TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO

ACO-UTR-399/2026

Processo	-	TC/017955/2024
Auditada	-	Secretaria Municipal de Assistência e Desenvolvimento Social
Objeto	-	Auditoria Programada – Combinando Operação e Conformidade, nos sistemas de controle e monitoramento da Secretaria

80ª Sessão Ordinária Não Presencial em Ambiente Virtual

AUDITORIA PROGRAMADA. SMADS. SISTEMAS DE CONTROLE E MONITORAMENTO DA SECRETARIA. SEGURANÇA DA INFORMAÇÃO. PROTEÇÃO DE DADOS PESSOAIS. LGPD. CONTROLES DE AUTENTICAÇÃO. DADOS SENSÍVEIS. ATAQUES DE FORÇA BRUTA. CONTROLE DE SESSÃO. CRIPTOGRAFIA. GESTÃO DE VULNERABILIDADES. RESPONSABILIDADE CONTRATUAL. 1. Os sistemas informatizados que tratam dados pessoais e sensíveis devem adotar controles técnicos e administrativos aptos a assegurar a proteção das informações contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Art. 5º, I, e art. 6º, VII, L 13.709/2018. ABNT NBR ISO/IEC 27002:2022. 2. A exposição de dados sensíveis em sistemas corporativos da Administração Pública caracteriza vulnerabilidade de segurança incompatível com os princípios da segurança e da proteção de dados previstos na Lei Geral de Proteção de Dados, impondo a adoção de medidas corretivas para mitigação dos riscos identificados. Art. 5º, I, e art. 6º, VII, L 13.709/2018. 3. A ausência de mecanismos de proteção contra-ataques de força bruta, de controles de sessão, de criptografia no tráfego de dados e de criptografia no armazenamento de credenciais de acesso configura fragilidade relevante dos controles de segurança da informação e demanda imediata adequação às boas práticas e normas técnicas aplicáveis. Art. 5º, I, e art. 6º, VII, L 13.709/2018. Seção 12.6, ABNT NBR ISO/IEC 27002:2022. 4. A Administração deve apurar eventual descumprimento de obrigações contratuais relacionadas à segurança da informação, promovendo a responsabilização do contratado, inclusive mediante glosa de valores e aplicação de penalidades, quando constatada a prestação inadequada dos serviços contratados. CONHECIDA. Votação unânime. DETERMINAÇÃO. 1. Elimine a exposição de dados sensíveis no sistema SISCR. 2. Implemente controles contra ataques de força bruta nos sistemas SISA, SISCR e SISRUA. 3. Apure eventual responsabilidade da Prodam-SP pelas vulnerabilidades identificadas, promovendo, se cabível, glosa de valores e aplicação de penalidades. 4. Implemente controle de sessão no sistema SISCR. 5. Adote certificados de segurança para criptografia do tráfego de dados no sistema SISRUA. 6. Criptografe as senhas armazenadas dos usuários dos sistemas da SMADS. 7. Apresente Plano de Ação contendo cronograma, responsáveis e indicadores para monitoramento das medidas corretivas. RECOMENDAÇÃO. 1. Promova ações de capacitação de usuários e gestores dos sistemas em boas práticas de segurança da informação e prevenção de incidentes. Votação por maioria.

A C Ó R D Ã O

Vistos e relatados estes autos, dos quais é Relator o Conselheiro ROBERTO BRAGUIM.

ACORDAM os Conselheiros do Tribunal de Contas do Município de São Paulo, à unanimidade, de conformidade com o relatório e voto do Relator, com fulcro nas manifestações exaradas pelos Órgãos Técnicos desta Corte, em conhecer da Auditoria realizada, determinando o seu competente registro.

ACORDAM, por maioria, pelos votos dos Conselheiros ROBERTO BRAGUIM – Relator, JOÃO ANTONIO e EDUARDO TUMA, em acolher as Propostas de Determinações contidas nos itens 7.1.1, 7.1.2 e 7.1.4 a 7.1.7 do Relatório de Auditoria, anotando **o prazo de 180 (cento e oitenta) dias** para que a Secretaria Municipal de Assistência e Desenvolvimento Social – SMADS adote as providências para seu cumprimento.

ACORDAM, por maioria, pelos mesmos votos, para viabilizar o monitoramento das determinações exaradas, que a SMADS deverá apresentar, **no prazo de 60 (sessenta) dias**, Plano de Ação detalhado contendo cronograma, responsáveis e indicadores de acompanhamento para as medidas corretivas adotadas.

