Ministério Público de Contas do Distrito Federal
Terceira Procuradoria

PROCESSO N.º 3.034/2010-e

PARECER: 368/2021–G3P/DA

EMENTA: Inspeção. Relatório Final. Secretaria de Estado de Saúde. Segurança da informação e integração dos sistemas de prontuário eletrônico. Fiscalização dos contratos de tecnologia da informação. Irregularidades. Falha de controle sobre os serviços prestados por prepostos. Sistema Unificado de Informações de Saúde do Distrito Federal. Falhas de segurança de acesso. Quantidade excessiva de perfis redundantes. Certificado de segurança de *site* vencida. Exposição de informações do Servidor Web da aplicação SIS/Trakcare. Ausência de política e práticas de segurança da informação. Ausência de integração dos sistemas existentes. MPCDF, no mérito, aquiesce com ajustes e acréscimos. Determinações e recomendações.

Os autos albergam, nesta fase, os resultados de Inspeção realizada pela Divisão de Fiscalização de Tecnologia da Informação da Secretaria de Fiscalização Especializada/TCDF, objetivando examinar a segurança da informação do módulo prontuário eletrônico do Sistema Integrado de Saúde da SES/DF (SIS/Trakcare) e a sua integração com os demais sistemas de prontuário utilizados pelas unidades de saúde do DF, bem como os procedimentos adotados para fiscalização dos contratos de TI, nos termos dos itens III.a.1 e III.a.2 da Decisão n.º 2.394/2020.

2. A Instrução registra que foi objeto da Inspeção o módulo de prontuário eletrônico do paciente – PEP do Sistema Integrado de Saúde – SIS implementado nas unidades de saúde geridas pela SES/DF[1], utilizando a plataforma tecnológica Trakcare[2]; salientando que os serviços técnicos especializados de manutenção, suporte técnico e atualização do SIS/Trakcare e seus módulos[3] são realizados à conta do Contrato n.º 19/2018, celebrado, por *inexigibilidade de licitação*, entre a SES e a Intersystems do Brasil Ltda, pelo montante de R$ 4.980.000,00, distribuídos da seguinte forma:

[1] A Secretaria de Estado de Saúde possui atualmente 240 (duzentas e quarenta) unidades de saúde e cerca de 32.000 usuários, que prestam serviços de assistência à saúde à população Fonte: PT 01 - DOD - aquisição novo sistema de informatização das unidades de saúde do DF (Processo SEI nº 00060-00464906/2019-53, arquivo na Aba Associados deste processo no e-TCDF).
[2] Sistema Unificado de Informação de Saúde da empresa Intersystems customizado para atender a SES/DF. Fonte: https://www.intersystems.com/products/trakcare.
[3] Módulos: Prontuário Eletrônico do Paciente, Laboratório, Gestão de Leitos, Farmácia (Alphalink), Material, Faturamento, Relatórios Estatísticos e Escalas. Fonte: PT 02 - Contrato nº 19/2018.

Ministério Público de Contas do Distrito Federal
Terceira Procuradoria

Tabela 1 – Contrato nº 19/2018

LOTE	DESCRIÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO	VALOR MENSAL	VALOR ANUAL
1	Manutenção, Suporte Técnico e Atualização Tecnológica para Banco de Dados CACHÉ, versão Enterprise, SIS - Sistema Integrado de Saúde na Plataforma Trakcare, Módulo SisMateriais (módulo de material e farmácia Alphalink), incluindo os módulos de laboratório (Labtrak) e o módulo de escalas licenças de usuários concorrentes	Licença	3750	R$ 28,90	R$ 108.375,00	R$ 1.300.500,00
2	Manutenção, Suporte Técnico e Atualização para o SIS - Sistema Integrado de Saúde na Plataforma Trakcare, Módulo SisMateriais (módulo de material e farmácia Alphalink), incluindo os módulos de laboratório (Labtrak) e o módulo de escalas licenças de usuários concorrentes.	Licença	3750	R$ 80,80	R$ 303.000,00	R$ 3.636.000,00
3	Manutenção, Suporte Técnico e Atualização Tecnológica para Ensemble (healthshare), Integrador de Plataformas para o SIS - Sistema Integrado de Saúde na Plataforma Trakcare.	Licença	1	R$ 3.625,00	R$ 3.625,00	R$ 43.500,00
					TOTAL	R$ 4.980.000,00

Fonte: PT02 - Contrato nº 19/2018 (arquivo associado ao processo)

3. Em complemento, aduz que, à época do exame, o contrato se encontrava em seu 2º Termo aditivo, com vigência de 16/4/2020 a 15/4/2021, no valor de R$ 5.398.658,04.

4. A Instrução indica que foram examinados *os controles de acesso/perfil de usuário*, a *existência de políticas/normativos*, *técnicas de autenticação*, *utilização de métodos criptográficos*, *proteção de informações do ambiente computacional*, além da *integração do SIS/Trakcare com os sistemas de prontuário eletrônico que são utilizados nas unidades de saúde geridas pelo IGES/DF6 (Sistema SOUL-MV7) e nas unidades de Atenção Básica de Saúde (Sistema e-SUS AB8)*.

5. Quanto aos procedimentos de fiscalização do Contrato n.º 19/2018 – SES/INTERSYSTEMS e seus aditivos, envolvendo a prestação dos serviços de manutenção, suporte técnico e atualização do Sistema Integrado de Saúde (SIS/Trakcare), restou abrangido o desembolso realizado no período de janeiro/2019 a maio/2020, no valor de R$ 10.609.489,60, conforme Ordens Bancárias que relaciona.

6. Passando ao resultado dos exames, a zelosa DIFTI apontou o **Achado 1** (*Ausência de informações pra fiscalização e controle dos serviços prestados)*, onde relata que, na análise do Processo SEI 00060-00222650/2018-28, autuado a fim de acompanhar a execução contratual[4], encontrou, basicamente, *ordens de serviço* da SES no decorrer da vigência contratual, ressentindo-se da autuação de instrumentos de controle eficazes a fim de subsidiar a fiscalização das obrigações entabuladas, conforme exige o art. 66 da Lei n.º 8.666/1993; tais

[4] Suporte técnico, manutenção e atualização do Sistema Integrado de Saúde – SIS/Trakcare e seus módulos (Contrato n.º 19/2018).

como *relatórios mensais de atividades*[5] detalhados e emitidos pela prestadora, em consonância com art. 19, I, "b", da IN n.º 4/2014 – SLTI/MPOG[6], objetivando mitigar riscos de superfaturamento e proporcionar o conhecimento exato do volume dos serviços prestados, bem como da força de trabalho alocada, a fim de auxiliar estimativas para contratações futuras.

