Os Desafios da Gestão na Implantação dos Testes de Vulnerabilidades Estáticos e Dinâmicos: Um Estudo de Caso da ANS

Luciene Pinheiro Capra	Universidade de Brasilia (UnB), Campus Darcy Ribeiro, Departamento de Engenharia Elétrica, CEP: 70910-900 - Brasilia - DF Brasil – **lucapra@hotmail.com**
Rafael Rabelo Nunes (Orientador)	Universidade de Brasilia (UnB), Campus Darcy Ribeiro, Departamento de Engenharia Elétrica, CEP: 70910-900 - Brasilia - DF Brasil - **rafaelrabelo@unb.br**

RESUMO

O avanço da transformação digital na administração pública tem ampliado a complexidade dos sistemas e a exposição das instituições a riscos cibernéticos. Nesse contexto, a gestão contínua de vulnerabilidades torna-se elemento estratégico da governança de segurança da informação, exigindo integração entre aspectos técnicos, organizacionais e contratuais. Este artigo tem como objetivo analisar os desafios de gestão na implantação de testes de vulnerabilidades estáticos (Static Application Security Testing – SAST) e dinâmicos (Dynamic Application Security Testing – DAST) no ciclo de desenvolvimento de sistemas de uma agência reguladora federal, a partir de um estudo de caso na Agência Nacional de Saúde Suplementar (ANS). A pesquisa utilizou abordagem qualitativa e descritiva, com base na observação participante realizada entre agosto de 2024 e outubro de 2025, analisando registros de reuniões, e-mails institucionais e anotações da equipe gestora responsável pela implantação dos testes. Os resultados evidenciam desafios agrupados em quatro dimensões: contratuais, metodológicas, humanas e institucionais. Entre os ajustes realizados destacam-se a criação da sprint de segurança, a readequação de indicadores de qualidade contratual, a adoção de estratégias de comunicação e escuta ativa para mitigar resistências e a formalização do aceite de risco em prazos não ajustáveis. Como contribuição, o estudo oferece um relato aplicado sobre a integração da segurança da informação ao ciclo de desenvolvimento de software em órgãos públicos, apresentando práticas gerenciais e institucionais que podem servir de referência para outras organizações que buscam fortalecer sua governança digital e resiliência cibernética.

Palavras-chave: cibersegurança governamental; gestão de risco em TI pública; gestão contínua de vulnerabilidades; DevSecOps.

ABSTRACT

The advancement of digital transformation in public administration has increased the complexity of systems and the exposure of institutions to cyber risks. In this context, continuous vulnerability management becomes a strategic element of information security governance, requiring integration between technical, organizational, and contractual aspects. This article aims to analyze the management challenges in implementing static (Static

Application Security Testing – SAST) and dynamic (Dynamic Application Security Testing – DAST) vulnerability tests in the system development cycle of a federal regulatory agency, based on a case study at the National Supplementary Health Agency (ANS). The research used a qualitative and descriptive approach, based on participant observation conducted between August 2024 and October 2025, analyzing meeting records, institutional emails, and notes from the management team responsible for implementing the tests. The results highlight challenges grouped into four dimensions: contractual, methodological, human, and institutional. Among the adjustments made, the following stand out: the creation of a security sprint, the readjustment of contractual quality indicators, the adoption of communication and active listening strategies to mitigate resistance, and the formalization of risk acceptance within non-adjustable deadlines. As a contribution, the study offers an applied account of the integration of information security into the software development cycle in public bodies, presenting managerial and institutional practices that can serve as a reference for other organizations seeking to strengthen their digital governance and cyber resilience.
Keywords: government cybersecurity; risk management in public IT; continuous vulnerability management; DevSecOps.

1 INTRODUÇÃO

O aumento da complexidade e sofisticação dos ciberataques requer uma abordagem proativa para a prevenção de incidentes de segurança (Garcia, 2023). Dentro dessa perspectiva preventiva, os testes de vulnerabilidades estáticos e dinâmicos se apresentam como instrumentos fundamentais, permitindo a detecção precoce de riscos, a redução da superfície de ataque e o fortalecimento da resiliência organizacional (Center for Internet Security, 2021). Entretanto, a implantação desses testes não se restringe a uma questão técnica: ela impõe desafios significativos à gestão, desde a governança dos processos até o engajamento das pessoas envolvidas e impactadas pelos novos procedimentos (Luz, 2011).

A insegurança cibernética constitui, hoje, um dos principais riscos aos quais pessoas e instituições estão expostas. A internet conecta indivíduos, governos e organizações em escala global, mas também amplia as oportunidades para exploração de vulnerabilidades e execução de ataques, independentemente de fronteiras geográficas. O Tribunal de Contas da União alertou, em relatório recente, que o aumento de incidentes de segurança da informação nos órgãos da administração pública federal ameaça a soberania digital nacional e compromete a prestação de serviços públicos essenciais (Brasil, 2024).

Em resposta a esse cenário, a Secretaria de Governo Digital (SGD) criou o Programa de Privacidade e Segurança da Informação (PPSI), baseado nos CIS Controls e nas melhores práticas internacionais. O programa define um conjunto de medidas voltadas à maturidade e à resiliência institucional, entre as quais se destaca a gestão contínua de vulnerabilidades — um processo estruturante que visa antecipar riscos e reduzir as oportunidades de ataque (Brasil, 2024a). Nesse contexto, os testes de vulnerabilidades, tanto estáticos (Static Application Security Testing – SAST) quanto dinâmicos (Dynamic Application Security Testing – DAST), constituem mecanismos essenciais para apontar vetores de ataque, identificar falhas e apoiar a implementação de medidas corretivas antes da entrada dos sistemas em ambiente produtivo (Center for Internet Security, 2021; Luz, 2011).

Apesar de sua relevância, a implantação de testes de vulnerabilidades na administração pública ainda enfrenta inúmeros obstáculos. Barreiras contratuais, limitações orçamentárias, resistências culturais e falta de patrocínio da alta gestão comprometem a integração da segurança ao ciclo de desenvolvimento de software. A partir dessa constatação, o problema de pesquisa que orienta este estudo consiste em compreender quais desafios de gestão emergem na implantação de testes de vulnerabilidades em órgãos públicos e de que forma podem ser superados.

