ACO-UTR-157/2025

Processo	-	TC/015683/2019
Auditada	-	Secretaria Municipal de Gestão
Objeto	-	Auditoria Programada – Avaliar, sob a ótica da Segurança da Informação em aplicações web, a efetividade dos controles de segurança implementados na aplicação do Sistema Eletrônico de Informações

61ª Sessão Ordinária Não Presencial

AUDITORIA. SEGES. SEGURANÇA DA INFORMAÇÃO. SISTEMA ELETRÔNICO. 1. A utilização de um mesmo certificado curinga em inúmeros subdomínios é uma situação que poderá ocasionar diversas vulnerabilidades, entre as possíveis consequências está o comprometimento da segurança, não só da aplicação ora analisada, mas também, dos demais subdomínios vinculados ao domínio principal, neste caso, o domínio da PMSP (prefeitura.sp.gov.br). 2. O ambiente de teste, por não possuir recurso de captcha, se mostra vulnerável a riscos de acessos indevidos, de quebra de integridade de dados e da exposição de informações sensíveis provenientes de ataques de força bruta ao sistema SEI. 3. Vulnerabilidade de arquivos SVG e de arquivos executáveis em ZIP na versão 4.0. CONHECIDA. RECOMENDAÇÃO. 1. Observar as irregularidades apontadas, evitando-as em procedimentos de controles de segurança futuros. Votação unânime.

A C Ó R D Ã O

Vistos e relatados estes autos, dos quais é Relator o Conselheiro EDUARDO TUMA.

ACORDAM os Conselheiros do Tribunal de Contas do Município de São Paulo, à unanimidade, de conformidade com o relatório e voto do Relator, em conhecer da Auditoria Programada, para fins de registro, tendo em vista que foi alcançada a finalidade ao apontar desacertos nos controles de segurança implementados na aplicação Sistema Eletrônico de Informações (SEI), utilizado pela Prefeitura Municipal de São Paulo (PMSP), sob a gestão da Secretaria Municipal de Gestão.

ACORDAM, à unanimidade, em determinar a emissão de ofício à Secretaria Municipal de Gestão, para que conheça do presente Acórdão, assim como dos apontamentos formulados no Relatório de Auditoria Programada, apresentado pela Secretaria de Controle Externo – SCE (peça 14), com a recomendação de observar as irregularidades apontadas, evitando-as em procedimentos de controles de segurança futuros.

ACORDAM, à unanimidade, em determinar, após o cumprimento das formalidades legais, o arquivamento dos autos.

Participaram do julgamento os Conselheiros RICARDO TORRES – Revisor, DOMINGOS DISSEI e JOÃO ANTONIO.

São Paulo, 18 de dezembro 2024.

ROBERTO BRAGUIM – Vice-Presidente no exercício da Presidência
EDUARDO TUMA– Relator

/affo

Assinado digitalmente por ROBERTO TANZI BRAGUIM
Data: 26/03/2025 16:32:14 -03:00
Signature powered by e-TCM Tribunal de Contas do Município de São Paulo

Assinado digitalmente por EDUARDO TUMA
Data: 26/03/2025 17:03:28 -03:00
Signature powered by e-TCM Tribunal de Contas do Município de São Paulo

61ª SESSÃO ORDINÁRIA NÃO PRESENCIAL
Item 92 – Pleno

TC 15.683/2019 – Auditoria Programada
Objeto: avaliar sob a ótica da Segurança da Informação em aplicações Web a efetividade dos controles de segurança implementados na aplicação Sistema Eletrônico de Informações (SEI)
Interessados: Secretaria Municipal de Gestão- Seges
Relator: Conselheiro Eduardo Tuma
Competência: Pleno

RELATÓRIO

Trata-se de Auditoria Programada com o objetivo de avaliar sob a ótica da Segurança da Informação em aplicações Web a efetividade dos controles de segurança implementados na aplicação Sistema Eletrônico de Informações (SEI), utilizado pela Prefeitura Municipal de São Paulo (PMSP), sob a gestão da Secretaria Municipal de Gestão-Seges, disponível no sítio da internet no endereço https://sei.prefeitura.sp.gov.br.

