota, embora mais complexa do que a simples leitura de registros DNS, é possível e agregaria à ferramenta uma camada de diagnóstico hoje ausente nas soluções disponíveis.

Outro ponto é que, com a recente atualização das especificações que regulamentam o DMARC, algumas *tags* foram descontinuadas e outras novas surgiram. Atualizar a ferramenta para acompanhar esta modernização do protocolo permitiria à comunidade ter um instrumento para auxiliar na adoção e na garantia de conformidade da implementação dos novos mecanismos trazidos pelas novas RFCs.

Por fim, o acréscimo de uma consulta automatizada a listas de reputação e de bloqueio (*spam lists*) dos domínios e dos respectivos endereços de IP de seus servidores MX, ofereceria um indicador reputacional do domínio e do servidor, permitindo detectar configurações tecnicamente corretas mas já associadas a histórico de abuso.

5.5.7. Extensão de navegador

Outra direção de continuidade da pesquisa desloca o objeto da investigação do administrador de domínio para o usuário final, elo em que a maior parte das soluções técnicas de autenticação de remetente, incluindo o próprio SPF, DKIM e DMARC, tende a ignorar. Ainda que um domínio esteja corretamente protegido contra falsificação direta, o usuário comum permanece exposto a variações do nome de exibição (vulnerabilidade na renderização do MUA), domínios visualmente semelhantes e outras formas de personificação que escapam ao escopo desta dissertação, precisamente porque a interface da maioria dos clientes de e-mail exibe de forma proeminente o nome do remetente declarado no cabeçalho “From”, sem confrontá-lo com informações que exigiriam maior conhecimento técnico para serem interpretadas, como o domínio de envelope, o resultado da verificação de SPF e DKIM ou o alinhamento efetivamente aplicado pelo DMARC.

Sugere-se, assim, o desenvolvimento de uma extensão de navegador voltada a clientes de webmail, capaz de inspecionar automaticamente os cabeçalhos de cada mensagem recebida e confrontar, de forma visual e acessível a um público não técnico, o nome e o endereço exibidos na interface com o domínio real de origem e com os resultados de autenticação retornados pelo servidor, alertando, de maneira explícita, eventuais divergências encontradas.

5.5.8. Registro defensivo de domínios visualmente semelhantes

Também seria conveniente investigar outros vetores de ataque de falsificação que esta pesquisa deliberadamente deixou de fora do escopo. A avaliação aqui realizada restringiu-se

à falsificação do domínio exato, e outros vetores de personificação que não dependem da configuração das extensões SMTP no domínio legítimo permanecem sem medição. Um levantamento da superfície de domínios visualmente semelhantes, incluindo registros homográficos e variações tipográficas (*typosquatting*), indicaria em que medida a proteção obtida pelos órgãos públicos federais brasileiros poderia ser contornada por outras técnicas de falsificação e forneceria subsídio a políticas de registro defensivo de domínios similares.

REFERÊNCIAS BIBLIOGRÁFICAS

- (1) TATANG, Dennis; ZETTL, Florian; HOLZ, Thorsten. **The evolution of DNS-based email authentication: measuring adoption and finding flaws**. In: *INTERNATIONAL SYMPOSIUM ON RESEARCH IN ATTACKS, INTRUSIONS AND DEFENSES (RAID)*, 24., 2021, San Sebastian, Spain. Proceedings [...]. New York: Association for Computing Machinery, 2021. p. 354–369. DOI: <https://doi.org/10.1145/3471621.3471842>.
- (2) RADICATI GROUP, INC. **Email Statistics Report, 2024-2028: executive summary**. London, UK: The Radicati Group, Inc., dez. 2024. Disponível em: <https://www.radicati.com/wp/wp-content/uploads/2024/10/Email-Statistics-Report-2024-2028-Executive-Summary.pdf>.
- (3) CHAUHAN, Prashant. D.; SHAH, Apurva. M. **Effectiveness of anti-spoofing protocols for email authentication**. In: IEEE. 2023 *3rd International Conference on Intelligent Communication and Computational Techniques (ICCT)*, Jaipur, Índia, 2023. Anais [...]. [S.l.]: IEEE, 2023. p. 1–5. DOI: <https://doi.org/10.1109/ICCT56969.2023.10076098>.
- (4) ANITHA, S.; MUTHUKUMARAN, M.; PARAMESH, R.; SANJAY KUMAR, S.; SHEIK MUSTHAFA, M. **AI based e-mail and domain spoofing detection**. *Research and Reviews: Advancement in Cyber Security*, v. 2, n. 3, p. 25–32, 2025. DOI: <https://doi.org/10.5281/zenodo.15573565>.
- (5) AJINA, A.; KUMAR, Ujwal. **Email spoofing & backlashes**. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, v. 8, n. 11, set. 2019. ISSN 2278-3075. DOI: <https://doi.org/10.35940/ijitee.J9310.0981119>.
- (6) PROOFPOINT. **O fator humano 2025: vol. 1, engenharia social**. [S.l.]: Proofpoint, 2025. Disponível em: <https://www.proofpoint.com/br/resources/threat-reports/human-factor-social-engineering>. Acesso em: 09 abr. 2026.
- (7) ESTADOS UNIDOS DA AMÉRICA. CISA; NSA; FBI; MS-ISAC. **Phishing guidance: stopping the attack cycle at phase one**. [S.l.], out. 2023. Disponível em: [https://www.dafcio.af.mil/Portals/64/Documents/Small%20Business%20Innovation%20Research%20\(SBIR\)/Resources/Phishing%20Guidance%20-%20Stopping%20the%20Attack%20Cycle%20at%20Phase%20One%20-2023%202024.pdf](https://www.dafcio.af.mil/Portals/64/Documents/Small%20Business%20Innovation%20Research%20(SBIR)/Resources/Phishing%20Guidance%20-%20Stopping%20the%20Attack%20Cycle%20at%20Phase%20One%20-2023%202024.pdf)
- (8) ANTI-PHISHING WORKING GROUP (APWG). **Phishing activity trends report: 1st quarter 2023**. [S.l.]: APWG, 2023. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q1_2023.pdf. Acesso em: 10 abr. 2026.
- (9) ANTI-PHISHING WORKING GROUP (APWG). **Phishing activity trends report: 2nd quarter 2023**. [S.l.]: APWG, 2023. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q2_2023.pdf. Acesso em: 10 abr. 2026.
- (10) ANTI-PHISHING WORKING GROUP (APWG). **Phishing activity trends report: 3rd quarter 2023**. [S.l.]: APWG, 2023. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q3_2023.pdf. Acesso em: 10 abr. 2026.

- (11) ANTI-PHISHING WORKING GROUP (APWG). **Phishing activity trends report: 4th quarter 2023**. [S.l.]: APWG, 2024. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf. Acesso em: 10 abr. 2026.
- (12) ANTI-PHISHING WORKING GROUP (APWG). **Phishing activity trends report: 1st quarter 2024**. [S.l.]: APWG, 2024. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q1_2024.pdf. Acesso em: 10 abr. 2026.
- (13) ANTI-PHISHING WORKING GROUP (APWG). **Phishing activity trends report: 2nd quarter 2024**. [S.l.]: APWG, 2024. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q2_2024.pdf. Acesso em: 10 abr. 2026.
- (14) ANTI-PHISHING WORKING GROUP (APWG). **Phishing activity trends report: 3rd quarter 2024**. [S.l.]: APWG, 2024. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q3_2024.pdf. Acesso em: 10 abr. 2026.
- (15) ANTI-PHISHING WORKING GROUP (APWG). **Phishing activity trends report: 4th quarter 2024**. [S.l.]: APWG, 2025. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q4_2024.pdf. Acesso em: 10 abr. 2026.
- (16) ANTI-PHISHING WORKING GROUP (APWG). **Phishing activity trends report: 1st quarter 2025**. [S.l.]: APWG, 2025. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q1_2025.pdf. Acesso em: 10 abr. 2026.
- (17) ANTI-PHISHING WORKING GROUP (APWG). **Phishing activity trends report: 2nd quarter 2025**. [S.l.]: APWG, 2025. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q2_2025.pdf. Acesso em: 10 abr. 2026.
- (18) ANTI-PHISHING WORKING GROUP (APWG). **Phishing activity trends report: 3rd quarter 2025**. [S.l.]: APWG, 2025. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q3_2025.pdf. Acesso em: 10 abr. 2026.
- (19) ANTI-PHISHING WORKING GROUP (APWG). **Phishing activity trends report: 4th quarter 2025**. [S.l.]: APWG, 2026. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q4_2025.pdf. Acesso em: 10 abr. 2026.
- (20) KUMAR, Akshay; SINGH, Jaspreet. **Unveiling the anatomy of phishing attacks: strategies, targets, and cybersecurity solutions**. In: *INTERNATIONAL CONFERENCE ON EVOLUTIONARY ALGORITHMS AND SOFT COMPUTING TECHNIQUES (EASCT)*, 2023. Anais [...]. [S.l.: s.n.], 2023. p. 1–6. DOI: <https://doi.org/10.1109/EASCT59475.2023.10393225>.
- (21) ESTADOS UNIDOS DA AMÉRICA. Office of the Director of National Intelligence. **Annual Threat Assessment of the U.S. Intelligence Community**. [S.l.]: Office of the Director of National Intelligence, mar. 2025. Disponível em: <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf>.
- (22) ESTADOS UNIDOS DA AMÉRICA. Office of the Director of National Intelligence. **Annual Threat Assessment of the U.S. Intelligence Community**. [S.l.]: Office of the Director of National Intelligence, mar. 2026. Disponível em: <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf>.

(23) AL-SINAYYID, Ali; JEWEL, Md Julfiker Ali; MANNURU, Venkatesh; SASIDHAR, Kadiyala. **Defending characteristics and attribution analysis for phishing attacks**. In: *International Conference on Computational Science and Computational Intelligence (CSCI)*, 2023. Anais [...]. [S.l.]: IEEE, 2023. p. 868–874. DOI: <https://doi.org/10.1109/CSCI62032.2023.00145>.

(24) GEORG, Marcus Aurélio Carvalho; RODRIGUES, Walisson Magno Silva; ALVES, Carlos André de Melo; SILVEIRA JÚNIOR, Aldery; NUNES, Rafael Rabelo. **Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação**. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, Porto, n. E54, p. 602-616, nov. 2022. DOI: <https://doi.org/10.5281/zenodo.7855320>. Disponível em: <https://www.risti.xyz/issues/ristie54.pdf>.

(25) KASPERSKY TEAM. **Phishing and spam: the wildest campaigns of 2025**. Kaspersky official blog, 11 fev. 2026. Disponível em: <https://www.kaspersky.com/blog/spam-and-phishing-2025/55295/%3E>. Acesso em: 9 abr. 2026.

(26) GANON, Max. **Threat Actors Exploit Government Website Vulnerabilities for Phishing Campaigns**. Cofense Blog, 29 jan. 2025. Disponível em: <https://cofense.com/blog/threat-actors-exploit-government-website-vulnerabilities-for-phishing-campaigns>. Acesso em: 12 out. 2025.

(27) NMACHI, Wosah Peace. **A framework for securing email entrances and mitigating phishing impersonation attacks**. *International Journal of Network Security & Its Applications (IJNSA)*, v. 15, n. 6, p. 15–?, nov. 2023. DOI: <https://doi.org/10.5121/ijnsa.2023.15602>.

(28) DAWKINS, Shanée; JACOBS, Jody. **NIST Phish Scale User Guide**. Gaithersburg, MD: National Institute of Standards and Technology, 2023. (NIST Technical Note, 2276). Disponível em: <https://doi.org/10.6028/NIST.TN.2276>. Acesso em: 09 abr. 2026.

(29) SAMONTE, Mary Jane; ACHACOSO, Luke Martin D. L.; AMPER, Alden Christian C.; ABALETA, Raphael M. **Designing an integration of anti-spoofing as security strategies for e-commerce email marketing to shield brand integrity**. In: *INTERNATIONAL CONFERENCE ON COMPUTER SYSTEMS (ICCS)*, 4., 2024. Anais [...]. [S.l.: s.n.], 2024. p. 172–180. DOI: <https://doi.org/10.1109/ICCS62594.2024.10795834>.

(30) HU, Hang; WANG, Gang. **End-to-end measurements of email spoofing attacks**. In: *USENIX SECURITY SYMPOSIUM*, 27., 2018a, Baltimore, MD. Proceedings [...]. [S.l.]: USENIX Association, 2018. p. 1095–1112. Disponível em: <https://www.usenix.org/conference/usenixsecurity18/presentation/hu>.

(31) MA, Jinrui; CHEN, Lutong; XUE, Kaiping; LUO, Bo; HUANG, Xuanbo; AI, Mingrui; ZHANG, Huanjie; WEI, David S. L.; ZHUANG, Yan. **FakeBehalf: Imperceptible Email Spoofing Attacks against the Delegation Mechanism in Email Systems**. In: *USENIX SECURITY SYMPOSIUM*, 33., 2024, Philadelphia, PA. Proceedings [...]. [S.l.]: USENIX Association, 2024. p. 1243–1260. Disponível em: <https://www.usenix.org/conference/usenixsecurity24/presentation/ma-jinrui>.

(32) KAMBOURAKIS, Georgios; GIL, Gerard Draper; SANCHEZ, Ignacio. **What email servers can tell to Johnny: an empirical study of provider-to-provider email security.** IEEE Access, v. 8, p. 130066–130081, 2020. DOI: <https://10.1109/ACCESS.2020.3009122>.

(33) SETHURAMAN, Sibi Chakkaravarthy; V. S., Devi Priya; REDDI, Tarun; REDDY, Mulka Sai Tharun; KHAN, Muhammad Khurram. **A comprehensive examination of email spoofing: issues and prospects for email security.** Computers & Security, v. 137, p. 103600, 2024. DOI: <https://doi.org/10.1016/j.cose.2023.103600>.

(34) BRASIL. Gabinete de Segurança Institucional. **Estratégia Nacional de Inteligência.** Brasília: Gabinete de Segurança Institucional, 2017. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/legislacao/politica-nacional-de-inteligencia-1/ENINT.pdf>.

(35) BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 12.527, de 18 de novembro de 2011. **Regula o acesso a informações.** Diário Oficial da União: seção 1, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm.

(36) BRASIL. Lei nº 9.883, de 7 de dezembro de 1999. **Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências.** Brasília, DF: Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos, 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/L9883.htm.

(37) AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Doutrina da Atividade de Inteligência.** Brasília: ABIN, 2023. Aprovada pela Portaria GAB/DG/ABIN/CC/PR nº 1.205, de 27 de novembro de 2023. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023>. Acesso em: 06 abr. 2026.

(38) BRASIL. Presidência da República. Casa Civil. Secretaria Especial para Assuntos Jurídicos. Decreto nº 11.816, de 6 de dezembro de 2023. **Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão, das Funções de Confiança e das Gratificações da Agência Brasileira de Inteligência.** Diário Oficial da União: seção 1, Brasília, DF, 7 dez. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11816.htm

(39) BRASIL. Gabinete de Segurança Institucional da Presidência da República. Portaria nº 59, de 26 de julho de 2018. **Institui, no âmbito da Agência Brasileira de Inteligência – ABIN, o Programa Nacional de Proteção do Conhecimento Sensível – PNPC, com a finalidade de promover a proteção de conhecimentos sensíveis relativos aos interesses e à segurança do Estado e da sociedade.** Diário Oficial da União, Brasília, DF, 27 jul. 2018. Seção 1. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/34380628/do1-2018-07-27-portaria-n-59-de-26-de-julho-de-2018-34380599.

(40) BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. **Aprova a Política Nacional de Segurança de Infraestruturas Críticas.** Diário Oficial da União, Brasília, DF, 23 nov. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm.

(41) BRASIL. Decreto nº 10.569, de 9 de dezembro de 2020. **Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas**. Brasília, DF: Presidência da República, 2020. 12 p. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm%3E.

(42) BRASIL. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa nº 1, de 27 de maio de 2020. **Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal**. Diário Oficial da União, Brasília, DF, 28 maio 2020. Seção 1, p. 13. Disponível em: <https://www.in.gov.br/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215>.

(43) BRASIL. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa nº 2, de 24 de julho de 2020. **Altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal**. Diário Oficial da União: seção 1, Brasília, DF, 27 jul. 2020, edição 142, p. 3. Disponível em: <https://www.in.gov.br/web/dou/-/instrucao-normativa-n-2-de-24-de-julho-de-2020-268684700%3E>.

(44) BRASIL. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021. **Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal**. Diário Oficial da União, Brasília, DF, 31 maio 2021, edição 101, seção 1, p. 15. Disponível em: <https://www.in.gov.br/web/dou/-/instrucao-normativa-gsi-pr-n-3-de-28-de-maio-de-2021-322963172%3E>.

(45) BRASIL. Decreto nº 10.748, de 16 de julho de 2021. **Institui a Rede Federal de Gestão de Incidentes Cibernéticos**. Brasília: Presidência da República, Secretaria-Geral, Subchefia para Assuntos Jurídicos, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10748.htm.

(46) BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. **Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança**. Brasília, DF: Presidência da República, Casa Civil, Secretaria Especial para Assuntos Jurídicos, 2023. 6 p. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 06 abr. 2026.

(47) BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. **Institui a Estratégia Nacional de Cibersegurança**. Diário Oficial da União, Brasília, DF, 5 ago. 2025. Seção 1, p. 2. Disponível em: <https://www.in.gov.br/web/dou/-/n-12.573-de-4-de-agosto-de-2025-64620784%3E>. Acesso em: 06 abr. 2026.