Parte-se da hipótese de que o sucesso da implantação não depende apenas da escolha de ferramentas adequadas, mas sobretudo da capacidade de adaptação institucional, envolvendo ajustes na governança, nos contratos e nas práticas de trabalho, além do fortalecimento da cultura organizacional voltada à segurança. Presume-se que a atuação estratégica do gestor de segurança da informação, articulando diferentes áreas e promovendo o envolvimento da alta administração, é determinante para a sustentabilidade do processo.

O objetivo deste artigo é analisar os desafios de gestão na implantação de testes de vulnerabilidades estáticos e dinâmicos no ciclo de desenvolvimento de sistemas em um órgão público federal, a partir de um estudo de caso conduzido na Agência Nacional de Saúde Suplementar (ANS). O foco recai sobre a dimensão gerencial do processo, examinando as dificuldades enfrentadas, as soluções implementadas e as lições aprendidas ao longo da implantação.

A justificativa para este estudo reside na escassez de pesquisas aplicadas sobre a integração da segurança da informação ao desenvolvimento de sistemas em instituições públicas brasileiras. Embora existam marcos normativos e boas práticas amplamente reconhecidos, ainda são raros os relatos empíricos que documentam como esses referenciais são operacionalizados na prática e quais barreiras precisam ser superadas. Ao relatar a experiência de uma agência reguladora federal, este trabalho busca oferecer evidências concretas e subsídios metodológicos para gestores públicos interessados em elevar o nível de maturidade de suas organizações em segurança cibernética.

Este artigo está estruturado da seguinte forma: a Seção 2 apresenta o referencial teórico sobre cibersegurança na administração pública e sua integração ao ciclo de desenvolvimento de sistemas; a Seção 3 descreve a metodologia adotada, com destaque para o estudo de caso e os procedimentos de coleta e análise de dados; a Seção 4 discute os resultados obtidos, organizados nas dimensões contratuais, metodológicas, humanas e institucionais; e, por fim, a Seção 5 apresenta as conclusões, as limitações do estudo e as recomendações para pesquisas futuras.

2. REFERENCIAL TEÓRICO

Nesta seção serão apresentados conceitos necessários para se compreenda o trabalho. Primeiro explica-se o contexto da cibersegurança na administração pública federal; na sequência contextualiza-se a segurança da informação no ciclo de vida de desenvolvimento de sistemas, e finaliza-se apresentando os desafios de gestor de segurança da informação na administração pública federal.

2.1 – A cibersegurança na administração pública federal

A migração dos dados e processos para ambientes online, criou um terreno fértil para cibercriminosos promoverem vazamentos de informações, sequestro

de dados, ataques de negação de serviço, fraudes e manipulação de informações. A partir do reconhecimento desta nova realidade, instituições, incluindo as do setor público, passaram a investir tempo e dinheiro em tecnologias que aumentassem sua resiliência institucional (Cobos, 2024).

Na administração pública, a gestão de segurança da informação vem exigindo uma abordagem multidimensional, estruturada sob normas e boas práticas. A insegurança cibernética é apontada como um dos principais riscos globais para os próximos anos, com ameaças que incluem paralisia de serviços críticos, danos à imagem das instituições e à soberania digital do Estado brasileiro, dentre outros. O Brasil figura entre uma das maiores superfícies de ataque expostas do mundo, uma vez que possui mais 160 milhões de pessoas conectadas e centenas de milhões de dispositivos em uso (Brasil, 2024).

Os ataques as instituições públicas têm provocado a interrupção de serviços essenciais em órgãos públicos de todas as esferas, impactando a lisura dos processos, a credibilidade das instituições e o atendimento às políticas públicas (Brasil, 2024). Incidentes amplamente divulgados como a paralisação de emissão de carteiras de vacinação (2021) e o vazamento de dados do INSS (2024), materializam os riscos e efeitos danosos que este ciberataques provocam na vida de milhões de cidadãos (Cobos, 2024).

Os fatores de risco vão desde os baixos níveis de maturidade em segurança da informação, até o desconhecimento ou dificuldade na adoção de controles de referência internacional como o NIST ou o CIS CONTROL. Limitações orçamentárias e falta de patrocínio da alta gestão, também figuram entre os principais motivos que contribuem para a maioria dos incidentes reportados. Falhas humanas comportamentais e culturais, inocentes ou intencionais, são responsáveis por cerca de 74% das violações em ambiente digital (Alves et al, 2024).

A administração pública federal (APF) tem feito um grande esforço para aumentar o grau de maturidade e resiliência das instituições públicas participantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP). O Programa de Privacidade e Segurança da informação (PPSI), liderado pela Secretaria de Governo Digital (SGD) e que se baseia em normas e melhores práticas internacionais, é "um conjunto de projetos e processos de adequação nas áreas de privacidade e segurança da informação", conforme definição da Cartilha do Programa (Brasil, 2024a).

O programa é fundamentado sobre normas como a Lei Geral de Proteção de Dados (LGPD), a Instrução Normativa Nº 01/2020, do Gabinete de Segurança Institucional (SGI), que instituiu o Sistema de Gestão de Segurança da Informação (SGSI), a Política Nacional de Segurança da Informação (PNSI), e padrões internacionais, tais como os controles do Center for Internet Security (CIS), do National Institute of Standards and Technology (NIST), da International Standardization Organization/Eletrotechnical Commission (ISO/IEC) e da Associação Brasileira de Normas Técnicas (ABNT NBR) (Brasil, 2024b).

O foco principal do PPSI é garantir conformidade, integridade e continuidade do negócio, por meio de uma atuação clara e progressiva, preconizando a governança, a confiança institucional, o envolvimento da alta administração e a melhoria contínua dos níveis de maturidade e resiliência institucionais. E embora quase nenhum Órgão da APF tenha implementado a totalidade dos controles da PPSI, o programa representa uma política estruturante evolutiva para a APF em relação a governança, proteção e confiabilidade na gestão da informação e dados pessoais (Brasil, 2024a).

