AUDITORIA DE CONFORMIDADE NO **SISTEMA DE REGULAÇÃO DE LEITOS DO ESTADO DO RIO GRANDE DO NORTE - REGULA RN**

NATAL/RN
2024

TCE RN
TRIBUNAL DE CONTAS DO ESTADO

SECEX
SECRETARIA DE CONTROLE EXTERNO

RELATÓRIO

Auditoria de conformidade no Sistema de Regulação de Leitos do Estado do Rio Grande do Norte - Regula RN

Natal/RN
2024

Relatório de auditoria de conformidade no Sistema de Regulação de Leitos do Estado do Rio Grande do Norte - Regula RN

ATO ORIGINÁRIO	Plano de Fiscalização Anual 2023-2024; Decisão n. 478/2023-TC; Processo n° 000736/2023-TC; Plano de Fiscalização Anual 2024-2025; Decisão n. 18/2024-TC; Processo n° 001343/2024-TC; ID 4.00.2023.092.000
ATO DE DESIGNAÇÃO	Portaria nº 006/2024 – SECEX/TCE/musRN, publicada no Diário Eletrônico do dia 10 de maio de 2024; Portaria nº 070/2024 – SECEX/TCE/RN, publicada no Diário Eletrônico do dia 31 de julho de 2024.
UNIDADE JURISDICIONADA	Secretaria de Estado da Saúde Pública - SESAP
OBJETO DA FISCALIZAÇÃO	Sistema de Regulação de Leitos do Estado do Rio Grande do Norte - Regula RN
OBJETIVO DA FISCALIZAÇÃO	Avaliar os controles e procedimentos relacionados ao Sistema de Regulação da Saúde, considerado como relevante/crítico para a Administração Pública Estadual, com ênfase em aspectos de segurança da informação e aderência às normas.
ÁREA TEMÁTICA	SAÚDE; TECNOLOGIA DA INFORMAÇÃO.
PERÍODO DE ABRANGÊNCIA	19/04/2024 - 30/08/2024
EQUIPE	
Membros	Eduardo Pereira Lima, Auditor de Controle Externo, Matrícula 9.874-4.
Coordenador	Alexandre Luiz Galvão Damasceno, Auditor de Controle Externo, 9.988-0.
Supervisor	Evandro Nunes Franco, Auditor de Controle Externo, Mat. 9.962-7.
Gestor da Unidade Técnica	Marcelo Santos de Araújo, Auditor de Controle Externo, 9.908-2.

RESUMO

A Secretaria de Estado da Saúde Pública do Rio Grande do Norte (SESAP) possui um sistema de regulação, baseado em protocolo de regulação de leitos, criado para efetivar as normas sobre as Políticas Nacionais de Saúde e resoluções do Conselho Federal de Medicina que definem os critérios de admissão e alta em Unidade de Terapia Intensiva (UTI). Este sistema de regulação está funcionando através do uso de uma plataforma eletrônica denominada “Regula RN”, desenvolvida por meio de um projeto patrocinado pela SESAP e executado pelo Laboratório de Inovação Tecnológica em Saúde (LAIS).

Estão sob o controle da referida ferramenta a regulação dos leitos de UTI adultos, pediátrica, neonatal e cuidados vasculares de urgência.

O uso de um sistema de informação para automatizar e controlar o processo de regulação com base em um protocolo bem definido é bastante benéfico e salutar para a sociedade, podendo gerar economia em larga escala, informações e dados estatísticos de extrema utilidade para a governança da administração pública de saúde, além de garantir de forma mais efetiva o controle, evitando erros e desvios. Mas, para que isso seja possível, faz-se necessário que o sistema funcione de forma adequada, seguindo rigorosamente os protocolos de regulação da SESAP em um ambiente seguro e confiável.

Considerando isso, esta ação teve como objetivo avaliar os controles e procedimentos relacionados ao “Regula RN’, considerado como relevante/crítico para a Administração Pública Estadual por estar sendo usado como principal ferramenta de regulação dos leitos públicos de UTI do Estado.