Vencido em parte o Conselheiro RICARDO TORRES – Revisor, conforme declaração de voto apresentada, que estipulou o prazo de 120 (cento e vinte) dias para a apresentação do Plano de Ação detalhado e, quanto ao prazo de 180 (cento e oitenta) dias para que a Origem adote as providências para o cumprimento das determinações realizadas, entendeu ser o caso de ressalvar a possibilidade de extensão do termo por igual prazo, em observância ao contexto realístico da Administração.

ACORDAM, à unanimidade, em recomendar à Pasta que sejam promovidas ações de capacitação dos usuários e gestores dos sistemas, visando à conscientização sobre boas práticas de segurança da informação e prevenção de incidentes.

ACORDAM, afinal, à unanimidade, em determinar, o envio de cópias do relatório, voto, declaração de voto e deste Acórdão à Secretaria Municipal de Assistência e Desenvolvimento Social e, após os trâmites legais, o arquivamento dos autos.

Participaram do julgamento os Conselheiros RICARDO TORRES – Revisor, JOÃO ANTONIO e EDUARDO TUMA.

São Paulo, 17 de junho de 2026.

DOMINGOS DISSEI – Presidente
ROBERTO BRAGUIM – Relator

/smv

Assinado digitalmente por ROBERTO TANZI BRAGUIM
Data: 21/07/2026 10:36:13 -03:00
Signature powered by e-TCM Tribunal de Contas do Município de São Paulo

Assinado digitalmente por DOMINGOS QDONE DISSEI
Data: 03/08/2026 13:44:12 -03:00
Signature powered by e-TCM Tribunal de Contas do Município de São Paulo

Item 3) e-TCM nº 17.955/2024

Interessadas: Secretaria Municipal de Assistência e Desenvolvimento Social (SMADS)

Objeto: Auditoria Programada Combinada (Operacional e Conformidade) com o objetivo de avaliar a adequação dos controles de segurança da informação nos sistemas SISORG, SISRUA, SISA e SISCR, da SMADS, com base na Lei Geral de Proteção de Dados, nas melhores práticas e normativos aplicáveis, como a NBR ISO 27002/2022 e o Manual de Segurança da Informação do TCMSP.

Relator: Conselheiro **Roberto Braguim**

RELATÓRIO

Trata-se de Auditoria Programada – Combinada (Operacional e Conformidade), que objetivou avaliar a adequação dos controles de segurança da informação nos sistemas SISORG (Sistema de Cadastro de Organizações), SISRUA (Sistema de Informação da Situação de Rua), SISA (Sistema de Informação do Atendimento aos Usuários) e SISCR (Sistema dos Centros de Referência de Assistência Social), da Secretaria Municipal de Assistência e Desenvolvimento Social (SMADS), com base na Lei Geral de Proteção de Dados, nas melhores práticas e normativos aplicáveis, como a NBR ISO 27002/2022 e o Manual de Segurança da Informação do TCMSP.

A análise desenvolvida pela Secretaria de Controle Externo (SCE), no período de 02/09/2024 a 31/01/2025, identificou vulnerabilidades críticas que comprometem a integridade, confidencialidade e disponibilidade das informações tratadas.

Ressalta-se que os Achados da Auditoria incluem informações pessoais sensíveis, cuja divulgação irrestrita pode comprometer a segurança institucional e cibernética tanto da Secretaria quanto da Prefeitura do Município de São Paulo.

Diante disso, tais informações se enquadram nas hipóteses de restrição de acesso estabelecidas pela Resolução nº 29/2019 do TCM e pelo Termo de Classificação de Informação/Restrição de Acesso (TCI/RA), exigindo a devida proteção e sigilo.

Em seu relatório de peça 7, a equipe técnica concluiu que não houve identificação de prejuízo concreto causado pelas vulnerabilidades identificadas nos sistemas abordados na Auditoria. Contudo, considerando a relevância das fragilidades detectadas, foi apresentada proposta de encaminhamento visando à apuração, pela SMADS, da ocorrência de descumprimento de dispositivos previstos nos instrumentos contratuais celebrados com a Prodam-SP, e de eventuais responsabilidades, com aplicação de apenação quando necessário, conforme item 7 do relatório de Auditoria, a seguir expostas:

7. PROPOSTAS DE ENCAMINHAMENTOS

7.1. Propostas de determinações

Determinar à **Secretaria Municipal de Assistência e Desenvolvimento Social (SMADS)**, que adote, no prazo de 180 dias, as seguintes providências:

