



SENADO FEDERAL

Auditoria do Senado Federal
Coordenação de Auditoria de Tecnologia da Informação

RELATÓRIO DE AUDITORIA N. 01/2022 COAUDTI/AUDIT

Ação 5.1 PAInt/2022

Auditoria de Testes em Soluções de Informática Legislativa e Parlamentar

Brasília

2022





SENADO FEDERAL

Auditoria do Senado Federal
Coordenação de Auditoria de Tecnologia da Informação

COORDENAÇÃO DE AUDITORIA DE TI
COAUDTI

AUDITOR-GERAL	André Luis Soares da Paixão
COORDENADOR GERAL	David Amaral dos Santos Allan Del Cistia Mello
ASSESSOR TÉCNICO	Bruno Martins Borba
COORDENAÇÃO DE AUDITORIA DE TECNOLOGIA DE INFORMAÇÃO	Yuri Moraes Bezerra
COORDENAÇÃO DE AUDITORIA CONTÁBIL E FINANCEIRA	Juliana do Nascimento Leite
COORDENAÇÃO DE AUDITORIA DE CONTRATAÇÕES	Filipe Mesquita Botrel
COORDENAÇÃO DE AUDITORIA DE GESTÃO DE PESSOAS	João Vicente Da Rocha Pessoa





SENADO FEDERAL

Auditoria do Senado Federal
Coordenação de Auditoria de Tecnologia da Informação

Sumário Executivo

O objeto desta ação de auditoria são os Processos de gestão (planejamento, especificação, normatização, implementação e execução) de testes de software, ao longo do ciclo de vida, para soluções e sistemas de informação legislativos ou parlamentares do Senado Federal.

O objetivo¹ é avaliar em que medida o Senado estabelece gestão de testes de software nas soluções e sistemas de informação legislativos ou parlamentares.

Portanto, considerando:

- i)* Previsão estabelecida no PAInt 2022 aprovado pelo Primeiro-Secretário em 17/3/2022, publicado no BASF n.º 8246, de 21/3/2022 (Documento nº 00100.089342/2021-75);
- ii)* Dinâmica dos trabalhos, item 8, da Notificação de Início de auditoria (NIA), NUP 00100.005075.2022-72;
- iii)* Questões de Auditoria, item 5, do Plano Individual De Auditoria Nº 5.6/2021 – COAUDTI/AUDIT/SF, NUP 00100.137065/2021-14;
- iv)* Análise das respostas das Solicitações de Auditoria (SAs) formalizadas junto ao Prodasen;

identificou-se achados que podem, a critério da Administração, servir como subsídio para a indução e a aplicação de melhores práticas no que tange a disciplina de Testes de Software. Foram encontrados os achados a seguir:

¹ Ambos, objeto e objetivo são elementos da Notificação de Início de Auditoria (NIA) – NUP 00100.005075.2022-72.





SENADO FEDERAL

 Auditoria do Senado Federal
 Coordenação de Auditoria de Tecnologia da Informação

Código do Achado	Achado	Natureza do achado	Provável(is) causa(s)
5.2	Há mecanismos/sistemáticas definidas, mas não há evidência do emprego dos mesmos no Senado Federal.	Boas práticas	Não aplicação de mecanismos/sistemáticas de teste por parte das equipes de desenvolvedores.
5.3.1	Não foram encontradas evidências suficientes de estabelecimento de gestão de testes de software para soluções e sistemas de informação legislativos ou parlamentares.	Boas práticas	Falta de prioridade do tema diante de outras demandas da unidade auditada.
5.3.2	Não foram encontrados elementos suficientes que demonstrem emprego de gestão de testes de software para soluções e sistemas de informação legislativos ou parlamentares.	Boas práticas	Falta de prioridade do tema diante de outras demandas da unidade auditada.
5.4.1	Não foram encontrados elementos suficientes que demonstrem como a gestão dos mecanismos/sistemáticas de testes de software empregados pelo Senado Federal, contribuem para o aprimoramento das soluções e sistemas de informação legislativos ou parlamentares, quanto aos aspectos de funcionalidade (achado 5.4.1) , confiabilidade (achado 5.4.2) , usabilidade (achado 5.4.3) , eficiência (achado 5.4.4) , manutenibilidade (achado 5.4.5) e portabilidade (achado 5.4.6) .	Boas práticas	Falta de prioridade do tema diante de outras demandas da unidade auditada.
5.5.1	Necessidade de aprofundamento nas atribuições de responsabilidades pelas atividades de garantia da qualidade em nível de Coordenação, Chefia de Serviço e equipe de desenvolvimento.	Boas práticas	Falta de prioridade do tema diante de outras demandas da unidade auditada.
5.5.2	Não foram encontradas evidências de que mecanismos/sistemáticas adotadas permitem avaliação mediante critérios (achado 5.5.2) , armazenar resultados de avaliações (achado 5.5.3) e resultados de avaliações revisados periodicamente (achado 5.5.4) .	Boas práticas	Falta de prioridade do tema diante de outras demandas da unidade auditada.

Fonte: Matriz de Achados. Códigos dos mesmos segue numeração do documento original NUP 00100.0754722022-10

Conforme Art. 76, § 2º, item IX da *Subseção III - Da comunicação dos resultados da Auditoria*, presente no Manual de Normas Operacionais da Auditoria do Senado Federal (MANOP/SF), publicado no Ato do Auditor-Geral Nº 2 de 2020, julga-se oportuno salientar os achados positivos encontrados nesta Ação de Auditoria, quais sejam:

Código do Achado	Achados Positivos	Natureza do achado	Provável(is) causa(s)
5.1.1	Existência de disciplina de testes baseada no processo/metodologia OpenUP.	Achado positivo	Necessidade da unidade auditada em disponibilizar informações e aculturar sobre processo e



SENADO FEDERAL

Auditoria do Senado Federal Coordenação de Auditoria de Tecnologia da Informação

			metodologia de testes às equipes desenvolvedoras.
5.1.2	Existência de execução de processo de atividades de testes de software.	Achado positivo	Necessidade de execução de testes durante o ciclo de desenvolvimento de software e necessidade de registro para possível acompanhamento por parte da gestão.
5.6	Há preocupação com a disciplina de teste de software por parte da unidade auditada muito antecipadamente a esta ação de auditoria.	Achado positivo	Falta de apoio da alta administração com recursos humanos e com capacitação.
5.7	Há presença de projeto estruturante no PDTI que aborda a disciplina de teste de software.	Achado positivo	