7. Relata que, embora o contrato preveja a prestação de serviços presenciais e não presenciais e, a esse teor, a constatação da existência de profissionais alocados nas dependências da SES; o processo de acompanhamento não permite o controle da Jurisdicionada sobre essa modalidade, o que obstrui a fiscalização do cumprimento das obrigações trabalhistas pela prestadora e impinge riscos de responsabilização subsidiária nos termos da Súmula 331/TST.

8. As constatações ensejaram a proposição de recomendar à SES/DF a adoção de medidas para estabelecer a regular fiscalização contratual, relativa à disponibilização de informações dos trabalhadores da contratada que prestam serviços de manutenção/suporte do Sistema SIS/Trakcare e a elaboração de relatórios de atividades mensais contemplando as seguintes informações: identificador (nº sequencial), ordem de serviço vinculada à atividade, tipo do serviço realizado pela prestadora, severidade, status, descrição, tempo de execução (data da abertura e fechamento), perfil(s) profissional(i)s que realizou(aram) o serviço, tempo de execução, produtos/resultados esperados e o cumprimento ou não do acordo de nível de serviço estabelecido em contrato, para efeito de acompanhamento do Contrato n.º 19/2018-SES/DF; de acordo com o art. 66 da Lei 8.666/93 e do art. 19, I, "b", da IN 04/2014-SLTI/MPOG.

9. Relata que, embora o contrato preveja a prestação de serviços presenciais e não presenciais e, a esse teor, a constatação da existência de profissionais alocados nas dependências da SES; o processo de acompanhamento não permite o controle da Jurisdicionada sobre essa atividade, o que obstrui a fiscalização do cumprimento das obrigações trabalhistas pela prestadora e impinge riscos de responsabilização subsidiária nos termos da Súmula 331/TST.

10. No **Achado 2** *(Quantidade excessiva de perfis de acesso redundantes)*, o Corpo Técnico, em síntese, descreve que a SES permite que núcleos de informatica vinculados aos hospitais criem perfis de acesso ao Sistema de Prontuário Eletrônico/SES, sem controle centralizado; implicando a definição excessiva de perfis redundantes e o estabelecimento de regras sem uniformidade, em confronto com as boas práticas, especialmente com o que recomenda o controle A.9.1.1 – Política de Controle de Acesso da ABNT NBR ISSO /IEC 27001:2013[7]; o que enseja o comprometimento da segurança da informação do sistema.

---

[5] Contendo identificador (nº sequencial), ordem de serviço vinculada à atividade, tipo do serviço realizado pela prestadora, severidade, status, descrição, tempo de execução (data da abertura e fechamento), perfil(s) profissional(i)s que realizou(aram) o serviço, tempo de execução, produtos/resultados esperados e o cumprimento ou não do acordo de nível de serviço estabelecido em contrato, em consonância com o item I.b do art. 19 da IN 04/2014-SLTI/MPOG.

[6] Recepcionada no DF pelo Decreto nº 37.667/2016.

[7] Esta Norma foi preparada para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI).

11. Ressalta que tais inconformidades são agravadas pela ausência de mecanismos de exclusão automática de acesso ao SIS/Trakcare, quando do desligamento/afastamento do servidor da atividade laboral ou de bloqueio do usuário por número máximo de tentativas sem sucesso; o que representa risco de violação de senhas e de nomes de usuários, além de favorecer situações de acesso indevido a prontuários eletrônicos.

12. Assim, a Unidade Técnica propõe recomendar à SES/DF que implemente regras/políticas de controle de acesso ao Sistema SIS/Trakcare visando a abarcar todas as unidades de saúde a serem definidas e formalmente estabelecidas pelo gestor da informação, em especial a atribuição de perfis de acesso, à luz dos controles A.9.1.1 – Política de Controle de Acesso.

13. Propõe recomendar, ainda, a gestão de acessos e autorizações ao sistema de prontuário eletrônico, com validação periódica de cadastros por parte dos titulares das unidades administrativas, de forma a inibir a possibilidade de acesso não autorizado por ex-servidores ou servidores afastados da jurisdicionada, de acordo com o controle A.9.2.3 da ABNT NBR ISO/IEC 27001:2013; bem como a adoção de medidas necessárias para ativar o bloqueio do usuário por número máximo de tentativas sem acesso, de acordo com o controle A.9.2.6 da ABNT NBR ISO 27001:2013.

14. No **Achado 3** *(Certificado de Segurança do site com data de validade expirada)*, a Unidade Especializada, em apertada síntese, constata a expiração, desde 5/6/2019, da validade do Certificado de Segurança[8] do sítio eletrônico da SES; o que se agrava em razão de o *site* utilizar um sistema de autenticação básica[9] (nome de usuário/senha), de fácil reprodução/clonagem por usuários mal-intencionados, ensejando risco potencial de ataque *phishing*[10] e perda de informações; porquanto o processo de autenticação da forma em que se encontra desenhado, aliado ao fato de o endereço do *site* apresentar alertas de segurança/conexão não confiável, poderá levar o usuário a uma página falsa/clonada criada com

---

A adoção de um SGSI é uma decisão estratégica para uma organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais, funcionários, tamanho e estrutura da organização.
O sistema de gestão da segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados.
É importante que um sistema de gestão da segurança da informação seja parte e esteja integrado com os processos da organização e com a estrutura de administração global e que a segurança da informação seja considerada no projeto dos processos, sistemas de informação e controles. É esperado que a implementação de um sistema de gestão de segurança da informação seja planejado de acordo com as necessidades da organização.

[8] Certificado de Segurança é uma ferramenta na qual uma autoridade certificadora (terceiro) valida a identidade do site/servidor, bem como fornece a chave criptográfica pública do site.
[9] No contexto de uma transação HTTP, a autenticação de acesso básico é um método para um agente de usuário HTTP (cliente) fornecer um nome de usuário e senha ao fazer uma requisição ao servidor (Wikpédia).
[10] é a tentativa fraudulenta de obter informações ou dados confidenciais, como nomes de usuário, senhas e detalhes de cartão de crédito, disfarçando-se como uma entidade confiável em uma comunicação eletrônica (Wikpédia).

o objetivo de obter informações sigilosas do *site* https://externo.saude.df.gov.br, que permite o acesso externo ao Sistema SIS/Trakcare via *internet*.

15. Diante disso, sugere recomendar à SES que restabeleça a data de validade do Certificado de Segurança do site de acesso externo ao sistema SIS/Trakcare, de forma a proteger a confidencialidade, a autenticidade e a integridade das informações, nos termos do controle A.10.1.2 – Gerenciamento de Chaves da ABNT NBR ISO/IEC 27001:2013.

16. Aventando a hipótese de que a situação possa ocorrer em outros órgãos e entidades do Distrito Federal propõe, ainda, recomendar ao Complexo Administrativo do Distrito Federal que mantenha válidos os Certificados de Segurança dos sites governamentais, de forma a proteger a confidencialidade, a autenticidade e a integridade das informações, nos termos do controle A.10.1.2 – Gerenciamento de Chaves da ABNT NBR ISO/IEC 27001:2013.