2.2 – O contexto da cibersegurança no desenvolvimento de sistemas

Todas as normas técnicas e boas práticas abordam a cibersegurança como parte fundamental da gestão de risco de informação. Garantir a disponibilidade, integridade e confidencialidade dos dados exige uma gestão de risco estruturada e abrangente, com a implementação de práticas sistemáticas de identificação, análise e mitigação de riscos, passando pela contínua avaliação de vulnerabilidades (ABNT, 2019).

A modernização dos sistemas é uma necessidade constante, e segundo o Guia do Framework do PPSI, a frequência de ciberataques revela a quantidade de vulnerabilidades encontradas em códigos, tornando a cibersegurança um ponto fundamental no ciclo de vida de desenvolvimento dos sistemas. Normas como ISO 27001/27002 e NIST salientam que medidas como gestão de vulnerabilidades, desenvolvimento seguro e inventário de componentes, e testes periódicos são fundamentais para reduzir a superfície de ataque das aplicações (Brasil, 2024b).

A integração dos controles da cibersegurança no ciclo de desenvolvimento de sistemas, conhecida como DevSecOps, implica em aplicar as práticas multidisciplinares em todas as etapas, orientado pelas normas internacionais e pelas exigências crescentes de resiliência operacional, conformidade e confiança do usuário (Center for Internet Security, 2021). É importante considerar ainda, uma abordagem estruturada para os sistemas críticos, chamados de as "Joias da Coroa", demandando a aplicação de controles mais rigorosos já na fase de desenvolvimento de sistemas (Silva et Al, 2025). Os testes de vulnerabilidades estáticos (Static Application Security Testing - SAST) e dinâmicos (Dynamic Application Security Testing – DAST), são recomendados pelas principais normas internacionais, como uma forma de minimizar a exposição a ataques e aumentar a conformidade reputacional dos sistemas (Brasil, 2024b).

Para um melhor entendimento, é importante explicar o que são os testes estáticos e dinâmicos, em que momento eles ocorrem e o que se espera com cada um. Nos testes SAST a intenção é avaliar o código fonte do sistema, em busca de falhas nas rotinas, tais como de SQL Injection e Cross-Site Scripting (XSS) (Garcia, 2023). Deve ser aplicado sempre que um código for escrito, alterado ou estiver para ser implantado em ambiente produtivo, podendo ser incorporado deste o início do desenvolvimento de qualquer aplicação, pois à medida que se integra a rotina dos desenvolvedores, reduz custos e retrabalho. O CIS Controls indica ainda que os testes SAST devem ser combinados com revisões manuais, a fim de detectar vulnerabilidades de lógica, que não são pegas por ferramentas (Center for Internet Security, 2021).

Já os testes dinâmicos (DAST) buscam falhas durante a execução da aplicação, simulando o comportamento de um atacante, com o foco de identificar falha de acesso, respostas indevidas ou comportamentos inesperados (Garcia, 2023). Segundo o Guia do Framework do PPSI, a aplicação dos testes deve ser feita na fase de homologação, repetida após correções de apontamentos críticos e, se for autorizado pela instituição, em ambiente produtivo. A análise das vulnerabilidades dos sistemas ganha robustez com o uso de ferramentas adequadas (Brasil, 2024b).

A literatura ressalta que investir em testes de vulnerabilidades previne perdas financeiras, vazamentos de informações e danos reputacionais, e deve ser encarada como uma exigência operacional e estratégica (Cobos, 2024). Além disso, é importante considerar que a combinação destes testes é

destacada pelas boas práticas e incentivada pelos arcabouços de referência, no que tange a gestão segura de software (Center for Internet Security, 2021).

2.3 – Os desafios de gestor de segurança da informação na APF

Garantir conformidade e proteção dos dados pessoais e sensíveis na administração pública é um desafio multidimensional para um gestor de segurança da informação. Questões institucionais, tecnológicas, financeiras, normativas e culturais são algumas das dimensões a serem trabalhadas quando se planeja a implementação de um processo de gestão de software (Brasil, 2024b).

Na dimensão institucional, o primeiro e maior desafio do gestor, muitas vezes, é engajar a alta gestão, para que haja patrocínio das políticas a serem implementadas. Embora a adesão do corpo diretivo seja primordial, a realidade é que a grande maioria não enxerga a área de tecnologia, e muito menos a segurança da informação, como uma prioridade estratégica (Brasil, 2024a).

A consolidação da governança, com estruturação de comitês formais, com integrantes que se interessem pelo debate e acompanhamento dos assuntos de tecnologia e segurança da informação é outra barreira a ser ultrapassada. A Cartilha do Programa de Privacidade e Segurança da Informação cita que é importante que a instituição tenha linhas claras de defesa, com delimitação de papéis, evitando que haja sobreposição de responsabilidades e conflitos de atribuições (Brasil, 2024a).

Essa mesma cartilha aponta que, na dimensão de conformidade, a instituição precisa ter agilidade e adaptabilidade para lidar com os desafios normativos, já que o tema é regido por leis, normas, boas práticas, arcabouços tecnológicos em constante evolução de prática e entendimento. Essa complexidade se estende pela prestação de contas, que carece de mão de obra especializada e sistemas robustos que possam monitorar e documentar todas as ações para fins de auditoria junto aos órgãos de controle (Brasil, 2024a).

O gestor de segurança precisa considerar ainda os desafios operacionais que abrangem falta de recursos humanos e orçamento. A insuficiência de profissionais especializados, alta rotatividade e dificuldade de retenção de talentos, se juntam a inadequabilidade do orçamento às necessidades de aquisição de ferramentas e contratação de serviços, além dos bloqueios e retenções financeiras que prejudicam o planejamento de contratações (Cobos, 2024).

Não se pode desvincular esses desafios operacionais, da dificuldade de acompanhar a evolução tecnológica, pois as restrições acima impactam diretamente as atualizações de sistemas, a promoção de segurança em ambientes complexos e com tecnologias emergentes. Além disso, a capacidade de resposta a incidentes também fica prejudicada pela falta de ferramental adequado para monitoramento e cruzamento de eventos, bem como de profissionais capacitados para atuarem, de forma eficaz, frente as suspeitas de incidentes (Alves, 2024).

