ACO-UTR-154/2025

Processo	-	TC/004207/2022
Interessada	-	Secretaria Municipal da Saúde
Objeto	-	Auditoria Extraplano – Avaliar sob a ótica da segurança da informação em aplicações web a efetividade dos controles de segurança implementados no sistema Gestão de Sistemas em Saúde

61ª Sessão Ordinária Não Presencial

AUDITORIA. SMS. SEGURANÇA DA INFORMAÇÃO. GESTÃO DE SISTEMAS EM SAÚDE. 1. As falhas identificadas no GSS demonstram vulnerabilidades de segurança da informação, que expõem o sistema a ataques cibernéticos, cujos danos podem resultar em perda ou sequestro de dados, bem como na paralisação dessa ferramenta de gestão utilizada. 2. Apresentado Plano de Ações elaborado pela PRODAM contendo medidas mitigatórias e/ou soluções com a posição das respectivas fases e prazo estimado com o intuito de sanar riscos à confidencialidade e à integridade dos dados, bem como à manutenção da disponibilidade dos serviços do sistema aos cidadãos. CONHECIDA. 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, considerando as manifestações dos Órgãos Técnicos desta Corte de Contas, cujos fundamentos acrescento às razões de decidir, em conhecer da presente Auditoria Extraplano, para fins de registro, visto que atendeu o objetivo de verificar, no âmbito da Secretaria Municipal da Saúde, a efetividade dos controles de segurança implementados no sistema Gestão de Sistemas em Saúde (GSS).

ACORDAM, à unanimidade, em determinar à **Secretaria de Controle Externo – SCE,** deste Tribunal, que:

1 - Acompanhe a implementação de todas as medidas propostas no Relatório de Auditoria Extraplano (conteúdo de acesso restrito) e a fase de cada solução indicada no Plano de Ações preparado pela PRODAM, de acordo com a estimativa de prazos informada pela SMS à peça 43 (fls. 4/5);

2 – Uma vez implantadas integralmente as melhorias mitigadoras de risco de vulnerabilidade (controles de segurança) no sistema Gestão de Sistemas em Saúde (GSS), verifique os resultados alcançados, de acordo com o exposto pela C-VIII, à peça 34.

ACORDAM, à unanimidade, em determinar a emissão de ofícios à Secretaria Municipal da Saúde e à PRODAM, acompanhados de cópias do relatório e voto do Relator e deste Acórdão.

ACORDAM, afinal, à unanimidade, em determinar, após cumpridas as 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 16:33:16 -03:00
Signature powered by e-TCM Tribunal de Contas do Município de São Paulo

Assinado digitalmente por EDUARDO TUMA
Data: 26/03/2025 17:03:34 -03:00
Signature powered by e-TCM Tribunal de Contas do Município de São Paulo

61ª SESSÃO ORDINÁRIA NÃO PRESENCIAL
Item 90 – Pleno

TC 4.207/2022. Auditoria Extraplano
Objeto: Secretaria Municipal da Saúde - Auditoria Extraplano - Avaliar sob a ótica da segurança da informação em aplicações web a efetividade dos controles de segurança implementados no sistema Gestão de Sistemas em Saúde.
Interessada: Secretaria Municipal de Saúde - SMS
Relator: Conselheiro Eduardo Tuma
Competência: Pleno

RELATÓRIO

Cuida-se de Auditoria Extraplano instaurada com o objetivo de avaliar, sob a ótica da segurança da informação em aplicações web, a efetividade dos controles de segurança implementados no Gestão de Sistemas em Saúde (GSS), sistema utilizado pela Secretaria Municipal da Saúde (SMS), disponível no site no endereço http://gss2.prefeitura.sp.gov.br/.

De acordo com o conteúdo da solicitação para instaurar o presente procedimento fiscalizatório (peça 1), o "GSS consiste em um sistema Web que tem por objetivo fazer, principalmente, o controle de estoques de medicamentos do Centro de Distribuição de Medicamentos e Correlatos (CDMEC) e de cada uma das, mais de 800, unidades de saúde da PMSP (UBSs, AMAs, Hospitais, etc)."

Uma vez em andamento os trabalhos, a Coordenadoria VIII solicitou ao Conselheiro Relator avaliar a recomendação de decretação de sigilo para o processo, por diversos motivos citados à peça 7, destacando-se o possível aumento de riscos à proteção da integralidade, confidencialidade e disponibilidade dos dados armazenados no sistema, na hipótese de identificação e divulgação de vulnerabilidades detectadas pela Auditoria.

À vista do exposto, o Relator determinou que, neste processo, não fossem inseridos dados extraídos do sistema da rede municipal da saúde, nem qualquer outra informação sigilosa que possam estar sujeitos aos riscos supra mencionados (peça 8).