(48) BRASIL. Decreto nº 12.572, de 4 de agosto de 2025. **Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal**. Brasília, DF: Presidência da República, Casa Civil, Secretaria Especial para Assuntos Jurídicos, 2025. Disponível em:

https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2025/Decreto/D12572.htm. Acesso em: 6 abr. 2026.

(49) BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Portaria SGD/MGI nº 852, de 28 de março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI**. Diário Oficial da União, Brasília, DF, 30 mar. 2023, Seção 1. Disponível em: <https://www.in.gov.br/web/dou/-/portaria-sgd-mgi-n-852-de-28-de-marco-de-2023-47375908>.

(50) BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Guia do Framework de Privacidade e Segurança da Informação: Programa de Privacidade e Segurança da Informação (PPSI)**. Versão 1.1.4. Brasília, dezembro de 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf

(51) TRIBUNAL DE CONTAS DA UNIÃO. **Matriz de riscos e controles para serviços de hospedagem Web, e-mail e DNS: entendendo riscos, para estimar custos e benefícios esperados com os controles**. Brasília: TCU, Secretaria-Geral de Controle Externo, 2024. 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

(52) ARORA, Moulik Singh; DADHANIA, Preksha J. **Threats, effects, and awareness of cybercrime: a survey**. *International Journal of Scientific Research in Engineering and Management (IJSREM)*, v. 8, n. 5, p. [1–10], maio 2024. DOI: <https://doi.org/10.55041/IJSREM32833>.

(53) D'ANGELONE, Marcello. **Email spoofing defence techniques: a comprehensive review and development of a novel measurement tool**. 2022. Trabalho de conclusão (Mestrado em Cybersecurity) — School of Computing, National College of Ireland, Dublin, 14 ago. 2022. 36 f. Orientador: Mark Monaghan. Disponível em: <https://norma.ncirl.ie/7116/1/marcellodangelone.pdf>.

(54) HU, Hang; WANG, Gang. **Revisiting email spoofing attacks**. arXiv preprint, arXiv:1801.00853 [cs.CR], 2018b. DOI: <https://doi.org/10.48550/arXiv.1801.00853>. Disponível em: <https://arxiv.org/abs/1801.00853>. Acesso em: 15 out. 2025.

(55) SHEN, Kaiwen; WANG, Chuhan; GUO, Minglei; ZHENG, Xiaofeng; LU, Chaoyi; LIU, Baojun; ZHAO, Yuxuan; HAO, Shuang; DUAN, Haixin; PAN, Qingfeng; YANG, Min. **Weak links in authentication chains: a large-scale analysis of email sender spoofing attacks**. In: *USENIX SECURITY SYMPOSIUM*, 30., 2021. Proceedings [...]. [S.l.]: USENIX Association, 2021. p. 3201–3217. Disponível em: <https://www.usenix.org/conference/usenixsecurity21/presentation/shen-kaiwen>.

(56) MAROOFI, Sourena; KORCZYŃSKI, Maciej; HÖLZEL, Arnold; DUDA, Andrzej. **Adoption of email anti-spoofing schemes: a large scale analysis**. *IEEE Transactions on Network and Service Management*, v. 18, n. 3, p. 3184–3196, 2021. DOI: <https://doi.org/10.1109/TNSM.2021.3065422>.

(57) ZHANG, Han; MI, Dengke; CHEN, Libo; LIU, Ming; SHI, Yong; XUE, Zhi. **Subdomain protection is needed: An SPF and DMARC-based empirical measurement study and proactive solution of email security.** In: *INTERNATIONAL SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS (SRDS)*, 42., 2023a. Anais [...]. [S.l.: s.n.], 2023. p. 140–150. DOI: <https://doi.org/10.1109/SRDS60354.2023.00023>.

(58) FOSTER, Ian D.; LARSON, Jon; MASICH, Max; SNOEREN, Alex C.; SAVAGE, Stefan; LEVCHENKO, Kirill. **Security by any other name: On the effectiveness of provider based email security.** In: *ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (CCS)*, 22., 2015, Denver, Colorado, USA. Proceedings [...]. New York: Association for Computing Machinery, 2015. p. 450–464. DOI: <https://doi.org/10.1145/2810103.2813607>.

(59) KUMAR, Ranjit. **Research methodology: a step-by-step guide for beginners.** 5. ed. Los Angeles: SAGE Publications, 2019.

(60) GUPTA, Surekha; PILLI, Emmanuel S.; MISHRA, Preeti; PUNDIR, Sumit; JOSHI, R. C. **Forensic analysis of E-mail address spoofing.** In: *INTERNATIONAL CONFERENCE – CONFLUENCE: THE NEXT GENERATION INFORMATION TECHNOLOGY SUMMIT*, 5., 2014, Noida. Proceedings [...]. Noida: IEEE, 2014. Disponível em: <https://doi.org/10.1109/CONFLUENCE.2014.6949302>.

(61) MARZUKI, Khairan; HANIF, Naufal; HARIYADI, I. Putu. **Application of Domain Keys Identified Mail, Sender Policy Framework, anti-spam, and anti-virus: the analysis on mail servers.** *International Journal of Electronics and Communications Systems*, v. 2, n. 2, p. 65–73, dez. 2022. DOI: <https://doi.org/10.24042/ijecs.v2i2.13543>.

(62) CHAUHAN, Prashant D.; SHAH, Apurva M. **Email spoofing: in today's era.** Research Square, 5 dez. 2022. Preprint (versão 1). DOI: <https://doi.org/10.21203/rs.3.rs-2328294/v1>.

(63) SUTISNA, Mochammad Arief; FADLIL, Abdul; RIADI, Imam. **Validasi E-mail Spoofing.** *JIMP – Jurnal Informatika Merdeka Pasuruan*, v. 5, n. 3, p. 16, dez. 2020. ISSN 2503-1945. Disponível em: <https://media.neliti.com/media/publications/464649-none-4423aeaf.pdf>

(64) BLECHSCHMIDT, Birk; STOCK, Ben. **Extended hell(o): a comprehensive large-scale study on email confidentiality and integrity mechanisms in the wild.** In: *USENIX ASSOCIATION. Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23)*, Anaheim, CA, ago. 2023. Anais [...]. [S.l.]: USENIX Association, 2023. p. 4895–4912. ISBN 978-1-939133-37-3. Disponível em: <https://www.usenix.org/conference/usenixsecurity23/presentation/blechschmidt>.

(65) DECCIO, Casey; YADAV, Tarun; BENNETT, Nathaniel; HILTON, Alden; HOWE, Michael; NORTON, Tanner; ROHDE, Jacob; TAN, Eunice; TAYLOR, Bradley. **Measuring email sender validation in the wild.** In: *INTERNATIONAL CONFERENCE ON EMERGING NETWORKING EXPERIMENTS AND TECHNOLOGIES (CoNEXT)*, 17., 2021, Virtual Event, Germany. Proceedings [...]. New York: Association for Computing Machinery, 2021. p. 230–242. DOI: <https://doi.org/10.1145/3485983.3494868>.

- (66) GIORGI, Giacomo; SARACINO, Andrea; MARTINELLI, Fabio. **Email spoofing attack detection through an end-to-end authorship attribution system**. In: *INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS SECURITY AND PRIVACY (ICISSP)*, 6., 2020. Proceedings [...]. [S.l.: s.n.], 2020. p. 64–74. DOI: <https://doi.org/10.5220/0008954600640074>.
- (67) MESHRAM, Bandu B.; MENDHE, Vikash; SINGH, Manish Kumar. **Tracing the invisible threads: a deep dive into email security & forensics**. *International Journal of Enhanced Research in Science, Technology & Engineering*, v. 13, n. 1, p. [s.p.], jan. 2024. ISSN 2319-7463. DOI: <https://doi.org/10.55948/IJERSTE.2024.0104>.
- (68) WANG, Chuhan; WANG, Chenkai; YANG, Songyi; LIU, Sophia; CHEN, Jianjun; DUAN, Haixin; WANG, Gang. **Email spoofing with SMTP smuggling: How the shared email infrastructures magnify this vulnerability**. In: *USENIX SECURITY SYMPOSIUM*, 34., 13–15 ago. 2025, Seattle, WA. Proceedings [...]. [S.l.]: USENIX Association, 2025. ISBN 978-1-939133-52-6. Disponível em: <https://www.usenix.org/system/files/usenixsecurity25-wang-chuhan.pdf>.
- (69) CROCKER, Dave. **Internet Mail Architecture. RFC 5598**. [S. l.]: Internet Engineering Task Force (IETF), julho 2009. Disponível em: <https://datatracker.ietf.org/doc/html/rfc5598>.
- (70) BIRTHRIYA, Kumar Santosh; JAIN, Ankit Kumar. **A comprehensive survey of phishing email detection and protection techniques**. *Information Security Journal: A Global Perspective*, v. 31, n. 4, p. 411–440, 2021. DOI: <https://doi.org/10.1080/19393555.2021.1959678>.
- (71) CHEN, Jianjun; PAXSON, Vern; JIANG, Jian. **Composition kills: a case study of email sender authentication**. In: *USENIX SECURITY SYMPOSIUM*, 29., 2020. Proceedings. [S.l.]: USENIX Association, 2020. p. 2183–2199. Disponível em: <https://www.usenix.org/conference/usenixsecurity20/presentation/chen-jianjun>.
- (72) KUMAR, Manish; HANUMANTHAPPA, M.; KUMAR, T. V. Suresh. **A Countermeasure Technique for Email Spoofing**. *International Journal of Advanced Research in Computer Science*, v. 4, n. 2, p. 128-133, jan./fev. 2013. Disponível em: <http://www.ijarcs.info>. ISSN 0976-5697.
- (73) LI, Ye; ULLAH, Abu Barkat; TRAN, Dat; MARROQUIN, Elisa Martinez; MA, Wanli. **A review of anti-phishing email control measures: why we need a novel digital signature scheme**. In: IEEE. *2025 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 30 jun.–4 jul. 2025, Veneza, Itália. [S.l.]: IEEE, 2025. DOI: <https://doi.org/10.1109/EuroSPW67616.2025.00067>.
- (74) YU, Beiyuan; LI, Pan; LIU, Jianwei; ZHOU, Ziyu; HAN, Yiran; LI, Zongxiao. **Advanced analysis of email sender spoofing attack and related security problems**. In: IEEE. *2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud) / 2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 2022. Anais [...]. [S.l.]: IEEE, 2022. p. 80–85. DOI: <https://doi.org/10.1109/CSCloud-EdgeCom54986.2022.00023>.

(75) KLENSIN, John C. **RFC 5321: Simple Mail Transfer Protocol**. [S. l.]: Network Working Group, out. 2008. Disponível em: <https://datatracker.ietf.org/doc/html/rfc5321>.

(76) DURUMERIC, Zakir; ADRIAN, David; MIRIAN, Ariana; KASTEN, James; BURSZTEIN, Elie; LIDZBORSKI, Nicolas; THOMAS, Kurt; ERANTI, Vijay; BAILEY, Michael; HALDERMAN, J. Alex. **Neither snow nor rain nor MITM...: An empirical analysis of email delivery security**. In: *INTERNET MEASUREMENT CONFERENCE (IMC)*, 2015, Tokyo, Japan. Proceedings [...]. New York: Association for Computing Machinery, 2015. p. 27–39. DOI: <https://doi.org/10.1145/2815675.2815695>.

(77) OPAZO, Bridget; WHITTEKER, Don; SHING, Chen-Chi. **Email trouble: secrets of spoofing, the dangers of social engineering, and how we can help**. In: *INTERNATIONAL CONFERENCE ON NATURAL COMPUTATION, FUZZY SYSTEMS AND KNOWLEDGE DISCOVERY (ICNC-FSKD)*, 13., 29–31 Jul. 2017, Guilin, China. Proceedings [...]. Piscataway, NJ: IEEE, 2017. DOI: <https://doi.org/10.1109/FSKD.2017.8393226>.

(78) RESNICK, Pete. (Ed.). **RFC 5322: Internet Message Format**. [S. l.]: Network Working Group, out. 2008. Disponível em: <https://datatracker.ietf.org/doc/html/rfc5322>.

(79) LI, Xinyan; ZHU, Yujia; ZHANG, Xiaou; JIE, Zhen; LIU, Qingyun. **SpoofingGuard: A content-agnostic framework for email spoofing detection via delivery graph**. In: *INTERNATIONAL CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK IN DESIGN (CSCWD)*, 26., 2023. Anais [...]. [S.l.: s.n.], 2023. p. 1098–1105. DOI: <https://doi.org/10.1109/CSCWD57460.2023.10152850>.

(80) CAMEJO, Chris. **Real or Fake? Spoof-Proofing Email With SPF, DKIM, and DMARC**. TrustedSec Blog, 13 jan. 2022. Disponível em: <https://trustedsec.com/blog/real-or-fake-spoof-proofing-email-with-spf-dkim-and-dmarc>. Acesso em: 12 out. 2025.

(81) MANE, Deepak; SHARMA, Geetanjali; SHINDE, Sandip; BANUBAKODE, Abhijit; SANGVE, Sunil; ANSARI, Maqsood Ahmed. **Reliable email spoofing detection using enhanced cybersecurity approaches**. *Advances in Nonlinear Variational Inequalities*, v. 28, n.3s, p. 199–210, 2025. ISSN 1092-910X. DOI: <https://doi.org/10.52783/anvi.v28.2924>.

(82) GALLO, Luigi; GENTILE, Danilo; RUGGIERO, Saverio; BOTTA, Alessio; VENTRE, Giorgio. **The human factor in phishing: collecting and analyzing user behavior when reading emails**. *Computers & Security*, v. 139, p. 103671, 2024. DOI: <https://doi.org/10.1016/j.cose.2023.103671>.

(83) SARKER, Orvila; JAYATILAKA, Asangi; HAGGAG, Sherif; LIU, Chelsea; BABAR, M. Ali. **A multi-vocal literature review on challenges and critical success factors of phishing education, training and awareness**. *Journal of Systems and Software*, v. 208, p. 111899, 2024. DOI: <https://doi.org/10.1016/j.jss.2023.111899>.

(84) VARSHNEY, Gaurav; KUMAWAT, Rahul; VARADHARAJAN, Vijay; TUPAKULA, Uday; GUPTA, Chandranshu. **Anti-phishing: a comprehensive perspective**. *Expert Systems with Applications*, v. 238, p. 122199, 2024. DOI: <https://doi.org/10.1016/j.eswa.2023.122199>.

(85) MAROOFI, Sourena; KORCZYŃSKI, Maciej; DUDA, Andrzej. **From Defensive Registration to Subdomain Protection: Evaluation of Email Anti-Spoofing Schemes for High-Profile Domains**. In: NETWORK TRAFFIC MEASUREMENT AND ANALYSIS CONFERENCE, 4., 2020, Berlim. Anais. Berlim: IFIP, 2020. p. 1-9. ISBN 978-3-903176-27-0. Disponível em: <https://api.semanticscholar.org/CorpusID:219956390>.

(86) AZKIA, Cidni Sika; SOLEHA, Anggun; NARISWARI, Sharfina. **Keamanan Email: SPF, DKIM, dan DMARC – Implementasi dan Pengujian Autentikasi Email dalam Pencegahan Email Phishing**. *International Journal of Informatics*, v. 1, n. 1, p. 1–6, 2025. Disponível em: <https://jurnal.untirta.ac.id/index.php/ijinf/article/view/34179/15455>.

(87) RAGHEB, Mohamed Sami; ELMEDANY, Wael; SHARIF, Mhd Saeed. **The effectiveness of DKIM and SPF in strengthening email security**. In: *INTERNATIONAL CONFERENCE ON FUTURE INTERNET OF THINGS AND CLOUD (FICLOUD)*, 10., 2023. Anais [...]. [S.l.: s.n.], 2023. p. 422–426. DOI: <https://doi.org/10.1109/FiCloud58648.2023.00068>.

(88) NANAAWARE, Tejas; MOHITE, Prashant; PATIL, Rajendra. **DMARCBBox – Corporate Email Security and Analytics using DMARC**. In: *IEEE INTERNATIONAL CONFERENCE FOR CONVERGENCE IN TECHNOLOGY (I2CT)*, 5., 2019, Bombay. Proceedings [...]. Bombay: IEEE, 2019. Disponível em: <https://doi.org/10.1109/I2CT45611.2019.9033552>.

(89) ZHANG, Han; CHEN, Libo; LIU, Ming; SHI, Yong; WU, Songyang; XUE, Zhi. **Both sides needed: a two-dimensional measurement study of email security based on SPF and DMARC**. In: *IEEE. 2023 19th International Conference on Mobility, Sensing and Networking (MSN)*, 2023b. IEEE, 2023b. p. 855–861. DOI: <https://doi.org/10.1109/MSN60784.2023.00126>.

(90) DEROUET, Estelle. **Fighting phishing and securing data with email authentication**. *Computer Fraud & Security*, v. 2016, n. 10, p. 5–8, 2016. DOI: [https://doi.org/10.1016/S1361-3723\(16\)30079-3](https://doi.org/10.1016/S1361-3723(16)30079-3). Disponível em: <https://www.sciencedirect.com/science/article/pii/S1361372316300793>.