17. A partir do **Achado 4** *(Exposição de informações do Servidor Web da aplicação SIS/Trakcare: fingerprinting)*, a Instrução relata que o acesso externo, via servidor Web, ao Sistema de Prontuário Eletrônico – SIS/Trakcare pode deixá-lo vulnerável a ataques, notadamente quando versões antigas de *software* sem correções de segurança atualizadas *o torna suscetível a explorações específicas de versões conhecidas*.

18. Nesse sentido, registra que, a fim de avaliar a vulnerabilidade das informações do servidor de aplicação do SIS/Trakcare, executou requisição HTTP[11] via *browser*, que retornou evidências de que as informações sobre o servidor Web do SIS/Trakcare estão expostas, *vez que a cada requisição HTTP da aplicação essas informações são passadas no cabeçalho da resposta (quando se acessa o código-fonte da página no navegador via comando).*

19. Ressalta que tais informações podem ser usadas por pessoas mal-intencionadas com a finalidade de explorar a aplicação objetivando identificar os recursos computacionais e encontrar vulnerabilidades (controle A.12.6.1 – Controles de vulnerabilidades técnicas da ABNT NBR ISO/IEC 27001:2013).

[11] O protocolo HTTP faz a comunicação entre o cliente e o servidor por meio de mensagens. O cliente envia uma mensagem de requisição de um recurso e o servidor envia uma mensagem de resposta ao cliente com a solicitação. (...) Uma mensagem, tanto de requisição quanto de resposta, é composta, conforme definido na RFC 2616, por uma linha inicial, nenhuma ou mais linhas de cabeçalhos, uma linha em branco obrigatória finalizando o cabeçalho e por fim o corpo da mensagem, opcional em determinados casos (Wikipédia – https://pt.wikipedia.org/wiki/Hypertext_Transfer_Protocol.

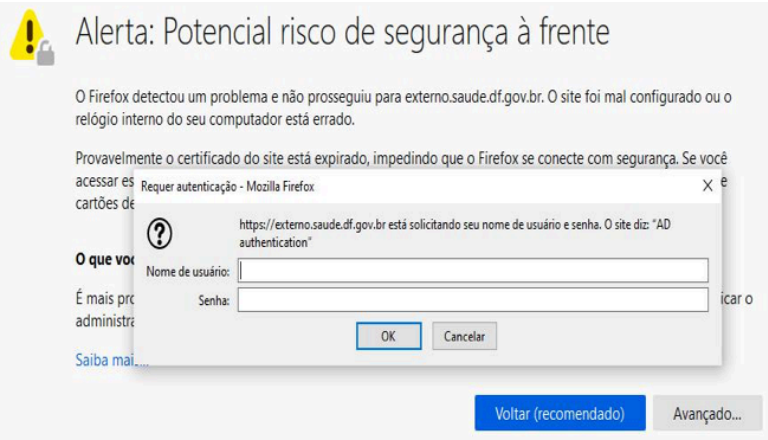
20. Adverte, ainda, que, consoante informação exibida a partir da exploração no *AD authentication*[12], verifica-se que a autenticação é realizada pelo *Active Directory*[13], o que pode propiciar o aparecimento de vulnerabilidades de injeção de comandos LDAP[14] na aplicação. Esclarece, *verbis*:

> 101. Registra-se que um ataque de injeção LDAP explora uma aplicação Web por meio da manipulação de parâmetros de entrada do usuário, a exemplo da autenticação básica, na qual o usuário digita nome e senha.
> 102. Neste caso, quando uma aplicação não consegue higienizar[15] corretamente a entrada de dados realizada pelo usuário, é possível que uma pessoa mal-intencionada tenha acesso aos serviços de diretório do sistema, por meio da inserção de comandos/instruções LDAP no parâmetro de entrada da aplicação.
> 103. Da mesma forma, podem ocorrer injeções de comando SQL que resultam em acessos indevidos, modificações não autorizadas e vazamentos de dados.

21. Assim, diante do potencial risco de ataques por meio de comandos LDAP/SQL, acessos indevidos, modificações não autorizadas e vazamento de dados, a Unidade Técnica propõe recomendar à SES que implemente ações técnicas que impeçam a exposição de informações do servidor Web da aplicação SIS/Trakcare; estendendo a recomendação aos

---

12



[13] O Active Directory é uma implementação de serviço de diretório no protocolo LDAP. (...) O Active Directory é um conjunto de arquivos localizados no servidor de domínio, no qual estão todas as informações que permitem controlar o acesso dos usuários à rede. Nele ficam registrados os nomes e senhas de usuários, suas permissões de acesso a arquivos, impressoras e outros recursos da rede, as cotas de disco, os computadores e horários que cada usuário pode utilizar, etc (Wikipédia).

[14] Lightweight Directory Access Protocol, ou LDAP, é um protocolo de aplicação aberto, livre de fornecedor e padrão de indústria para acessar e manter serviços de informação de diretório distribuído sobre uma rede de Protocolo da Internet (IP). Serviços de diretório desempenham um papel importante no desenvolvimento de aplicações intranet e Internet permitindo o compartilhamento de informações sobre usuários, sistemas, redes, serviços e aplicações através da rede (Wikipédia).

[15] A prática de higienizar a entrada de dados de uma aplicação é um procedimento para evitar a digitação de caracteres especiais, erros de digitação e falta de padronização que ocasionam a execução de comandos indesejados e acessos indevidos ao sistema, bem como base de dados com informações incorretas. Fonte: https://dbios.com.br/gestao-de-dados/higienizacao-de-dados-o-que-e-e-por-que-e-tao-importante/

demais órgãos e entidades do complexo administrativo do DF, no que toca às aplicações Web instaladas em seus sítios eletrônicos (controle A.12.6.1 – Controles de vulnerabilidades técnicas da ABNT NBR ISO/IEC 27001:2013).

22. Sugere, ainda, que a Corte recomende aos órgãos e entidades do complexo administrativo do DF a utilização de técnicas de prevenção para sanar possíveis vulnerabilidades de injeção por meio de comandos LDAP/SQL nas aplicações Web instaladas nos sites do Complexo Distrital, em conformidade com o controle A.12.6.1 – Controles de Vulnerabilidades Técnicas da ABNT NBR ISO/IEC 27001:2013.

23. Por meio do **Achado 5** *(Ausência de política e práticas de segurança da informação adequadas)*, a zelosa Instrução esclarece que a implementação da segurança da informação inclui, além dos sistemas de informação da organização, qualquer forma de informação armazenada que tenha valor para a organização ou para os indivíduos.