Para ter uma garantia mínima de que o sistema foi desenvolvido de forma adequada, ou seja, de que o sistema automatizou os protocolos de regulação de forma correta, foi necessário validá-lo com base nos protocolos e verificar se estava sendo realmente usado pelas unidades de regulação. Para ter uma garantia mínima de que o sistema funciona corretamente foi necessário fazer uma validação do ambiente no qual o sistema opera sob o aspecto de segurança da informação.

Assim, as questões de auditoria trabalhadas pela equipe de auditores buscaram obter respostas para as seguintes perguntas: O sistema “Regula RN” e a forma como este é usado pelos seus usuários seguem os protocolos de regulação definidos pela SESAP? O sistema “Regula RN” opera com um grau de segurança adequado que garanta a consistência das regras de negócio, a disponibilidade do serviço e a sustentabilidade de sua operação?

O presente trabalho foi conduzido com observância aos princípios e padrões estabelecidos pelo Tribunal de Contas do Estado do Rio Grande do Norte e em conformidade com as Normas de Auditoria do Setor Público – NBASP, adotadas por meio da Resolução nº 010/2020-TCE.

Esta ação possui como benefícios estimados a informação sobre o estado atual do sistema considerando as questões levantadas, a avaliação do sistema sob a ótica da conformidade perante os protocolos de regulação e os pontos de ajustes ou de atenção necessários para a manutenção e o funcionamento correto da plataforma “Regula RN”.

Para realizar a avaliação pretendida, a equipe de auditoria usou das seguintes técnicas: coleta de informações através de entrevistas e questionários direcionados aos principais *stakeholders* (médicos reguladores, colaboradores da central de regulação, membros da TI da SESAP e membros do projeto no LAIS); visita *in loco* à central de regulação e a uma unidade de regulação para verificação através da observação e realização de entrevistas direcionadas; e uso efetivo do sistema para conferir a aderência de suas funcionalidades às regras dos protocolos de regulação.

Durante a fase de execução, a auditoria constatou que o sistema é de extrema importância para a sociedade potiguar, automatizando e melhorando de forma expressiva o serviço de regulação, além de servir como uma ferramenta de controle e geração de informações estratégicas para a atuação da SESAP. Além disso, foi possível verificar que o sistema foi desenvolvido de forma adequada aos protocolos de regulação. No entanto, a equipe de auditoria identificou pontos de fragilidade, considerando aspectos relacionados à segurança da informação, que devem ser trabalhados de forma urgente para que o serviço seja mantido de forma segura e com alta disponibilidade.

Por fim, para cada achado de auditoria foi sugerida a adoção de medidas que visam mitigar os riscos identificados que possam comprometer a segurança da informação no âmbito da plataforma eletrônica “Regula RN”, como: implantar procedimentos de segurança da informação para tratar incidentes; gerir dados pessoais sensíveis; capacitar usuários em procedimentos de segurança da informação; dotar o setor de Tecnologia da Informação da SESAP com a infraestrutura adequada para possibilitar a hospedagem da plataforma “Regula RN” em ambiente seguro, com alta disponibilidade e resiliente.