A **Secretaria de Controle Externo – SCE** apresentou seu Relatório de Auditoria Programada, no qual, após informações obtidas, identificou em conclusão cinco vulnerabilidades sobre o Sistema Eletrônico de Informações (SEI) (peça 14 - 28.09.20):

> **3.1. Introdução**
>
> O Sistema Eletrônico de Informações (SEI), localizado no endereço eletrônico https://sei.prefeitura.sp.gov.br, é um sistema de gestão de processos e documentos eletrônicos, desenvolvido pelo Tribunal Regional Federal da 4ª Região (TRF-4), que engloba diversos módulos e funcionalidades, a fim de promover a eficiência da administração pública em diferentes esferas (peça 7).
>
> A PMSP assinou um acordo de cooperação técnica com o Tribunal Regional Federal da 4ª Região para uso do SEI em 01.12.2014.
>
> Atualmente, o SEI é utilizado em diversos órgãos nacionais, como os Tribunais Federais da 1ª, 3ª e 4ª regiões, o Conselho Administrativo de Defesa Econômica (Cade), a Defensoria Pública da União (DPU), o Tribunal de Justiça Militar do Estado de São Paulo (TJMSP), o Ministério das Comunicações (MC) e o Ministério da Economia (ME), entre outros. É o sistema escolhido para o projeto do Processo Eletrônico Nacional (PEN), do qual a PMSP também participa.
>
> (...)
>
> **4. CONCLUSÕES**

> À vista dos testes e análises realizadas no Sistema Eletrônico de Informações – SEI, a auditoria chegou aos seguintes apontamentos referentes à segurança da informação em aplicações *web*:
>
> **4.1.** A SG deve apresentar a análise e a avaliação de riscos que embasaram tecnicamente a adoção da solução criptográfica por meio de Wildcard Certificate ou Certificados Curingas, assim como, deve apresentar os controles de segurança utilizados para garantir a segurança dos certificados, dos domínios e dos subdomínios envolvidos. (subitem 3.4.1.1);
>
> **4.2.** A SG deve tomar providências para evitar a exposição de informações sensíveis contidas no arquivo PhpInfo().php dos ambientes de Produção e Teste do sistema SEI. (subitem 3.4.1.2);
>
> **4.3.** A SG deve tomar providências urgentes a fim de mitigar os riscos de acessos indevidos, de quebra de integridade dos dados e de exposição de informações sensíveis provenientes de ataques de força bruta ao sistema SEI. (subitem 3.4.3.1);
>
> **4.4.** A SG deve implementar a devida sanitização durante o upload de arquivos do tipo SVG, a fim de que sejam mitigados os riscos de execução de códigos maliciosos no sistema SEI. (subitem 3.4.6.1);
>
> **4.5.** A SG deve implementar a devida sanitização durante o upload de arquivos do tipo ZIP, a fim de que sejam mitigados os riscos de execução de códigos maliciosos no sistema SEI. (subitem 3.4.6.2).
>
> Consignamos que, embora as vulnerabilidades demonstradas no sistema SEI sejam de baixo risco, esta auditoria não procurou apontar as probabilidades de ataques em um cenário real no qual isso poderia acontecer. Nosso objetivo é confirmar que existem vulnerabilidades e que a Administração deve corrigi-las.
>
> Sugerimos restrição inicial completa à publicidade deste TC, pois o presente relatório expõe vulnerabilidades de segurança da informação que ainda serão objeto de análise e correção pelo órgão responsável. As vulnerabilidades do sistema SEI, reveladas nesta auditoria, podem ser utilizadas para ataques maliciosos de pessoas mal intencionadas.