24. Salienta a preocupação com a segurança da informação levou à elaboração de diversos modelos e práticas internacionais consolidados *para proteção da informação e comumente considerados como as melhores práticas de mercado que objetivam a eficiência e melhor retorno dos investimentos e proteção às organizações*.

25. Registrando que o objetivo de um sistema de gestão de segurança é a preservação da confidencialidade, integridade e disponibilidade das informações; salienta que os sistemas de prontuário eletrônico da SES integram o escopo dos sistemas informatizados daquela Secretaria de Estado, razão pela qual devem estar inseridos na política de segurança da informação do órgão.

26. Nesse contexto, destaca que as manifestações da SES aos questionamentos formais da Inspeção indicam que os documentos destinados a viabilizar a política de segurança em torno dos sistemas de prontuário eletrônico não existem ou não são conhecidos; refletindo a *ausência de políticas e práticas de segurança de informação formalizadas*; o que dificulta a boa governança e a gestão da segurança da informação, potencializando riscos.

27. Como consequência da *ausência de uma Política de Segurança da Informação – PSI e da implementação de boas práticas de segurança*, o Corpo Técnico constata que a SES não possui servidor designado para identificar e analisar incidentes de segurança do Sistema de Prontuário Eletrônico.

28. No mesmo sentido, a Inspeção registra que a SES não tem conhecimento da existência de *classificação da informação com definição de níveis de sigilo*; circunstância que, a despeito de os sistemas de prontuário eletrônico sabidamente conterem dados sensíveis e sigilosos de pacientes, não permitem distingui-los; o que vai de encontro às recomendações ISO 27002 e COBIT 2019 (prática APO01.07[16]) e não possibilita estabelecer de forma adequada a relevância e a criticidade das informações sob sua guarda.

[16] APO01.07 Defina informações (dados) e propriedade do sistema - definir e manter responsabilidades pela propriedade da informação (dados) e sistemas de informação. Certifique-se de que os proprietários classificam as informações e os sistemas e os protegem de acordo com sua classificação. Resultados da prática: Diretrizes de classificação de dados, Diretrizes de segurança e controle de dados e Procedimentos de integridade de dados.

29. Reafirmando as fragilidades encontradas[17], destaca a necessidade de a Jurisdicionada adotar abordagem baseada em riscos para segurança da informação em conformidade com a ABNT NBR ISSO 27001, ISSO 27002, ISSO 27005 e ISSO 27014.

30. Salientando a inexistência de termo de responsabilidade para acesso ao sistema, evidencia que a Jurisdicionada não implementou política de autorização de acesso; o que não permite a cientificação de cada usuário acerca de suas atribuições e responsabilidades, bem como das potenciais ameaças que possam causar.

31. Registra que, a despeito da elevada criticidade do Sistema de Prontuário Eletrônico, o sistema utiliza a autenticação com um único fator, mediante senha *forte* de troca obrigatória; sem o uso de autenticação multifatorial para contas de acesso privilegiado (senha, PIN, frase/certificação digital, *token*, *smart card*/biomentria; o que representa baixo nível de segurança, impondo riscos de vazamento ou alteração de dados e vulnerabilidade que pode ser explorada por ameaças como *links* maliciosos encaminhados via e-mail e instalação de *malware*.

32. O diagnóstico técnico, ao fim, registra um baixo nível de maturidade da segurança da informação do sistema SIS/Trakcare e a existência de potencial risco de vazamento e alteração de dados do sistema, além da falta de orientação e capacitação de usuários internos e internos.

33. Desse modo, o Corpo Técnico sugere que a SES seja instada a elaborar, divulgar e utilizar Política de Segurança da Informação e, quando necessário, os normativos dela derivados (ex: procedimentos de Controle de Acesso Lógico e Físico, Cadastramento de Usuários etc.); conforme as boas práticas de segurança da informação (COBIT 5, ABNT ISO 27001:2013, ABNT ISO 27002:2013, ABNT ISO 27014:2013) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18).

34. Recomenda, ainda, que a Jurisdicionada adote medidas necessárias para melhorar a segurança do processo de identificação e acesso ao Sistema de Prontuário Eletrônico – SIS/Trakcare, de forma a assegurar níveis de risco aceitáveis, nos termos das normas ABNT NBR ISO 27001:2013 e ABNT ISO 27005:2019; além de proceder à classificação da

[17] 151. A jurisdicionada informa que não tem conhecimento da existência de classificação da informação (item 2.e, Nota nº 1) o que não permite estabelecer de forma adequada qual é a informação mais relevante e crítica para organização; também elenca sistemas que tratam de dados pessoais (item 2.b, Nota nº 1) e sistemas críticos (item 2.c, Nota nº 1), falta de controle para exclusão de acesso ao sistema, ausência de autenticação multifatorial para sistemas considerados críticos (item 2.l, Nota nº 1), ausência de acompanhamento de incidentes de segurança da informação (item 2.n, Nota nº 1) e ausência de documento com procedimentos de recuperação de sistemas (item 2.j, Nota nº 1).
152. Outro aspecto relevante é que o sistema em exame é acessado por meio da internet, que é um ambiente hostil46, o que se traduz na elevação dos riscos a que a SES/DF está exposta e, portanto, torna-se necessário reavaliações periódicas dos níveis de riscos e respectivas medidas de tratamento de riscos (ISO 27001 e ISO 27005).

informação para permitir a possibilidade de aplicar critérios de segurança com base nos ativos mais críticos e relevantes para SES/DF, nos termos da norma ABNT NBR ISO 27002:2013.

35. Além disso, sugere que a Corte recomende que a SES adote abordagem baseada em riscos para Segurança da Informação conforme estabelece a ISO 27001:2013, ISO 27002:2013, ISO 27005:2019 e ISO 27014:2013 e elabore e utilize termo, preferencialmente em formato digital, para cientificar os usuários do Sistema SIS/Trakcare quanto às suas responsabilidades e obrigações, bem como indicações de possíveis vulnerabilidades decorrentes do mal-uso dos sistemas, mantendo o registro de ciência dos usuários.

36. No **Achado 6** *(Ausência de barramento de dados nos sistemas de prontuário)*, a Instrução, ao passo em que registra o uso de 3 sistemas de prontuário eletrônico no Distrito Federal (SIS/Trakcare, para boa parte das unidades de saúde da Secretaria; Sistema SOUL-MV, utilizado pelas unidades de saúde geridas pelo IGES/DF; e o Sistema e-SUS AB, em uso pelas unidades de atenção básica de saúde), evidencia a ausência de barramento de dados[18] que permita integrar as informações dos sistemas existentes; impondo, desse modo, o isolamento dos dados.

37. Segundo o Corpo Técnico, as circunstâncias encontradas elevam o risco dos operadores da saúde no acompanhamento adequado da evolução dos pacientes e não garante o acesso aos dados de forma contínua.