Fonte: Matriz de Achados. Códigos dos mesmos segue numeração do documento original NUP 00100.0754722022-10

Com relação às recomendações, é mister fazer-se notar as orientações do coordenador da COAUDTI registradas por comunicação à equipe de auditoria em 30/06/2022 por correio eletrônico, intitulado “RES: Auditoria de testes - matriz de achados preliminar”:

- Aglutinar as recomendações com base nas “causas prováveis”, conforme preconiza o MANOP (art. 95, § 4º);
- Endereçar as recomendações de acordo com a responsabilidade atribuída no RASF ou em Atos internos que se relacionem com a consecução das demandas decorrentes da recomendação².

Portanto, as recomendações da ação de *Auditoria de Testes em Soluções de Informática Legislativa e Parlamentar* são:

Ao PRODASEN:

Estabelecer mecanismos de gestão de testes de software para soluções e sistemas de informação legislativos ou parlamentares, bem como certificar-se do emprego dos mecanismos/sistemáticas de testes de software junto às equipes de desenvolvimento³.

² e.g.: É de competência do CGTI e não do Prodasen coordenar a formulação de normas e estratégias de TI, inclusive quanto a testes e qualidade de software. Neste exemplo, a recomendação seria feita ao CGTI.

³ Base referencial: ABNT NBR ISO/IEC 14598-6 e ABNT NBR ISO/IEC 25001





SENADO FEDERAL

Auditoria do Senado Federal
Coordenação de Auditoria de Tecnologia da Informação

Ao CGTI:

- i) Definir política, diretriz, objetivo ou estratégia para “gestão de testes de software” com base em boas práticas de mercado, a exemplo da ISO ISO/IEC 14598-2, combinado com estudos e diagnósticos próprios, a exemplo do Relatório final do Grupo de Trabalho estabelecido pela Portaria da Diretora-Geral nº 6374, de 2019, conforme competência deste Comitê disposta no Art. 9º, inciso II do ATC nº 8, de 2016 que Institui a Política de Governança de Tecnologia da Informação do Senado Federal (PGTI/SF);
- ii) Avaliar a conveniência e a oportunidade de restabelecer plano de ação e recomendações exaradas pelo Grupo de Trabalho (GT) instituído pela PDG N° 6374⁴, de 2019, bem como envidar esforços para retomar Projeto estruturante “Melhoria dos Processos de Garantia da Qualidade de Produtos de Software”.

Ao ILB:

Prover as ações de capacitação relacionadas a “garantia da qualidade de produtos de software” priorizadas no Plano Diretor de TI, conforme competência deste órgão, disposta no art. 12 da Política de Capacitação e Desenvolvimento dos Servidores do Senado Federal, considerando serem ações de capacitação já priorizadas pelo Comitê de Governança de TI (CGTI), atendendo aos princípios (incisos II e III do art. 3º) e diretrizes (inciso I do art. 6º) da referida política.

⁴ Foi prorrogada pela Portaria da Diretora-Geral N° 7408 de 2019. Relatório final NUP 00100.132105/2019-17.





SENADO FEDERAL

Auditoria do Senado Federal
Coordenação de Auditoria de Tecnologia da Informação

Lista de Siglas

Sigla	Descrição
AUDIT	Auditoria do Senado Federal
CGTI	Comitê de Governança de TI
COAUDIT	Coordenação de Auditoria de TI
MA	Matriz de Achados
MP	Matriz de Planejamento
PAInt	Plano Anual de Auditoria Interna
GT	Grupo de trabalho
MANOP/SF	Manual de Normas Operacionais da Auditoria do Senado Federal
MAVP	Matriz de Achados Versão Preliminar
NIA	Notificação de Início de Auditoria
NUP	Número Único de Protocolo
PDG	Portaria do Diretor-Geral
RASF	Regulamento Administrativo do Senado Federal
SA	Solicitação de Auditoria
SF	Senado Federal
TCU	Tribunal de Contas da União





SENADO FEDERAL

Auditoria do Senado Federal
Coordenação de Auditoria de Tecnologia da Informação

Índice

1. Introdução	1
1.1 Importância do tema	1
1.2 Teste de software: a visão do TCU	2
2. Justificativa PAInt	4
3. Objeto	4
4. Objetivo	5
5. Objetivos específicos	5
6. Delimitações de escopo	6
7. Questões de auditoria	6
8. Metodologia	7
9. Alinhamento aos objetivos estratégicos	7
10. Achados de auditoria e manifestação da Unidade auditada	7
11. Aspectos positivos da gestão	15
12. Conclusão	17
13. Recomendações	18



1. Introdução

1.1 Importância do tema

Teste de software é controle de qualidade. O propósito é verificar se o produto corresponde às funcionalidades esperadas no desenvolvimento e às necessidades dos usuários. Envolve estratégias que remetem à escolha das condições de teste, parâmetros de teste, simulações de uso real e análise dos resultados obtidos conforme critérios preestabelecidos ligados aos objetivos organizacionais.

Na medida em que o emprego de Sistemas de Informação Digitais abrange, de maneira sistemática, a rotina de organizações públicas e privadas, crescem as pressões por desenvolvimento de software em curto espaço de tempo. Tempo e qualidade se encontram em relações inversas, ou seja, procura-se cada vez mais qualidade em softwares que devem ser desenvolvidos em cada vez menos tempo.

Este paradoxo parece ter levado ao surgimento de métodos ágeis de desenvolvimento e a modelos de qualidade de software com fundamentos trazidos pela engenharia de software. É o caso da NM ISO/IEC 9126-1:2008, que trata da qualidade de produtos de software e designa 6 atributos a serem avaliados: funcionalidade, confiabilidade, usabilidade, eficiência, manutenibilidade e portabilidade.