(91) RAULOT, Adrien. **Bypassing phishing protections with email authentication**. 2019. Trabalho de conclusão (Mestrado em Security and Network Engineering) — University of Amsterdam, Amsterdam, 4 fev. 2019. Orientadores: Marat Nigmatullin; Alex Stavroulakis. Disponível em: <https://rp.os3.nl/2018-2019/p61/report.pdf>.

(92) SHUKLA, Sanjeev; MISRA, Manoj; VARSHNEY, Gaurav. **Spoofed email based cyberattack detection using machine learning**. *Journal of Computer Information Systems*, v. 65, n. 2, p. 159–171, 2023. DOI: <https://doi.org/10.1080/08874417.2023.2270452>.

(93) HUREAU, O.; BAYER, J.; DUDA, A.; KORCZYŃSKI, M. **Spoofed emails: an analysis of the issues hindering a larger deployment of DMARC**. In: RICHTER, P.; BAJPAI, V.; CARISIMO, E. (ed.). *Passive and active measurement – PAM 2024*. Cham: Springer, 2024. (Lecture Notes in Computer Science, v. 14537). DOI: https://doi.org/10.1007/978-3-031-56249-5_10.

(94) KITTERMAN, Scott. **RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1**. Internet Engineering Task Force (IETF), 2014. Disponível em: <https://datatracker.ietf.org/doc/html/rfc7208>.

(95) CROCKER, Dave; HANSEN, Tony; KUCHERAWY, Murray. (Eds.). **RFC 6376: DomainKeys Identified Mail (DKIM) Signatures**. [S. l.]: Internet Engineering Task Force (IETF), set. 2011. Disponível em: <https://datatracker.ietf.org/doc/html/rfc6376>.

(96) HANSEN, Tony; CROCKER, Dave; HALLAM-BAKER, Phillip. **RFC 5585: DomainKeys Identified Mail (DKIM) Service Overview**. [S.l.]: Internet Engineering Task Force (IETF), jul. 2009. Disponível em: <https://datatracker.ietf.org/doc/html/rfc5585>.

(97) BIRTHRIYA, Kumar Santosh; AHLAWAT, Priyanka; JAIN, Ankit Kumar. **Detection and prevention of spear phishing attacks: a comprehensive survey**. *Computers & Security*, v. 151, p. 104317, 2025. DOI: <https://doi.org/10.1016/j.cose.2025.104317>.

(98) KUCHERAWY, Murray; ZWICKY, Elizabeth. (Eds.). **RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC)**. [S. l.]: RFC Editor, mar. 2015. Disponível em: <https://datatracker.ietf.org/doc/html/rfc7489>.

(99) HERR, Todd; LEVINE, John R. (eds.). **Domain-Based Message Authentication, Reporting, and Conformance (DMARC)**. RFC 9989. [S.l.]: IETF, maio 2026. Disponível em: <https://datatracker.ietf.org/doc/html/rfc9989>.

(100) BROTMAN, Alex (ed.). **Domain-Based Message Authentication, Reporting, and Conformance (DMARC) Aggregate Reporting**. RFC 9990. [S.l.]: IETF, maio 2026. Disponível em: <https://datatracker.ietf.org/doc/html/rfc9990>.

(101) JONES, Steven M.; VESELY, Alessandro. (eds.). **Domain-Based Message Authentication, Reporting, and Conformance (DMARC) Failure Reporting**. RFC 9991. [S.l.]: IETF, maio 2026. Disponível em: <https://datatracker.ietf.org/doc/html/rfc9991>.

(102) KUCHERAWY, Murray. **Message Header Field for Indicating Message Authentication Status**. RFC 8601. [S.l.]: IETF, maio 2019. Disponível em: <https://datatracker.ietf.org/doc/html/rfc8601>.

(103) KUCHERAWY, Murray. **RFC 7372: Email Authentication Status Codes**. [S. l.]: Internet Engineering Task Force (IETF), set. 2014. Disponível em: <https://datatracker.ietf.org/doc/html/rfc7372>.

(104) IYER, R. Padmavathi; ATREY, Pradeep K.; VARSHNEY, Gaurav; MISRA, Manoj. **Email spoofing detection using volatile memory forensics**. In: *IEEE CONFERENCE ON COMMUNICATIONS AND NETWORK SECURITY (CNS)*, 2017. Anais [...]. [S.l.: s.n.], 2017. p. 619–625. DOI: <https://doi.org/10.1109/CNS.2017.8228692>.

(105) RATHOD, Tejal; JADAV, Nilesh Kumar; TANWAR, Sudeep; ALABDULATIF, Abdulatif; GARG, Deepak; SINGH, Anupam. **A comprehensive survey on social engineering attacks, countermeasures, case study, and research challenges**. *Information Processing & Management*, v. 62, n. 1, p. 103928, 2025. DOI: <https://doi.org/10.1016/j.ipm.2024.103928>.

(106) GARCIA, Helton; NUNES, Rafael Rabelo; SOUZA NETO, João. **Q.U.A.S.E.: uma metodologia ágil para diagnóstico de ataques de phishing**. In: *SIMPÓSIO BRASILEIRO DE CIBERSEGURANÇA (SBSEG)*, 25., 2025, Foz do Iguaçu/PR. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2025. p. 710-722. DOI: <https://doi.org/10.5753/sbseg.2025.10509>.

(107) JALDA, Chaitra Sai; NANDA, Ashok Kumar; PITCHAI, R. **Spoofing e-mail detection using stacking algorithm**. In: *INTERNATIONAL CONFERENCE ON SMART STRUCTURES AND SYSTEMS (ICSSS)*, 8., 2022. Anais [...]. [S.l.: s.n.], 2022. p. 1–4. DOI: <https://doi.org/10.1109/ICSSS54381.2022.9782173>.

(108) PONGCHANCHAI, Natthamon; VISOOTTIVISETH, Vasaka; OU, Kento; YAMAI, Nariyoshi; KITAGAWA, Naoya. **Countermeasure against spoofed e-mails using display name as a user authenticator**. In: *IEEE. 2018 Seventh ICT International Student Project Conference (ICT-ISPC)*, 2018. IEEE, 2018. p. 1–6. DOI: <https://doi.org/10.1109/ICT-ISPC.2018.8523883>.

(109) CHRYSANTHOU, Anargyros; PANTIS, Yorgos; PATSAKIS, Constantinos. **The anatomy of deception: Measuring technical and human factors of a large-scale phishing campaign**. *Computers & Security*, v. 140, p. 103780, 2024. DOI: <https://doi.org/10.1016/j.cose.2024.103780>.

(110) ABDULLAH, Ahmad Syukri; MOHD, Masnizah. **Spear phishing simulation in critical sector: telecommunication and defense sub-sector**. In: *2019 International Conference on Cybersecurity (ICoCSec)*, 2019. Anais [...]. [S.l.]: IEEE, 2019. p. 26–31. DOI: <https://doi.org/10.1109/ICoCSec47621.2019.8970803>.

(111) BISHNOI, Ayush; GARV; BISHNOI, Sagar; GUPTA, Neha. **Comprehensive assessment of reverse social engineering to understand social engineering attacks**. In: *INTERNATIONAL CONFERENCE ON SMART SYSTEMS AND INVENTIVE TECHNOLOGY (ICSSIT)*, 5., 2023. Anais [...]. [S.l.: s.n.], 2023. p. 681–685. DOI: <https://doi.org/10.1109/ICSSIT55814.2023.10061054>.

(112) STAFFORD, Christina D. **Weakest link: assessing factors that influence susceptibility to falling victim to phishing attacks and methods to mitigate**. 2020. Dissertação (Mestrado em Cybersecurity) – Utica College, Utica, 2020. Disponível em: <https://search.proquest.com/openview/ef5824dbfa8c6505509390467a7489ad/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y>

(113) ARSHAD, A.; REHMAN, A. U.; JAVAID, S.; ALI, T. M.; SHEIKH, J. A.; AZEEM, M. **A Systematic Literature Review on Phishing and Anti-Phishing Techniques**. *Pakistan Journal of Engineering and Technology (PakJET)*, v. 4, n. 1, p. 163-168, 2021. Disponível em: <https://journals.uol.edu.pk/pakjet/article/view/750/504>.

(114) KOLUPURI, Sai Venkata Jaswant; PAUL, Ananya; BHOWMICK, Rajat Subhra; GANGULI, Isha. **Scams and frauds in the digital age: ML-based detection and prevention strategies**. In: *PROCEEDINGS OF THE 26th INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING AND NETWORKING (ICDCN '25)*, 2025, [s.l.]. Anais [...]. New York: Association for Computing Machinery, 2025. p. 340–345. DOI: <https://doi.org/10.1145/3700838.3703672>.

(115) AL-MUSIB, Norah Saud; AL-SERHANI, Faeiz Mohammad; HUMAYUN, Mamoon; JHANJHI, N. Z. **Business email compromise (BEC) attacks**. *Materials Today: Proceedings*, v. 81, p. 497–503, 2023. DOI: <https://doi.org/10.1016/j.matpr.2021.03.647>.

(116) ALMUTAIRI, Amirah; KANG, BooJoong; ALHASHIMY, Nawfal. **Business email compromise: a systematic review of understanding, detection, and challenges**. *Computers & Security*, v. 158, p. 104630, 2025. DOI: <https://doi.org/10.1016/j.cose.2025.104630>.

(117) BONHARD, S. Kanj; VILLALTA, P. Garcia; ROSÉS, O.; PEGUEROLES, J. A **review of tactics, techniques, and procedures (TTPs) of MITRE framework for business email compromise (BEC) attacks**. *IEEE Access*, v. 13, p. 50761–50776, 2025. DOI: <https://doi.org/10.1109/ACCESS.2025.3552523>.

(118) ADIL, Muhammad Abdullah. **Analysis of phishing attacks and effective countermeasures**. *TechRxiv*, 25 jun. 2025. DOI: <https://doi.org/10.36227/techrxiv.175087100.06475579/v1>.

(119) CÂNDIDO, Guilherme Dieguez; SILVA, Igor Ramos Bezerra da; GONÇALVES, Emílio; SOUZA, Leonardo de Paiva; NETO, João Souza; NUNES, Rafael Rabelo. **StopEmailSpoofing: uma solução para detecção de vulnerabilidade de domínios à ataques falsificação de e-mail**. *RISTI – Revista Ibérica de Sistemas e Tecnologias de Informação*, n. 60, p. 57-73, dez. 2025. DOI: 10.17013/risti.60.57-73. Disponível em: <https://scielo.pt/pdf/rist/n60/2183-0126-rist-60-57.pdf>.

APÊNDICES

A- ANÁLISE DO COMPORTAMENTO INDIVIDUAL DOS AGRUPAMENTOS

A.1. ADMINISTRAÇÃO E ECONOMIA

Composto por 23 órgãos, o grupo partiu de um patamar de vulnerabilidade ligeiramente superior ao da amostra geral. Em fevereiro de 2025, 15 dos 23 domínios (65,22%) encontravam-se em alguma condição de exposição, contra 64,77% no conjunto total da APF. Essa proximidade inicial entre este segmento e o panorama geral, contudo, não se manteve ao longo do período, já que seu comportamento revelou um padrão de resposta às ações de mitigação notavelmente mais concentrado e tardio do que o observado na amostra geral. Os resultados podem ser verificados no Gráfico A.1 e na Tabela A.1.

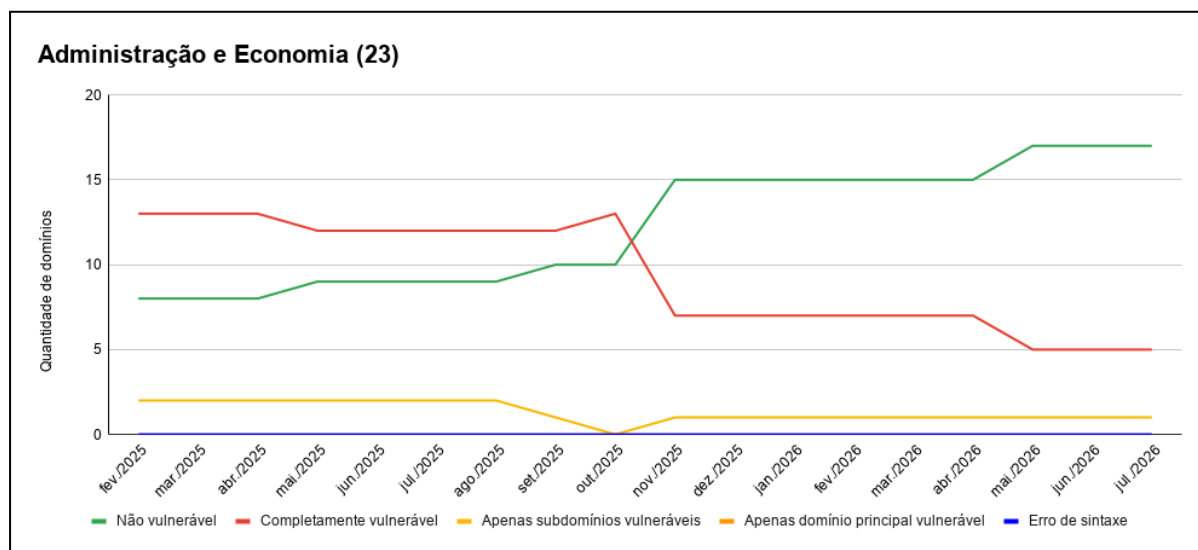


Gráfico A.1. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Administração e Economia”.

Tabela A.1. Dados coletados referentes aos 23 domínios do grupo “Administração e Economia”.

	Não Vulneráveis	Vulneráveis			
		Completamente Vulneráveis	Apenas Subdomínios	Apenas Domínio Principal	Erro de Sintaxe
fev./2025	8	13	2	0	0
mar./2025	8	13	2	0	0
abr./2025	8	13	2	0	0
mai./2025	9	12	2	0	0
jun./2025	9	12	2	0	0
jul./2025	9	12	2	0	0

ago./2025	9	12	2	0	0
set./2025	10	12	1	0	0
out./2025	10	13	0	0	0
nov./2025	15	7	1	0	0
dez./2025	15	7	1	0	0
jan./2026	15	7	1	0	0
fev./2026	15	7	1	0	0
mar./2026	15	7	1	0	0
abr./2026	15	7	1	0	0
mai./2026	17	5	1	0	0
jun./2026	17	5	1	0	0
jul./2026	17	5	1	0	0

Ao final do período de observação, como ilustrado no Gráfico A.2, o grupo atingiu 73,91% de domínios protegidos, contra 26,09% ainda vulneráveis, uma variação de +39,13 pontos percentuais, notavelmente superior à melhoria média da amostra geral (+30,61).

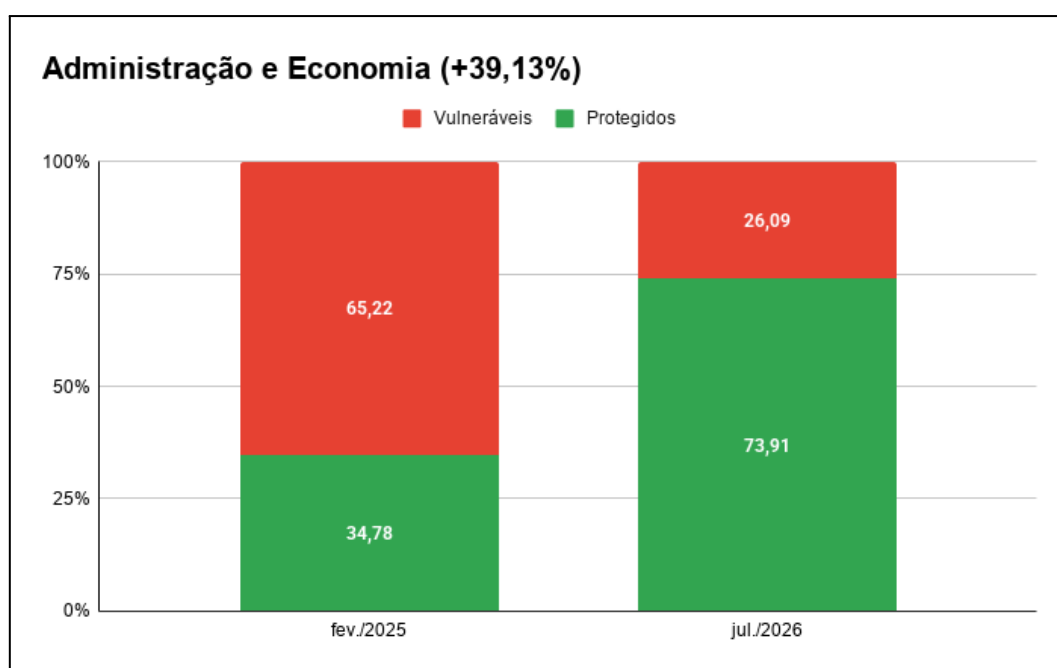


Gráfico A.2. Variação do estado de vulnerabilidade dos domínios do grupo “Administração e Economia” no período analisado.

A.2. AGRICULTURA E ORGANIZAÇÃO AGRÁRIA

Composto por 10 órgãos, este agrupamento partiu de um índice de vulnerabilidade de 70% em fevereiro de 2025, patamar superior ao verificado na amostra geral (64,77%). Trata-se, no entanto, do grupo cujo comportamento ao longo do período mais se distancia do padrão observado no panorama geral e nos demais grupos, sobretudo por concentrar parte de sua melhoria em um momento anterior ao início de qualquer ação de mitigação. Os resultados podem ser verificados no Gráfico A.3 e na Tabela A.2.