38. Assim, a Instrução sugere recomendar à SES/DF que envide esforços para criação de barramento de dados único ou de uma solução técnica que integre as informações dos prontuários eletrônicos dos Sistemas SIS/Trakcare, SOUL-MV e e-SUS AB de forma a permitir disponibilização da informação consolidada de prontuários dos pacientes aos profissionais de saúde, conforme as boas práticas descritas no COBIT 2019 (DSS04 – Gerenciamento de Continuidade), ISO 27001:2013, ISO 27002:2013 e ISO 27005:2019.

39. Ao fim, a Divisão de Fiscalização de Tecnologia da Informação reúne as recomendações, *verbis*:

> I. recomendar à SES/DF que:
> a) adote as medidas pertinentes para estabelecer a regular fiscalização contratual, relativa à disponibilização de informações dos trabalhadores da contratada que prestam serviços de manutenção/suporte do Sistema SIS/Trakcare e a elaboração de relatório de atividades mensais contemplando as seguintes informações: identificador

[18] 182. O barramento de dados permitiria que um profissional de saúde pudesse obter as informações do paciente de forma transparente, como se o sistema de prontuário eletrônico fosse um só, permitindo que o profissional de saúde da SES/DF fosse capaz de realizar o diagnóstico considerando o histórico de saúde do paciente. Desse modo, as informações que estão em mais de um sistema de prontuário eletrônico poderiam ser acessadas de forma única.
183. A ausência de barramento de dados para esses sistemas fragiliza a disponibilidade da informação. A título de exemplo, para se obter a informação de um paciente é necessário consultar até três sistemas, que podem estar ou não disponíveis no momento da demanda, dificultando assim a elaboração de um diagnóstico preciso, ou até a consulta do resultado de algum exame realizado.
184. Além disso, a falta de uma arquitetura de barramento de dados construída entre os sistemas de prontuários eletrônicos utilizados nas unidades de saúde do GDF torna dificultosa a produção de informações gerenciais que auxiliem a tomada de decisão na área de Saúde.

(nº sequencial), ordem de serviço vinculada à atividade, tipo do serviço realizado pela prestadora, severidade, status, descrição, tempo de execução (data da abertura e fechamento), perfil(s) profissional(i)s que realizou(aram) o serviço, tempo de execução, produtos/resultados esperados e o cumprimento ou não do acordo de nível de serviço estabelecido em contrato, para efeito de acompanhamento do Contrato nº 19/2018-SES/DF, de acordo com o art. 66 da Lei 8.666/93 e o item I.b do art. 19 da IN 04/2014-SLTI/MPOG (Achado 1);

b) implemente as seguintes medidas relacionadas ao gerenciamento e política de controle de acesso do Sistema SIS/Trakcare (Achado 2):

b.1) regras/políticas de controle que abarquem todas as unidades de saúde a serem definidas e formalmente estabelecidas pelo gestor da informação, em especial a atribuição de perfis de acesso, à luz dos controles A.9.1.1 - Política de Controle de Acesso;

b.2) gestão de acessos e autorizações ao sistema de prontuário eletrônico, com validação periódica de cadastros por parte dos titulares das unidades administrativas, de forma a inibir a possibilidade de acesso não autorizado por ex-servidor ou servidor afastado da jurisdicionada, de acordo com o controle A.9.2.3 da ABNT NBR ISO/IEC 27001:2013;

b.3) medidas necessárias para ativar o bloqueio do usuário por número máximo de tentativas sem acesso, de acordo com o controle A.9.2.6 da ABNT NBR ISO 27001:2013;

c) restabeleça a data de validade do Certificado de Segurança do site de acesso externo ao sistema SIS/Trakcare, de forma a proteger a confidencialidade, a autenticidade e a integridade das informações, nos termos do controle A.10.1.2 – Gerenciamento de Chaves da ABNT NBR ISO/IEC 27001:2013 (Achado 3);

d) implemente ações técnicas que não permitam a exposição de informações do servidor Web da aplicação SIS/Trakcare, vez que podem permitir que pessoas mal-intencionadas encontrem vulnerabilidades e exposições comuns, deixando o sistema vulnerável a ataques, nos termos do controle A.12.6.1 – Controles de Vulnerabilidades Técnicas da ABNT NBR ISO/IEC 27001:2013 (Achado 4);

e) implemente as seguintes medidas relacionadas às Políticas e Práticas de Segurança da Informação (Achado 5):

e.1) elabore, divulgue e utilize sua Política de Segurança da Informação e, quando necessário, os normativos dela derivados (ex: procedimentos de Controle de Acesso Lógico e Físico, Cadastramento de Usuários etc.), conforme recomenda as boas práticas de Segurança da Informação (COBIT 5, ABNT ISO 27001:2013, ABNT ISO 27002:2013, ABNT ISO 27014:2013) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18);

e.2) tome as medidas necessárias para melhorar a segurança do processo de identificação e acesso ao Sistema de Prontuário Eletrônico – SIS/Trakcare, de forma a assegurar níveis de risco aceitáveis, nos termos das normas ABNT NBR ISO 27001:2013 e ABNT ISO 27005:2019;

e.3) estabeleça classificação da informação para permitir a possibilidade de aplicar critérios de segurança com base nos ativos mais críticos e relevantes para SES/DF, nos termos da norma ABNT NBR ISO 27002:2013;

e.4) passe a adotar abordagem baseada em riscos para Segurança da Informação conforme estabelece a ISO 27001:2013, ISO 27002:2013, ISO 27005:2019 e ISSO 27014:2013;

e.5) elabore e faça uso de termo, preferencialmente em formato digital, que cientifique os usuários do Sistema SIS/Trakcare quanto às suas responsabilidades e obrigações, bem como indicações de possíveis vulnerabilidades decorrentes do mal-uso dos sistemas, mantendo o registro da ciência pelos usuários;

> f) envide esforços para criação de barramento de dados único ou de uma solução técnica que integre as informações dos prontuários eletrônicos dos Sistemas SIS/Trakcare, SOUL-MV e e-SUS AB de forma a permitir disponibilização da informação consolidada de prontuários dos pacientes aos profissionais de saúde, conforme as boas práticas descritas no COBIT 2019 (DSS04 – Gerenciamento de Continuidade), ISO 27001:2013, ISO 27002:2013 e ISO 27005:2019 (Achado 6);
> II. recomendar ao Complexo Administrativo do Distrito Federal que:
> a) mantenha válidos os Certificados de Segurança dos sites governamentais, de forma a proteger a confidencialidade, a autenticidade e a integridade das informações, nos termos do controle A.10.1.2 – Gerenciamento de Chaves da ABNT NBR ISO/IEC 27001:2013;
> b) implemente ações técnicas que não permitam a exposição de informações das aplicações instaladas nos servidores Web (sites governamentais), vez que podem permitir que pessoas mal-intencionadas encontrem vulnerabilidades e exposições comuns, deixando o sistema vulnerável a ataques, nos termos do controle A.12.6.1 – Controles de Vulnerabilidades Técnicas da ABNT NBR ISO/IEC 27001:2013;
> c) utilize técnicas de prevenção para sanar possíveis vulnerabilidades de injeção por meio de comandos LDAP/SQL nas aplicações Web instaladas nos sites governamentais, em conformidade com o controle A.12.6.1 – Controles de Vulnerabilidades Técnicas da ABNT NBR ISO/IEC 27001:2013.
> III. autorizar:
> a) o envio do Relatório Final de Inspeção, do Voto Condutor e da Decisão que vier a ser proferida à SES/DF e ao Complexo Administrativo Distrital, para subsidiar a adoção das medidas acima mencionadas;
> b) o retorno dos autos à SESPE, para os devidos fins.