Sumário

GLOSSÁRIO

- **AND** - Acordos de Não Divulgação, instrumento jurídico que estabelece obrigações de sigilo e confidencialidade entre as partes envolvidas. Também conhecido como Termo de Sigilo e Confidencialidade ou NDA (Non Disclosure Agreement).
- **ANS**- Acordo de Nível de Serviço,contrato de terceirização e fornecedor de tecnologia que descreve um nível de serviço que um fornecedor promete oferecer ao cliente.
- **Backup** - Cópia de segurança de dados digitais, como arquivos, fotos, documentos e softwares, em um dispositivo ou sistema.
- **Ciberataque** - Ação intencional que visa invadir sistemas de computação e redes de informação, com o objetivo de prejudicar pessoas, empresas ou instituições.
- **FUNCERN** - Fundação de Apoio à Educação e ao Desenvolvimento Tecnológico
- **GDPR** – General Data Protection Regulation, lei europeia que estabelece regras para o tratamento de dados pessoais de cidadãos da União Europeia (UE). O GDPR entrou em vigor em maio de 2018, substituindo uma diretiva de 1995.
- **Github** - plataforma de desenvolvimento colaborativo que permite armazenar, compartilhar e gerenciar projetos de software.
- **IEC** - International Electrotechnical Commission, organização internacional que prepara e publica normas para tecnologias elétricas, eletrônicas e relacionadas.
- **ISO** - International Organization for Standardization, organização não-governamental que estabelece padrões para a padronização e normatização de sistemas.
- **LAIS** - Laboratório de Inovação Tecnológica em Saúde
- **NBR ISO/IEC** - Norma técnica brasileira que corresponde a normas internacionais desenvolvidas pela ISO (International Organization for Standardization) e pela IEC (International Electrotechnical Commission)
- **PCA** - Política de Controle de Acesso, conjunto de condições que define se um usuário tem acesso permitido ou negado a um recurso protegido.
- **Regula RN** - Sistema de Informação usado para a Regulação de Leitos Hospitalares da Secretaria de Saúde do Estado do RN
- **SESAP** - Secretaria de Estado da Saúde Pública do Rio Grande do Norte
- **SI** - Sistema de Informação, conjunto de componentes interligados que coletam, processam, armazenam e distribuem informações para apoiar a tomada de decisões e o controle de uma organização.
- **SUS** - Sistema Único de Saúde
- **TI** - Tecnologia da Informação
- **WhatsApp** - Aplicativo de mensagens instantâneas e chamadas de voz que permite enviar e receber diversos tipos de arquivos, como texto, fotos, vídeos, documentos, localização, entre outros.

1. INTRODUÇÃO

1.1. Deliberação que originou o trabalho

O Pleno do Tribunal de Contas do Estado do Rio Grande do Norte aprovou, nos termos prescritos na Resolução nº 017/2016–TCE, de 26 de julho de 2016, o Plano de Fiscalização Anual 2023-2024, por meio da Decisão n° 478/2023-TC, em sessão ordinária n° 00018ª, de 28 de março de 2023 - PLENO, fazendo constar a fase de planejamento da ação fiscalizatória destinada à realização de Auditoria de conformidade no Sistema de Regulação de Leitos do Estado do Rio Grande do Norte - Regula RN, identificada sob o n° ID 4.00.2023.092.000.

O prosseguimento da ação (fases de execução e relatório) se deu no Plano de Fiscalização Anual 2024-2025, aprovado por meio da Decisão n° 18/2024-TC, em sessão ordinária n° 00018ª, de 26 de março de 2024 - PLENO.

1.2. Visão geral do objeto

O Regula RN é uma plataforma eletrônica fruto de ação voluntária e colaborativa no enfrentamento à Covid-19 pela equipe de pesquisadores em Tecnologia da informação (TI) do LAIS (Laboratório de inovação tecnológica em saúde), em atendimento a uma demanda da Secretaria de Saúde Pública do Estado do Rio Grande do Norte, que necessitava de um sistema de regulação de leitos para a rede estadual de saúde, com o fito de otimizar o tempo de resposta do SUS para a utilização dos leitos ofertados no RN.

Finalizado o período pandêmico, a plataforma sofreu evoluções, passando a ter informações para regulação de leitos, linhas especializadas (ortopedia, vascular, pediatria, neonatal, psiquiatria, cardiologia, neurologia, infectologia, entre outras), exames de alta complexidade e procedimentos clínicos/cirúrgicos. Abrangendo serviços da rede SUS e privados contratualizados, cuja cobertura se dá em todas as regiões de saúde do RN.

A ferramenta se propõe a oferecer mais transparência, por meio da disponibilização de acesso à sala de situação pública à população, profissionais de saúde e gestores, integrantes da SESAP, pesquisadores e órgãos de fiscalização.

Além dos serviços oferecidos pela ferramenta já em funcionamento, a referida plataforma eletrônica está sendo ampliada para proporcionar um ambiente exclusivo para a gestão hospitalar, que deverá funcionar em toda a rede estadual em um futuro próximo.

1.3. Objetivo, escopo e questões de auditoria

Esta auditoria tem como principal objetivo avaliar os controles e procedimentos relacionados à Plataforma de Regulação do Acesso à Assistência em Saúde - Regula RN, considerada uma ferramenta eletrônica de alta relevância para a Administração Pública Estadual.