Devidamente oficiadas (peças 17/22 e 27/32), a Secretaria Municipal de Educação informou que a Sra. Malde Vilas Boas não é mais titular da Secretaria Executiva de Gestão (peça 35).

A Secretaria do Governo Municipal, Secretaria Executiva de Gestão e a Sra. Malde Maria Vilas Bôas deixaram transcorrer in albis o prazo para manifestação (peça 36).

Novamente oficiadas (peças 38/43, 51/52), a Secretaria do Governo Municipal apresentou defesa (peças 46 e 49). A Secretaria Executiva de Gestão e Malde Maria Vilas Bôas deixaram de se manifestar no prazo concedido (peça 55).

Realizada Mesa Técnica na qual foram discutidas todas as vulnerabilidades encontradas pela **Auditoria** no sistema SEI, em 09.09.2021 (peça 56).

À peça 57, esta Relatoria determinou à Origem para que fossem atualizadas as informações referentes ao processo SEI, com destaque à previsão de implantação da nova versão do sistema (4.0) pelo Município de São Paulo, integração com outros sistemas e novas funcionalidades, justificativas para utilização dos certificados curinga, medidas adotadas para evitar a exposição de informações sensíveis contidas no arquivo PhpInfo().php dos ambientes de Produção e Teste do sistema SEI, providências adotadas a fim de mitigar os riscos de acessos indevidos, de quebra de integridade dos dados e de exposição de informações sensíveis provenientes de ataques de força bruta ao sistema SEI, competindo a esta Secretaria a obtenção dos dados necessários junto à Prodam e à Secretaria Municipal de Inovação e Tecnologia.

Em novo relatório, a **SCE** constatou que ainda persistiam quatro das cinco vulnerabilidades inicialmente apontadas (peça 79 - 04.05.2023):

> **4. CONCLUSÃO**
> Com relação às vulnerabilidades apontadas no Relatório de Auditoria Programada deste TC, peça 14, verificamos se ainda permanecem no sistema SEI versão 4.0. A constatação é a seguinte:
> **4.1.** A questão dos Certificados Coringas ainda permanece. Destacamos que não foram juntadas nos autos as manifestações da Prodam sobre o tema. Além disso, consignamos que o apontamento em tela não será sanado com novas versões do sistema SEI. Este ponto se refere à certificação, que é de responsabilidade da SG. (subitem 3.2)
> **4.2.** Verificamos que o acesso ao arquivo Phpinfo().php foi realizado sem sucesso no ambiente de produção. Desta forma, o apontamento foi sanado. (subitem 3.3)
> **4.3.** A vulnerabilidade de força bruta permanece presente na versão 4.0. (subitem 3.4)
> **4.4.** A vulnerabilidade de arquivos SVG permanece presente na versão 4.0. (subitem 3.5)
> **4.5.** A vulnerabilidade de arquivos executáveis em arquivos ZIP permanece presente na versão 4.0. (subitem 3.6)

A Secretaria Municipal de Gestão - Seges apresentou novos esclarecimentos às peças 95/97, os quais foram analisados pela **SCE**, que manteve os apontamentos constantes dos **itens 4.1, 4.3, 4.4 e 4.5** da conclusão do seu Relatório de Inspeção (peça 79), destacando que o **item 4.2** já havia sido superado (peça 100, fls 7).

À peça 102, a **Assessoria Jurídica - AJ** acompanhou a **Auditoria**, concluindo seu parecer como segue:

> Tendo em vista a natureza eminentemente técnica do trabalho realizado e as constatações apresentadas, além da inércia da Origem quando instada a se manifestar por diversas vezes nos autos (peças 25, 36, 55, 62, 68, 74, 86 e 92), entendo prescindível a análise jurídica das questões.

> Ante o exposto, destaco e acompanho integralmente as conclusões da Especializada, por seus próprios fundamentos, sem vislumbrar acréscimos de ordem estritamente jurídica.