O setor público comunga com o privado em algumas preocupações afeitas às consequências do desenvolvimento de software que não atenda às expectativas de qualidade. Observa-se alguns exemplos práticos:

- Quais os danos à reputação ou à imagem de um Órgão Público caso um sistema de votação ou um portal de informações deixe de funcionar por falta de testes, incluindo nesta perspectiva os testes de segurança da informação?
- Quais os resultados ou custos legais caso um software possua falhas de conformidade com a Lei N° 13.709 (Lei Geral de Proteção de dados) ou com a Lei N° 12.527 (Lei de Acesso à Informação)?
- Qual o impacto de um erro de software que calcula a folha de pagamentos deste órgão?

Deixa-se claro que testar software não é uma atividade trivial. Exige conhecimentos, habilidades e infraestrutura e métodos específicos. Uma estratégia bem elaborada, ordenada e planejada



deve ser delineada para o provimento de tais insumos, sejam eles de ordem intelectual, financeira ou física.

No entanto, aportar recursos e tempo na estratégia de testes pode levar à grandes transformações e retorno ao negócio. Estudo⁵ recente da *Tricentis* com título “*How Investing in Testing Transformation Adds Business Value*” revela esforços das organizações em transformar práticas de teste de software em atividades contínuas para acelerar desenvolvimento de software e melhorar aspectos da qualidade do mesmo. Entre as cinco práticas adotadas estão:

- Implementação de testes contínuos para atender às demandas de frequência e urgência da organização;
- Alocação de orçamentos de teste adequados e foco na melhoria de habilidades;
- Integração dos analistas de testes às equipes multifuncionais de desenvolvimento;
- Não focar somente em agilidade, uma vez que pode impactar negativamente na experiência do usuário;
- Automação de testes funcionais durante todo o ciclo de desenvolvimento.

Por último, registra-se que **muitas das preocupações do corpo de governança de Órgãos públicos podem ser mitigadas**, direcionando empenho na estruturação da disciplina chamada *Teste de Software*.

1.2 Teste de software: a visão do TCU

Sob perspectiva sistêmica, o TCU, no que tange software, mesmo que contratado, compartilha o entendimento que este deve ser provido de documentação específica e evidências de que foram testados:

“No caso da contratação do serviço de desenvolvimento de um sistema de informação, a solução de TI pode englobar, entre outros elementos: os softwares do sistema, devidamente documentados e com evidências de que foram testados” (Guia de boas práticas em contratação de soluções de TI – Riscos e controles para o planejamento da contratação, p. 17).

⁵ Estudo completo pode ser acessado em <https://www.tricentis.com/resources/forrester-research-modernize-testing/>



“Que o planejamento de sistema preveja realização formal de homologação[...] das alterações implementadas no sistema[...] que realize adequadamente os testes e homologação do sistema, mantendo documentação dos procedimentos realizados” (Acórdão 914/2006-Plenário).

Também há preocupação do Órgão com testes relacionados à segurança dos softwares no que tange a proteção, segurança e integridade das informações. Fato é balizado pelo Acórdão 1768/2022 – PLENÁRIO, cujo tema é a avaliar a “*maturidade das organizações públicas federais quanto à implementação de controles críticos de segurança da informação e segurança cibernética*”. Portanto, é necessário que as organizações estejam atentas à gestão contínua de testes de vulnerabilidades, segundo o TCU.

Julga-se oportuno lembrar que o próprio texto constitucional de 1988, ao mesmo tempo em que proporciona maior relevância ao papel do TCU por meio do Art. 71, insta os poderes ao melhor controle de suas atividades com vistas a garantir melhor e mais eficiente aplicação dos recursos públicos.

Art. 74. Os Poderes Legislativo, Executivo e Judiciário manterão, de forma integrada, sistema de controle interno com a finalidade de: [...] II - comprovar a legalidade e **avaliar os resultados, quanto à eficácia e eficiência**, da gestão orçamentária, financeira e patrimonial (CF, 1988)

Neste aspecto relacionado à gestão de recursos públicos, fato também observado no art. 70 da Constituição Federal de 1988, faz-se referência a estudos⁶ que mostram que testes de software, em especial os automatizados, podem trazer mais rapidez na entrega de produtos e economizar orçamento na medida em que diminuem consideravelmente o tempo gasto para lançamento de produto de software.

Observando mais detidamente o aspecto orçamentário do desenvolvimento de software, um erro introduzido na fase de requerimento de software custará 5x mais para ser corrigido na fase de design, 10x mais na fase na fase de codificação, 50x mais na fase de teste, 130x mais na fase de integração e 368x mais na fase operacional⁷. Ou seja, descobrir um erro de software na fase

⁶ BATTINA, Dhaya Sindhu. Artificial Intelligence in Software Test Automation: A Systematic Literature Review. International Journal of Emerging Technologies and Innovative Research, p. 2349-5162, 2019.

⁷ LAZIC, Ljubomir; MASTORAKIS, Nikos. Cost Effective Software Test Metrics. WSEAS Transactions on Computers, 2008.



em que o sistema já está operacional e disponível para seus usuários é extremamente oneroso quando comparado com fases anteriores. Quando mais cedo a detecção, melhor.

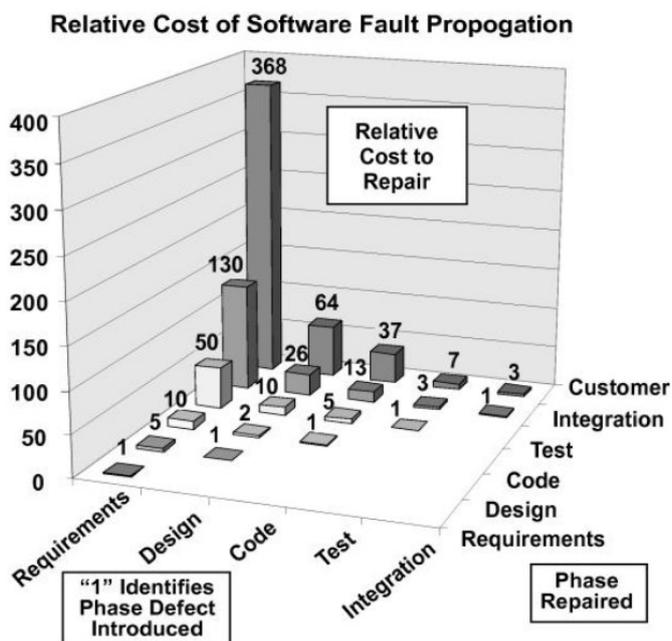


Fig. 10 Cost of Fixing a Defect [10]

Os estudos evidenciam a importância de código bem implementado, software documentado e, principalmente, testado.