Concluindo os trabalhos, a **Secretaria de Controle Externo** emitiu o Relatório de Auditoria Extraplano (peça 10 – 17/05/2023), no qual consignou que "O conteúdo deste relatório foi excluído ou editado para não comprometer a segurança do sistema GSS, em atendimento ao despacho de peça 8."

No tocante aos resultados dos testes aplicados, registrou a identificação de falhas bastante significativas que podem ocasionar a "perda de dados, roubo de

informações e na total inoperância do sistema GSS, caso sejam exploradas por meio de ataques cibernéticos", motivos pelos quais propôs a seguinte determinação:

> *7.1.1. Determinar à SMS que apresente um plano de ações e que evidencie a implementação de melhorias no sistema GSS, a fim de mitigar as vulnerabilidades de segurança da informação, as quais possibilitam ataques cibernéticos que podem resultar em perda ou sequestro de dados, bem como na paralisação do sistema."*

Em virtude da excepcionalidade deste tipo de auditoria, envolvendo segurança cibernética, com base na exposição de motivos da SCE-C.VIII (peça 11) e na autorização do Conselheiro Relator (peça 12), houve a realização de reunião técnica presencial com a participação de técnicos da Secretaria Municipal de Saúde e dos Auditores da SCE envolvidos no trabalho realizado, objetivando a transmissão de cópias controladas do relatório de auditoria, razão pela qual AUD sugeriu recomendar à SMS apresentar plano com medidas mitigatórias e respectivos prazos de implementação (peças 14/15 – 15/08/2023) .

A **Assessoria Jurídica,** pronunciando-se sobre o processado (peças 17/18 – 28/08/2023), acompanhou as conclusões da Auditoria, que por seu caráter eminentemente técnico não demandam acréscimos de ordem jurídica, bem como endossou a sugestão para que a Origem apresente plano de trabalho contendo as medidas mitigatórias da vulnerabilidades detectadas no sistema GSS, a serem adotadas, com prazos estabelecidos.

A SMS, oficiada para manifestar-se a respeito das conclusões dos Órgãos Técnicos desta Corte de Contas, encaminhou "informações apresentadas pelo Departamento de Tecnologia da Informação e Comunicação - SMS/CTIC" (peça 30), as quais foram analisadas pela **Auditoria** (peça 34 – 30/10/2023), que constatou necessitar de informação complementar quanto ao prazo, conforme especificado nos seguintes termos:

> *"3.1. O plano de ações apresentado pela SMS para implementação de melhorias para mitigação de riscos de segurança da informação do sistema GSS não informa qual é o prazo para a conclusão das ações propostas, a fim de que seja possível verificarmos posteriormente os resultados positivos do trabalho realizado."*

Novamente oficiada, a Origem, tomando ciência das posteriores manifestações da **Auditoria** e da **Assessoria Jurídica** (peça 34 e 36/37) apresentou informações técnicas à peça 43 (29/02/2024), sobre a etapa atualizada de cada providência indicada por AUD e os prazos estimados para a conclusão das medidas ainda não totalmente implementadas, sendo a última estimada para estar concluída em dezembro de 2024.

Ao manifestar-se sobre o acrescido, a **Assessoria Jurídica** (peças 46/47 - 11/03/2024), entendeu respondido o item 3.1 formulado por AUD (peça 34) e, destacando

os resultados alcançados na presente auditoria, opinou no sentido de que "o processo se encontra em condições de registro e conhecimento, sem prejuízo de eventuais medidas cabíveis, a critério superior."

A **Procuradoria da Fazenda Municipal** (peça 50 – 23/03/2024) enalteceu o trabalho desenvolvido pelos Órgãos Técnicos deste Tribunal de Contas, relevante colaboração do Controle Externo para o aprimoramento das funções de governo e, ressaltando que a presente auditoria extraplano alcançou seus objetivos, requereu seja ela conhecida e registrada.

Ao manifestar-se, a **Secretaria Geral** (peças 52/53 – 14/06/2024) acompanhou os entendimentos manifestados pela Coordenadoria VIII e pela AJ e concluiu que a presente auditoria, tendo cumprido suas finalidades, "encontra-se em condições de ser submetida à apreciação do Nobre Conselheiro Relator, para conhecimento, registro e deliberação."

É o Relatório.

VOTO

A presente Auditoria Extraplano, realizada no âmbito da Secretaria Municipal de Saúde - SMS, tem por objetivo avaliar, sob a ótica da segurança da informação em aplicações web, a efetividade dos controles de segurança implementados no sistema Gestão de Sistemas em Saúde (GSS).