E fechando, mas não esgotando, as dimensões de desafios de um gestor público, tem a questão cultural da instituição, que precisa considerar um processo de capacitação contínua dos usuários, garantindo que eles sejam mais uma barreira contra-ataques de fishing, ransoware e engenharia social (Brasil, 2024a). Um outro ponto de vista da questão cultural é o entendimento de que experiências externas precisam ser avaliadas e adequadas à estrutura e dinâmica organizacional. Forçar mudanças ou acelerar etapas de uma

implantação de gestão de software, por exemplo, por ser danoso ao projeto e até traumático, por isso o gestor de segurança da informação precisa ser estrategista e sistemático (Alves, 2024).

3. METODOLOGIA

Esta pesquisa possui natureza aplicada, pois busca gerar conhecimento direcionado à solução de um problema prático relacionado à implantação de testes de vulnerabilidades no contexto da administração pública, contribuindo para o aprimoramento de processos de gestão de segurança da informação (Gil, 2010).

Quanto aos objetivos, trata-se de um estudo descritivo, uma vez que procura detalhar fenômenos observados em um ambiente organizacional real, e exploratório, ao identificar fatores e condições que influenciam a adoção de práticas de segurança cibernética (Cervo; Bervian; Da Silva, 2007).

A abordagem é qualitativa, pois se preocupa em compreender a natureza dos processos, comportamentos e interações envolvidos, priorizando a interpretação dos significados em vez da quantificação dos dados (Minayo; Deslandes; Gomes, 2007). Essa escolha se justifica porque o fenômeno estudado envolve variáveis de difícil mensuração, como cultura organizacional, resistência à mudança e governança institucional.

Do ponto de vista dos procedimentos técnicos, optou-se por um estudo de caso, método apropriado para a investigação de fenômenos contemporâneos dentro de seu contexto real, especialmente quando as fronteiras entre o fenômeno e o contexto não estão claramente definidas (Yin, 2001). Essa escolha é reforçada por Bressan (2000), ao destacar que o estudo de caso é adequado a disciplinas voltadas à prática, como a engenharia e a administração, permitindo compreender situações complexas sob múltiplas dimensões.

A técnica de coleta de dados adotada foi a observação participante, combinada com análise documental. A observação foi conduzida pela gestora de segurança da informação responsável pela implantação, o que possibilitou registrar percepções diretas sobre o comportamento das equipes e os resultados das decisões de gestão. Os dados foram complementados por registros de reuniões, e-mails institucionais e anotações de campo, garantindo uma triangulação de fontes e maior robustez interpretativa.

A amostra é não probabilística e por conveniência, composta pelos membros da equipe de segurança da informação da Agência Nacional de Saúde Suplementar (ANS) — dois servidores efetivos e dois terceirizados — diretamente envolvidos na implantação dos testes de vulnerabilidades. O período de coleta de dados compreendeu agosto de 2024 a outubro de 2025, período em que o processo foi planejado, executado e avaliado.

4. RESULTADOS E DISCUSSÕES

A implantação dos testes de vulnerabilidades na Agência Nacional de Saúde Suplementar (ANS) foi conduzida de forma gradual e planejada, partindo da definição do ferramental e da modelagem contratual até a execução efetiva dos testes e a identificação das dificuldades encontradas ao longo do processo.

A etapa inicial consistiu em avaliar as alternativas de contratação disponíveis e as características técnicas das ferramentas de análise. Diante do pequeno número de servidores responsáveis pela gestão de segurança e da complexidade de gerenciar múltiplos contratos independentes, optou-se por um

modelo de contratação integrada, em que o serviço de Centro de Operações de Segurança (SOC) incluísse o ferramental necessário para a execução dos testes. O termo de referência da licitação definiu requisitos mínimos, como a capacidade de realizar análises de vulnerabilidade em tempo de desenvolvimento, gerar relatórios automáticos e permitir correções antes da homologação. No pregão eletrônico, a empresa vencedora ofertou a ferramenta Veracode, amplamente reconhecida por sua aderência às boas práticas de segurança da informação e conformidade com normas internacionais.

Concluída a contratação, iniciou-se a fase de capacitação das equipes de desenvolvimento, infraestrutura e segurança da informação. O treinamento foi conduzido pela empresa contratada, com o objetivo de nivelar conhecimentos e alinhar os fluxos de trabalho às novas exigências. Considerando a menor complexidade técnica e o caráter mais previsível dos testes sobre o código-fonte, optou-se por iniciar o processo pelos testes estáticos (SAST). Essa escolha permitiu maior controle sobre os resultados e reduziu a dependência de outras áreas.

Em um primeiro momento, o SOC realizava os testes e encaminhava relatórios detalhados às equipes de desenvolvimento, que realizavam as correções sob orientação da equipe de segurança. Com o amadurecimento do processo e o aumento da familiaridade dos profissionais com a ferramenta, as atividades foram gradualmente internalizadas, permanecendo sob a supervisão da área de governança de segurança da informação.

Na sequência, foi implantada a fase de testes dinâmicos (DAST), destinados a avaliar vulnerabilidades durante a execução das aplicações. Essa etapa revelou-se mais desafiadora, pois exigia interação entre diferentes equipes e níveis hierárquicos, uma vez que as correções de falhas frequentemente envolviam componentes sob responsabilidade de áreas distintas. Além disso, foi necessário redefinir critérios de criticidade e fluxos de tratamento de vulnerabilidades, bem como integrar as ações ao processo de gestão de riscos de TIC já existente na instituição.

Durante a execução do projeto, observou-se que, embora a ANS possuísse uma estrutura madura de governança e gestão de riscos, a introdução dos testes de vulnerabilidades implicou ajustes metodológicos, contratuais e culturais. As discussões sobre prazos, responsabilidades e prioridades evidenciaram que o sucesso da implantação dependia tanto da competência técnica quanto da coordenação entre as dimensões organizacionais e humanas.

A análise das anotações e registros de campo permitiu identificar e categorizar as principais dificuldades enfrentadas durante a implantação dos testes. Elas se distribuíram em quatro dimensões inter-relacionadas:

1. Fatores contratuais, relacionados aos impactos nos indicadores de qualidade e na conformidade com os prazos estabelecidos;
2. Fatores metodológicos, ligados à necessidade de adaptação dos fluxos e cronogramas de desenvolvimento;
3. Fatores humanos, associados à resistência inicial e à curva de aprendizado das equipes; e
4. Fatores institucionais, vinculados às restrições normativas e à pressão por cumprimento de prazos regulatórios.