Destarte, verifica-se que apoiar iniciativas relacionadas à disciplina de testes de software não só potencializa a qualidade do mesmo, mas, sobremaneira, induz a organização à economia junto ao Erário.

2. Justificativa PAInt

Não obstante a importância do tema registrada no item 1.1 no qual se registra a capacidade dos testes de software em mitigar preocupações do corpo de governança e também a referência às ações do TCU registradas no item 2.2, a própria gestão do Senado Federal se refere ao tema no Plano Anual de Auditoria Interna – PAInt, publicado no BASF Nº 8246, de 21/3/2022, NUP 00100.089342/2021-75.

Ao estabelecer e autorizar, para o exercício de 2022, as atividades e ações de controle que serão executadas pela Auditoria do Senado Federal – AUDIT, o PAInt estabelece a Ação de Controle objeto deste relatório com as seguintes justificativas, todas relacionadas a risco:

i) materialidade.

Definida como a importância relativa (ou significância) de um assunto dentro do contexto na qual é considerada. Além do valor monetário, a materialidade inclui questões de importância social e política, conformidade, transparência, governança e accountability⁸.

ii) tempo desde a última auditoria.

Até presente momento, nunca foi realizada auditoria com tal tema.

iii) qualidade e aderência dos controles internos.

Adere a controles internos mitigando falhas de software e proporcionando softwares com mais qualidade.

iv) relevância do objeto para o alcance dos objetivos estratégicos.

Relevante aos objetivos conforme associação apontada no item 9 deste relatório.

3. Objeto

Conforme apresentado no Sumário Executivo, o objeto desta ação de auditoria são os Processos de gestão (planejamento, especificação, normatização, implementação e execução) de testes de software, ao longo do ciclo de vida, para soluções e sistemas de informação legislativos ou parlamentares do Senado Federal.

4. Objetivo

Avaliar em que medida o Senado estabelece gestão de testes de software nas soluções e sistemas de informação legislativos ou parlamentares.

5. Objetivos específicos

- Verificar se o Senado Federal possui e executa política ou metodologia ou processo de testes de software;
- Identificar mecanismos e sistemáticas de testes de software empregados e que tenham como objetivo garantir: i. funcionalidade; ii. confiabilidade; iii. usabilidade; iv. eficiência; v. manutenibilidade; vi. portabilidade;
- Avaliar em que medida a gestão dos mecanismos e sistemáticas de testes de software empregados pelo Senado Federal, contribuem para

⁸ TCU. Manual de Auditoria Operacional. Brasília, 2020. 111 p. Anexo da Portaria-SEGECEX Núm. 18.



a qualidade das soluções e sistemas de informação legislativos ou parlamentares, quanto aos aspectos de: i. funcionalidade; ii. confiabilidade; iii. usabilidade; iv. eficiência; v. manutenibilidade; vi. portabilidade.

6. Delimitações de escopo

As análises desta ação de auditoria estão relacionadas às atividades ligadas aos processos de testes em soluções de informática legislativa e parlamentar realizados pela Secretaria de Tecnologia da Informação do Senado Federal – PRODASEN.

7. Questões de auditoria

Conforme Matriz de Planejamento (MP), NUP 00100.035725.2022-12, segue:

Código da questão	Questão de auditoria
5.1	O Senado Federal possui e executa política, processo ou metodologia de atividades de testes de software (*1)?
5.2	Quais são os mecanismos/sistemáticas de testes de software empregados pelo Senado Federal?
5.3	Em que medida o Senado Federal estabelece e emprega gestão de testes de software para soluções e sistemas de informação legislativos ou parlamentares?
5.4	Em que medida a gestão dos mecanismos e sistemáticas de testes de software empregados pelo Senado Federal, contribuem para o aprimoramento das soluções e sistemas de informação legislativos ou parlamentares, quanto aos aspectos de funcionalidade, confiabilidade, usabilidade, eficiência, manutenibilidade e portabilidade?
5.5	Os mecanismos / sistemáticas adotadas permitem estabelecer responsabilidades pelas atividades de garantia da qualidade, julgamentos de avaliação mediante critérios e resultados de avaliações organizados e revisados periodicamente no processo de avaliação da qualidade?

(*1) Conjunto de programas, procedimentos e documentação, desenvolvido para o atendimento de necessidades específicas do órgão ou entidade pública, assim como aqueles previamente desenvolvidos e disponíveis no mercado para a utilização na forma em que se encontram ou com modificações (IN 01 de 17 Jan. 20011 - Governo Federal).

(*2) Capacidade do produto de software de prover funções que atendam às necessidades explícitas e implícitas, quando o software estiver sendo utilizado sob condições especificadas.

(*3) Capacidade do produto de software de manter um nível de desempenho especificado, quando usado em condições especificadas.

(*4) Capacidade do produto de software de ser compreendido, aprendido, operado e atraente ao usuário, quando usado sob condições especificadas.

(*5) Capacidade do produto de software de apresentar desempenho apropriado, relativo à quantidade de recursos usados, sob condições especificadas.

(*6) Capacidade do produto de software de ser modificado. As modificações podem incluir correções, melhorias ou adaptações do software devido a mudanças no ambiente e nos seus requisitos ou especificações funcionais.

(*7) Capacidade do produto de software de ser transferido de um ambiente para outro.

8. Metodologia

Os seguintes procedimentos e técnicas foram empregados na ação de auditoria de Testes em Soluções de Informática Legislativa e Parlamentar:

- Indagação escrita;
- Análise documental;
- Correlação das informações obtidas com as questões de auditoria e achados;
- Revisão analítica;
- Apresentação da Matriz de Achados e relatório preliminar às unidades auditadas para análise e eventuais sugestões de modificações identificadas pelo auditado.