À peça 109, a **Procuradoria da Fazenda Municipal – PFM** se manifestou destacando as conclusões da presente Auditoria, concluindo o seguinte:

> Posto isto, esta Procuradoria da Fazenda, ante o teor eminentemente adjetivo e instrumental deste procedimento, requer que a presente Auditoria seja conhecida e registrada, com o posterior encaminhamento à Origem das conclusões e recomendações que se fizerem cabíveis na espécie.

À peça 111, a **Secretaria Geral – SG** assim concluiu seu parecer:

> Com a detida análise, verifica-se que a Auditoria em questão cumpriu seu objetivo, predisposto no art. 8º da Resolução 06/00[1], diante das minuciosas conclusões alcançadas pelos órgãos técnicos preopinantes.
>
> Passo a análise das vulnerabilidades encontradas pela Auditoria do sistema SEI, de acordo com a numeração do seu Relatório de Inspeção (peça 79, fls. 6/7).
>
> **4.1. A questão dos Certificados Coringas ainda permanece. Destacamos que não foram juntadas nos autos as manifestações da Prodam sobre o tema. Além disso, consignamos que o apontamento em tela não será sanado com novas versões do sistema SEI. Este ponto se refere à certificação, que é de responsabilidade da SG. (subitem 3.2)**
>
> Em seu Relatório inicial, a SCE destacou que (peça 14, fls. 7/8):
>
> De modo geral, um certificado curinga funciona de forma semelhante aos certificados convencionais, isto é, um par de chaves criptografadas e auto assinadas, baseadas no protocolo Security Socket Layer (SSL), que protegem um domínio específico.
>
> (...)
>
> Por padrão, a opção pela utilização de certificados curingas como forma de proteção criptográfica na maioria das vezes dá-se pelo menor custo financeiro envolvido na aquisição, manutenção e gerenciamento desse tipo de certificado, assim como pela facilidade na extensão do uso e aparente facilidade no gerenciamento operacional.

[1] **Art.8º -** Auditorias constituem procedimentos de fiscalização realizados com as seguintes finalidades:
I - levantar dados e informações de natureza contábil, financeira, orçamentária e patrimonial, nos órgãos e entidades da Administração Direta e Indireta do Município, e analisálos quanto aos aspectos técnicos de legalidade e legitimidade de sorte a subsidiar o julgamento das contas anuais ou de atos de gestão dos responsáveis;
II - avaliar, do ponto de vista operacional, as atividades e sistemas desses órgãos e entidades, bem como aferir os resultados alcançados pelos projetos ou programas governamentais sob sua responsabilidade, ou por aqueles decorrentes de seus objetivos institucionais.

> Por outro lado, a utilização de um mesmo certificado curinga em inúmeros subdomínios é uma situação que poderá ocasionar diversas vulnerabilidades de segurança, (...)
>
> Entre as possíveis consequências da exploração desse tipo de vulnerabilidade está o comprometimento da segurança, não só da aplicação ora analisada, mas também, dos demais subdomínios vinculados ao domínio principal, neste caso, o domínio da PMSP (prefeitura.sp.gov.br).
> (...)
> Dessa forma, é necessário que a Secretaria de Gestão apresente a análise e avaliação de riscos que subsidiaram a adoção da solução criptográfica por meio de Wildcard Certificate ou Certificados Curingas e apresente os controles de segurança utilizados para garantir a segurança dos certificados, domínios e subdomínios envolvidos.

Após ciência do Relatório de Inspeção de SCE (peça 79), a Seges (peça 95), colacionou as respostas da sua área ARQUIP, da Empresa de Tecnologia de Informação e Comunicação do Município de São Paulo-PRODAM (peça 96, fls. 3) - empresa contratada para hospedar o SEI e que forneceu a infraestrutura de segurança e operação, e também o histórico de atualizações aplicadas ao SEI sob orientação do TRF-4 (peça 97).