Essas categorias sintetizam a complexidade do processo de implantação e orientam a análise dos resultados que serão apresentados a seguir, permitindo compreender de forma sistêmica como as dimensões se entrelaçam na efetiva incorporação dos testes de vulnerabilidades em uma instituição pública.

4.1. Fatores Contratuais

A análise dos registros observacionais revelou que um dos principais desafios enfrentados durante a implantação dos testes de vulnerabilidades na ANS esteve relacionado aos fatores contratuais. O contrato de desenvolvimento de sistemas vigente na instituição estabelece um conjunto de indicadores de qualidade que orientam a avaliação do desempenho das empresas contratadas. Esses indicadores — definidos no termo de referência — mensuram prazos, conformidade técnica e aderência às especificações, influenciando diretamente a aceitação das entregas e o cumprimento das metas contratuais.

A introdução dos testes dinâmicos (Dynamic Application Security Testing – DAST) impactou de maneira significativa tais indicadores. Por ocorrer em fases mais avançadas do ciclo de desenvolvimento, o DAST frequentemente identificava vulnerabilidades que exigiam retrabalho e correções fora do cronograma inicialmente previsto, o que, segundo a métrica contratual, poderia representar queda de desempenho e descumprimento de prazos. Em contraste, os testes estáticos (Static Application Security Testing – SAST) foram incorporados de forma mais harmônica, uma vez que suas verificações são realizadas sobre o código-fonte ainda em desenvolvimento, permitindo correções imediatas e minimizando o impacto nos prazos e nos indicadores de qualidade.

Para compatibilizar as exigências contratuais com os novos requisitos de segurança, a equipe de gestão promoveu uma série de ajustes procedimentais e operacionais. Definiu-se que apenas as vulnerabilidades classificadas como médias ou críticas seriam tratadas de maneira prioritária, evitando sobrecarga desnecessária das equipes e assegurando que o esforço técnico estivesse proporcional ao nível de risco. Paralelamente, foi criada uma etapa adicional no ciclo de desenvolvimento — a chamada sprint de segurança —, com duração de quinze dias, dedicada exclusivamente à correção das vulnerabilidades críticas antes da homologação e da entrada do sistema em ambiente produtivo.

Essa medida teve papel estratégico. Ao incorporar a sprint de segurança como parte oficial do processo de desenvolvimento, tornou-se possível corrigir as falhas críticas sem comprometer os prazos pactuados, mantendo a integridade dos indicadores contratuais. Já as vulnerabilidades de severidade média passaram a ser tratadas no período de garantia do sistema, normalmente de trinta dias após a entrega final, o que reduziu tensões entre as equipes técnicas e a área de fiscalização contratual. A adoção desse modelo mostrou-se eficaz para equilibrar segurança, cronograma e conformidade contratual, reduzindo os impactos administrativos e operacionais da implantação.

A experiência também evidenciou a relevância de alinhar os instrumentos contratuais aos objetivos estratégicos de segurança da informação. A previsibilidade de cláusulas que tratam de segurança — e que permitem a introdução de novas práticas e normativos durante a execução do contrato — mostrou-se essencial para garantir flexibilidade jurídica e aderência técnica às boas práticas internacionais. O fato de o termo de referência da ANS já prever a necessidade de observância de novos dispositivos legais e normativos relacionados à segurança da informação foi determinante para o êxito da adaptação, assegurando respaldo normativo às mudanças e reduzindo resistências por parte da contratada.

Essa constatação converge com as orientações presentes na Estrutura de Segurança Cibernética do NIST (CSF 2.0) e no Guia do Framework de Privacidade e Segurança da Informação (Brasil, 2024b), que recomendam a inclusão de

cláusulas contratuais específicas voltadas à segurança cibernética. Tais dispositivos devem possibilitar o aperfeiçoamento contínuo dos mecanismos de proteção, conforme evoluem os riscos, as ameaças e os marcos regulatórios.

Em síntese, os resultados demonstram que a efetiva implantação dos testes de vulnerabilidades depende não apenas da adoção de ferramentas e metodologias adequadas, mas também da maturidade contratual e institucional. A integração entre segurança da informação e gestão de contratos constitui um eixo estruturante da governança digital, permitindo que a inovação tecnológica avance de forma sustentável, com segurança e respaldo jurídico-administrativo.

4.2. Fatores Metodológicos

Além dos ajustes contratuais, a implantação dos testes de vulnerabilidades demandou revisões metodológicas significativas. O processo de desenvolvimento de sistemas da ANS adota uma abordagem híbrida, baseada em práticas ágeis como Scrum e Kanban, adaptadas à cultura organizacional e às exigências de rastreabilidade e controle típicas do setor público. A introdução dos testes estáticos (SAST) e dinâmicos (DAST) alterou a dinâmica dessas metodologias, exigindo reavaliação dos fluxos de trabalho, dos prazos e das interações entre as equipes.

Inicialmente, a execução dos testes provocou impactos diretos na metodologia estabelecida, sobretudo pela necessidade de inserir novas etapas no ciclo de desenvolvimento e de reordenar atividades de homologação e entrega. As vulnerabilidades identificadas durante as fases intermediárias passaram a demandar correções imediatas, o que afetava o planejamento das sprints e comprometia a previsibilidade das entregas. A solução adotada consistiu na integração das correções de vulnerabilidades médias e críticas dentro das releases subsequentes, de modo que o tratamento dos achados ocorresse de forma estruturada, sem desorganizar o fluxo de desenvolvimento. Essa adaptação garantiu que cada ciclo evolutivo do sistema incorporasse as melhorias de segurança de maneira incremental.

Outro ajuste importante foi a criação da “sprint de segurança”, posicionada antes da transição para o ambiente de produção. Essa etapa, já consolidada nas práticas internas, passou a concentrar a resolução das vulnerabilidades críticas detectadas nos testes DAST. Com isso, tornou-se possível eliminar falhas graves sem comprometer os prazos formais de entrega. As vulnerabilidades de severidade média, por sua vez, foram incluídas no período de garantia do sistema, permitindo que as equipes mantivessem o equilíbrio entre segurança e produtividade.