40. É o que basta a relatar.

41. Passo à análise do presente feito, informando, preliminarmente, que atuo nos autos em substituição, consoante o disposto na Lei n.º 13.024/2014, na Resolução n.º 304/2017, no Ato Normativo n.º 1/2015-MPC e na r. Decisão Administrativa n.º 46/2017-TCDF.

42. Preliminarmente, o Ministério Público de Contas constata a celebração, em 14/4/2021, do Terceiro Termo Aditivo ao Contrato, no valor de 5.679.388,26, já considerando o reajuste contratual no percentual de 5,20% (IPCA acumulado) e vigência de 12 meses. (DODF n.º 74, de 22/4/2021, p. 29).

43. Quanto ao aspecto envolvendo a falha de controle da Jurisdicionada sobre os serviços prestados pelos prepostos da contratada e a possibilidade de responsabilização subsidiária do Distrito Federal na forma da Súmula 331/TST; o MPCDF, no mérito, está de acordo com a sugestão do Corpo Técnico e com a necessidade de estabelecer a efetiva fiscalização contratual, relativa à disponibilização de informações dos trabalhadores da contratada que prestam serviços de manutenção/suporte do Sistema SIS/Trakcare e a elaboração de relatórios de atividades mensais.

44. Remansosa a Jurisprudência do TCU quanto ao tema:

> Após pronunciamento do STF na Ação Declaratória de Constitucionalidade (ADC) 16, a nova redação da Súmula TST 331 implica responsabilidade subsidiária da Administração pelos débitos trabalhistas na terceirização no setor público, em razão

da inobservância do dever legal de fiscalização sobre a empresa contratada (culpa in vigilando) . (Acórdão 1521/2016-Plenário | Relator: BENJAMIN ZYMLER)

45. No entanto, o MPCDF entende que a sugestão deve ser posta em termos de determinação, ao esteio do art. 66 da Lei n.º 8.666/1993 c/c art. 19, I, "b", da Instrução Normativa n.º 4/2014 (recepcionada na forma do Decreto n.º 37.667/2016).

46. Dito isso, considero preocupantes as constatações do Corpo Técnico envolvendo as vulnerabilidades do módulo de prontuário eletrônico do paciente – PEP[19] do Sistema Integrado de Saúde – SIS, que agrega dados e informações sensíveis de pacientes atendidos pela rede pública de saúde.

47. As falhas apontadas pela Divisão de Fiscalização de Tecnologia da Informação da Corte, além de evidenciarem a precariedade das medidas de segurança e integração de dados e informações no âmbito da SES, em detrimento do exercício eficiente dos serviços públicos que presta aquele órgão no desempenho de sua atividade fim; patenteia o descaso com o tratamento de dados sensíveis[20] sob sua cura; o que, no entendimento do Ministério Público de Contas, sob ambos os enfoques, deve ser repelido pela Corte.

48. Não há dúvidas de que a agilidade e a eficiência do atendimento médico, em muito dependem dos dados e informações de prontuário disponíveis ao profissional de saúde, notadamente em um ambiente de disseminação mundial de uma nova doença, como o que é imposto, atualmente, pela COVID-19.

49. De sorte que a Jurisdicionada, especialmente neste momento, deve privilegiar a fidedignidade, a segurança e a integração da informação registrada e disponível, notadamente quando o custo do sistema eletrônico que contrata, por *inexigibilidade de licitação*, há mais de uma década, para – em conjunto com os demais sistemas utilizados, viabilizar tais fins, suplantou – de 2009 a 2019 – a cifra dos R$ 82.000.000,00[21].

50. De outro lado, sabe-se que a Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados), cuja vigência iniciou no último dia 3 de maio, dá particular atenção ao *tratamento*[22] e

---

[19] O repositório com informações clínicas dos pacientes atendidos pela Rede de Saúde Pública do DF surgiu com a aquisição do Sistema Integrado de Saúde do DF (Trakcare) e subsequente implantação do Prontuário Eletrônico do Paciente - PEP. Dessa forma, seria possível o compartilhamento de registros clínicos entre todas as Unidades de Saúde no DF. (fonte: Relatório de Auditoria Operacional n.º 3/2020 – DIATI/COLES/SUBCI/CGDF (Processo n.º 00480-00002953/2020-91-e).

[20] Art. 5º Para os fins desta Lei, considera-se:
[...]
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (Lei n.º 13.709/2018).

[21] Fonte: Relatório de Auditoria Operacional n.º 3/2020 – DIATI/COLES/SUBCI/CGDF (Processo n.º 00480-00002953/2020-91-e).

[22] Art. 5º Para os fins desta Lei, considera-se:
[...]

à segurança dados sensíveis, em especial àqueles referentes à *saúde*, impondo aos denominados *agentes de tratamento*[23] a adoção de medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito; conforme dispõem expressamente os artigos 46 e 47 da aludida norma[24].

51. Na mesma linha, o art. 49 da Lei 13.709/2018[25] exige que os sistemas utilizados para o *tratamento* de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na Lei e demais normas regulamentares; o que, no entendimento do *Parquet* de Contas, na ausência da formulação de regras de boas práticas e de governança específicas a que alude o art. 50 da Lei[26], torna necessária e obrigatória a utilização, pela Secretaria de Estado de Saúde, das boas práticas, modelos paradigmáticos e normas técnicas referenciadas na Inspeção; sob pena de responsabilidade na forma da lei, o que, nesse caso, poderá impingir danos ao Distrito Federal.

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

[23] Art. 5º Para os fins desta Lei, considera-se:
[...]
VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
[...]
IX - agentes de tratamento: o controlador e o operador;

[24] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
[...]
§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.
Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.
[25] Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.
[26] Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Ministério Público de Contas do Distrito Federal
Terceira Procuradoria

52. Quanto a isso, importante alertar que o art. 42 da Lei n.º 13.709/2018[27] estabelece que o *controlador* ou o *operador* (*agentes de tratamento*), em razão do exercício da atividade de *tratamento* de dados pessoais, que causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, fica obrigado a repará-lo.