A PRODAM esclareceu que (peça 96, fls. 2) :

> (...) o certificado Wildcard possuía a chave privada em servidor controlado apenas pela área de Segurança e Suporte, o que permite somente acesso restrito, e que a força de criptografia do certificado seguia as melhores práticas atuais e era a mesma do certificado de domínio único, ressalvando que em caso de uma improvável quebra de criptografia ou vazamento, como o certificado era utilizado em vários sites, a amplitude do impacto seria maior.

Todavia, para a SCE, o qual acompanho, a vulnerabilidade permanece porque "não foram apresentados os elementos técnicos (análise, avaliação de riscos e controles de segurança) que embasaram tecnicamente a adoção da solução criptográfica por meio de Wildcard Certificate ou Certificados Curingas" (peça 100 fls. 2).
Quanto ao apontamento 4.2 o mesmo já havia sido saneado no Relatório de Inspeção (peça 79, fls. 6).

4.3. A vulnerabilidade de força bruta permanece presente na versão 4.0. (subitem 3.4)
A PRODAM argumentou que apenas o ambiente de teste, por não possuir "recurso de captcha" habilitado, possui a vulnerabilidade de riscos de acessos indevidos, de quebra de integridade dados e da exposição de informações sensíveis provenientes de ataques de força bruta ao sistema SEI (pela 96, fls. 2).
A SCE, com o propósito de confirmar a afirmação da PRODAM, realizou testes no ambiente de Produção (peça 100, fls. 6):

> Foi verificado que sistema SEI não bloqueou as requisições automatizadas, tampouco exigiu o recurso captcha. Observando a Tabela 1, do primeiro ao quinto usuário, temos requisições com usuário e senha inválidos. A

> sexta requisição foi feita com usuário e senhas válidos, sendo que a ferramenta de automação foi capaz de acessar o sistema SEI. Dessa forma, foi constatado que os argumentos da Prodam não são capazes de superar o apontado, mantendo-se a conclusão.

Com isso, a SCE manteve a sua conclusão, a qual acompanho, que a vulnerabilidade ainda persiste.

4.4. A vulnerabilidade de arquivos SVG permanece presente na versão 4.0. (subitem 3.5)
4.5. A vulnerabilidade de arquivos executáveis em arquivos ZIP permanece presente na versão 4.0. (subitem 3.6)

Em relação a esses dois apontamentos, para a SCE a PRODAM (peça 96, fls 2) não trouxe novos elementos esclarecedores (peça 100, fls. 7):

> A Prodam argumenta que caso a aplicação não consiga tratar/sanitizar no momento do upload desse tipo de arquivo, a mitigação existia na camada de antivírus do NAS, uma vez que em nenhum momento o arquivo era salvo no disco local do host que hospeda a aplicação.
>
> A despeito dos esclarecimentos, quando da realização dos procedimentos para a elaboração do Relatório de Inspeção, conforme evidenciado no item 3.5 daquele relatório (peça 79, fl. 5), a vulnerabilidade se mantinha.

Assim, a meu ver, diante do caráter instrumental deste feito, entendo, s.m.j., que a presente Auditoria Programada reúne condições de ser submetida à apreciação do Nobre Conselheiro Relator, para conhecimento e deliberação, conforme disposto no parágrafo único do art. 11 da Resolução nº 06/00[2].

É o relatório.

VOTO

Cuidam os autos de Auditoria Programada com o objetivo de avaliar sob a ótica da Segurança da Informação em aplicações Web a efetividade dos controles de segurança implementados na aplicação Sistema Eletrônico de Informações (SEI), utilizado pela Prefeitura Municipal de São Paulo (PMSP), sob a gestão da Secretaria Municipal de Gestão, disponível no sítio da internet no endereço https://sei.prefeitura.sp.gov.br.