Essas alterações metodológicas também exigiram negociação intersetorial. As áreas de negócio, responsáveis pela divulgação dos novos sistemas desenvolvidos aos entes regulados, precisaram ajustar seus prazos e compreender o valor agregado das novas práticas de segurança. O diálogo contínuo e a apresentação de evidências sobre os ganhos obtidos — como a redução de falhas em produção e a melhoria da confiabilidade dos sistemas — foram determinantes para o aceite institucional das mudanças.

Do ponto de vista da governança, as modificações foram submetidas ao Comitê de Governança Digital, que validou as alterações no processo e conferiu legitimidade às adaptações propostas. O patrocínio da alta administração foi igualmente essencial para consolidar a nova metodologia e assegurar a permanência das práticas de segurança no ciclo de desenvolvimento.

Os resultados obtidos indicam que o alinhamento entre metodologia e segurança da informação é um fator crítico para o sucesso da integração de controles automatizados no desenvolvimento de software. Conforme apontam Franco e Santos (2013), o apoio institucional é decisivo para o avanço das ações de segurança da informação na administração pública federal. A experiência da ANS corrobora essa perspectiva, demonstrando que o comprometimento da alta gestão e a autonomia conferida à equipe de segurança foram determinantes para a consolidação do processo.

Em síntese, a adaptação metodológica evidenciou que a implantação de testes de vulnerabilidades não deve ser tratada como uma ação pontual, mas como um processo contínuo de aprimoramento organizacional. A incorporação dos princípios de segurança no ciclo de desenvolvimento demanda uma abordagem iterativa, sustentada por diálogo, patrocínio e flexibilidade institucional, garantindo que a proteção da informação seja internalizada como parte natural do processo de entrega de valor público.

4.3. Fatores humanos

A dimensão humana mostrou-se uma das mais sensíveis e determinantes para o êxito da implantação dos testes de vulnerabilidades na ANS. A força de trabalho responsável pelo desenvolvimento de sistemas é composta majoritariamente por profissionais terceirizados, o que cria um contexto de alta rotatividade, vínculos contratuais distintos e diferentes níveis de maturidade técnica. Essa característica estrutural impôs desafios adicionais à gestão da mudança e à consolidação das novas práticas de segurança.

Durante as etapas iniciais da implantação, observou-se resistência considerável por parte das equipes de desenvolvimento e infraestrutura. Embora todos os profissionais tenham sido submetidos a treinamentos sobre o uso da ferramenta e sobre os objetivos dos testes SAST e DAST, muitos demonstraram insatisfação com o aumento do retrabalho e com a percepção de que as novas exigências poderiam comprometer o ritmo das entregas. As críticas recaíam principalmente sobre a forma como os relatórios de vulnerabilidades eram apresentados, considerados, em alguns casos, excessivamente rigorosos e pouco adaptados à realidade dos projetos em andamento.

Diante desse cenário, a equipe gestora adotou uma abordagem humanizada e iterativa, baseada na escuta ativa e na valorização das contribuições dos profissionais. Foram promovidas reuniões específicas — algumas deliberadamente não gravadas — para que os desenvolvedores pudessem expressar livremente suas percepções e propor ajustes nos procedimentos. Essa prática teve um efeito psicológico positivo, reduzindo o sentimento de imposição e aumentando o senso de pertencimento dos envolvidos.

Além disso, implementaram-se ações de acompanhamento direto e de suporte contínuo pela equipe de segurança da informação, especialmente nos primeiros ciclos de execução dos testes. O diálogo constante entre o time de desenvolvimento e o provedor do serviço de segurança permitiu ajustar parâmetros da ferramenta, reinterpretar achados e calibrar expectativas quanto ao esforço necessário para correção das vulnerabilidades. A cada nova iteração, foram apresentados resultados concretos sobre a melhoria dos códigos e a redução do número de achados críticos, fortalecendo a confiança nas novas práticas.

Com o passar dos meses, esse processo de aprendizagem coletiva produziu efeitos perceptíveis: o nível de resistência diminuiu e as equipes passaram a incorporar espontaneamente os princípios de segurança em suas rotinas. O

foco migrou do cumprimento obrigatório das verificações para a preocupação genuína com a integridade dos sistemas desenvolvidos. A cultura de segurança, antes percebida como um entrave operacional, começou a se consolidar como parte integrante da qualidade das entregas.

Essa experiência confirma o que Paula e Oliveira-Castro (2021) destacam em seus estudos sobre o comportamento organizacional em políticas de segurança da informação: a eficácia de uma política depende menos de mecanismos sancionadores e mais da capacidade institucional de influenciar comportamentos por meio de conscientização, diálogo e reforço positivo. No caso da ANS, o tratamento respeitoso e participativo dos profissionais foi decisivo para transformar resistência em engajamento e para legitimar as mudanças implementadas.

Por fim, cabe ressaltar que a gestão de fatores humanos na segurança da informação vai além da capacitação técnica. Ela envolve a construção de uma cultura organizacional de confiança e corresponsabilidade, na qual os colaboradores compreendem que a adoção de práticas de segurança não é um obstáculo, mas um meio de proteger o trabalho coletivo e a missão institucional. Ao reconhecer o papel estratégico das pessoas como primeira linha de defesa, a ANS avançou não apenas na implantação técnica dos testes de vulnerabilidades, mas também na consolidação de uma postura organizacional orientada à segurança.

4.4. Fatores institucionais

Os fatores institucionais exerceram influência decisiva sobre a implantação dos testes de vulnerabilidades, especialmente em razão da estrutura organizacional da ANS e da natureza regulatória de suas atividades. A maior parte dos projetos de desenvolvimento de sistemas é demandada pelas áreas finalísticas, responsáveis por operacionalizar políticas públicas e implementar alterações normativas. Essas áreas são fortemente condicionadas por prazos legais e vacâncias regimentais, o que impõe cronogramas rígidos e, muitas vezes, pouco flexíveis para absorver ajustes decorrentes de novas exigências técnicas.