7.1.1. Eliminar a exposição de dados sensíveis no sistema SISCR por estar em desacordo com os artigos 5º, inciso I e 6º, inciso VII da Lei nº 13.709/18, bem como da seção 12.6, Gestão de vulnerabilidades técnicas, da norma brasileira ABNT ISO/IEC 27.002 (**item 3.1**);

7.1.2. Aplicar os controles relativos a ataques de força bruta aos sistemas SISA, SISCR e SISRUA, por estar em desacordo com os artigos 5º, inciso I e 6º, inciso VII da Lei nº 13.709/18, bem como da seção 12.6, Gestão de vulnerabilidades técnicas, da norma brasileira ABNT ISO/IEC 27.002 (**item 3.1**);

7.1.3. Adotar o uso de mensagens genéricas como "Usuário ou Senha Inválidos" quando houver logins malsucedidos nos sistemas SISCR e SISRUA, por estar em desacordo com os artigos 5º, inciso I e 6º, inciso VII da Lei nº 13.709/18, bem como da seção 12.6, Gestão de vulnerabilidades técnicas, da norma brasileira ABNT ISO/IEC 27.002 (**item 3.1**);

7.1.4. Apurar as eventuais responsabilidades da Prodam-SP nas vulnerabilidades identificadas e eventualmente proceder à glosa dos valores por serviços cobrados e não realizados ou deficientes, bem como proceda à penalização da Prodam-SP, caso os serviços de segurança da informação estejam previstos nos contratos dos sistemas SISA, SISCR e SISRUA, contrariando os artigos 5º, inciso I e 6º, inciso VII da Lei nº 13.709/18, bem como da seção 12.6, Gestão de vulnerabilidades técnicas, da norma brasileira ABNT ISO/IEC 27.002 (**item 3.1**);

7.1.5. Aplicar o controle de sessão nos itens de menu, implementando mais uma camada de segurança no sistema SISCR, por estar em desacordo com os artigos 5º, inciso I e 6º, inciso VII da Lei nº 13.709/18, bem como da seção 12.6, Gestão de vulnerabilidades técnicas, da norma brasileira ABNT ISO/IEC 27.002 (**item 3.2**);

7.1.6. Adotar certificados de segurança para o sistema SISRUA para tráfego de dados criptografados, por estar em desacordo com os artigos 5º, inciso I e 6º, inciso VII da Lei nº 13.709/18, bem como da seção 12.6, Gestão de vulnerabilidades técnicas, da norma brasileira ABNT ISO/IEC 27.002 (**item 3.3**);

7.1.7. Criptografar as senhas armazenadas dos usuários dos sistemas da SMADS, por estar em desacordo com os artigos 5º, inciso I e 6º, inciso VII da Lei nº 13.709/18, bem como da seção 12.6, Gestão de vulnerabilidades técnicas, da norma brasileira ABNT ISO/IEC 27.002 (**item 3.4**).

No desenvolvimento da instrução, determinei, então, o encaminhamento de ofícios à SMADS, para apresentação dos devidos esclarecimentos acerca das questões suscitadas nas peças 10, 16, 21, 31 e 42.

Sobrevieram as manifestações da Pasta, peças 14, 26 e 36 que, levadas à análise de SCE, peças 30 e 49, não se mostraram suficientes para superação dos apontamentos lançados no Relatório inicial, à exceção do item 7.1.3, relativo à adoção de mensagens genéricas nos erros de autenticação.

Ouvida, a Procuradoria da Fazenda Municipal pugnou pelo conhecimento e registro da Auditoria.

Por fim, a Secretaria Geral acompanhou a monifestação da equipe técnica da Coordenadoria VIII e destacou que o objetivo da Auditoria foi cumprido, reunindo condições de ser apreciada por esta Corte de Contas.

É o relatório.

VOTO

Em julgamento Auditoria Programada – Combinada (Operacional e Conformidade) instaurada, no âmbito da Secretaria Municipal de Assistência e Desenvolvimento Social (SMADS), com o objetivo de avaliar a adequação dos controles de segurança da informação nos sistemas SISORG[1], SISRUA[2], SISA[3] e SISCR[4], com base na Lei Geral de Proteção de Dados, nas melhores práticas e normativos aplicáveis, como a NBR ISO 27002/2022 e o Manual de Segurança da Informação do TCMSP.

Os principais resultados encontrados no curso da Auditoria foram fragilidades nos controles de autenticação, com exposição de dados sensíveis no sistema SISCR e falta de controles eficazes contra ataques de força bruta nos sistemas SISA, SISCR e SISRUA.