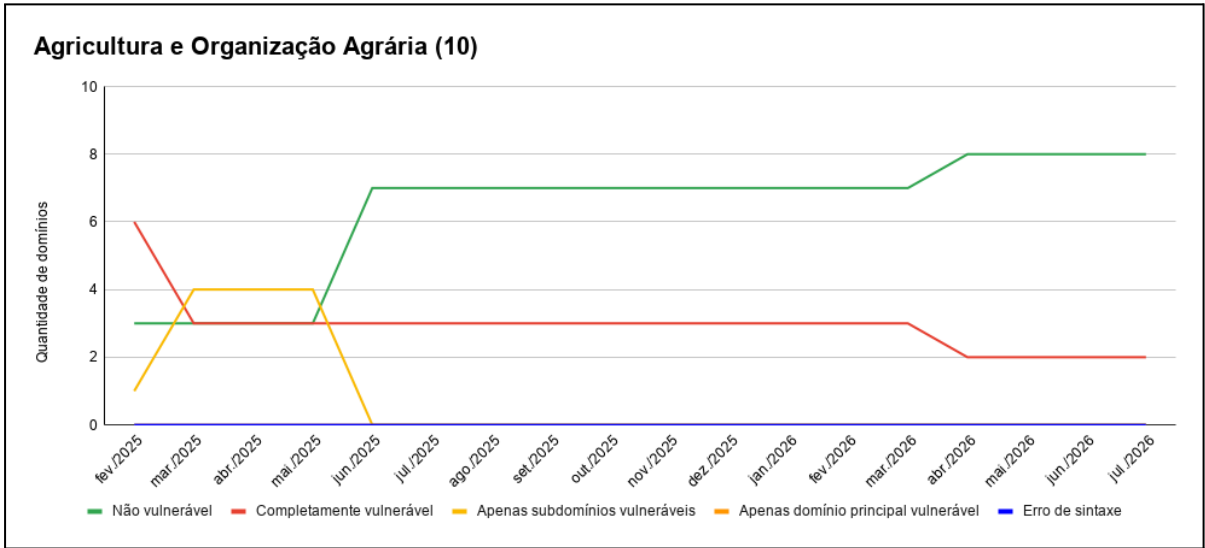


Gráfico A.3. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Agricultura e Organização Agrária”.

Tabela A.2. Dados coletados referentes aos 10 domínios do grupo “Agricultura e Organização Agrária”.

	Não Vulneráveis	Vulneráveis			
		Completamente Vulneráveis	Apenas Subdomínios	Apenas Domínio Principal	Erro de Sintaxe
fev./2025	3	6	1	0	0
mar./2025	3	3	4	0	0
abr./2025	3	3	4	0	0
mai./2025	3	3	4	0	0
jun./2025	7	3	0	0	0
jul./2025	7	3	0	0	0
ago./2025	7	3	0	0	0
set./2025	7	3	0	0	0
out./2025	7	3	0	0	0
nov./2025	7	3	0	0	0

dez./2025	7	3	0	0	0
jan./2026	7	3	0	0	0
fev./2026	7	3	0	0	0
mar./2026	7	3	0	0	0
abr./2026	8	2	0	0	0
mai./2026	8	2	0	0	0
jun./2026	8	2	0	0	0
jul./2026	8	2	0	0	0

Ao final do período, como evidenciado no Gráfico A.4, o grupo alcançou 80% de domínios protegidos, com 20% ainda vulneráveis, o que representa uma variação positiva de 50 pontos percentuais, superando a melhoria verificada na amostra geral (+30,61). É preciso, todavia, relembrar que esse avanço decorreu majoritariamente de dois movimentos concentrados em março e junho de 2025, anteriores ao início de qualquer ação de mitigação da pesquisa, e não de uma resposta às intervenções institucionais ou individualizadas adotadas posteriormente.

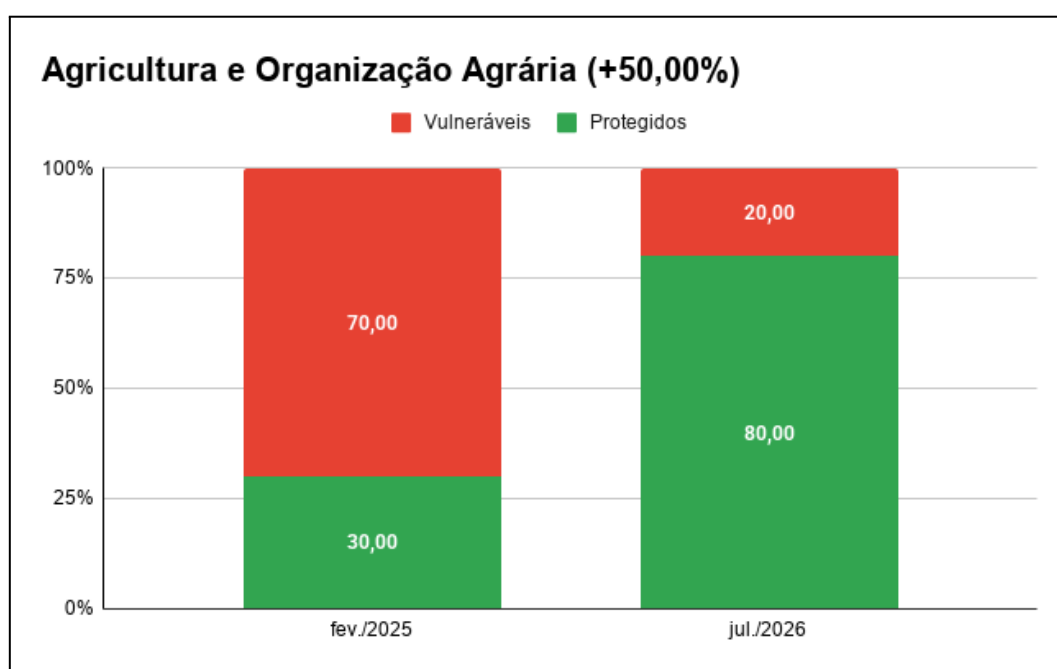


Gráfico A.4. Variação do estado de vulnerabilidade dos domínios do grupo “Agricultura e Organização Agrária” no período analisado.

A.3. PREVIDÊNCIA, ASSISTÊNCIA SOCIAL, TRABALHO E HABITAÇÃO

Composto por 13 órgãos, este grupo partiu de um patamar de vulnerabilidade de 69,23% em fevereiro de 2025, ligeiramente superior ao verificado na amostra geral (64,77%). Ao final do período, o segmento revelou um desempenho também positivo, embora modesto. Os resultados podem ser verificados no Gráfico A.5 e na Tabela A.3.

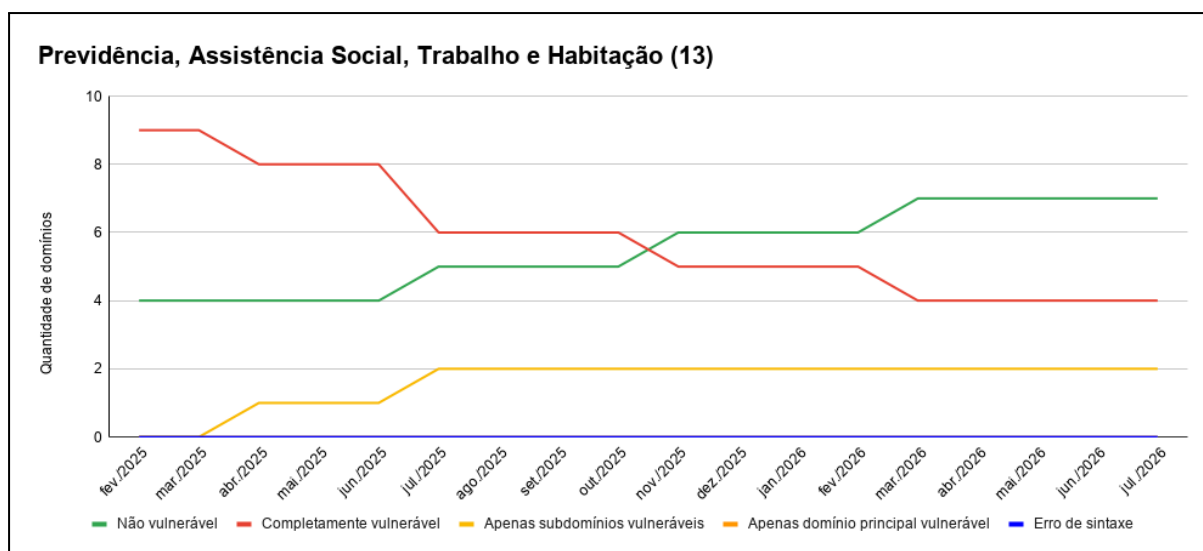


Gráfico A.5. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Previdência, Assistência Social, Trabalho e Habitação”.

Tabela A.3. Dados coletados referentes aos 13 domínios do grupo “Previdência, Assistência Social, Trabalho e Habitação”.

	Não Vulneráveis	Vulneráveis			
		Completamente Vulneráveis	Apenas Subdomínios	Apenas Domínio Principal	Erro de Sintaxe
fev./2025	4	9	0	0	0
mar./2025	4	9	0	0	0
abr./2025	4	8	1	0	0
mai./2025	4	8	1	0	0
jun./2025	4	8	1	0	0
jul./2025	5	6	2	0	0
ago./2025	5	6	2	0	0
set./2025	5	6	2	0	0
out./2025	5	6	2	0	0
nov./2025	6	5	2	0	0
dez./2025	6	5	2	0	0
jan./2026	6	5	2	0	0
fev./2026	6	5	2	0	0
mar./2026	7	4	2	0	0
abr./2026	7	4	2	0	0
mai./2026	7	4	2	0	0

jun./2026	7	4	2	0	0
jul./2026	7	4	2	0	0

Ao final do período, como se pode observar no Gráfico A.6, o grupo atingiu 53,85% de domínios protegidos contra 46,15% ainda vulneráveis, uma variação de 23,08 pontos percentuais positivos, inferior à média da amostra geral (+30,61). Somando-se o fato de que parte relevante de sua melhoria ocorreu por meio de reduções de severidade — refletidas no acúmulo de dois domínios permanentemente classificados como “Apenas Subdomínios Vulneráveis” desde julho de 2025 até julho de 2026 — e não por eliminação completa da exposição, esse resultado indica que este agrupamento constitui um caso de refração às ações de mitigação empregadas na pesquisa, sobretudo às ações mais recentes e de maior eficácia observada na amostra geral.

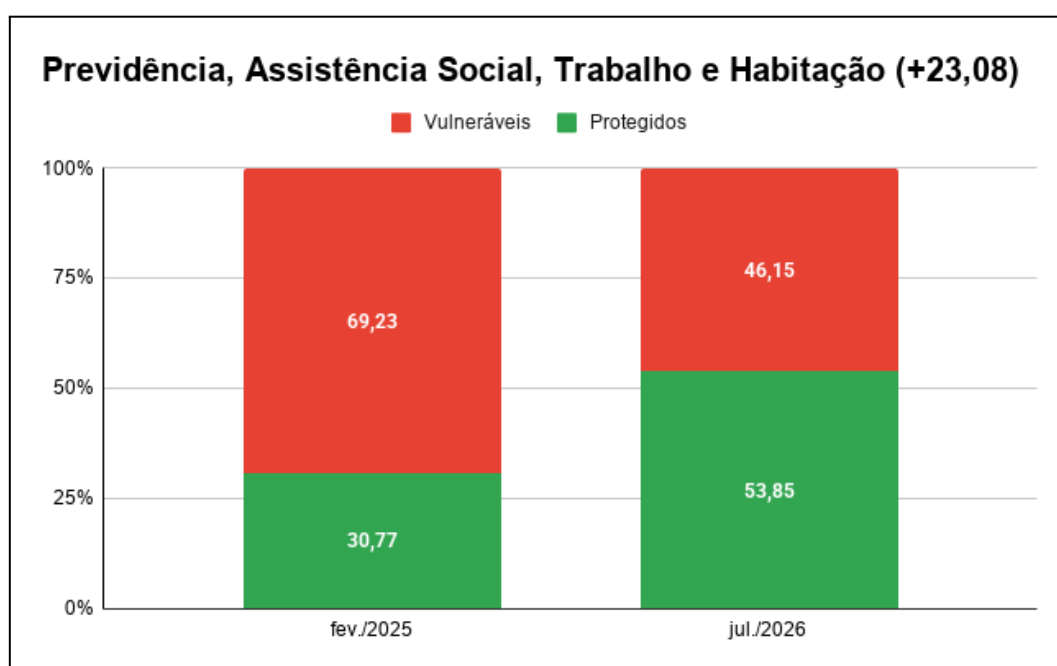


Gráfico A.6. Variação do estado de vulnerabilidade dos domínios do grupo “Previdência, Assistência Social, Trabalho e Habitação” no período analisado.

A.4. CIÊNCIA, TECNOLOGIA E COMUNICAÇÕES

Composto por 16 órgãos, este agrupamento partiu de um patamar de vulnerabilidade de 56,25% em fevereiro de 2025, inferior aos 64,77% observados na amostra geral no mesmo período. Já nesse ponto de partida, o segmento demonstrava, portanto, uma exposição consideravelmente menor do que a do conjunto total da APF, característica que se manteve ao longo de praticamente todo o período de observação. Os resultados podem ser verificados no Gráfico A.7 e na Tabela A.4.

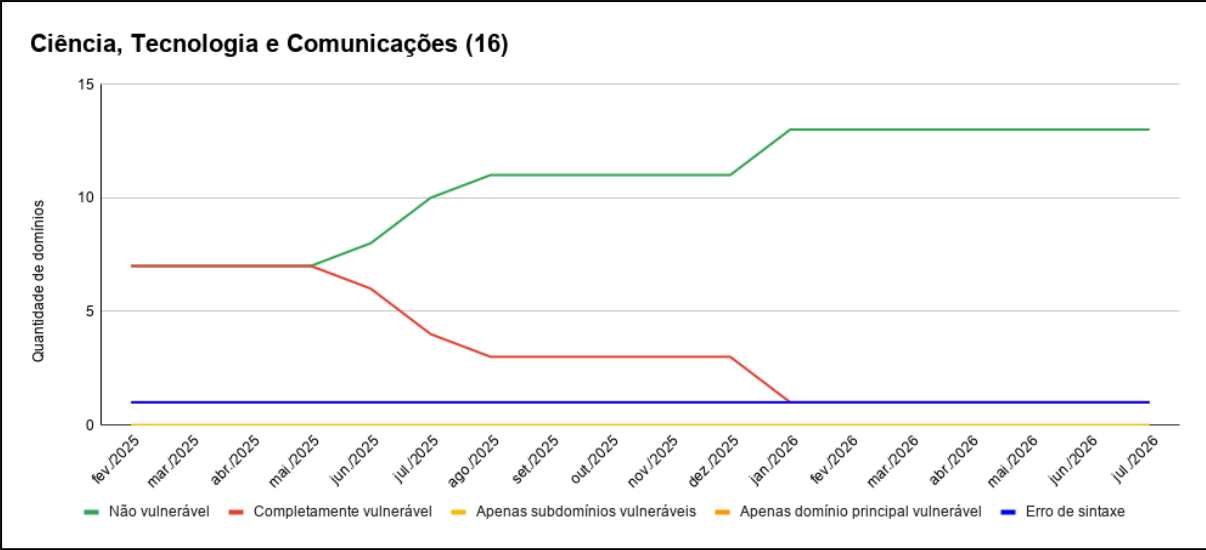


Gráfico A.7. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Ciência, Tecnologia e Comunicações”.

Tabela A.4. Dados coletados referentes aos 16 domínios do grupo “Ciência, Tecnologia e Comunicações”.

	Não Vulneráveis	Vulneráveis			
		Completamente Vulneráveis	Apenas Subdomínios	Apenas Domínio Principal	Erro de Sintaxe
fev./2025	7	7	0	1	1
mar./2025	7	7	0	1	1
abr./2025	7	7	0	1	1
mai./2025	7	7	0	1	1
jun./2025	8	6	0	1	1
jul./2025	10	4	0	1	1
ago./2025	11	3	0	1	1
set./2025	11	3	0	1	1
out./2025	11	3	0	1	1
nov./2025	11	3	0	1	1
dez./2025	11	3	0	1	1
jan./2026	13	1	0	1	1
fev./2026	13	1	0	1	1
mar./2026	13	1	0	1	1
abr./2026	13	1	0	1	1
mai./2026	13	1	0	1	1
jun./2026	13	1	0	1	1

jul./2026	13	1	0	1	1
-----------	----	---	---	---	---

Ao final do período, como ilustrado pelo Gráfico A.8, o grupo atingiu a marca de 81,25% de domínios protegidos contra 18,75% vulneráveis, uma variação positiva de 37,50 pontos percentuais — resultado superior à melhoria média da amostra geral (+30,61). Trata-se, portanto, de um padrão de mitigação que se mostrou consistente com o comportamento geral na primeira fase do estudo, mas que se descolou dele justamente no momento em que a amostra como um todo mais se beneficiou da comunicação individualizada e do apelo normativo.