53. Em igual sentido, o art. 52 da Lei[28] impõe sanções administrativas aos *agentes de tratamento* de dados por infrações à norma geral.

54. Por fim, digno de registro e espécie, ademais, o alegado desconhecimento, pela Secretaria de Estado de Saúde, acerca da existência de classificação de informação com definição de níveis de sigilo, conforme deslinda o Corpo Técnico.

55. É que a Lei n.º 12.527/2011 (Lei de Acesso à Informação), editada há uma década, e destinada a assegurar e concretizar o direito fundamental de acesso à informação, impõe ao Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus

---

[27] Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:
I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
[...]
Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

[28] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
[...]
I - advertência, com indicação de prazo para adoção de medidas corretivas;
II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III - multa diária, observado o limite total a que se refere o inciso II;
IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI - eliminação dos dados pessoais a que se refere a infração;
[...]
X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

órgãos e entidades, assegurando a sua proteção[29] e estabelece que as autoridades públicas adotarão as providências necessárias para que o pessoal a elas subordinado hierarquicamente conheça as normas e observe as medidas e procedimentos de segurança para tratamento de informações sigilosas[30].

56. No mesmo sentido e idêntica redação, os artigos 27 e 28 da Lei distrital n.º 4.990/2012. Já os artigos 32 e 33 da aludida norma expressamente estabelecem, *verbis*:

> Art. 32. A autoridade máxima de cada órgão ou entidade deve publicar, anualmente, em seu sítio oficial na Rede Mundial de Computadores, os seguintes dados e informações administrativas, nos termos do regulamento:
> I – rol das informações que tenham sido desclassificadas nos últimos doze meses;
> II – rol de documentos classificados em cada grau de sigilo, com identificação para referência futura;
> III – relatório estatístico contendo a quantidade de pedidos de informação recebidos, atendidos e indeferidos, bem como informações genéricas sobre os solicitantes.
> § 1º Os órgãos e as entidades devem manter exemplar da publicação prevista no caput para consulta pública em suas sedes.
> § 2º Os órgãos e as entidades devem manter extrato com a lista de informações classificadas, acompanhadas da data, do grau de sigilo e dos fundamentos da classificação.
> Art. 33. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, à vida privada, à honra e à imagem das pessoas, bem como às liberdades e às garantias individuais.
> § 1º Às informações pessoais de que trata este artigo, aplica-se o seguinte:
> I – seu acesso é restrito, independentemente de classificação de sigilo e pelo prazo de cem anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se refiram;
> [...]
> § 2º Aquele que obtiver acesso às informações de que trata este artigo responderá por seu uso indevido. (destaquei).

57. Em regulamentação, o tema é tratado em detalhes pelo Decreto n.º 34.276/2013, a partir do artigo 25. Já o Decreto n.º 35.382/2014 regulamenta especificamente o art. 42 da Lei n.º 4.990/2012 e, em seu art. 46, estabelece:

> Art. 46. No tratamento da informação classificada deverão ser utilizados sistemas de informação e canais de comunicação seguros que atendam aos padrões mínimos de qualidade e segurança definidos pelo Poder Executivo.
> § 1º A transmissão de documento controlado por meio de sistemas de informação deverá ser realizada, no âmbito da rede corporativa, por meio de canal seguro, como forma de mitigar o risco de quebra de segurança.
> § 2º A autenticidade da identidade do usuário da rede deverá ser garantida, no mínimo, pelo uso de certificado digital.
> § 3º Os sistemas de informação de que trata o caput deverão ter níveis diversos de controle de acesso e utilizar recursos criptográficos adequados aos respectivos graus de sigilo.

[29] Art. 25.
[30] Art. 26.

> § 4º Os sistemas de informação de que trata o caput deverão manter controle e registro dos acessos autorizados e não autorizados e das transações realizadas por prazo igual ou superior ao de restrição de acesso à informação.

58. De modo que, à exortação para classificação da informação, na forma proposta pelo Corpo Técnico, entendo devam ser agregadas as normas de cumprimento compulsório de esteio.

59. Assim, embora aquiescendo com as sugestões relacionadas pelo Corpo Técnico, entendo que, para a Secretaria de Estado de Saúde, órgão ao qual foi particularmente dirigida a atividade de Inspeção e onde restaram efetivamente constatadas as falhas graves, as proposições devem ser dirigidas em forma de *determinação*, com acréscimo dos fundamentos legais que agrego; mantendo-se as *recomendações* voltadas ao Complexo Administrativo do Distrito Federal.

60. Importante ainda anotar que a Controladoria Geral do Distrito Federal, no final do exercício de 2019, realizou atividade de fiscalização objetivando examinar aspectos funcionais inerentes aos módulos administrativos e clínicos do Sistema Unificado de Informações de Saúde (SIS/Trakcare), responsáveis pelo registro eletrônico dos pacientes; envolvendo, portanto, semelhante objeto e o mesmo contrato[31]; mas com enfoque direcionado à eficácia e à efetividade operacional do sistema.

61. O Relatório de Auditoria Operacional n.º 3/2020 – DIATI/COLES/SUBCI/CGDF, no e. Tribunal, encontra-se encartado no Processo n.º 00480-00002953/2020-91-e, e aguarda exame da e. Corte. O substancioso exame do Órgão de Controle Interno do Distrito Federal corrobora diversos pontos registrados na Inspeção sob exame e traz em conclusão, *verbis*:

> Apesar do significativo valor desembolsado à contratada até o final de 2019, o Sistema TrakCare ainda está longe de atender, efetivamente, aos seus usuários, bem como à população do DF. Dentre os problemas identificados, foi verificada a ausência de integração com outros sistemas informatizados da Rede de Saúde, bem como a falta de padronização de suas funções e telas em diferentes Unidades Médicas. Além disso, não há o compartilhamento de registros clínicos dos pacientes entre todas as Unidades de Saúde no DF. Foi constatado, também, que vários usuários desconfiam da veracidade dos relatórios gerenciais fornecidos e, por isso, os analisam com certa desconfiança. Evidenciou-se que a SES/DF não possui um programa de treinamento continuado do TrakCare.
>
> Ademais, foram identificadas falhas em suas regras de negócio, a exemplo da possibilidade de encerramento de atendimentos médicos sem que os mesmos sejam adequadamente registrados. Ainda, boa parte das regras de recuperação de procedimentos médicos, para fins de faturamento, permanecem latentes, tendo em vista a deficiência de capacitação nos módulos do Sistema, bem como a ausência de documentação atualizada. Evidenciou-se, também, que durante o processo de faturamento, uma quantidade significativa de procedimentos médicos realizados pelo SUS é glosada, em razão do descompasso entre os dados (CNES e SIGTAP) do Ministério da Saúde e o Sistema TrakCare. (destaquei).

[31] Contrato n.º 19/2018 – SES/Intersystems.