Neste trabalho foram enfatizados aspectos de Segurança da Informação e aderência às normas, considerando os protocolos vigentes de regulação de leitos e acesso aos cuidados vasculares, a seguir listados:

- Protocolo de Regulação para Acesso a Leitos de UTI Geral atualizado em 13 de setembro de 2021;
- Protocolo de Regulação para Acesso a Leitos Clínicos atualizado em 13 de setembro de 2021;
- Protocolo de Regulação para Acesso a Leitos em UTI Pediátrica atualizado em 14 de setembro de 2021;
- Protocolo de Regulação para Acesso a Leitos em UTI Neonatal atualizado em 14 de setembro de 2021; e
- Protocolo de Acesso aos Cuidados Vasculares de Urgência atualizado em 07 de fevereiro de 2022 (Portaria SEI Nº 174).

A necessidade de verificação desses protocolos fez com que essa validação formasse a lista das primeiras questões de auditorias.

Tratando-se de uma auditoria que envolve o uso de um sistema de informação, é sabido que existe o risco de, mesmo aderindo aos protocolos de forma correta, o sistema não garanta o seu efetivo funcionamento por razões de segurança da informação, tais como: manipulação de dados, corrompimento funcional do sistema, acessos indevidos, entre outros. Dessa forma, essa ação também expandiu seu escopo de análise para considerar os itens de segurança da informação que possam impactar no risco da quebra dos protocolos supracitados. Com o objetivo de aferir a segurança da informação que envolve esses aspectos, foi usada como base de validação a aderência a alguns itens da norma ISO 27001, próprios para este fim. Os itens identificados como mais relevantes para essas análises, tornando-se parte das questões de auditoria, foram:

- Se o sistema, seu ambiente de hospedagem e seu uso atendem às normas que prezam pela forma segura como os controles organizacionais estão implantados;
- Se a organização possui os cuidados relacionados aos controles de pessoas que possuem acesso ao sistema ou aos artefatos deste sistema;
- Se a organização trabalha processos de segurança relacionados aos controles físicos dos ativos de TI relacionados ao Regula RN;
- Se a instituição implementa Controles Tecnológicos visando aprimorar a Segurança da Informação que tange o sistema Regula RN.

1.4. Metodologia utilizada e limitações inerentes a auditoria

A presente auditoria foi conduzida com observância aos princípios e padrões estabelecidos pelo Tribunal de Contas do Estado do Rio Grande do Norte e em conformidade com as Normas Brasileiras de Auditoria do Setor Público – NBASP, adotadas por meio da

Resolução n° 010/2020-TCE. O referido arcabouço normativo foi consolidado convergindo com as Normas Internacionais de Auditoria das Entidades Fiscalizadoras Superiores, emitidas pela Organização Internacional de Entidades Fiscalizadoras Superiores – INTOSAI.

Tratando-se de uma auditoria de conformidade, conforme a NBASP 400, fica clara a necessidade de validar as funcionalidades do sistema com os requisitos necessários para tornar os protocolos de regulação de leitos próprios de forma automatizada. Também deve-se considerar a necessidade de verificar alguns quesitos de segurança da informação, para garantir um baixo risco nos processos e atores envolvidos no uso do sistema e seu ambiente de hospedagem. Para tornar isso possível, foram usados os métodos abaixo para coleta de informação, análise e verificação.

Objetivando coletar informações sobre o correto funcionamento das funcionalidades do sistema, a qualidade de seu funcionamento, a aceitabilidade do sistema por parte de seus usuários da SESAP e os procedimentos seguros adotados para a manutenção da integridade dos dados do sistema Regula-RN, foram realizadas entrevistas com três grupos de atores:

- usuários do sistema pertencentes ao quadro da Central de Regulação;
- usuários do sistema pertencentes ao Hospital Geral Dr. João Machado;
- colaboradores do LAIS responsáveis pelo desenvolvimento do sistema; e
- representantes da equipe de Tecnologia da Informação da SESAP.

As perguntas realizadas na entrevista foram direcionadas considerando as questões de auditoria. Todas as entrevistas foram gravadas com a devida autorização dos entrevistados, para servir como base de evidências.