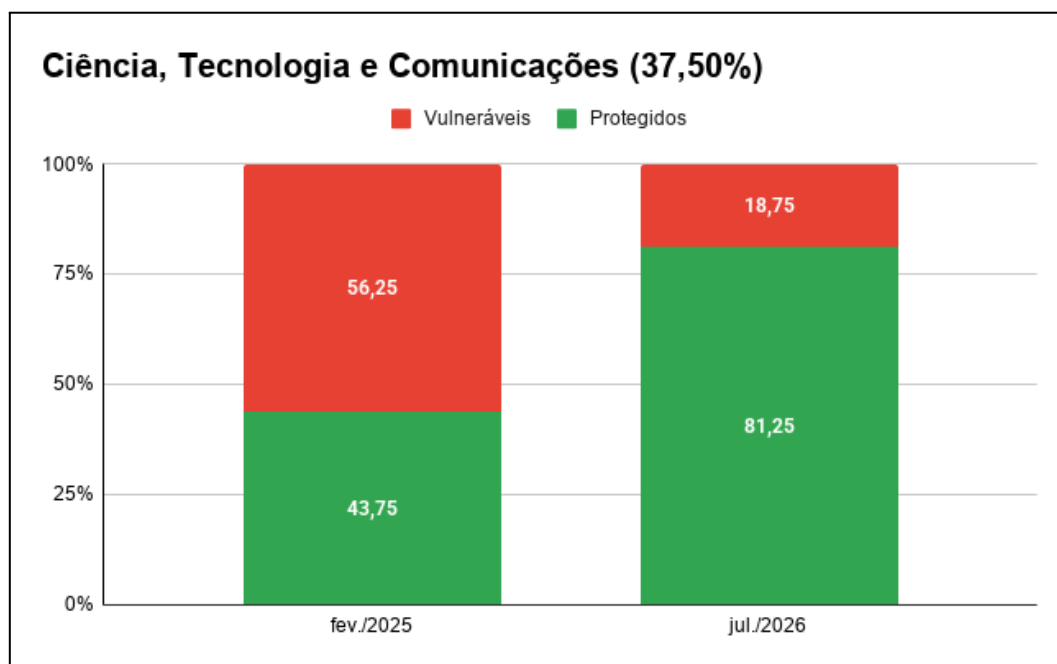


Gráfico A.8. Variação do estado de vulnerabilidade dos domínios do grupo “Ciência, Tecnologia e Comunicações” no período analisado.

A.5. CULTURA E EDUCAÇÃO

Este agrupamento constitui o maior recorte da amostra, reunindo 123 dos 281 órgãos analisados, o que corresponde a cerca de 44% do total. Essa proporção, como já mencionado, implica que a trajetória deste grupo tem peso considerável na composição da curva geral da amostra, o que deve ser levado em conta na leitura dos resultados. Em fevereiro de 2025, o grupo apresentava 68,29% de domínios vulneráveis, patamar próximo, embora ligeiramente superior, ao verificado na amostra geral (64,77%). Os resultados deste segmento podem ser verificados no Gráfico A.9 e na Tabela A.5.

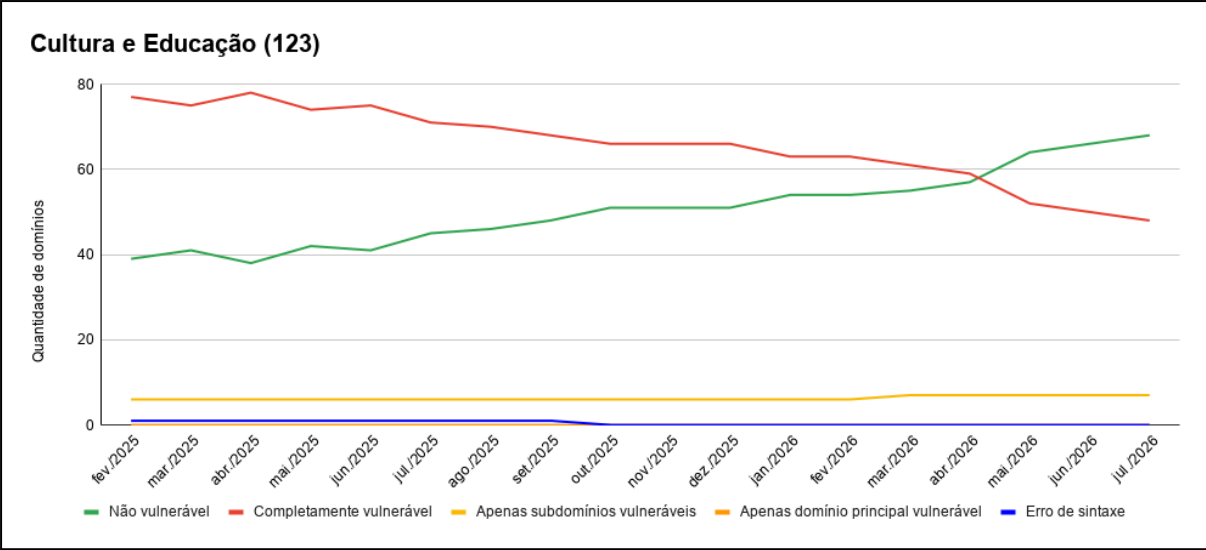


Gráfico A.9. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Cultura e Educação”.

Tabela A.5. Dados coletados referentes aos 123 domínios do grupo “Cultura e Educação”.

	Não Vulneráveis	Vulneráveis			
		Completamente Vulneráveis	Apenas Subdomínios	Apenas Domínio Principal	Erro de Sintaxe
fev./2025	39	77	6	0	1
mar./2025	41	75	6	0	1
abr./2025	38	78	6	0	1
mai./2025	42	74	6	0	1
jun./2025	41	75	6	0	1
jul./2025	45	71	6	0	1
ago./2025	46	70	6	0	1
set./2025	48	68	6	0	1
out./2025	51	66	6	0	0
nov./2025	51	66	6	0	0
dez./2025	51	66	6	0	0
jan./2026	54	63	6	0	0
fev./2026	54	63	6	0	0
mar./2026	55	61	7	0	0
abr./2026	57	59	7	0	0
mai./2026	64	52	7	0	0
jun./2026	66	50	7	0	0

jul./2026	68	48	7	0	0
-----------	----	----	---	---	---

Ao final do período, como se pode confirmar pelo Gráfico A.10, o grupo atingiu 55,28% de domínios protegidos, restando 44,72% ainda vulneráveis, uma variação de 23,57 pontos percentuais positivos. O resultado foi inferior à melhoria média da amostra geral (+30,61), apesar da forte resposta ao terceiro alerta individualizado. Além disso, destaca-se a persistência da categoria “Apenas Subdomínios Vulneráveis”, que não apenas se manteve estável ao longo de quase toda a série, como também chegou a aumentar ligeiramente no início de 2026 — padrão semelhante ao observado no conjunto geral da amostra, em que as vulnerabilidades parciais mostraram-se consistentemente mais resistentes às ações de mitigação do que os casos de vulnerabilidade completa.

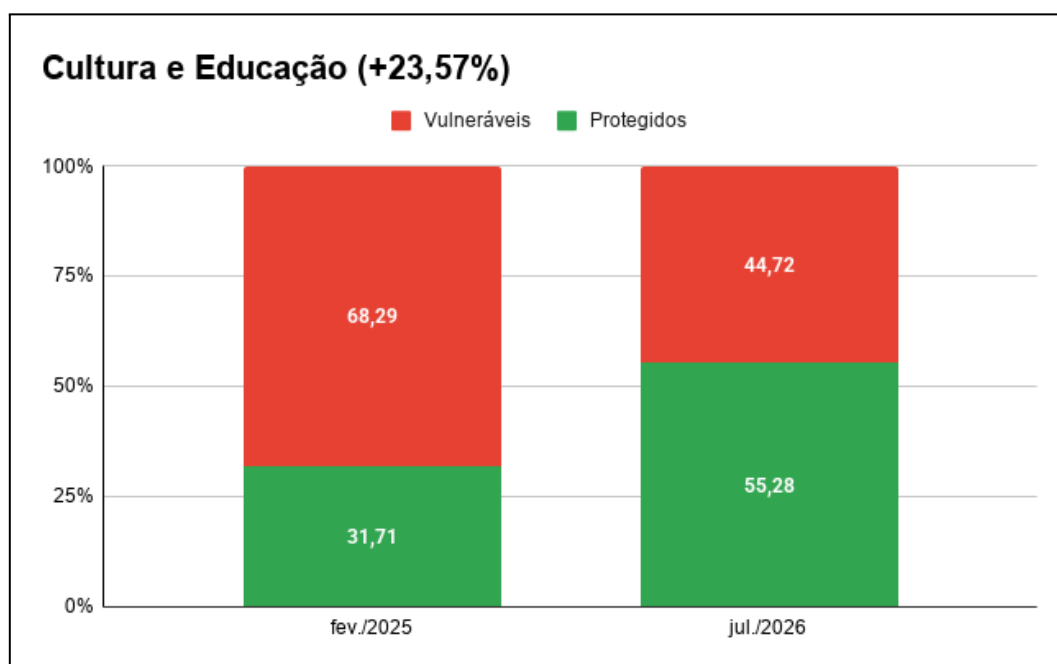


Gráfico A.10. Variação do estado de vulnerabilidade dos domínios do grupo “Cultura e Educação” no período analisado.

A.6. DEFESA NACIONAL, SEGURANÇA PÚBLICA E RELAÇÕES EXTERIORES

Composto por 14 órgãos, o agrupamento partiu de um patamar de vulnerabilidade de 57,14% em fevereiro de 2025, valor inferior ao verificado na amostra geral no mesmo período (64,77%). Este grupo, portanto, iniciou a pesquisa em posição relativamente mais favorável do que o conjunto total da APF, característica que se manteve, com variações pontuais, ao longo de todo o período observado. Os resultados podem ser verificados no Gráfico A.11 e na Tabela A.6.

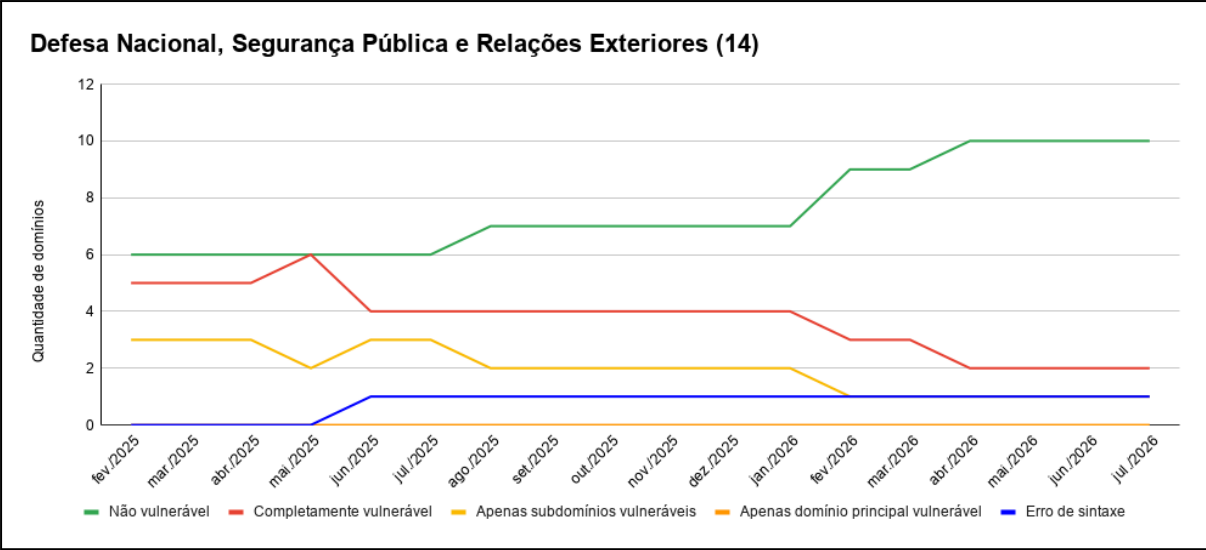


Gráfico A.11. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Defesa Nacional, Segurança Pública e Relações Exteriores”.

Tabela A.6. Dados coletados referentes aos 14 domínios do grupo “Defesa Nacional, Segurança Pública e Relações Exteriores”.

	Não Vulneráveis	Vulneráveis			
		Completamente Vulneráveis	Apenas Subdomínios	Apenas Domínio Principal	Erro de Sintaxe
fev./2025	6	5	3	0	0
mar./2025	6	5	3	0	0
abr./2025	6	5	3	0	0
mai./2025	6	6	2	0	0
jun./2025	6	4	3	0	1
jul./2025	6	4	3	0	1
ago./2025	7	4	2	0	1
set./2025	7	4	2	0	1
out./2025	7	4	2	0	1
nov./2025	7	4	2	0	1
dez./2025	7	4	2	0	1
jan./2026	7	4	2	0	1
fev./2026	9	3	1	0	1
mar./2026	9	3	1	0	1
abr./2026	10	2	1	0	1
mai./2026	10	2	1	0	1

jun./2026	10	2	1	0	1
jul./2026	10	2	1	0	1

Ao final do período, como ilustrado pelo Gráfico A.12, o segmento atingiu 71,43% de domínios protegidos contra 28,57% ainda vulneráveis, uma variação positiva de 28,57 pontos percentuais — resultado muito próximo, embora ligeiramente inferior, à melhoria média da amostra geral (+30,61). É interessante notar que, apesar de ter partido de uma posição inicial mais favorável do que o conjunto geral, o grupo praticamente equiparou seu ganho percentual ao da amostra como um todo.

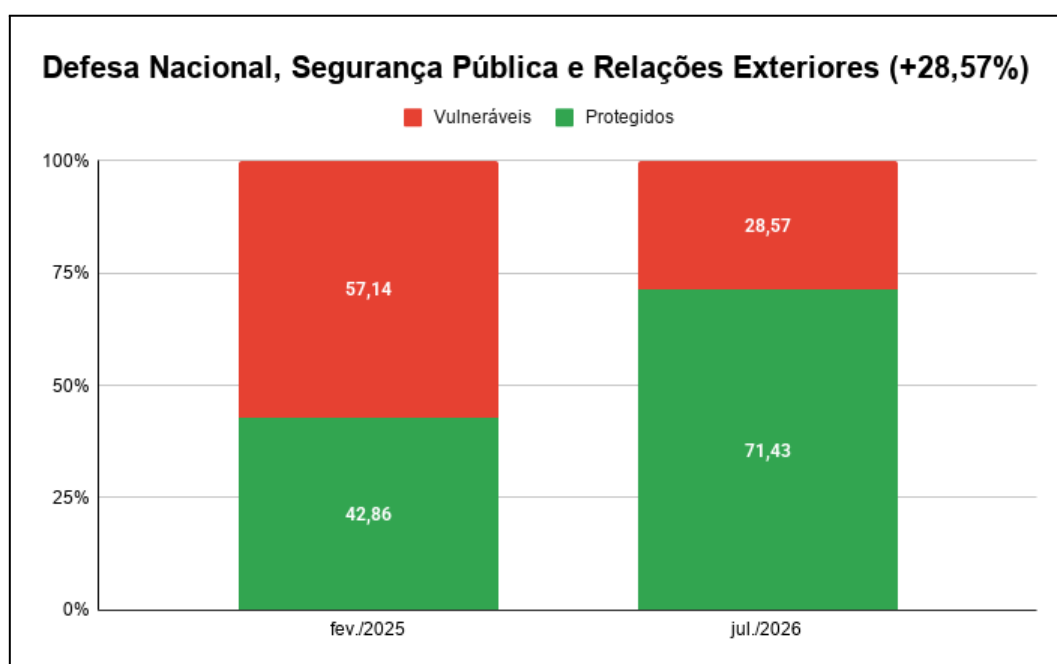


Gráfico A.12. Variação do estado de vulnerabilidade dos domínios do grupo “Defesa Nacional, Segurança Pública e Relações Exteriores” no período analisado.

A.7. DESPORTO, LAZER E DIREITOS DA CIDADANIA

Composto por 10 órgãos, o agrupamento partiu de um patamar de vulnerabilidade de 80% em fevereiro de 2025, substancialmente superior aos 64,77% observados na amostra geral no mesmo período. Trata-se, portanto, de um grupo que iniciou a pesquisa em condições bastante mais precárias do que as do conjunto agregado da APF. Os resultados podem ser verificados no Gráfico A.13 e na Tabela A.7.

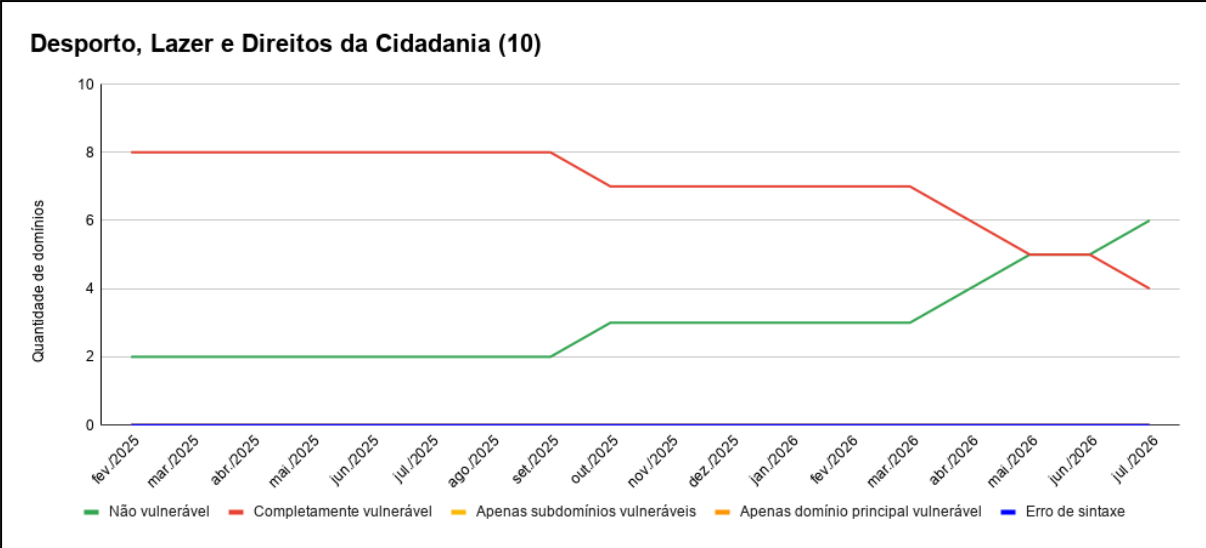


Gráfico A.13. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Desporto, Lazer e Direitos da Cidadania”.