Foi identificado também o acesso aos menus do SISCR sem controle de sessão, comprometendo a segurança do sistema e igualmente o tráfego de dados no SISRUA sem criptografia, expondo informações a interceptações. Por fim, as senhas dos usuários dos

[1] Sistema de Cadastro de Organizações.
[2] Sistema de Informação da Situação de Rua.
[3] Sistema de Informação do Atendimento aos usuários.
[4] Sistema dos Centros de Referência de Assistência Social.

sistemas da SMADS são armazenadas sem criptografia, aumentando o risco de acessos não autorizados.

Ressalto que os achados da Auditoria incluem informações pessoais sensíveis, cuja divulgação irrestrita pode comprometer a segurança institucional e cibernética tanto da Secretaria quanto da própria Prefeitura do Município de São Paulo.

Diante disso, tais informações se enquadram nas hipóteses de restrição de acesso estabelecidas pela Resolução nº 29/2019 do TCM e pelo Termo de Classificação de Informação/Restrição de Acesso (TCI/RA), exigindo a devida proteção e sigilo.

A vasta análise realizada pela Secretaria de Controle Externo (SCE), consubstanciada no Relatório de peça 7 e nas manifestações de peças 30 e 49, trouxe, em síntese, propostas de encaminhamento visando eliminar a exposição de dados sensíveis no SISCR, aplicar controles contra ataques de força bruta nos sistemas SISA, SISCR e SISRUA, implementar controle de sessão nos menus do SISCR, adotar criptografia no tráfego de dados do SISRUA e criptografar as senhas armazenadas dos usuários. Tais ações objetivam garantir maior segurança e conformidade dos sistemas da SMADS com as normas vigentes.

A larga instrução processual foi marcada por diversas oportunidades de manifestação conferidas à Secretaria e ao

responsável indicado, mas as intervenções apresentadas não foram suficientes para afastar os apontamentos mencionados.

As falhas relacionadas pela Auditoria demonstram, em resumo, a exposição de dados sensíveis, ausência de controles contra ataques de força bruta, falta de controle de sessão, ausência de certificados de segurança para tráfego criptografado e armazenamento de senhas sem criptografia.

Embora a SMADS tenha informado que, em alguns casos, não tenha conseguido identificar os problemas apontados, afirmou ter encaminhado as demandas à Prodam para análise e correção. Em outros pontos, reconheceu as falhas e informou que está tomando providências, para obtenção de estimativas de prazo e custo para adequações, ou aguardando iniciativas de unificação de cadastros pela Prefeitura.

Conforme bem detalhado pela Auditoria, não houve apresentação de soluções concretas ou prazos para correção das vulnerabilidades, reforçando a necessidade de medidas urgentes para garantir a conformidade com a legislação vigente e as normas de segurança da informação.

Ante o exposto, com fulcro nas manifestações exaradas pelos Órgãos Técnicos deste Tribunal, que agrego ao presente,

Conheço da Auditoria realizada, determinando o seu competente registro.

Acolho as Propostas de Determinações contidas nos itens 7.1.1, 7.1.2 e 7.1.4 a 7.1.7 do Relatório de Auditoria[5], anotando o prazo de 180 dias para que a Secretaria Municipal de Assistência e Desenvolvimento Social (SMADS) adote as providências para seu cumprimento.

Para viabilizar o monitoramento das determinações exaradas, a SMADS deverá apresentar, no prazo de 60 dias, Plano de Ação detalhado contendo cronograma, responsáveis e indicadores de acompanhamento para as medidas corretivas adotadas.

Recomendo, ainda, à Pasta que sejam promovidas ações de capacitação dos usuários e gestores dos sistemas, visando