1.4.1. Verificação do sistema através da manipulação de uma versão posta em ambiente próprio de homologação

A verificação da aderência da plataforma eletrônica Regula RN aos protocolos oficiais de regulação foi realizada por meio da utilização do sistema, pela equipe de auditoria, em um ambiente de testes disponibilizado pela equipe de desenvolvedores do LAIS. O referido ambiente foi disponibilizado contendo dados de *backup* do ambiente de produção.

Nesse ambiente foram realizadas simulações de regulação utilizando funcionalidades destinadas aos médicos reguladores, médicos dos hospitais com os leitos regulados e super-usuários do sistema.

1.4.2. Visitas técnicas aos dois ambientes de uso do sistema, considerando os perfis dos principais atores (usuários)

Por fim, com o objetivo de constatar, *in loco*, a utilização do sistema pelas unidades de regulação, tanto nos hospitais, como pela central de regulação, foram realizadas visitas técnicas nesses dois ambientes de uso do sistema. Além disso, foram coletadas informações que pudessem verificar se os usuários estavam cientes das responsabilidades perante o uso do sistema frente aos protocolos, a qualidade e a usabilidade do sistema, a

capacitação dos usuários no Regula RN e os itens de segurança da informação envolvidos nesse contexto.

1.4.3. Limitações

As restrições de tempo e quantidade de membros da equipe de auditoria alocada para esta ação limitou a amplitude das verificações, como: visita a apenas duas unidades de regulação; redução do escopo de verificação de itens de boas práticas de segurança da informação; e verificação de alguns itens por meio de coleta de informações declaradas em entrevistas.

Ademais, por se tratar da primeira auditoria de sistemas realizada pela equipe do TCE, foram necessários estudos que consumiram tempo e prolongaram a fase de planejamento.

1.5. Benefícios Estimados

É mister relatar o ganho qualitativo, quantitativo e efetivo no serviço de regulação de leitos prestado à população com o auxílio da plataforma eletrônica Regula RN. Houve redução de gastos proveniente da informatização deste serviço, além das demais contribuições periféricas fornecidas pela implantação da referida ferramenta. Pode-se, também, considerar os ganhos intrínsecos das informações coletadas e usadas em tomadas de decisões feitas pela SESAP nos níveis estratégicos, táticos e operacionais.

A consolidação do uso da ferramenta a tornou indispensável no processo de melhoria contínua da prestação do serviço público de regulação da saúde no Estado do Rio Grande do Norte. Sendo assim, a descontinuidade ou interrupção do uso do sistema, bem como o seu mau funcionamento pode representar perdas significativas à população.

Nesse contexto, estima-se que a presente ação fiscalizatória, focada na aderência da plataforma eletrônica aos protocolos de regulação, bem como nos aspectos de segurança da informação, proporcionará os seguintes benefícios qualitativos:

- Redução de risco de parada de serviços relevantes aos cidadãos;
- Adequação às normas de Segurança da Informação e, consequentemente, melhora na proteção de dados pessoais sensíveis;
- Aumento da confiança dos usuários no sistema;
- Aumento da cultura organizacional focada na segurança da informação;
- Redução de risco em ciberataques;
- Aumento na velocidade de respostas e incidentes de segurança da informação.

2. ACHADOS DE AUDITORIA

Nesta seção, serão apresentadas as irregularidades/impropriedades ou pontos de atenção que foram identificados ao longo da fase de execução da auditoria, e que precisam ser detalhados para demonstrar a visão real do objeto auditado. No detalhamento dos achados serão destacados os seguintes aspectos: título, situação encontrada, objetos nos quais o achado foi constatado, critério de auditoria, evidências que comprovem a existência do

achado, causas e efeitos da ocorrência do achado, conclusão da equipe a respeito do achado e a proposta de encaminhamento.

2.1. Da operação do sistema sem cobertura contratual

Todo sistema de informação, ao ser construído, passa por duas fases em seu ciclo de vida: a fase de projeto de construção, onde o sistema é projetado, codificado, testado e validado; e a fase de operação, quando o sistema é posto para ser usado de forma definitiva pelos seus usuários. Essas fases são bem distintas e necessitam de atividades e cuidados específicos.