Tabela A.7. Dados coletados referentes aos 10 domínios do grupo “Desporto, Lazer e Direitos da Cidadania”.

	Não Vulneráveis	Vulneráveis			
		Completamente Vulneráveis	Apenas Subdomínios	Apenas Domínio Principal	Erro de Sintaxe
fev./2025	2	8	0	0	0
mar./2025	2	8	0	0	0
abr./2025	2	8	0	0	0
mai./2025	2	8	0	0	0
jun./2025	2	8	0	0	0
jul./2025	2	8	0	0	0
ago./2025	2	8	0	0	0
set./2025	2	8	0	0	0
out./2025	3	7	0	0	0
nov./2025	3	7	0	0	0
dez./2025	3	7	0	0	0
jan./2026	3	7	0	0	0
fev./2026	3	7	0	0	0
mar./2026	3	7	0	0	0
abr./2026	4	6	0	0	0
mai./2026	5	5	0	0	0

jun./2026	5	5	0	0	0
jul./2026	6	4	0	0	0

Ao final do período, como se exhibe no Gráfico A.14, o grupo atingiu 60% de domínios protegidos contra 40% ainda vulneráveis, uma variação de 40 pontos percentuais positivos — resultado superior à melhoria média da amostra geral (+30,61). Esse resultado, contudo, decorre de uma trajetória qualitativamente distinta da observada no panorama geral. Enquanto a amostra agregada apresentou uma curva de recuperação relativamente contínua desde julho de 2025, este agrupamento permaneceu praticamente inerte por quase um ano — de fevereiro de 2025 a março de 2026, com uma única exceção pontual em outubro —, concentrando a quase totalidade de sua melhoria nos quatro meses finais da pesquisa, em resposta exclusivamente às ações de comunicação individualizada (segundo e terceiro alertas, mais especificamente). Vale registrar, ainda, que este grupo não apresentou, em nenhum momento da série, casos classificados como “Apenas Subdomínios Vulneráveis”, “Apenas Domínio Principal Vulnerável” ou “Erro de Sintaxe” — o que destoa do padrão observado na amostra geral, na qual essas categorias parciais, embora minoritárias, mantiveram-se como um resíduo persistente ao longo de todo o período.

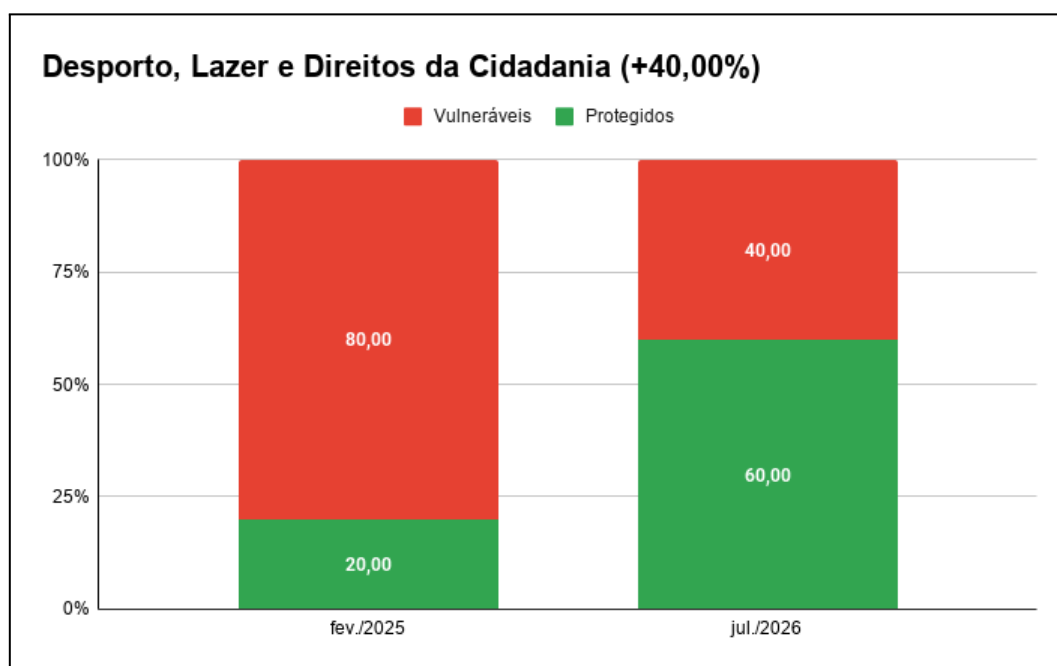


Gráfico A.14. Variação do estado de vulnerabilidade dos domínios do grupo “Desporto, Lazer e Direitos da Cidadania” no período analisado.

A.8. ENERGIA E GESTÃO AMBIENTAL

Composto por 20 órgãos, este agrupamento partiu de um patamar de vulnerabilidade de apenas 45% em fevereiro de 2025, consideravelmente inferior aos 64,77% observados na amostra geral no mesmo período. Este grupo, portanto, iniciou a pesquisa em uma condição bastante mais favorável do que o conjunto da APF, o que já antecipa uma margem de melhoria naturalmente menor do que a observada no panorama geral. Os resultados podem ser verificados no Gráfico A.15 e na Tabela A.8.

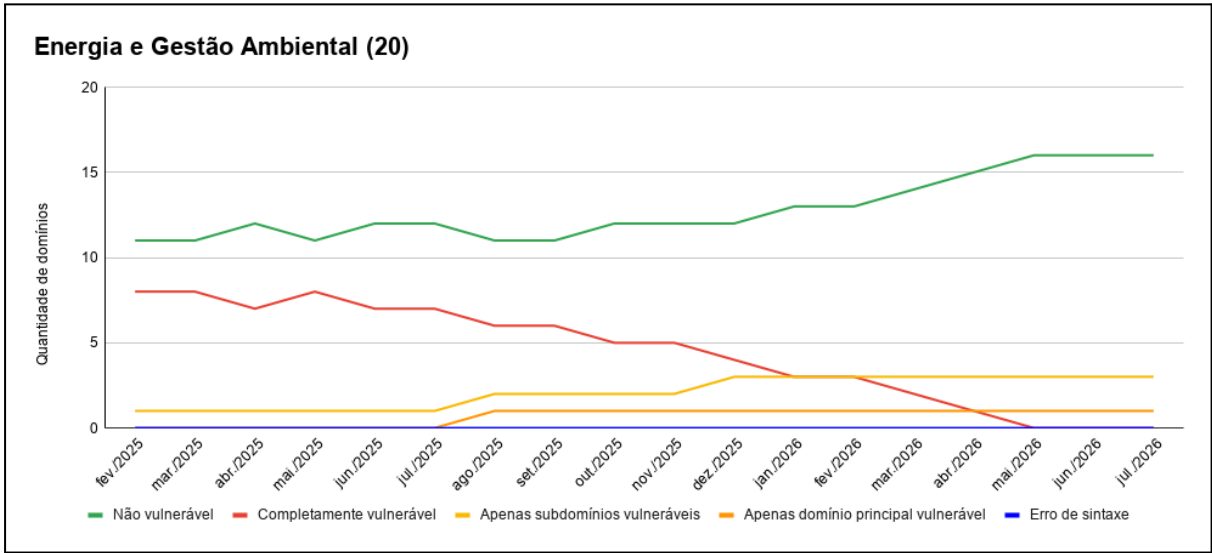


Gráfico A.15. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Energia e Gestão Ambiental”.

Tabela A.8. Dados coletados referentes aos 20 domínios do grupo “Energia e Gestão Ambiental”.

	Não Vulneráveis	Vulneráveis			
		Completamente Vulneráveis	Apenas Subdomínios	Apenas Domínio Principal	Erro de Sintaxe
fev./2025	11	8	1	0	0
mar./2025	11	8	1	0	0
abr./2025	12	7	1	0	0
mai./2025	11	8	1	0	0
jun./2025	12	7	1	0	0
jul./2025	12	7	1	0	0
ago./2025	11	6	2	1	0
set./2025	11	6	2	1	0
out./2025	12	5	2	1	0
nov./2025	12	5	2	1	0

dez./2025	12	4	3	1	0
jan./2026	13	3	3	1	0
fev./2026	13	3	3	1	0
mar./2026	14	2	3	1	0
abr./2026	15	1	3	1	0
mai./2026	16	0	3	1	0
jun./2026	16	0	3	1	0
jul./2026	16	0	3	1	0

Ao final do período, como evidenciado no Gráfico A.16, o grupo atingiu 80% de domínios protegidos contra 20% ainda vulneráveis, uma variação positiva de 25 pontos percentuais, inferior à melhoria média da amostra geral (+30,61). Essa diferença, como mencionado anteriormente, deve ser interpretada considerando-se o ponto de partida mais favorável deste agrupamento, 20 pontos percentuais acima da média geral, ou seja, a margem disponível para ganho era naturalmente menor. Mais relevante do que a variação percentual bruta é o fato de que este foi o único grupo a eliminar por completo a categoria “Completamente Vulnerável”.

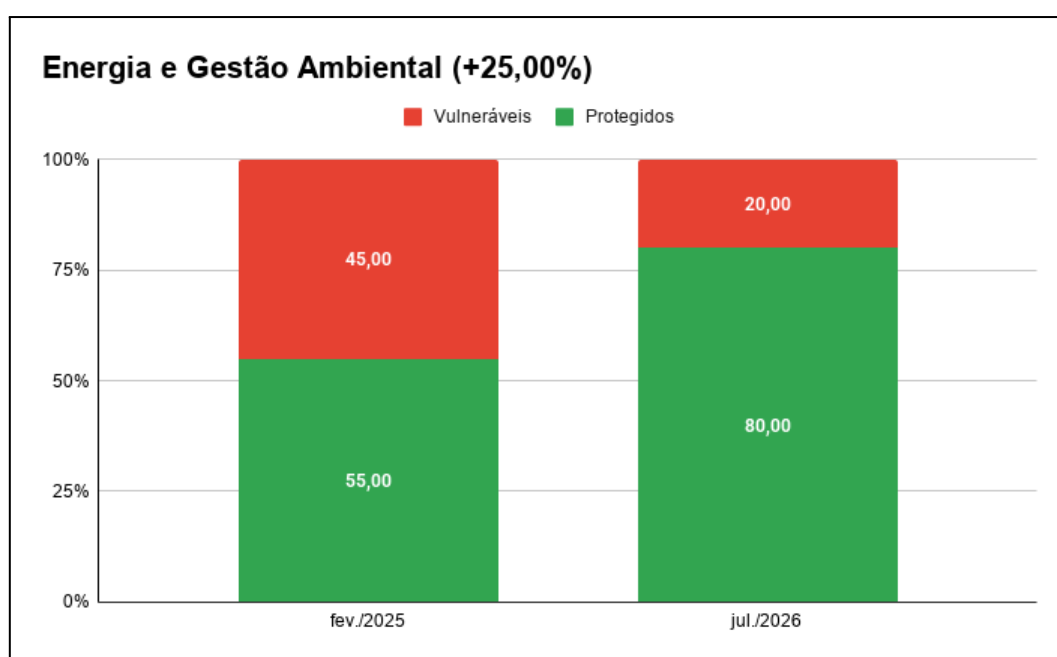


Gráfico A.16. Variação do estado de vulnerabilidade dos domínios do grupo “Energia e Gestão Ambiental” no período analisado.

A.9. INDÚSTRIA, COMÉRCIO E SERVIÇOS

Trata-se do menor recorte da amostra, composto por apenas 6 órgãos. Em fevereiro de 2025, o grupo apresentava 83,33% de domínios vulneráveis (5 de 6), patamar substancialmente superior aos 64,77% verificados na amostra geral no mesmo período, o que já indicava, no

início da pesquisa, uma condição de exposição bem mais crítica do que a média da APF. É importante registrar que a reduzida dimensão deste agrupamento faz com que cada domínio individual corresponda a aproximadamente 16,7 pontos percentuais do total, de modo que variações aparentemente expressivas devem ser interpretadas com cautela. Os resultados podem ser verificados no Gráfico A.17 e na Tabela A.9.

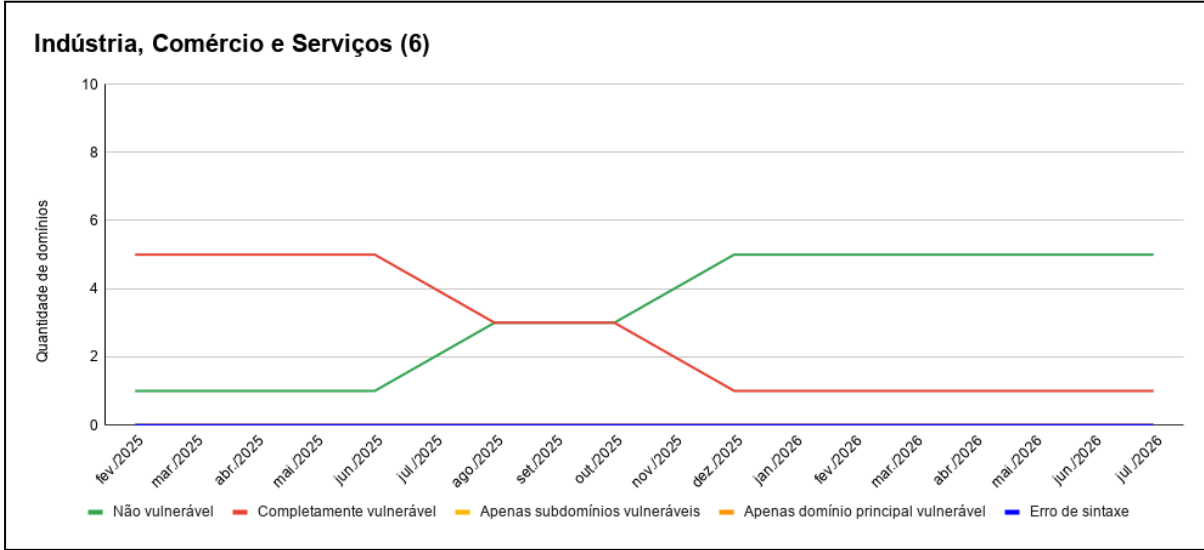


Gráfico A.17. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Indústria, Comércio e Serviços”.

Tabela A.9. Dados coletados referentes aos 6 domínios do grupo “Indústria, Comércio e Serviços”.

	Não Vulneráveis	Vulneráveis			
		Completamente Vulneráveis	Apenas Subdomínios	Apenas Domínio Principal	Erro de Sintaxe
fev./2025	1	5	0	0	0
mar./2025	1	5	0	0	0
abr./2025	1	5	0	0	0
mai./2025	1	5	0	0	0
jun./2025	1	5	0	0	0
jul./2025	2	4	0	0	0
ago./2025	3	3	0	0	0
set./2025	3	3	0	0	0
out./2025	3	3	0	0	0
nov./2025	4	2	0	0	0
dez./2025	5	1	0	0	0
jan./2026	5	1	0	0	0

fev./2026	5	1	0	0	0
mar./2026	5	1	0	0	0
abr./2026	5	1	0	0	0
mai./2026	5	1	0	0	0
jun./2026	5	1	0	0	0
jul./2026	5	1	0	0	0

Ao final do período, constatou-se uma completa inversão do cenário de vulnerabilidade em relação ao início da pesquisa. Passou-se de 1 domínio protegido e 5 completamente vulneráveis (em fevereiro de 2025) para 5 protegidos e 1 completamente vulnerável (em julho de 2026). Como evidenciado pelo Gráfico A.18, o grupo atingiu, portanto, 83,33% de domínios protegidos contra 16,67% vulneráveis, uma variação de 66,66 pontos percentuais positivos — o maior ganho percentual entre os agrupamentos, e bastante superior à melhoria média da amostra geral (+30,61). Esse resultado, como já mencionado, deve ser relativizado à luz do tamanho reduzido do grupo. Vale destacar, por fim, que este foi outro grupo a não apresentar, em nenhum momento da série, qualquer caso de vulnerabilidade parcial, situação que contrasta com a persistência dessas categorias observada no comportamento geral da amostra.