Nesse contexto, a introdução dos testes dinâmicos (DAST) representou uma mudança disruptiva na dinâmica institucional. A necessidade de reservar tempo para a execução dos testes e para as correções de vulnerabilidades críticas afetou diretamente os prazos de entrega estabelecidos em normativos e acordos de nível de serviço. Essa alteração gerou insatisfação entre gestores e demandantes, que, pressionados por prazos legais, manifestaram resistência à readequação do cronograma. A tensão entre a necessidade de conformidade normativa e a exigência de segurança evidenciou um dilema clássico da administração pública: conciliar eficiência operacional e proteção da informação em ambientes regulados por marcos rígidos.

Para lidar com essa situação, a equipe de segurança da informação promoveu um processo estruturado de sensibilização e negociação institucional. As alterações metodológicas foram apresentadas e validadas junto ao Comitê de Governança Digital, órgão responsável por deliberar sobre mudanças de maior impacto nos processos de tecnologia. Esse movimento buscou garantir legitimidade e transparência, fortalecendo o patrocínio da alta administração para as novas práticas.

Nos casos em que a readequação de prazos não foi aceita pelas áreas demandantes, instituiu-se um procedimento formal de aceite de risco. Por meio desse instrumento, os gestores responsáveis pelas áreas solicitantes passaram

a assumir expressamente os riscos decorrentes da não execução integral dos testes de segurança ou da impossibilidade de correção tempestiva das vulnerabilidades identificadas. Os riscos documentados passaram, então, a ser monitorados pelo Comitê de Gestão de Riscos e Conformidade, assegurando rastreabilidade e responsabilização institucional.

Essa prática representou um avanço significativo na governança de riscos da informação, ao integrar as decisões sobre segurança ao processo formal de gestão de riscos corporativos da instituição. O alinhamento entre as esferas técnica e estratégica consolidou o entendimento de que a segurança da informação não é uma responsabilidade isolada da área de tecnologia, mas um componente transversal da governança pública.

A experiência também reforça o que Nunes, Perini e Pinto (2021) argumentam sobre a centralidade do patrocínio da alta administração para a efetividade das políticas de segurança: quando a decisão sobre a assunção de riscos é compartilhada e institucionalmente reconhecida, aumenta-se a accountability e a adesão aos controles estabelecidos. No caso da ANS, a maturidade pré-existente em gestão de riscos — já consolidada na cultura organizacional — foi um fator facilitador para a aceitação e institucionalização desse novo processo.

Além disso, observou-se um efeito indireto e positivo: áreas demandantes passaram a realizar consultas prévias à equipe de tecnologia antes de propor alterações normativas que impactassem sistemas. Essa prática emergente indica um amadurecimento institucional no sentido de reconhecer o papel estratégico da tecnologia da informação como elemento estruturante da ação regulatória.

Em síntese, os resultados demonstram que a superação dos desafios institucionais dependeu da articulação entre liderança, governança e cultura organizacional. O envolvimento da alta administração, a formalização dos mecanismos de aceite de risco e o fortalecimento dos comitês de governança permitiram que a implantação dos testes de vulnerabilidades se transformasse não apenas em um ganho técnico, mas em um processo de aprendizado institucional e de aprimoramento da governança digital.

5. CONCLUSÃO

Este artigo teve como propósito analisar os desafios de gestão na implantação de testes de vulnerabilidades estáticos e dinâmicos no ciclo de desenvolvimento de sistemas de um órgão público federal, a partir de um estudo de caso realizado na Agência Nacional de Saúde Suplementar (ANS). A pesquisa, de caráter qualitativo e natureza aplicada, baseou-se na técnica de observação participante realizada entre agosto de 2024 e outubro de 2025, possibilitando o registro de experiências, percepções e resultados diretamente observados no ambiente institucional.

Os achados evidenciam que a implantação de testes de vulnerabilidades em órgãos públicos envolve desafios que extrapolam o campo técnico e se estendem às dimensões contratual, metodológica, humana e institucional. Cada uma dessas esferas demandou ações de adaptação e coordenação específicas: revisão de cláusulas e indicadores contratuais, adequação da metodologia de desenvolvimento, fortalecimento da comunicação e da escuta ativa das equipes e, sobretudo, o alinhamento estratégico com a alta administração. Tais aspectos revelam que o sucesso de iniciativas dessa natureza depende de integração entre governança, cultura organizacional e gestão de pessoas.

Os resultados permitem afirmar que a segurança da informação não pode ser tratada apenas como requisito tecnológico, mas como um processo organizacional que exige mudanças culturais e comportamentais. Estratégias de conscientização, transparência na comunicação e valorização da participação das equipes mostraram-se eficazes para reduzir resistências e consolidar práticas de segurança de forma sustentável. Da mesma forma, o empoderamento dos gestores institucionais quanto à tomada de decisão sobre os riscos a serem assumidos contribuiu para fortalecer a corresponsabilidade e a maturidade da gestão.

A principal contribuição deste estudo reside na sistematização de uma experiência prática de implantação de testes de vulnerabilidades em uma instituição pública, oferecendo subsídios empíricos que podem orientar outros gestores na integração da segurança ao ciclo de desenvolvimento de software. O relato fornece um panorama realista dos desafios e soluções aplicáveis, funcionando como um guia de referência para órgãos que buscam aprimorar sua governança digital e resiliência cibernética.

Reconhece-se, contudo, que a pesquisa apresenta limitações decorrentes de seu caráter assistêmico e do número reduzido de participantes observados. Ainda assim, a riqueza descritiva e a análise reflexiva contribuem para preencher uma lacuna na literatura, marcada pela escassez de estudos empíricos sobre a implantação prática de controles de segurança na administração pública.

Como perspectiva para trabalhos futuros, recomenda-se a realização de estudos comparativos em diferentes instituições públicas e privadas, com o objetivo de construir protocolos padronizados e replicáveis de implantação de testes de vulnerabilidades. Tais pesquisas podem fortalecer a base empírica e favorecer o desenvolvimento de modelos integrados de gestão de riscos e segurança da informação, adequados às especificidades do setor público brasileiro.

REFERÊNCIAS

ABNT. **ABNT ISO/IEC 27005:2019 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação**. Rio de Janeiro: ABNT, 2019.

ABNT. **ABNT ISO/IEC 31000:2018 - Gestão de riscos – Diretrizes**. Rio de Janeiro: ABNT, 2018.