Na fase de projeto de criação, as principais atividades e cuidados estão relacionados com a forma como os requisitos necessários ao negócio serão resolvidos pelo sistema (sendo estes requisitos funcionais ou não funcionais). Nessa fase, o sistema ou módulo do sistema não está em uso, mas sendo construído e validado. Essa fase se encerra quando o sistema é construído e entregue ao cliente.

Na fase de operação, as principais atividades e cuidados estão voltados para a sustentação do sistema de acordo com métricas esperadas de desempenho, de disponibilidade e de proteção aos dados, dentre outras. Nessa fase, espera-se que o serviço oferecido pelo sistema esteja disponível aos usuários, com dados protegidos e íntegros. Para tanto, há necessidade de se ter equipe responsável e dotada de conhecimentos especializados para executar essas atividades, bem como possuir infraestrutura tecnológica adequada. Normalmente, essa fase não possui um ciclo de vida pré definido, e dura enquanto o sistema encontrar-se em uso e manter o fluxo de negócio que se propôs automatizar.

Situação encontrada

Como já descrito na seção 1.2 deste relatório, o Regula RN foi concebido a partir de uma ação voluntária e colaborativa no enfrentamento à Covid-19 pela equipe de pesquisadores em Tecnologia da informação do LAIS, em atendimento a uma demanda da Secretaria de Saúde Pública do Estado do Rio Grande do Norte.

No decorrer dos anos, a plataforma sofreu evoluções, fruto da parceria da SESAP com o LAIS, e foi ganhando cada vez mais importância no aprimoramento dos serviços públicos de saúde prestados à população. No entanto, apesar da plataforma eletrônica ser atualmente a principal ferramenta utilizada nos hospitais e centrais de regulação do Estado, foi constatado pela equipe de auditoria que o contrato firmado entre a SESAP e a FUNCERN aborda o desenvolvimento da ferramenta, mas não contempla a manutenção da plataforma em ambiente de operação (produção).

A equipe de auditoria observou que o sistema foi posto em operação usando a infraestrutura tecnológica da Universidade Federal do Rio Grande do Norte (UFRN), e mantido pelos bolsistas do projeto. Esse cenário se mostra frágil e de alto risco de descontinuidade, pois não possui cobertura contratual que contemple a infraestrutura e os serviços necessários para manutenção do sistema em ambiente de operação, dependendo atualmente de

acordos extracontratuais entre a SESAP e o LAIS, não havendo, por exemplo, Acordo de Nível de Serviço (ANS) que estabeleça os padrões mínimos de qualidade dos serviços prestados de sustentação da plataforma eletrônica.

Apesar do sistema estar funcionando sem aparentes problemas de disponibilidade, desempenho e segurança, este cenário caracteriza-se como irregular, pois não há contrato que cubra o serviço prestado. Dessa forma, é possível afirmar que o "Regula RN" está operando e sendo mantido por uma instituição terceira, sem a devida formalização contratual com definições de responsabilidades e níveis mínimos de qualidade do serviço ofertado.

Objetos nos quais o achado foi constatado

Contrato n° 69/2021 (processo n° 00610004.003009/2020-15).

Evidências

- Entrevista feita com desenvolvedores do LAIS: https://drive.google.com/drive/folders/1UA33vGq97Eomo29LPJPQI_kGW07RSvgQ
- Afirmação feita em entrevista com a equipe de TI da SESAP: https://drive.google.com/drive/folders/1EI_ea553PLmYLohF4A45WdANPgF2phxg
- Inexistência no objeto do Contrato n° 69/2021 de previsão de serviço de manutenção do sistema em ambiente de operação.

Critérios

Artigo 60, parágrafo único, da Lei n° 8.666/1993.

Causa

A falta de um contrato próprio para a prestação de serviço de sustentação, hospedagem e suporte do sistema Regula RN entre o LAIS e a SESAP aparece como causa primária dessa situação encontrada, e causa secundária para diversas outras situações encontradas nesta ação.

Efeito

- Aumento do risco de interrupção e descontinuidade do sistema "Regula RN".

Proposta de encaminhamento

Recomenda-se que a SESAP adote providências no sentido de dotar a unidade responsável pela Tecnologia da Informação de infraestrutura necessária para suportar a hospedagem do

"Regula RN", ou adote os meios dispostos na Lei 14.133/2021 para viabilizar a contratação do serviço de hospedagem e sustentação do "Regula RN".