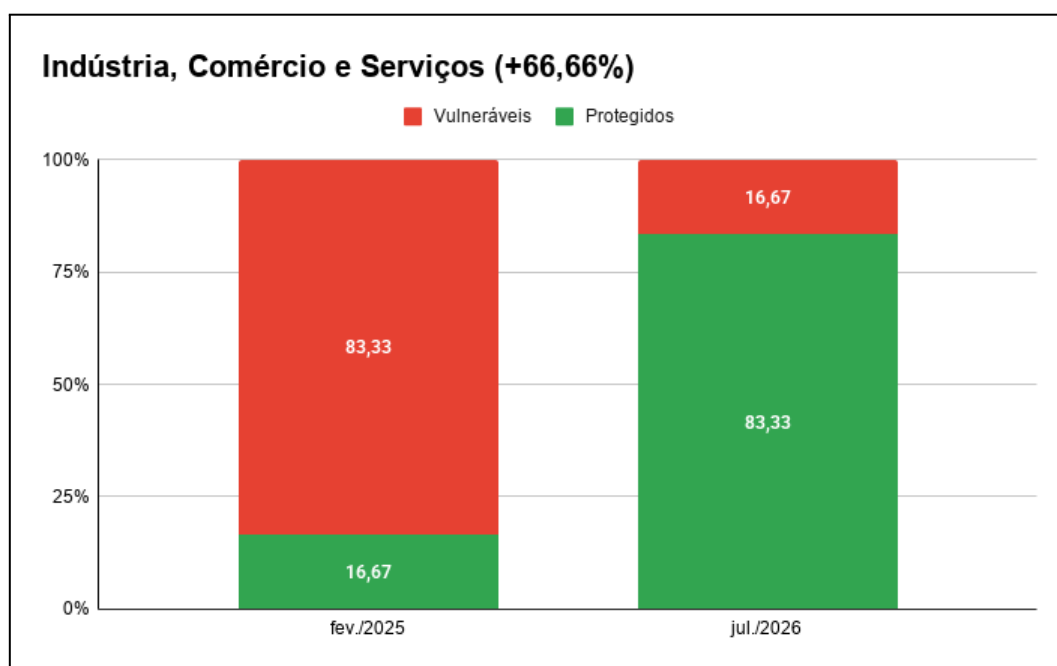


Gráfico A.18. Variação do estado de vulnerabilidade dos domínios do grupo “Indústria, Comércio e Serviços” no período analisado.

A.10. LEGISLATIVO, JUDICIÁRIO E ESSENCIAIS À JUSTIÇA

Composto por 10 órgãos, o agrupamento partiu de um patamar de vulnerabilidade de 50% em fevereiro de 2025, índice inferior ao de 64,77% observado na amostra geral no mesmo período. Desta forma, este grupo iniciou a pesquisa em uma posição relativamente mais confortável do que o conjunto agregado da APF. Os resultados podem ser verificados no Gráfico A.19 e na Tabela A.10.

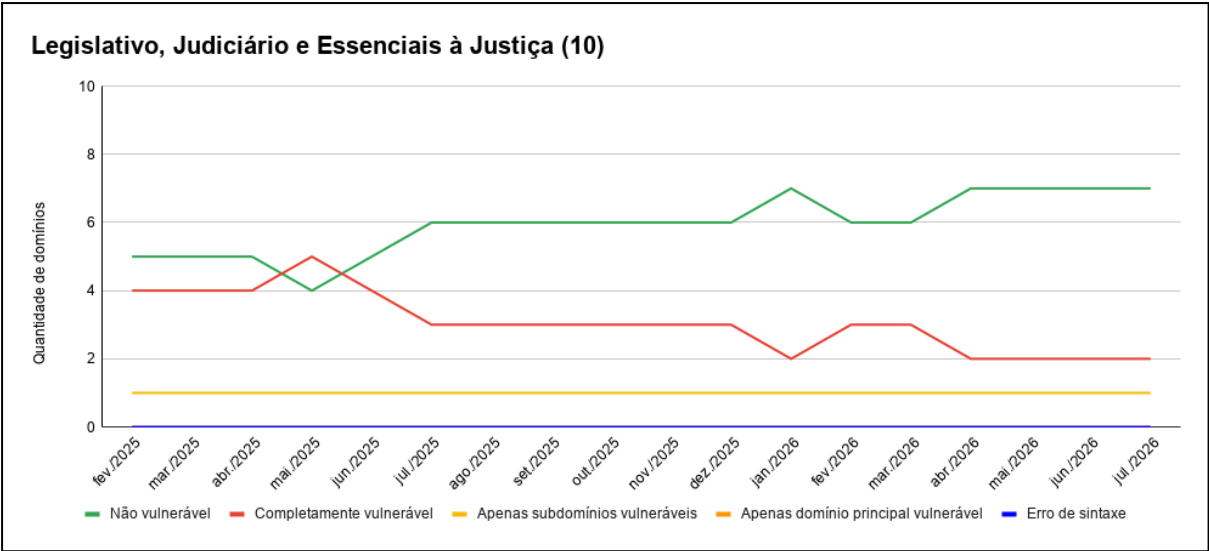


Gráfico A.19. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Legislativo, Judiciário e Essenciais à Justiça”.

Tabela A.10. Dados coletados referentes aos 10 domínios do grupo “Legislativo, Judiciário e Essenciais à Justiça”.

	Não Vulneráveis	Vulneráveis			
		Completamente Vulneráveis	Apenas Subdomínios	Apenas Domínio Principal	Erro de Sintaxe
fev./2025	5	4	1	0	0
mar./2025	5	4	1	0	0
abr./2025	5	4	1	0	0
mai./2025	4	5	1	0	0
jun./2025	5	4	1	0	0
jul./2025	6	3	1	0	0
ago./2025	6	3	1	0	0
set./2025	6	3	1	0	0
out./2025	6	3	1	0	0
nov./2025	6	3	1	0	0

dez./2025	6	3	1	0	0
jan./2026	7	2	1	0	0
fev./2026	6	3	1	0	0
mar./2026	6	3	1	0	0
abr./2026	7	2	1	0	0
mai./2026	7	2	1	0	0
jun./2026	7	2	1	0	0
jul./2026	7	2	1	0	0

Ao final do período, como demonstrado pelo Gráfico A.20, o grupo atingiu a marca de 70% de domínios protegidos contra 30% vulneráveis, uma variação positiva de 20 pontos percentuais e inferior à melhoria média da amostra geral (+30,61).

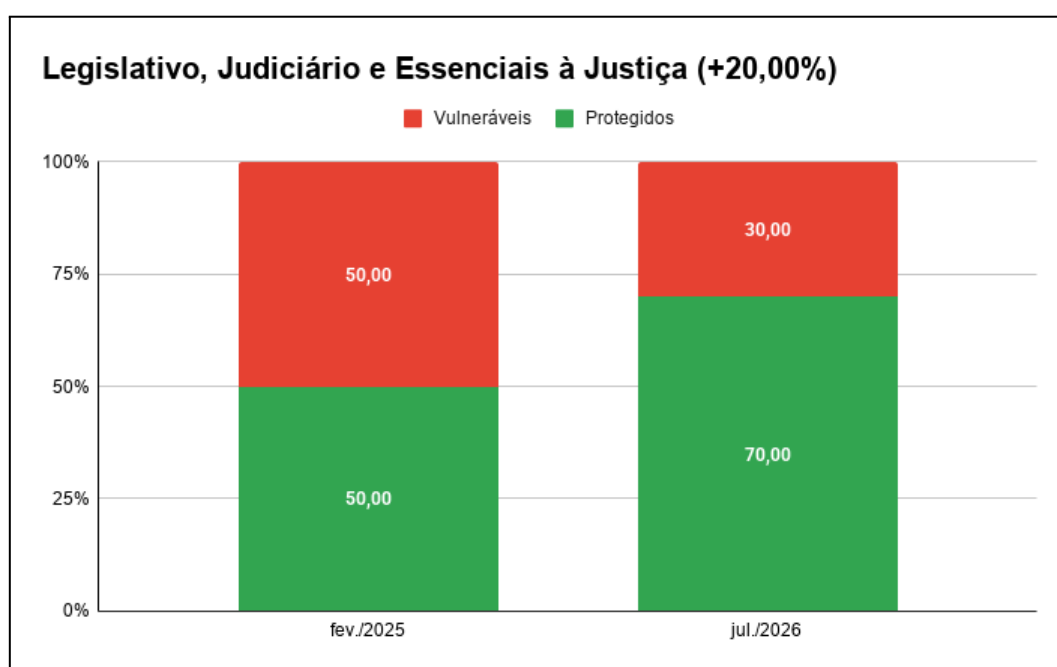


Gráfico A.20. Variação do estado de vulnerabilidade dos domínios do grupo “Legislativo, Judiciário e Essenciais à Justiça” no período analisado.

A.11. SAÚDE E SANEAMENTO

Composto por 12 órgãos, este agrupamento partiu de um patamar de vulnerabilidade de 75% em fevereiro de 2025, substancialmente superior aos 64,77% observados na amostra geral no mesmo período. Este grupo iniciou a pesquisa, portanto, em uma condição mais crítica do que a do conjunto agregado da APF, cenário que se reverteria ao longo do período observado. Os resultados podem ser verificados no Gráfico A.21 e na Tabela A.11.

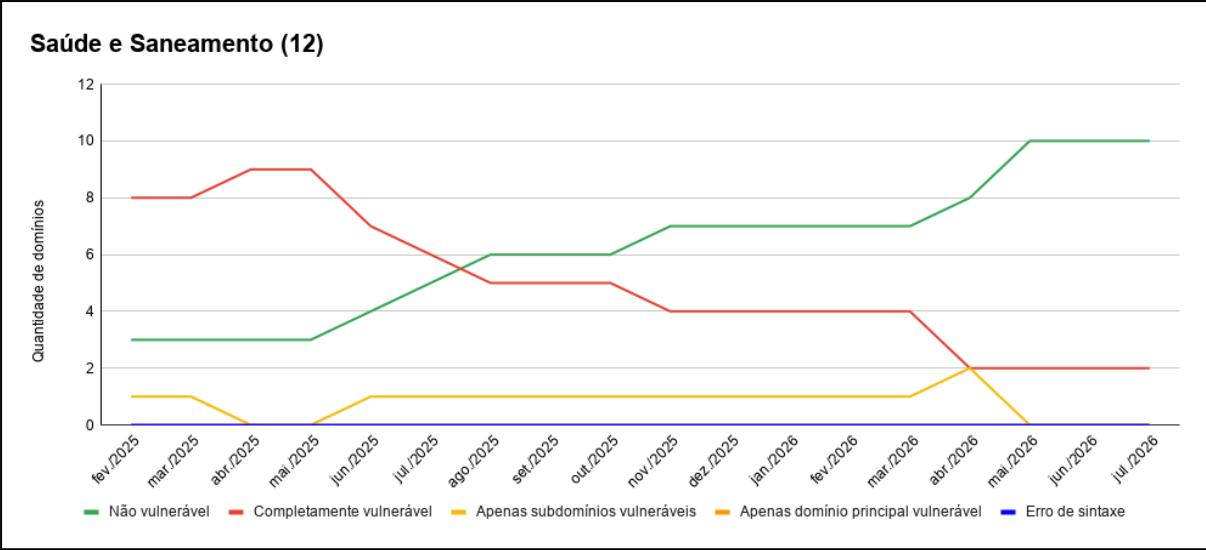


Gráfico A.21. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Saúde e Saneamento”.

Tabela A.11. Dados coletados referentes aos 12 domínios do grupo “Saúde e Saneamento”.

	Não Vulneráveis	Vulneráveis			
		Completamente Vulneráveis	Apenas Subdomínios	Apenas Domínio Principal	Erro de Sintaxe
fev./2025	3	8	1	0	0
mar./2025	3	8	1	0	0
abr./2025	3	9	0	0	0
mai./2025	3	9	0	0	0
jun./2025	4	7	1	0	0
jul./2025	5	6	1	0	0
ago./2025	6	5	1	0	0
set./2025	6	5	1	0	0
out./2025	6	5	1	0	0
nov./2025	7	4	1	0	0
dez./2025	7	4	1	0	0
jan./2026	7	4	1	0	0
fev./2026	7	4	1	0	0
mar./2026	7	4	1	0	0
abr./2026	8	2	2	0	0
mai./2026	10	2	0	0	0
jun./2026	10	2	0	0	0

jul./2026	10	2	0	0	0
-----------	----	---	---	---	---

Ao final do período, como se observa no Gráfico A.22, o grupo atingiu 83,33% de domínios protegidos contra 16,67% ainda vulneráveis, uma variação de 58,33 pontos percentuais positivos, resultado expressivamente superior à melhoria média da amostra geral (+30,61) e um dos maiores ganhos entre os agrupamentos temáticos. Esse desempenho decorre de uma trajetória de melhoria praticamente contínua ao longo de todo o período, com respostas identificáveis a quase todas as ações realizadas, o que configura um dos padrões de resposta mais consistentes e abrangentes do conjunto.

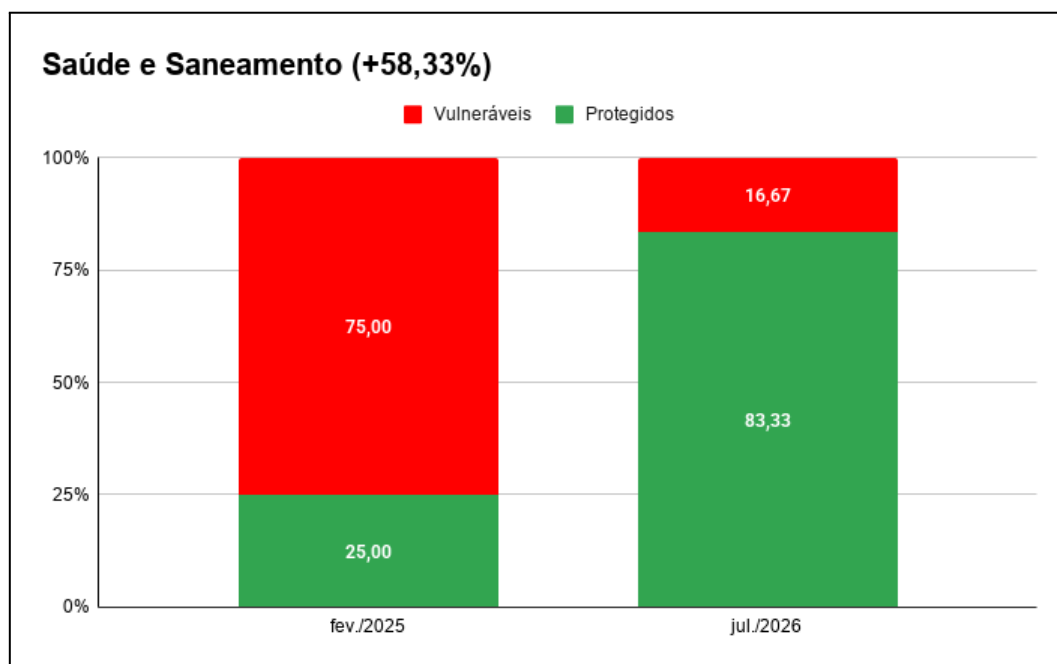


Gráfico A.22. Variação do estado de vulnerabilidade dos domínios do grupo “Saúde e Saneamento” no período analisado.

A.12. TRANSPORTE E URBANISMO

Composto por 24 órgãos, o grupo partiu de um patamar de vulnerabilidade de 58,33% em fevereiro de 2025, inferior aos 64,77% verificados na amostra geral. Assim, este segmento iniciou a pesquisa em condições relativamente mais favoráveis do que as do conjunto da APF. Os resultados podem ser verificados no Gráfico A.23 e na Tabela A.12.

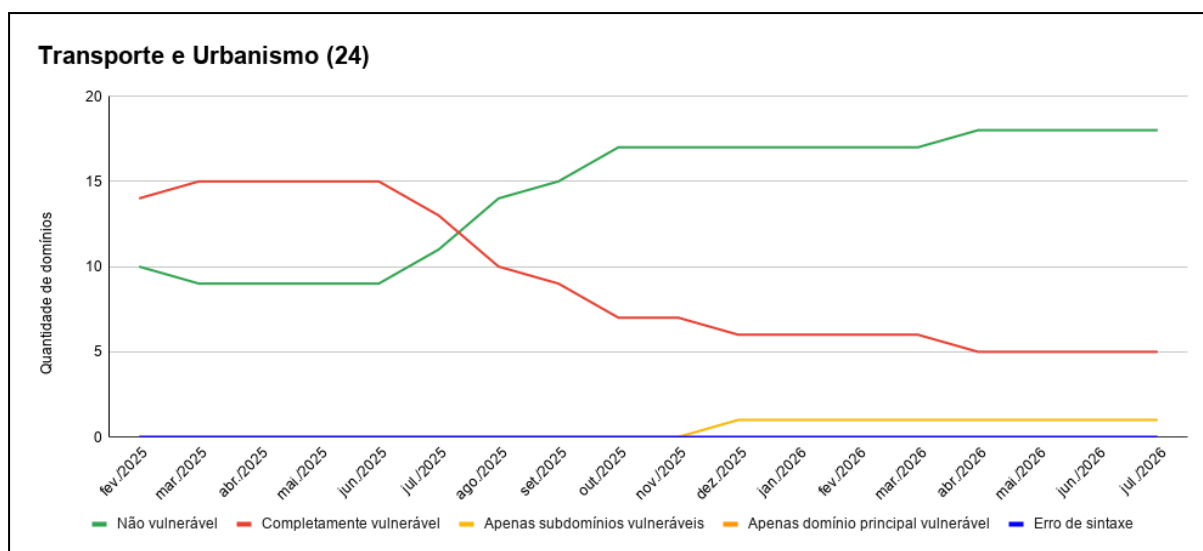


Gráfico A.23. Evolução da mitigação da vulnerabilidade ao longo da investigação nos domínios do segmento de “Transporte e Urbanismo”.