ALVES, Ângela Rayne Nogueira *et al.* **Fator Humano Na Segurança Da Informação: Um Mapeamento Dos Comportamentos De Risco No Ambiente Digital**. v. 17, 2024.

ALVES, Renato Solimar; QUEIROZ, Carlos Eduardo Mancini; NUNES, Rafael Rabelo. Os Tribunais Têm Estrutura Para Gerenciar Riscos De Segurança Da Informação? Um estudo à luz das três linhas. **Revista CEJ**, n. Nº 86, p. 145–160, 2023.

ARAÚJO, Jotácia Estrela Barbosa *et al.* Percepção sobre educação ambiental e política dos 3R'S dos estudantes de escola pública no município de Pombal-PB. **Revista Brasileira de Gestão Ambiental**, v. 12, n. 3, p. 28–33, 2018.

BRASIL - SECRETARIA DE GOVERNO DIGITAL. **Cartilha do Programa de Privacidade e Segurança da Informação**. Brasília, 2024a. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/cartilha_ppsi.pdf

BRASIL - SECRETARIA DE GOVERNO DIGITAL. **Guia do Framework de Privacidade e Segurança da Informação**. Brasília, 2024b. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf

BRASIL - TRIBUNAL DE CONTAS DA UNIÃO. **Lista de Alto Risco da Administração Pública Federal**. Brasília: Tribunal de Contas da União, 2024. Disponível em: https://sites.tcu.gov.br/listadealtorisco/.

BRESSAN, Flávio. **O Método do Estudo de Caso**. v. 1, n. 1, 2000.

CENTER FOR INTERNET SECURITY. **CIS Critical Security Controls**, 2021. Disponível em: https://www.cisecurity.org/controls/v8-1

CERVO, Amado Luiz; BERVIAN, Pedro Alcino; DA SILVA, Roberto. **Metodologia Científica**. 6ª ed. São Paulo, Brasil: Pearson Prentice Hall, 2007.

COBOS, Estefania Vergara. **Cybersecurity Economics For Emerging Markets**. *[S.l.]*: Banco Mundial, 2024. Disponível em: www.worldbank.org.

FRANCO, Luisa Helena Santos; SANTOS, Carlos Denner. Fatores que Influenciam na Adoção de Práticas de Gestão de Segurança da Informação na Administração Pública Federal. 2013.

GARCIA, Osvaldo César Dias Dos Santos. **A importância do teste de penetração na avaliação das vulnerabilidades de uma plataforma Web**. Dissertação (Mestrado em Informática) — Lisboa - Portugal: Instituto Superior de Tecnologias Avançadas, 2023.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 5ª ed. São Paulo, Brasil: Atlas, 2010.

LUZ, HELDER JEFFERSON FERREIRA DA. **ANÁLISE DE VULNERABILIDADES EM JAVA WEB APPLICATIONS**. Dissertação (Curso de Bacharelado em Ciência da Computação) - Marília - São Paulo: Centro Universitário Eurípides de Marília, Fundação de Ensino "Eurípides Soares da Rocha", 2011.

MACHADO, Raphael; NASCIMENTO, Luiz. **Frameworks de Segurança: Uma Análise Comparativa entre CIS Controls, NIST CSF e ISO/IEC 27001**. Rio de Janeiro: Clavis Segurança da Informação, 2023.

MINAYO, Maria Cecília de Souza (org); DESLANDES, Suely Ferreira; GOMES, Romeu. **Pesquisa social: Teoria, método e criatividade**. 26ª ed. Petrópolis - RJ: Vozes, 2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **A Estrutura de Segurança Cibernética do NIST (CSF) 2.0.**, 2024. Disponível em: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=958049

NUNAN, Angelo Eduardo; FILHO, Mário José de Moraes Costa; LIMA, Adriana Almeida. Implantação da segurança na gestão da informação na administração pública: um estudo de caso no Tribunal de Contas do Estado do Amazonas. **Rev. Serv. Público**, n. Jan/mar, p. 109–130, 2016.

NUNES, Rafael Rabelo; PERINI, Marcela Teixeira Batista Sidrim; PINTO, Inácio Emiliano Melo Mourão. A gestão de riscos como instrumento para a aplicação efetiva do Princípio Constitucional da Eficiência. **Revista Brasileira de Políticas Públicas**, v. 11, n. 3, p. 259–281, 2021.

PAULA, Rafael Almeida de; OLIVEIRA-CASTRO, Jorge Mendes de. Análise Comportamental Das Políticas De Segurança Da Informação – Um Estudo De Caso. **Desafio Online**, v. 9, p. 27–46, 2021.

BRASIL. **Lei Nº 9.961 de 28 de janeiro de 2000.** Cria a Agência Nacional de Saúde Suplementar – ANS e dá outras providências. 2000. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9961.htm. Acesso em: 5 nov. 2025

SANTOS, Lígia Cássia M. C.; PRADO, Edmir Parada Vasques; CHAIM, Marcos Lordello. **Técnicas e ferramentas para detecção de vulnerabilidades em ambientes de desenvolvimento ágil de software.** 2020.

SILVA, Edvan Gomes da *et al.* Revisão Sistemática sobre Frameworks de Modelagem de Ameaças em Segurança Cibernética. **Revista Ibérica de Sistemas e Tecnologias de Informação**, n. N.º E77, p. 74–87, 2025.

SILVA, Edvan Gomes da *et al.* Tomada de Decisão em Segurança Cibernética: Modelo para Identificação de Joias da Coroa. **Revista Ibérica de Sistemas e Tecnologias de Informação**, p. 60–73, 2025.

TRIGOS, Maria Luciana; NUNO, Claudinei Di. O impacto de ações de conscientização na segurança da informação. **Revista Científica Multidisciplinar Núcleo do Conhecimento**, v. 03, n. 10, p. 46–72, 2021.

VIANNA, Eduardo Wallier; FERNANDES, Jorge Henrique Cabral. **O Gestor Da segurança Da informação No espaço cibernético Governamental: Grandes Desafios, Novos Perfis E Procedimentos.** v. 9, n. nº 1, p. 65, 2015.

YIN, Robert k. **Estudo de Caso - Planejamento e Métodos.** 2ª ed. Porto Alegre - RS - Brasil: Bookman, 2001.