9. Alinhamento aos objetivos estratégicos

A presente auditoria alinha-se aos seguintes objetivos e diretrizes estratégicas do Senado Federal estabelecidos no Ato da Comissão Diretora N° 5, de 2015:

Aumentar a eficiência e a racionalidade no uso dos recursos públicos:

“Iniciativas que, direta ou indiretamente, tenham como consequência o **aumento da eficiência e da racionalidade devem ser valorizadas**. O alcance da eficiência será monitorado e avaliado com o auxílio de indicadores de gestão.” (ATC 5, 2015)

Melhorar de maneira contínua os processos de trabalho:

“**Os processos de trabalho devem estar definidos, mapeados e normatizados, bem como monitorados e avaliados de maneira periódica e contínua**. Deve ocorrer o fortalecimento e capacitação da gestão para que seja mais eficiente, econômica e sustentável.”

10. Achados de auditoria e manifestação da Unidade auditada

A manifestação da Unidade auditada está registrada na MAVP (Matriz de Achados Versão Preliminar) encaminhada pelo Coordenador-Geral do PRODASEN por e-mail e arquivada no drive interno da AUDIT.



Foram encontrados os seguintes achados à luz dos objetivos da ação, do seu escopo e da metodologia estabelecidos⁹:

Cód. 5.1.1 – Achado: Existência de uma disciplina de testes baseada no processo/metodologia OpenUP.

Natureza do achado: Achado positivo

Critério: ISO/IEC 14598-2: Avaliação de produto de software - Parte 2: Planejamento e gestão, capítulo 6: requisitos e recomendações para apoio à avaliação de software, seção 6.1: geral:

“A organização deve elaborar uma política e planos para todas as atividades de avaliação. Para todas as atividades de avaliação devem também ser definidas as responsabilidades da função de apoio.”

Efeitos ou possíveis consequências: Redução da assimetria informacional entre equipes de desenvolvimento, minimização de erros de sistemas e melhoria final na qualidade de software além de aderência aos controles internos.

Evidência: Evidenciou-se:

i) o OpenUP, que o inciso IV do artigo 14 do Normativo da Gestão do Ciclo de Vida de Produtos de Software (V 4.1) recomenda que "sempre que possível" seja aplicada.

<http://dsvp/docsist/sqqad/gestaodemand2/index.htm>

ii) a disciplina de teste de software em

http://dsvp/docsist/sqqad/gestaodemand2/openup/disciplines/test_FB85069.html?nodeId=f398aba8.

Manifestação da Unidade auditada: “Procede e serão adotadas medidas para atendimento no escopo de projeto de qualidade previsto no PDTI”.

Cód. 5.1.2 – Achado: Existência de execução de processo de atividades de testes de software.

Natureza do achado: Achado positivo

Critério: ISO/IEC 14598-2: Avaliação de produto de software - Parte 2: Planejamento e gestão, capítulo 3: características de qualidade aplicáveis:

“Os objetivos estabelecidos para qualidade **podem ser tanto orientados a produto quanto a processo** (por exemplo, confiabilidade ou

⁹ Conforme registrado na Matriz de Achados, NUP 00100.0754722022-10.



manutenibilidade como características de qualidade de produto; todos os testadores estão habituados ao uso de testes e foram treinados no uso de ferramentas de teste como meta de qualidade de processo).”

Efeitos ou possíveis consequências: Testes registrados e controlados para benchmark¹⁰ futuro. Melhoria contínua do processo de garantia de qualidade de software e aderência aos controles internos.

Evidência: Tela do Gertiq e arquivo “TestesJanMai22Colep.xlsx” enviado pela unidade auditada e que faz parte do conjunto de papéis de trabalho da auditoria.

Manifestação da Unidade auditada: “Procede e serão adotadas medidas para atendimento no escopo de projeto de qualidade previsto no PDTI”.

Cód. 5.2 – Achado: Há mecanismos/sistemáticas definidas, mas não há evidência do emprego dos mesmos no Senado Federal.

Natureza do achado: Boas práticas.

Critério: ABNT NBR ISO/IEC 14598-6: Avaliação de produto – Parte 6: Documentação de módulos de avaliação, Nota 2 item B.4.1(entrada para avaliação) e item B.6.3 (Instruções de avaliação):

“informação de produto inclui [...] relatório de teste[...] relatório de revisão de programa, relatório de verificação de programa.”

“Dados de falha são extraídos dos **relatórios de teste**. Caso os relatórios de teste não estejam disponíveis, executam-se os testes. [...] **Para cada falha, a localização e o momento da ocorrência são registrados.**”

Efeitos ou possíveis consequências: Potencial prejuízo de garantia de qualidade de software bem como da aderência aos controles internos.

Evidência: A documentação evidenciada não deixa claro se os mecanismos/sistemáticas são, de fato, empregados pelo Senado Federal

<http://dsvp/docsist/sqqad/gestaodemanpd2/index.htm> (OpenUP)

http://dsvp/docsist/sqqad/gestaodemanpd2/openup/disciplines/test_FB85069.html?nodeId=f398aba8 (teste de software)

<http://dsvp/docsist/sqqad/gestaodemanpd2/openup/tasks/eld=3555b3b5>

¹⁰ Avaliação padronizada, que proporciona comparação de sistemas ou componentes mediante critérios, para estabelecimento de melhores práticas dentro de um contexto específico.



(Testes do Desenvolvedor)

Manifestação da Unidade auditada: “Procede e serão adotadas medidas para atendimento após a conclusão do projeto de qualidade previsto no PDTI”.

Cód. 5.3.1 – Achado: Não foram encontradas evidências suficientes de estabelecimento de gestão de testes de software para soluções e sistemas de informação legislativos ou parlamentares.

Natureza do achado: Boas práticas.