Tabela A.12. Dados coletados referentes aos 24 domínios do grupo “Transporte e Urbanismo”.

	Não Vulneráveis	Vulneráveis			
		Completamente Vulneráveis	Apenas Subdomínios	Apenas Domínio Principal	Erro de Sintaxe
fev./2025	10	14	0	0	0
mar./2025	9	15	0	0	0
abr./2025	9	15	0	0	0
mai./2025	9	15	0	0	0
jun./2025	9	15	0	0	0
jul./2025	11	13	0	0	0
ago./2025	14	10	0	0	0
set./2025	15	9	0	0	0
out./2025	17	7	0	0	0
nov./2025	17	7	0	0	0
dez./2025	17	6	1	0	0
jan./2026	17	6	1	0	0
fev./2026	17	6	1	0	0
mar./2026	17	6	1	0	0
abr./2026	18	5	1	0	0
mai./2026	18	5	1	0	0
jun./2026	18	5	1	0	0

jul./2026	18	5	1	0	0
-----------	----	---	---	---	---

Ao final do período, como se pode atestar por meio do Gráfico A.24, o agrupamento atingiu 75% de domínios protegidos, mantendo 25% vulneráveis, uma variação positiva de 33,33 pontos percentuais, resultado ligeiramente superior à melhoria média da amostra geral (+30,61). Persistiu, ao final do estudo, 1 domínio com apenas subdomínios vulneráveis, inalterado desde dezembro de 2025, reproduzindo, também neste segmento, o padrão de maior resistência às vulnerabilidades parciais.

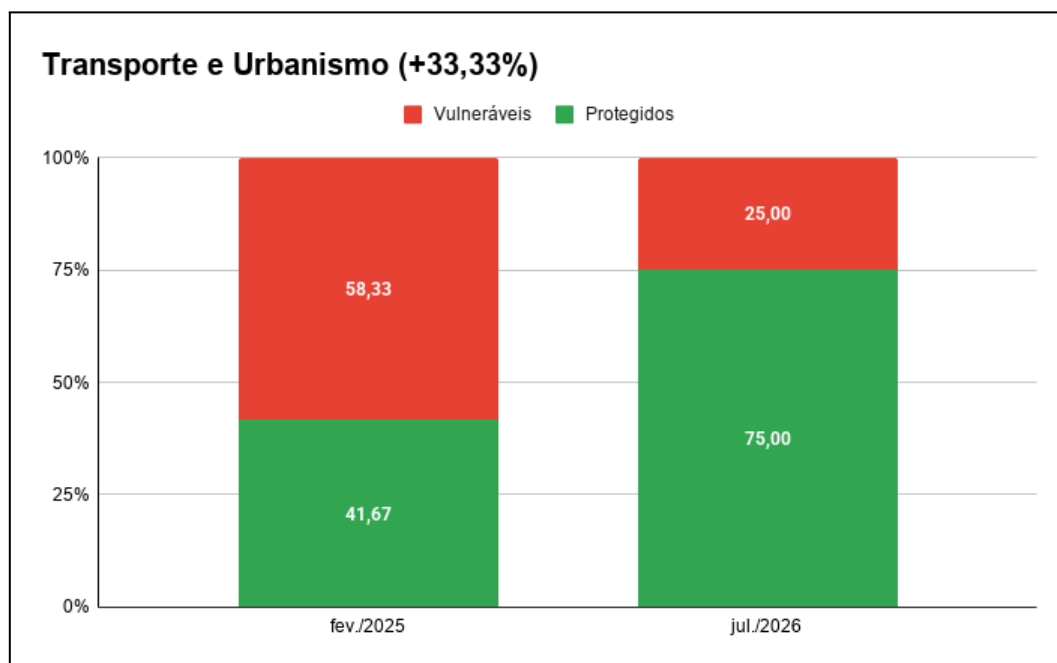


Gráfico A.24. Variação do estado de vulnerabilidade dos domínios do grupo “Transporte e Urbanismo” no período analisado.

B- RESPOSTAS RECEBIDAS A PARTIR DOS ALERTAS INDIVIDUAIS

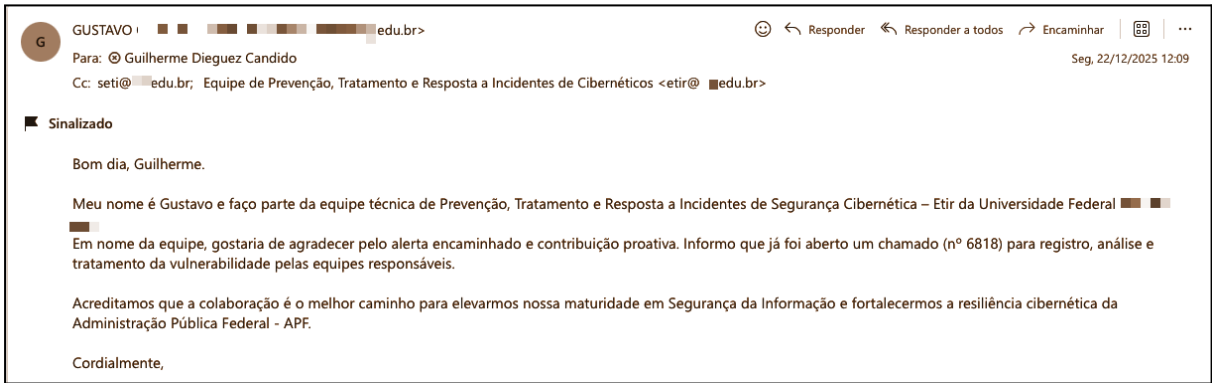


Figura B.1. Resposta de órgão da amostragem a um dos alertas individualizados

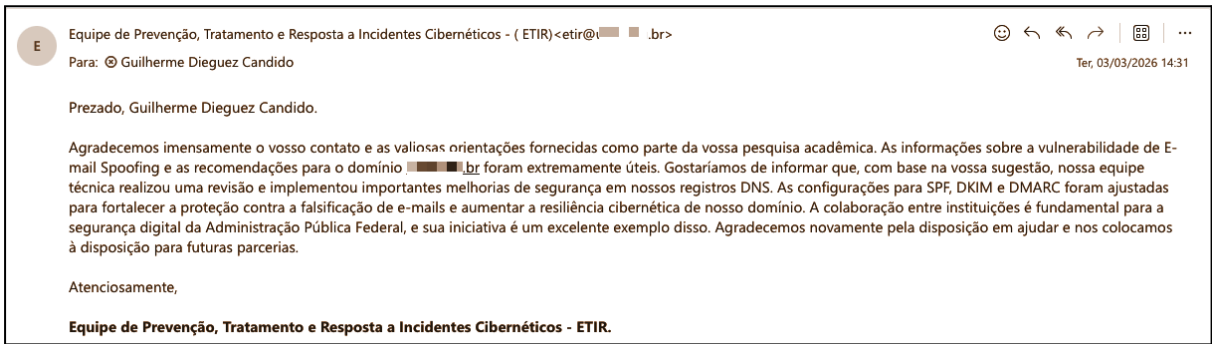


Figura B.2. Resposta de órgão da amostragem a um dos alertas individualizados

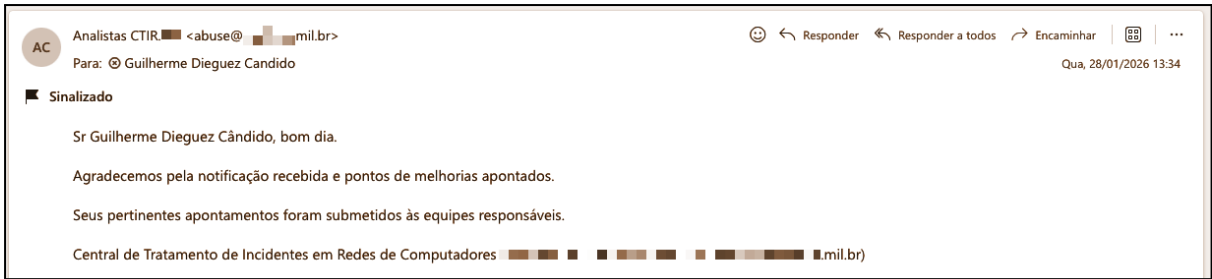


Figura B.3. Resposta de órgão da amostragem a um dos alertas individualizados

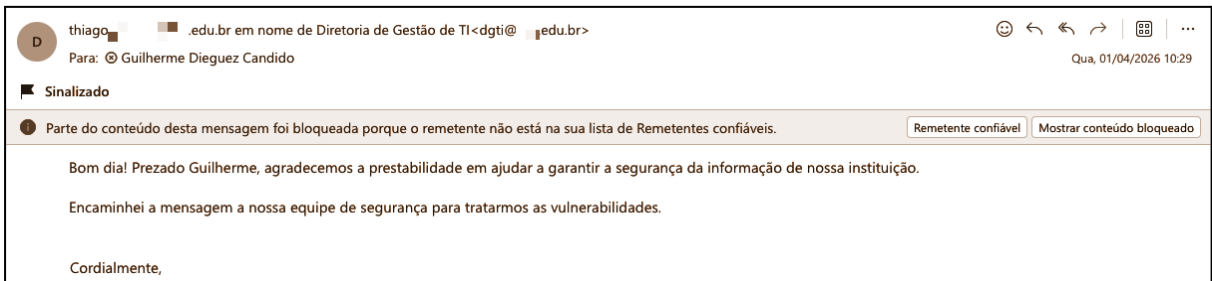


Figura B.4. Resposta de órgão da amostragem a um dos alertas individualizados.

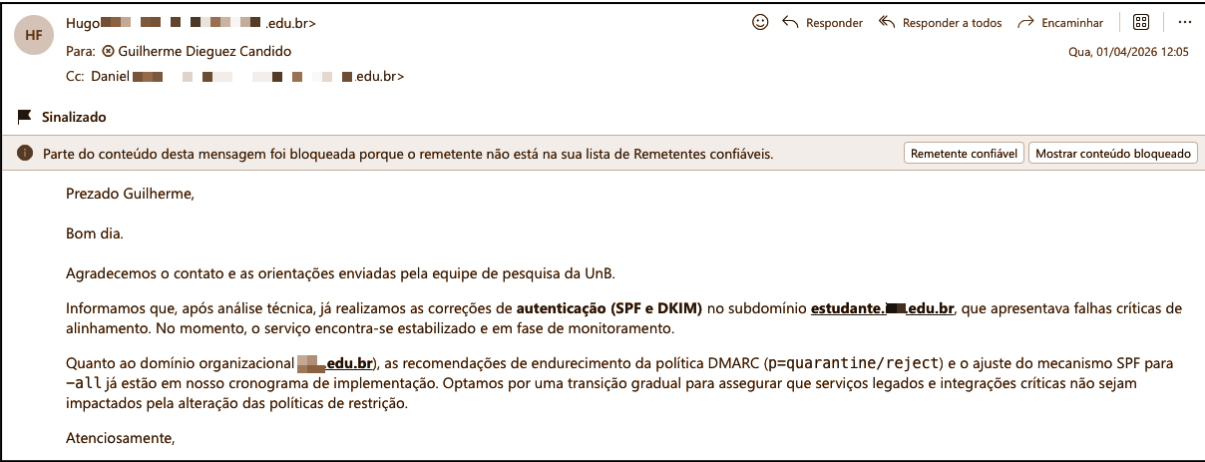


Figura B.5. Resposta de órgão da amostragem a um dos alertas individualizados

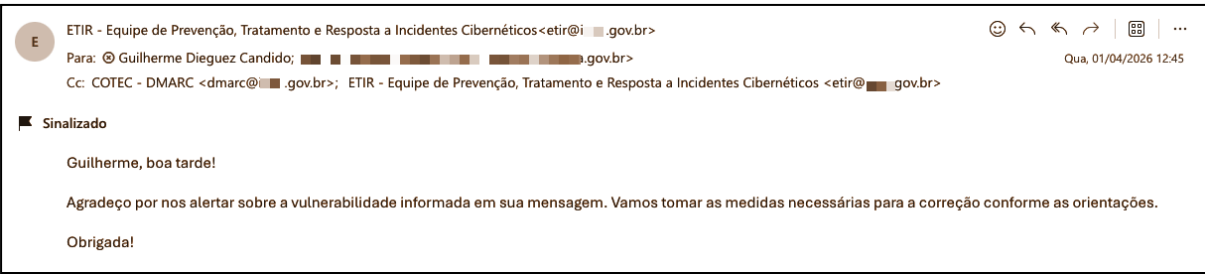


Figura B.6. Resposta de órgão da amostragem a um dos alertas individualizados

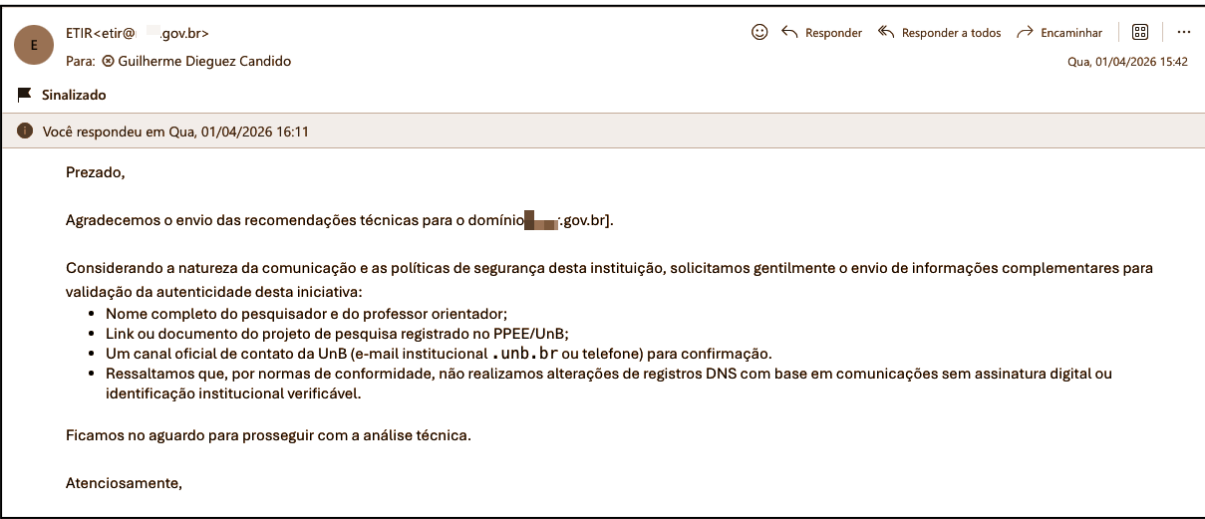


Figura B.7. Resposta de órgão da amostragem a um dos alertas individualizados

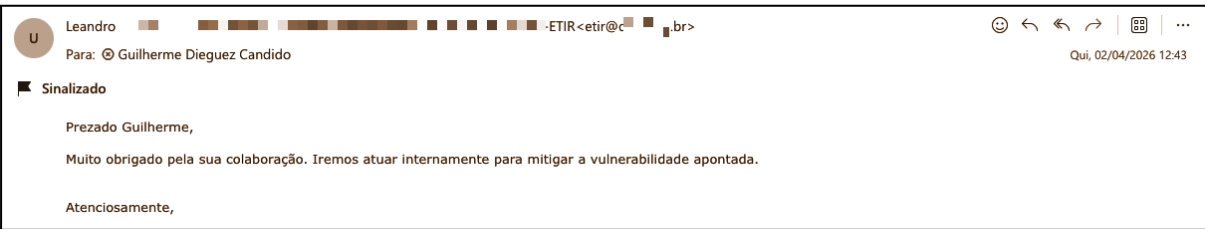


Figura B.8. Resposta de órgão da amostragem a um dos alertas individualizados

ANEXOS

A- CERTIFICADO DE REGISTRO DE SOFTWARE

		
		
	REPÚBLICA FEDERATIVA DO BRASIL	
	MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS	
	INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL	
	DIRETORIA DE PATENTES, PROGRAMAS DE COMPUTADOR E TOPOGRAFIAS DE CIRCUITOS	
	Certificado de Registro de Programa de Computador	
	Processo Nº: BR512025006327-0	
	<p>O Instituto Nacional da Propriedade Industrial expede o presente certificado de registro de programa de computador, válido por 50 anos a partir de 1º de janeiro subsequente à data de 01/01/2025, em conformidade com o §2º, art. 2º da Lei 9.609, de 19 de Fevereiro de 1998.</p>	
	Título: StopEmailSpoofing	
Data de publicação: 01/01/2025		
Data de criação: 01/01/2025		
Titular(es): FUNDAÇÃO UNIVERSIDADE DE BRASILIA		
Autor(es): RAFAEL RABELO NUNES; JOÃO SOUZA NETO; GUILHERME DIEGUEZ CANDIDO		
Linguagem: OUTROS		
Campo de aplicação: TC-04		
Tipo de programa: PD-01		
Algoritmo hash: SHA-256		
Resumo digital hash: 06C5F5999FC3DB90D2FB9F9E2B384E4497A753DF4238F41C45CFE493CF9BEECC		
Expedido em: 09/12/2025		
		
Aprovado por: ERICA GUIMARAES CORREA Chefe da DIPTO		

Figura C.1. Certificado de Registro de Programa de Computador no INPI