[2] **Art. 11 da Resolução nº 06/004** (redação conferida pelo art. 1º da Resolução nº 02/02) - Cada auditoria formará processo específico, autuado a partir da Ordem de Serviço correspondente emitida, de ofício, pela Secretaria de Fiscalização e Controle, no caso das auditorias constantes do Plano Anual, ou, tratando-se de auditoria extraplano, da ordem de execução emanada nos termos do artigo anterior. **Parágrafo único** - O Relator, ao apreciar o relatório de auditoria, deliberará sobre a conveniência e oportunidade de submetê-lo à apreciação do Plenário ou sobre a sua remessa ao processo das contas anuais, para subsidiar seu julgamento, podendo expedir determinações ou recomendações tendentes ao aperfeiçoamento dos órgãos, atividades ou serviços auditados para, se for o caso, posterior confronto.

O procedimento de Auditoria, previsto no artigo 44, III do Regimento Interno deste Egrégio Tribunal de Contas, foi devidamente instruído, garantidos o direito ao contraditório e a ampla defesa aos interessados.

O Relatório de Auditoria Programada, apresentado pela **Secretaria de Controle Externo – SCE** (peça 14 - 28.09.20) indicou a existência de apontamentos de vulnerabilidades relativas à segurança do Sistema Eletrônico de Informações – SEI, dos quais, após esclarecimentos e argumentações efetuados pela Origem, apenas um restou superado, qual seja, o constante do **item 4.2** do Relatório de Inspeção.[3] As irregularidades que persistiram vêm a ser:

> **4.1.** A SG deve apresentar a análise e a avaliação de riscos que embasaram tecnicamente a adoção da solução criptográfica por meio de Wildcard Certificate ou Certificados Curingas, assim como, deve apresentar os controles de segurança utilizados para garantir a segurança dos certificados, dos domínios e dos subdomínios envolvidos. (subitem 3.4.1.1);
> (...)
>
> **4.3.** A SG deve tomar providências urgentes a fim de mitigar os riscos de acessos indevidos, de quebra de integridade dos dados e de exposição de informações sensíveis provenientes de ataques de força bruta ao sistema SEI. (subitem 3.4.3.1);
>
> **4.4.** A SG deve implementar a devida sanitização durante o upload de arquivos do tipo SVG, a fim de que sejam mitigados os riscos de execução de códigos maliciosos no sistema SEI. (subitem 3.4.6.1);
>
> **4.5.** A SG deve implementar a devida sanitização durante o upload de arquivos do tipo ZIP, a fim de que sejam mitigados os riscos de execução de códigos maliciosos no sistema SEI. (subitem 3.4.6.2).

Em razão da natureza eminentemente técnica do trabalho realizado e as constatações apresentadas, além da inércia da Origem quando instada a se manifestar por diversas oportunidades (peças 25, 36, 55, 62, 68, 74, 86 e 92), não houve nos autos formulação de análise jurídica das questões destacadas.

Ante todo o exposto**, CONHEÇO, para fins de registro**, da presente Auditoria Programada, uma vez alcançada a sua finalidade ao apontar desacertos nos controles de segurança implementados na aplicação Sistema Eletrônico de Informações (SEI), utilizado pela Prefeitura Municipal de São Paulo (PMSP), sob a gestão da Secretaria Municipal de Gestão.

[3] **Item 4.2.** Verificamos que o acesso ao arquivo PHpinfo().php foi realizado sem sucesso no ambiente de produção. Desta forma, o apontamento foi sanado. (subitem 3.3)

Expeça-se ofício, encaminhando cópia do Relatório, Voto e Acordão, dirigido à Secretaria Municipal de Gestão para que conheça da presente decisão, assim como dos apontamentos formulados no Relatório de Auditoria Programada, apresentado pela Subsecretaria de Controle Externo – SCE (peça 14), com a RECOMENDAÇÃO de observar as irregularidades apontadas, evitando-as em procedimentos de controles de segurança futuros.

Cumpridas as formalidades legais, arquivem-se os autos.

EDUARDO TUMA
CONSELHEIRO RELATOR

Assinado digitalmente
por EDUARDO TUMA
Data: 17/01/2025
09:03:00 -03:00
Signature powered by e-TCM
Tribunal de Contas do Município de São Paulo