Critério: Baseados no conceito de gestão utilizado desde a Notificação de Início de Auditoria, qual seja, o agregado das dimensões planejamento, especificação, normatização, implementação e execução:

i) ABNT NBR ISO/IEC 25001: Avaliação da qualidade de produto de software: planejamento e gestão, introdução:

Deve haver

“**Orientação e sugestões práticas** de alto nível para o uso de **normas** apropriadas para os diversos casos de aplicação[...]”

ii) NM ISO/IEC 9126-1: qualidade de produto: modelo de qualidade. A.1.2, métricas de qualidade como arcabouço para especificação, implementação e execução de testes de software:

“Convém que, no desenvolvimento de um produto de software, os produtos intermediários sejam avaliados **utilizando-se métricas** internas, as quais medem propriedades intrínsecas [...] O propósito básico destas métricas internas é assegurar que a qualidade externa e a qualidade em uso requeridas sejam alcançadas [...] Métricas internas oferecem a usuários, avaliadores, **executores de teste** e desenvolvedores os benefícios de poderem avaliar a qualidade do produto de software e considerar questões relativas à qualidade bem antes do produto de software tornar-se executável.”

Efeitos ou possíveis consequências: Possibilidade de não aderência aos controles internos de qualidade estabelecidos, uma vez que o foco do registro do teste parece estar mais na solução de falhas do que na administração, governança ou análise crítica dos mesmos em um processo mais amplo de gestão.

Evidência: Tíquete de teste:

<https://gertiq.senado.leg.br/redmine/issues/125512>



<https://gertiq.senado.leg.br/redmine/issues/125456>

<https://gertiq.senado.leg.br/redmine/issues/125454>

Tíquete de implementação relacionado:

<https://gertiq.senado.leg.br/redmine/issues/124786>

<https://gertiq.senado.leg.br/redmine/issues/123497>

<https://gertiq.senado.leg.br/redmine/issues/120606>

Manifestação da Unidade auditada: “Procede e serão adotadas medidas para atendimento após a conclusão do projeto de qualidade previsto no PDTI”.

Cód. 5.3.2 – Achado: Não foram encontrados elementos suficientes que demonstrem emprego de gestão de testes de software para soluções e sistemas de informação legislativos ou parlamentares.

Natureza do achado: Boas práticas.

Critério: Análogos aos apontados no achado código 5.3.1, uma vez que objeto é o mesmo, alterando-se apenas a relação. Em 5.3.2 busca-se evidencição do emprego de gestão de testes enquanto em 5.3.1 busca-se o estabelecimento da gestão de testes. Registra-se que não se emprega (5.3.2) algo que não está, previamente, estabelecido (5.3.1).

Efeitos ou possíveis consequências: Perda da qualidade do software ou alta taxa de erros por não emprego de gestão de teste, além de possível não conformidade aos controles internos.

Evidência: Unidade auditada informou não haver documentação de evidência.

Manifestação da Unidade auditada: “Procede e serão adotadas medidas para atendimento após a conclusão do projeto de qualidade previsto no PDTI”.

Cód. 5.4.1, 5.4.2, 5.4.3, 5.4.4, 5.4.5 e 5.4.6 – Achado: Não foram encontrados elementos suficientes que demonstrem como a gestão dos mecanismos/sistemáticas de testes de software empregados pelo Senado Federal, contribuem para o aprimoramento das soluções e sistemas de informação legislativos ou parlamentares, quanto aos aspectos de funcionalidade (5.4.1), confiabilidade (5.4.2), usabilidade (5.4.3), eficiência (5.4.4), manutenibilidade (5.4.5) e portabilidade (5.4.6).

Natureza do achado: Boas práticas.

Critério: NM ISO/IEC 9126-1: qualidade de produto: modelo de qualidade, item 6, modelo de qualidade para qualidade interna e externa, figura 4:



Efeitos ou possíveis consequências: Perda da qualidade de software em seus aspectos de **funcionalidade, confiabilidade, usabilidade, eficiência, manutenibilidade e portabilidade**, além de possível não aderência aos controles internos.

Evidência: Unidade auditada informou não haver documentação de evidência para qualquer das dimensões supracitadas.

Manifestação da Unidade auditada: Para as dimensões funcionalidade (5.4.1) e confiabilidade (5.4.2) a manifestação registrada é: “Procede e serão adotadas medidas para atendimento após a conclusão do projeto de qualidade previsto no PDTI”.

Para as demais dimensões a manifestação registrada é: “Procede, mas não há previsão de adoção de medidas para atendimento porque sua adoção requer um grau de maturidade maior em relação à disciplina de testes”.

Cód. 5.5.1 – Achado: Necessidade de aprofundamento nas atribuições de responsabilidades pelas atividades de garantia da qualidade em nível de Coordenação, Chefia de Serviço e equipe de desenvolvimento.

Natureza do achado: Boas práticas.

Critério:

i) No nível estratégico - ISO/IEC 14598-2: Avaliação de produto de software - Parte 2: Planejamento e gestão, capítulo 6: requisitos e recomendações para apoio à avaliação de software, seção 6.1: geral:

“A organização deve elaborar uma política e planos para todas as atividades de avaliação. **Para todas as atividades de avaliação devem também ser definidas as responsabilidades da função de apoio.**”

ii) No nível tático/operacional - ISO/IEC 14598-3: Avaliação de produto - Parte 3: Processo para desenvolvedores, item 6.4.1:

“O desenvolvedor deve especificar ações (procedimentos) para coleta de dados, a serem executadas para obter valores reais para cada métrica externa. **Isto inclui especificação de cronogramas, responsabilidades** e uso de ferramentas de coleta de dados e de análise. Se necessário treinamento especial, convém que isso também seja planejado.”



Efeitos ou possíveis consequências: Comprometimento das atividades de introdução, manutenção e melhoria contínua do processo de garantia da qualidade do software uma vez que os responsáveis não estão claramente definidos além de possível não aderência aos controles internos.

Evidência: Enviadas pela unidade auditada:

Arquitetura Java:

<https://portaldesenv.senado.leg.br/xwiki/bin/view/Arquitetura/ArquiteturaJava>

Ferramenta SonarQube:

<https://portaldesenv.senado.leg.br/xwiki/bin/view/SuporteDesenvolvimento/FerramentaSonar>

Solução de armazenamento e análise de logs:

<https://portaldesenv.senado.leg.br/xwiki/bin/view/SuporteDesenvolvimento/AgregadorLogs>

Ferramenta de monitoramento de aplicações:

<https://portaldesenv.senado.leg.br/xwiki/bin/view/Arquitetura/StatusMetricasAplicacao>

Manifestação da Unidade auditada: “Procede e serão adotadas medidas para atendimento após a conclusão do projeto de qualidade previsto no PDTI”.