Recomenda-se que a SESAP avalie a possibilidade de realizar uma ação para preparar a sua infraestrutura de TI, bem como e sua equipe técnica, para assumir a hospedagem e sustentação da operação do sistema, elaborando urgentemente um plano de adaptação de infraestrutura, atendimento, segurança da informação e outro plano de encerramento de projeto, com procedimentos próprios para tratar os riscos envolvidos.

Benefícios esperados

Redução do risco de interrupção do serviço disponibilizado pelo Sistema Regula RN para a população, gerando queda na qualidade da prestação do serviço de regulação fornecido pela SESAP.

Regularização do contrato de prestação de serviço entre o LAIS e a SESAP para hospedagem e operação do sistema Regula RN.

Redução no risco de embates jurídicos sobre o uso do sistema Regula RN por parte de ambos os envolvidos.

Assegurar o compliance dos requisitos legais, estatutários, regulamentares e contratuais relacionados aos aspectos de segurança da informação da proteção de dados pessoais.

2.2. Da ausência de planejamento para continuidade da sustentação do sistema após término do contrato

Situação Encontrada

Como já foi descrito na seção anterior, atualmente o contrato firmado entre o LAIS e a SESAP para o desenvolvimento do projeto de construção do sistema Regula RN tem como escopo a construção do projeto. E este contrato está sendo usado como instrumento para manter o sistema operando e disponível para os locais de regulação do RN. Além da situação apresentada na seção anterior, foi verificado que o contrato trata dos exercícios para os anos de 2021, 2022, 2023 e 2024, estando o contrato vigente para ser encerrado no fim do ano de 2024. Apesar dos alertas emitidos pela equipe de TI da SESAP sobre a iminente finalização deste contrato, ainda não foram tomadas ações para iniciar o processo de renovação e regularização contratual ou transferência de tecnologia para absorção da operação do sistema em infraestrutura própria da SESAP ou em infraestrutura de nuvem contratada.

Objetos

Sistema Regula RN e Instrumento Contratual entre SESAP e LAIS que regem os termos do Projeto Regula RN.

Evidências

- Entrevista feita com desenvolvedores do LAIS: https://drive.google.com/drive/folders/1UA33vGq97Eomo29LPJPQI_kGW07RSvgQ
- Afirmação feita em entrevista com a equipe de TI da SESAP: https://drive.google.com/drive/folders/1EI_ea553PLmYLohF4A45WdANPgF2phxg
- Contrato entre SESAP e Fundação de Apoio à Educação e ao Desenvolvimento Tecnológico (FUNCERN): https://drive.google.com/drive/folders/16vu-iv3Wx0Qg8nQ66xB4LwxnyAd-xrPI

Critério

- NBR ISO/IEC 27001 versão 2022 (item 6.5)

Causa

Como já foi dito, a falta de um contrato próprio para a prestação de serviço de sustentação, hospedagem e suporte do sistema Regula RN entre o LAIS e a SESAP aparece como causa primária dessa situação encontrada, e causa secundária para diversas outras situações encontradas nesta ação. Além disso, o único contrato que mantém a equipe do LAIS desenvolvendo o projeto e, através deste, mantendo o sistema em operação está para se encerrar no ano de 2024.

Efeito

- Aumento considerável no risco de interrupção do sistema Regula RN para a sociedade;
- Aumento considerável no risco de problemas jurídicos quanto ao uso de um serviço de terceiros sem contrato próprio.
- Contratação emergencial de um serviço que, poderia ter seguido o planejamento natural sem a necessidade de realizar a contratação de forma emergencial, dado que já era sabido pela administração os prazos contratuais vigentes.

Proposta de encaminhamento

Além do já recomendado na seção anterior, recomenda-se que a SESAP inicie uma ação para avaliar a renovação contratual do projeto, ou uma ação para que a equipe técnica da SESAP avalie os impactos de redução ou parada do sistema, junto com os responsáveis pela regulação.

Também, recomenda-se que a SESAP elabore um plano de gestão e manutenção do serviço de regulação, sem o uso do Sistema Regula RN, para reduzir o impacto da parada do sistema atual.