O GSS, classificado como sistema Web, tem por objetivo principal "o controle de estoques de medicamentos do Centro de Distribuição de Medicamentos e Correlatos (CDMEC) e de cada uma das mais de 800 unidades de saúde da PMSP (UBSs, AMAs, Hospitais, etc)," além de armazenar "centenas de milhares de receitas de medicamentos controlados, dos quase 12 mil usuários deste serviço", configurando dados sensíveis que devem ser protegidos, tanto em relação aos cidadãos cadastrados, quanto à segurança da gestão pública.

Por essas razões, bem como pelas vulnerabilidades identificadas pela Auditoria nos controles de segurança do GSS, autorizei a não inserção de informações de caráter sigiloso, neste processo, motivo pelo qual o Relatório de Auditoria contém o aviso de que "*o conteúdo deste relatório foi excluído ou editado para não comprometer a segurança do sistema GSS*", cuja versão integral impressa foi entregue, pessoalmente, aos representantes da SMS, pelos Auditores, na reunião ocorrida em 06/06/2023

Feito este introito, analiso os resultados do trabalho realizado pela C-VIII, a partir do contexto de *"vulnerabilidade latente de cada site, pois, cada um, à sua maneira, pode apresentar falhas em sua infraestrutura de software (servidores de aplicação e banco de dados), na proteção da rede de computadores e desenvolvimento de aplicações, bem*

como todas as falhas possíveis no universo da internet", conforme justificativa exposta no relatório técnico.

As falhas identificadas no GSS, de acordo com os testes realizados pelos Auditores, demonstram vulnerabilidades de segurança da informação, que expõem o sistema a ataques cibernéticos, cujos danos podem resultar em perda ou sequestro de dados, bem como na paralisação dessa ferramenta de gestão utilizada pela SMS.

Ante tais constatações, a Especializada apontou a necessidade de a Origem apresentar plano de trabalho com as medidas de aperfeiçoamento do sistema GSS e correspondente prazo de implementação, com o intuito de "mitigar eventuais riscos à confidencialidade e à integridade dos dados, bem como à manutenção da disponibilidade dos serviços do sistema aos cidadãos."

O Plano de Ações elaborado pela PRODAM e apresentado pela Secretaria Municipal de Saúde (peças 30 e 43), contém onze medidas mitigatórias e/ou soluções com a posição das respectivas fases e o prazo estimado para a implementação de cada item, bem como a indicação do mês de dezembro/2024, como prazo final de execução do referido plano.

A Auditoria irá acompanhar os resultados da implementação dessas ações e avalia-los, conforme por ela anunciado em suas manifestações (peças 15 e 34).

Imperioso destacar a importância do trabalho de iniciativa da Secretaria de Controle Externo, por intermédio da C.VIII, considerando que não só o sistema GSS está sendo resguardado, mas também a rede municipal e talvez até a de outros entes da Federação, reflexo esse identificado pelo TCU, igualmente em sede de auditoria de segurança da informação (Proc. 017.413/2023-0).

Ao apreciar a "auditoria operacional com objetivo de promover a melhoria na gestão de riscos de segurança da informação no contexto dos serviços de hospedagem web, e-mail e resolução de nomes em organizações públicas federais", o TCU constatou as vulnerabilidades para ataques a sistemas federais através de invasão de sistemas municipais, consoante assim explicitado pelo Relator (Acórdão 523/2024 - Plenário. Min. Aroldo Cedraz):

> *"6. A* segurança cibernética *interessa a todo o ecossistema de organizações que se conecta via internet, devido à movimentação lateral executada pelos agentes de ameaça. Por exemplo, a* segurança cibernética *de uma secretaria municipal de saúde interessa ao Ministério da Saúde, porque a secretaria municipal acessa sistemas do Ministério que não estão expostos na internet. Caso um agente de ameaça consiga invadir e obter uma credencial na secretaria municipal, poderá acessar esse sistema do Ministério, aumentando a superfície de ataque do Ministério.*

> *7. Desta forma, a auditoria teve como escopo domínios de organizações públicas de todas as esferas e poderes, de forma a buscar uma gestão de risco sistêmico mais efetiva."*

Aborda, outrossim, diversos fatores que propiciam ataques cibernéticos, entre os quais a negligência dos entes públicos quanto à adoção das boas práticas de segurança da informação publicadas e o desconhecimento da relação favorável custo-benefício de algumas configurações de segurança recomendadas.