Cód. 5.5.2, 5.5.3 e 5.5.4 – Achado: Não foram encontradas evidências de que mecanismos/sistemáticas adotadas permitem avaliação mediante critérios (5.5.2), armazenar resultados de avaliações (5.5.3) e resultados de avaliações revisados periodicamente (5.5.4).

Natureza do achado: Boas práticas.

Critério:

i) ISO/IEC 14598-3: Avaliação de produto – Parte 3: Processo para desenvolvedores, item 5.4 – atributos internos:

“Alguns atributos internos podem ser utilizados para monitorar tendências no desenvolvimento, quando eles são **medidos periodicamente** [...] Medidas de tendências são utilizadas para antecipar a identificação de problemas relacionados tanto com o produto quanto com o processo de desenvolvimento.”



ii) ABNT NBR ISO/IEC 25001: Avaliação da qualidade de produto de software: planejamento e gestão, introdução, item 6.4 – Análise e uso de resultados de avaliação:

“Após o processo de análise, os dados obtidos devem ser interpretados e apresentados a todas as partes envolvidas. **Os dados coletados também devem ser armazenados** para fins de referência para projetos futuros.”

Efeitos ou possíveis consequências: Perda da qualidade da avaliação de testes de software uma vez que não há evidenciação de: i) avaliação mediante critérios, ii) armazenamento de resultados de avaliações para uso futuro e iii) periodicidade na avaliação de resultados; além de possível não aderência aos controles internos.

Evidência: Unidade auditada informou não haver documentação de evidência.

Manifestação da Unidade auditada: “Procede, mas não há previsão de adoção de medidas para atendimento porque sua adoção requer um grau de maturidade maior em relação à disciplina de testes”.

Cód. 5.6 – Há preocupação com a disciplina de teste de software por parte da unidade auditada muito antecipadamente à esta ação de auditoria.

Natureza do achado: Achado positivo.

Critério: data documental. Evidenciados documentos associados ao tema com data retroativa ao início da auditoria.

Efeitos ou possíveis consequências: Perda da qualidade da avaliação de testes de software além de possível não aderência aos controles internos.

Evidência: Relatório final do Grupo de Trabalho sobre Aceite e Disponibilização de Aplicações Corporativas no Senado Federal – NUP 00100.132105/2019-17.

Manifestação da Unidade auditada: “Procede e foram propostas medidas para atendê-la e sua execução será iniciada quando houver disponibilidade de recursos humanos.”

Cód. 5.7 – Achado: Há presença de projeto estruturante no PDTI que aborda a disciplina de teste de software.

Natureza do achado: Achado Positivo.



Critério: registro do projeto ID 25 no PDTI.

Efeitos ou possíveis consequências: Perda da qualidade da avaliação de testes de software além de possível não aderência aos controles internos.

Evidência: Resposta às Solicitações de Auditoria enviadas pela unidade auditada, cujo trecho transcreve-se: “Este projeto encontra-se em estado de suspensão temporária em função de prioridades relacionadas à segurança das aplicações, que também é um aspecto de qualidade, que por diversos motivos se sobrepõe aos demais. Espera-se que brevemente seja possível retomar este projeto do PDTI no ritmo adequado.”

Manifestação da Unidade auditada: “Procede e foram propostas medidas para atendê-la e sua execução será iniciada quando houver disponibilidade de recursos humanos.”

11. Aspectos positivos da gestão

Este tópico destaca as boas práticas e ações positivas adotadas pela gestão no âmbito do objeto da ação de auditoria tema do relatório:

11.1 – Existência de disciplina de testes baseada no processo/metodologia OpenUP.

Corresponde ao achado 5.1.1 da Matriz de Achados NUP 00100.0754722022-10.

De fato, é positivo que o PRODASEN disponibilize documentação relativa à existência de processo ou metodologia de atividades de testes de software.

o Normativo da Gestão do Ciclo de Vida de Produtos de Software (V 4.1), disponibilizado oficialmente pelo PRODASEN à sua equipe de desenvolvimento como orientação, é evidência do Órgão na formalização da disciplina de teste de software. O item IV do Art. 14, foi verificado e traz atenção ao tema: “Deve-se executar sempre que possível a integração dos itens de software do produto, aplicando as técnicas de integração contínua e testes.”

O resultado esperado é a redução da assimetria informacional entre equipes de desenvolvimento, a minimização de erros de sistemas e a melhoria final na qualidade de software além de aderência aos controles internos.

11.2 – Existência de execução de processo de atividades de testes de software.

Corresponde ao achado 5.1.2 da Matriz de Achados NUP 00100.0754722022-10.



As evidências apontaram testes executados e registrados, que podem ser usados para benchmark futuro.

O Sistema Gertiq consigna a execução de processos de atividades de teste de software com registros cujos campos prenotam elementos úteis e auditáveis como título do tíquete, nº do tíquete, categoria, situação, responsáveis, datas de início e fim, unidade demandante e sistema testado.

O resultado esperado é a melhoria contínua do processo de garantia de qualidade de software, bem como a aderência aos controles internos.

- 11.3 – Há preocupação com a disciplina de teste de software por parte a unidade auditada muito antecipadamente a esta ação de auditoria.** Corresponde ao achado 5.6 da Matriz de Achados NUP 00100.0754722022-10.

Achado positivo externado pelo estudo feito pelo GT estabelecido pela Portaria da Diretora-Geral nº 6374, de 2019 na conclusão de seu relatório: “há, ainda, muitas oportunidades de evolução da disciplina de teste de software durante o ciclo de desenvolvimento de aplicações dentro do Senado Federal”.

O próprio GT, no bojo das recomendações exaradas sugere:

“Melhoria dos processos de garantia da qualidade de produtos de software: englobará as ações recomendadas referentes a gestão da qualidade e melhoria nos processos de teste. Pelo tamanho, sugere-se dividir em subprojetos ou fases.”