[5] **7.1.1.** Eliminar a exposição de dados sensíveis no sistema SISCR por estar em desacordo com os artigos 5º, inciso I e 6º, inciso VII da Lei nº 13.709/18, bem como da seção 12.6, Gestão de vulnerabilidades técnicas, da norma brasileira ABNT ISO/IEC 27.002 (**item 3.1**);
7.1.2. Aplicar os controles relativos a ataques de força bruta aos sistemas SISA, SISCR e SISRUA, por estar em desacordo com os artigos 5º, inciso I e 6º, inciso VII da Lei nº 13.709/18, bem como da seção 12.6, Gestão de vulnerabilidades técnicas, da norma brasileira ABNT ISO/IEC 27.002 (**item 3.1**);
7.1.4. Apurar as eventuais responsabilidades da Prodam-SP nas vulnerabilidades identificadas e eventualmente proceder à glosa dos valores por serviços cobrados e não realizados ou deficientes, bem como proceda à penalização da Prodam-SP, caso os serviços de segurança da informação estejam previstos nos contratos dos sistemas SISA, SISCR e SISRUA, contrariando os artigos 5º, inciso I e 6º, inciso VII da Lei nº 13.709/18, bem como da seção 12.6, Gestão de vulnerabilidades técnicas, da norma brasileira ABNT ISO/IEC 27.002 (**item 3.1**);
7.1.5. Aplicar o controle de sessão nos itens de menu, implementando mais uma camada de segurança no sistema SISCR, por estar em desacordo com os artigos 5º, inciso I e 6º, inciso VII da Lei nº 13.709/18, bem como da seção 12.6, Gestão de vulnerabilidades técnicas, da norma brasileira ABNT ISO/IEC 27.002 (**item 3.2**);
7.1.6. Adotar certificados de segurança para o sistema SISRUA para tráfego de dados criptografados, por estar em desacordo com os artigos 5º, inciso I e 6º, inciso VII da Lei nº 13.709/18, bem como da seção 12.6, Gestão de vulnerabilidades técnicas, da norma brasileira ABNT ISO/IEC 27.002 (**item 3.3**);
7.1.7. Criptografar as senhas armazenadas dos usuários dos sistemas da SMADS, por estar em desacordo com os artigos 5º, inciso I e 6º, inciso VII da Lei nº 13.709/18, bem como da seção 12.6, Gestão de vulnerabilidades técnicas, da norma brasileira ABNT ISO/IEC 27.002 (**item 3.4**).

à conscientização sobre boas práticas de segurança da informação e prevenção de incidentes.

Determino, por fim, o envio de cópias deste Relatório e Voto e do Acórdão decorrente à Secretaria Municipal de Assistência e Desenvolvimento Social (SMADS).

Após os trâmites legais, arquivem-se os autos.

É como voto.

TCM, 1º de junho de 2026.

ROBERTO TANZI BRAGUIM:03999981873

Assinado de forma digital por ROBERTO TANZI BRAGUIM:03999981873
Dados: 2026.06.01 09:24:54 -03'00'

ROBERTO BRAGUIM
Conselheiro Corregedor

CAPS/RB

Processo: **TC/17955/2024**
Origem: Secretaria Municipal de Assistência e Desenvolvimento Social
Objeto: Auditoria Programada - Combinada (Operacional e Conformidade) - nos sistemas de controle e de monitoramento da Secretaria Municipal de Assistência e Desenvolvimento Social - SMADS

DECLARAÇÃO DE VOTO

1. Diante do judicioso voto do Exmo. Conselheiro Relator Roberto Braguim, cujos fundamentos decisórios convergem integralmente com meu entendimento, peço vênia para divergir pontualmente, apenas no que diz respeito aos prazos adotados.

2. Isto porque, a despeito dos prazos regimentais previstos e justamente propostos pelo Conselheiro Relator, entendo se tratar de questão técnica que envolve complexidade considerável que justifica a possibilidade, em vistas aos artigos 20 e 22 da LINDB, de extensão dos prazos determinados.

3. Desta feita, sobretudo em relação ao prazo para apresentação de Plano de Ação detalhado, contendo cronograma, responsáveis e indicadores de acompanhamento para as medidas corretivas adotadas, entendo ser viável estipular o prazo de 120 dias, ainda que seja preferível que a Origem o faça com a maior brevidade possível diante da urgência que o assunto requer.

4. No mesmo sentido, quanto ao prazo de 180 dias para que a Origem adote as providências para o cumprimento das determinações

realizadas, entendo ser o caso de ressalvar a possibilidade de extensão do termo por igual prazo, em observância ao contexto realístico da Administração, recomendando-se, no entanto, que sejam cumpridas com a maior brevidade possível.

5. Dessa forma, **CONVIRJO** integralmente com o Relator no que tange aos fundamentos decisórios e determinações, com a ressalva dada aos prazos estipulados para as ações a serem realizadas pela Origem.

É como voto, Senhor Presidente.

Ricardo Torres
Conselheiro

Assinado digitalmente por RICARDO EZEQUIEL TORRES
Date: 06/16/2026 09:44:30 -03:00
Signature powered by e-TCM
Tribunal de Contas do Município de São Paulo