Da mesma forma que a presente auditoria extraplano identificou os tipos de ameaças e possíveis danos ao sistema GSS, o TCU, no processo acima referido, projetou os danos em dimensões muito maiores, nas seguintes extensões:

> "2. Ao longo do relatório serão apresentados sete riscos cuja consolidação sinaliza a existência do seguinte risco macro:
>
> Devido ao baixo percentual de domínios governamentais implementar as configurações de segurança recomendadas pelas boas práticas para serviços de hospedagem web, e-mail e DNS, *poderá ocorrer a manipulação de tráfego de rede, comprometimento de contas de usuários, roubo, vazamento e perda de dados ou mesmo disrupção dos sistemas das organizações, o que poderá levar à perda de disponibilidade, integridade e confidencialidade das informações, e impactar os programas, ações e objetivos das organizações, além da perda de confiança dos cidadãos e possíveis sanções legais."*

O tema é inesgotável porque requer constante checagem dos controles de segurança de informações, correções necessárias e, sobretudo, implementação das boas práticas recomendadas para a melhoria na gestão de riscos de segurança da informação, tal qual vem atuando a SCE, cujo trabalho foi enaltecido pela PFM em sua manifestação.

Nesse contexto, evidencia-se que o presente procedimento fiscalizatório atendeu sua finalidade restando, entretanto, decidir quanto ao conteúdo do Relatório de Auditoria Extraplano excluído ou editado para não comprometer a segurança do sistema GSS, em atendimento ao despacho de peça 8.

Invocando o mesmo Julgado do TCU (Acórdão 523/2024), a questão avaliada considera que a "divulgação ostensiva de algumas informações pode colocar em risco a segurança das instituições", motivo pelo qual o Plenário deliberou:

> *"9.3. classificar, com fulcro no art. 23, VII, da Lei 12.527/2011 e art. 9º, VII, da Resolução-TCU 294/2018, as peças 8, 9, 10 e 22 deste processo como sigilosas, em grau reservado, restringindo seu acesso a autoridades e servidores do Tribunal de Contas da União e das organizações mencionadas no subitem 9.1;"*

No presente caso, conforme retro exposto, o GSS controla os estoques de medicamentos do Centro de Distribuição de Medicamentos e Correlatos (CDMEC) e de todas as unidades de saúde da PMSP (UBSs, AMAs, Hospitais, etc), além de armazenar as

receitas de medicamentos controlados e os dados dos usuários deste serviço, envolvendo questões estratégicas e de segurança do sistema de saúde da Municipalidade de São Paulo e a privacidade dos usuários.

Tanto essas informações contidas no sistema GSS, que tenham sido acessadas na realização deste trabalho, quanto os métodos empregados pela Equipe Auditora, os pontos do sistema GSS por ela testados, os correspondentes resultados, as vulnerabilidades detectadas e as respectivas soluções propostas, devem receber classificação sigilosa em grau reservado, com amparo no art. 23, III e VII da Lei Federal nº 12.527/2011 e do art. 13, §1º, I e II e art. 14 da Resolução nº 29/19 deste Tribunal de Contas.

Logo, fica restrito às autoridades e aos servidores autorizados deste Tribunal de Contas, o acesso às referidas informações coligidas durante os trabalhos de auditoria, que não foram inseridas nos autos deste processo ou que se encontram editadas com tarjas de confidencialidade.

Ante todo o exposto e considerando as manifestações da SCE, AJ, PFM e SG, cujos fundamentos acrescento às razões de decidir, **CONHEÇO da presente Auditoria Extraplano, para fins de registro**, vez que atendeu o seu objetivo de verificar, no âmbito da Secretaria Municipal de Saúde, a efetividade dos controles de segurança implementados no sistema Gestão de Sistemas em Saúde (GSS).

Dê-se ciência à Secretaria de Controle Externo a fim de que:

1 - acompanhe a implementação de todas as medidas propostas no Relatório de Auditoria Extraplano (conteúdo de acesso restrito) e a fase de cada solução indicada no Plano de Ações preparado pela PRODAM, de acordo com a estimativa de prazos informada pela SMS à peça 43 (fls. 4/5);

2 – uma vez implantadas integralmente as melhorias mitigadores de risco de vulnerabilidade (controles de segurança) no sistema Gestão de Sistemas em Saúde (GSS), verifique os resultados alcançados, de acordo com o exposto pela C VIII à peça 34.

Expeçam-se ofícios à Secretaria Municipal de Saúde e à PRODAM, encaminhando cópia do relatório, voto e do Acórdão a ser proferido pelo Pleno.

Após, cumpridas as formalidades legais, arquivem-se os autos.

EDUARDO TUMA
CONSELHEIRO RELATOR

Assinado digitalmente por EDUARDO TUMA
Data: 17/01/2025 09:03:02 -03:00
Signature powered by e-TCM
Tribunal de Contas do Município de São Paulo