- 11.4 – Há presença de projeto estruturante no PDTI que aborda a disciplina de teste de software.** Corresponde ao achado 5.7 da Matriz de Achados NUP 00100.0754722022-10.

É positivo que PRODASEN e CGTI tenham um entendimento uníssono e já estejam corroborando com a relevância do tema, no entanto, cabe lembrar que o projeto se encontra sobrestado conforme apontado pela unidade auditada na resposta às Solicitações de Auditoria.

Com relação ao projeto estruturante informado, o TAP apresentado visa “implementar **melhorias ao longo de todo o processo de desenvolvimento e implantação de soluções de TI**, em especial as relacionadas a ações de garantia e controle da qualidade dos



produtos de software, de modo a **reduzir** a quantidade de defeitos e indisponibilidades das aplicações, **melhorando a percepção geral de qualidade dos produtos do Prodasen.**”

Como objetivos gerais se observa claramente a chamada de atividades conduzidas pela disciplina de teste de software, a saber:

“Reduzir a **quantidade de defeitos** observados nos produtos de software, tanto em homologação quanto em produção e **reduzir a ocorrência** e o impacto de **falhas** na implantação de soluções no ambiente de produção.”

Como objetivos específicos, faz-se notar efetiva a busca de elementos e sistemáticas de teste de software:

“**Evoluir as práticas de teste de software**, mascarar dados sensíveis em dsv e hmlm, flexibilizar autenticação para as operações de teste e homologação, criar modelo para **criação de cenários de teste predefinidos**, **capacitar desenvolvedores** em testes, implantar testes unitários e de aceitação em projetos de cada coordenação.”

12. Conclusão

A função precípua da Auditoria Interna é *“aumentar e proteger o valor organizacional, fornecendo avaliação, assessoria e conhecimento objetivos baseados em riscos”*¹¹.

À luz desta missão, cabe ratificar que o objetivo desta ação de auditoria foi avaliar em que medida o Senado estabelece gestão de testes de software nas soluções e sistemas de informação legislativos ou parlamentares.

Com base nos papéis de trabalho¹² e análises feitas, considera-se respondidas as questões de auditoria que iniciaram os estudos para a Ação ora em tela, quais sejam:

Questão 1: O Senado Federal possui e executa política ou metodologia ou processo de atividades de testes de software?

Questão 2: Quais são os mecanismos e sistemáticas de testes de software empregados pelo Senado Federal?

Questão 3: Em que medida o Senado Federal estabelece e emprega gestão de testes de software para soluções e sistemas de informação legislativos ou parlamentares?

¹¹ Instituto dos Auditores Internos do Brasil – IIA.

¹² Os papéis de trabalho representam o conjunto de documentos ou apontamentos, elaborados ou colhidos pelo auditor durante o processo de auditoria, contendo informações e provas, preparados de forma a fundamentar a sua opinião (PETER, M. G. A.; MACHADO, M. V. V. Manual de Auditoria Governamental. 2. ed. São Paulo: Editora Atlas, 2014. ISBN 978-85-224-9180-3.).



Questão 4: Em que medida a gestão dos mecanismos e sistemáticas de testes de software empregados pelo Senado Federal, contribuem para o aprimoramento das soluções e sistemas de informação legislativos ou parlamentares, quanto aos aspectos de: i. funcionalidade; ii. confiabilidade; iii. usabilidade; iv. eficiência; v. manutenibilidade; e vi. portabilidade?

Portanto, concluindo, esta AUDIT entende haver oportunidades de melhorias tanto na manutenção de práticas identificadas nos achados positivos quanto no aprimoramento de mecanismos identificados nas recomendações finais mencionadas no item 12 deste relatório.

13. Recomendações

Seguem as recomendações finais exaradas por esta AUDIT:

Ao PRODASEN:

- i) Estabelecer mecanismos de gestão de testes de software para soluções e sistemas de informação legislativos ou parlamentares, bem como certificar-se do emprego dos mecanismos/sistemáticas de testes de software junto às equipes de desenvolvimento¹³.

Ao CGTI:

- i) Definir política, diretriz, objetivo ou estratégia para “gestão de testes de software” com base em boas práticas de mercado, a exemplo da ISO ISO/IEC 14598-2, combinado com estudos e diagnósticos próprios, a exemplo do Relatório final do Grupo de Trabalho estabelecido pela Portaria da Diretora-Geral nº 6374, de 2019, conforme competência deste Comitê disposta no Art. 9º, inciso II do ATC nº 8, de 2016 que Institui a Política de Governança de Tecnologia da Informação do Senado Federal (PGTI/SF);
- ii) Avaliar a conveniência e a oportunidade de restabelecer plano de ação e recomendações exaradas pelo Grupo de Trabalho (GT) instituído pela PDG N° 6374¹⁴, de 2019, bem como envidar esforços para retomar Projeto estruturante “Melhoria dos Processos de Garantia da Qualidade de Produtos de Software”.

¹³ Base referência: ABNT NBR ISO/IEC 14598-6 e ABNT NBR ISO/IEC 25001

¹⁴ Foi prorrogada pela Portaria da Diretora-Geral N° 7408 de 2019. Relatório final NUP 00100.132105/2019-17.



Ao ILB:

Prover as ações de capacitação relacionadas a “garantia da qualidade de produtos de software” priorizadas no Plano Diretor de TI, conforme competência deste órgão, disposta no art. 12 da Política de Capacitação e Desenvolvimento dos Servidores do Senado Federal, considerando serem ações de capacitação já priorizadas pelo Comitê de Governança de TI (CGTI), atendendo aos princípios (incisos II e III do art. 3º) e diretrizes (inciso I do art. 6º) da referida política.

De acordo.

Encaminhem-se os autos ao Auditor-Geral, para ciência e análise.

COAUDTI, 20 de agosto de 2022

assinado digitalmente

Yuri Morais Bezerra - Coordenador

assinado digitalmente

André Ferrari de Aquino - Auditor-Líder

assinado digitalmente

Helio Marçola Junior - Auditor

assinado digitalmente

Marcelo Silva Cunha - Auditor