62. Em face do exposto, no mérito, de acordo com a zelosa Instrução e com os ajustes que propõe, aquiescendo com as sugestões registradas; o Ministério Público de Contas sugere à Corte que, tomando conhecimento dos documentos agregados:

I – determine à Secretaria de Estado de Saúde que adote as medidas pertinentes para estabelecer a regular fiscalização contratual, relativa à disponibilização de informações dos trabalhadores da contratada que prestam serviços de manutenção/suporte do Sistema SIS/Trakcare e a elaboração de relatório de atividades mensais contemplando as seguintes informações: identificador (nº sequencial), ordem de serviço vinculada à atividade, tipo do serviço realizado pela prestadora, severidade, status, descrição, tempo de execução (data da abertura e fechamento), perfil(s) profissional(i)s que realizou(aram) o serviço, tempo de execução, produtos/resultados esperados e o cumprimento ou não do acordo de nível de serviço estabelecido em contrato, para efeito de acompanhamento do Contrato nº 19/2018-SES/DF, de acordo com o art. 66 da Lei 8.666/93 e do art. 19, I, "b", da IN 04/2014-SLTI/MPOG (Achado 1);

II – determine, ainda, à Secretaria de Estado de Saúde que, em estrita observância à Lei n.º 13.709/2018[32], adote medidas de segurança, técnicas e administrativas necessárias à proteção dos dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito e, em especial:

a) implemente as seguintes medidas relacionadas ao gerenciamento e política de controle de acesso do Sistema SIS/Trakcare (Achado 2):

a.1) regras/políticas de controle que abarquem todas as unidades de saúde a serem definidas e formalmente estabelecidas pelo gestor da informação, em especial a atribuição de perfis de acesso, à luz dos controles A.9.1.1 - Política de Controle de Acesso;

a.2) gestão de acessos e autorizações ao sistema de prontuário eletrônico, com validação periódica de cadastros por parte dos titulares das unidades administrativas, de forma a inibir a possibilidade de acesso não autorizado por ex-servidor ou servidor afastado da jurisdicionada, de acordo com o controle A.9.2.3 da ABNT NBR ISO/IEC 27001:2013;

a.3) medidas necessárias para ativar o bloqueio do usuário por número máximo de tentativas sem acesso, de acordo com o controle A.9.2.6 da ABNT NBR ISO 27001:2013;

b) restabeleça a data de validade do Certificado de Segurança do site de acesso externo ao sistema SIS/Trakcare, de forma a proteger a confidencialidade, a autenticidade e a integridade das informações, nos termos do controle A.10.1.2 – Gerenciamento de Chaves da ABNT NBR ISO/IEC 27001:2013 (Achado 3);

c) implemente ações técnicas que não permitam a exposição de informações do servidor Web da aplicação SIS/Trakcare, vez que podem permitir que pessoas mal-intencionadas encontrem vulnerabilidades e exposições comuns, deixando o sistema vulnerável

[32] Vigência integral a partir de 3 de maio de 2021.

a ataques, nos termos do controle A.12.6.1 – Controles de Vulnerabilidades Técnicas da ABNT NBR ISO/IEC 27001:2013 (Achado 4);

d) implemente as seguintes medidas relacionadas às Políticas e Práticas de Segurança da Informação (Achado 5):

d.1) elabore, divulgue e utilize sua Política de Segurança da Informação e, quando necessário, os normativos dela derivados (ex: procedimentos de Controle de Acesso Lógico e Físico, Cadastramento de Usuários etc.), conforme recomenda as boas práticas de Segurança da Informação (COBIT 5, ABNT ISO 27001:2013, ABNT ISO 27002:2013, ABNT ISO 27014:2013) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18);

d.2) tome as medidas necessárias para melhorar a segurança do processo de identificação e acesso ao Sistema de Prontuário Eletrônico – SIS/Trakcare, de forma a assegurar níveis de risco aceitáveis, nos termos das normas ABNT NBR ISO 27001:2013 e ABNT ISO 27005:2019;

d.3) nos termos da Lei n.º 4.990/2012 e normas regulamentares de esteio, estabeleça classificação da informação para permitir a possibilidade de aplicar critérios de segurança com base nos ativos mais críticos e relevantes para SES/DF, observada a norma ABNT NBR ISO 27002:2013;

d.4) passe a adotar abordagem baseada em riscos para Segurança da Informação conforme estabelece a ISO 27001:2013, ISO 27002:2013, ISO 27005:2019 e ISSO 27014:2013;

d.5) elabore e faça uso de termo, preferencialmente em formato digital, que cientifique os usuários do Sistema SIS/Trakcare quanto às suas responsabilidades e obrigações, bem como indicações de possíveis vulnerabilidades decorrentes do mal-uso dos sistemas, mantendo o registro da ciência pelos usuários;

e) envide esforços para criação de barramento de dados único ou de uma solução técnica que integre as informações dos prontuários eletrônicos dos Sistemas SIS/Trakcare, SOUL-MV e e-SUS AB de forma a permitir disponibilização da informação consolidada de prontuários dos pacientes aos profissionais de saúde, conforme as boas práticas descritas no COBIT 2019 (DSS04 – Gerenciamento de Continuidade), ISO 27001:2013, ISO 27002:2013 e ISO 27005:2019 (Achado 6);

II – recomende ao Complexo Administrativo do Distrito Federal que:

a) mantenha válidos os Certificados de Segurança dos sites governamentais, de forma a proteger a confidencialidade, a autenticidade e a integridade das informações, nos termos do controle A.10.1.2 – Gerenciamento de Chaves da ABNT NBR ISO/IEC 27001:2013;

b) implemente ações técnicas que não permitam a exposição de informações das aplicações instaladas nos servidores Web (sites governamentais), vez que podem permitir que pessoas mal-intencionadas encontrem vulnerabilidades e exposições comuns, deixando o sistema vulnerável a ataques, nos termos do controle A.12.6.1 – Controles de Vulnerabilidades Técnicas da ABNT NBR ISO/IEC 27001:2013;

Ministério Público de Contas do Distrito Federal
Terceira Procuradoria

c) utilize técnicas de prevenção para sanar possíveis vulnerabilidades de injeção por meio de comandos LDAP/SQL nas aplicações Web instaladas nos sites governamentais, em conformidade com o controle A.12.6.1 – Controles de Vulnerabilidades Técnicas da ABNT NBR ISO/IEC 27001:2013.

III – autorize:

a) o envio do Relatório Final de Inspeção, do Voto Condutor e da Decisão que vier a ser proferida à SES/DF e ao Complexo Administrativo Distrital, para subsidiar a adoção das medidas acima mencionadas; e

b) o retorno dos autos à SESPE, para os devidos fins.

É o parecer.

Brasília, 27 de maio de 2021.

Demóstenes Tres Albuquerque
Procurador em substituição