Benefícios esperados

Redução do risco de interrupção do serviço disponibilizado pelo Sistema Regula RN para a população, gerando queda na qualidade da prestação do serviço de regulação fornecido pela SESAP.

Regularização do contrato de prestação de serviço entre o LAIS e a SESAP para hospedagem e operação do sistema Regula RN.

Redução no risco de embates jurídicos sobre o uso do sistema Regula RN por parte de ambos os envolvidos.

Assegurar o compliance dos requisitos legais, estatutários, regulamentares e contratuais relacionados aos aspectos de segurança da informação da proteção de dados pessoais.

2.3. Da ausência de infraestrutura física adequada para manter o datacenter da SESAP apto para hospedar o sistema Regula RN de maneira segura

Situação Encontrada

Para garantir a segurança física da hospedagem do Regula RN, as normas de segurança orientam que os perímetros de segurança sejam definidos e usados para proteger áreas que contenham informações e outros ativos associados ao sistema. As seguintes diretrizes devem ser consideradas e implementadas, quando apropriado, para perímetros de segurança física:

- definir perímetros de segurança e a localização e resistência de cada um dos perímetros de acordo com os requisitos de segurança da informação relacionados aos ativos dentro do perímetro;
- ter perímetros fisicamente sólidos para um edifício ou local contendo instalações de tratamento da informação (ou seja, convém que não haja lacunas no perímetro ou áreas onde um arrombamento pode ocorrer facilmente). Convém que os telhados externos, paredes, tetos e pisos do local sejam de construção sólida e todas as portas externas sejam adequadamente protegidas contra acesso não autorizado por meio de mecanismos de controle (por exemplo, barras, alarmes, fechaduras). Portas e janelas devem ser trancadas quando estiverem sem monitoração e uma proteção externa seja considerada para janelas, particularmente no andar térreo; convém que os pontos de ventilação também sejam considerados.
- alarmar, monitorar e testar todas as portas de incêndio do perímetro de segurança, em conjunto com as paredes, para estabelecer o nível de resistência requerido, de acordo com as normas adequadas. Convém que eles operem no modo à prova de falhas.

Considerando esses aspectos, o Data center da SESAP fica localizado em um local com baixa segurança e sem condições adequadas para assegurar o sistema contra desastres ou incidentes graves que possam comprometer os dados e o funcionamento do sistema. Além disso, o local usado não possui a devida segurança física ou o registro adequado dos acessos realizados. Assim, é possível afirmar que não existe infra estrutura física adequada para manter o Datacenter da SESAP de forma a hospedar o sistema Regula RN de maneira segura.

Objetos

Sistema Regula RN

Evidências

- Afirmação feita em entrevista com a equipe de TI da SESAP: https://drive.google.com/drive/folders/1EI_ea553PLmYLohF4A45WdANPgF2phxg

Critério

- NBR ISO/IEC 27001 versão 2022 (item 7.1)

Causa

A infraestrutura física onde fica o datacenter da SESAP aparece como principal causa. As salas são fechadas e controladas com chaves físicas, sem o uso de alarmes.

Efeito

- Aumento no risco de interrupção do sistema Regula RN para a sociedade;

Proposta de encaminhamento

Recomenda-se que a SESAP elabore um projeto para reforçar a segurança física do datacenter onde será hospedado o sistema Regula RN.

Benefícios esperados

Redução do risco de interrupção do serviço disponibilizado pelo Sistema Regula RN para a população, gerando queda na qualidade da prestação do serviço de regulação fornecido pela SESAP.

2.4. Da ausência de uma política de segurança da informação

Um sistema de gestão de segurança da informação (SGSI) é um processo estratégico que visa garantir a confidencialidade, disponibilidade, integridade e autenticidade dos ativos institucionais. Ele é fundamentado nas normas da família NBR ISO/IEC 27000 e pode ser ou não informatizado. O SGSI ajuda na gestão dos riscos e vulnerabilidades e cria uma governança eficaz, além de identificar possíveis pontos de melhoria e definir planos de ação para corrigir as deficiências encontradas. A implementação do SGSI deve seguir um processo bem definido, que envolve diversos passos. Ao seguir estes passos, é possível garantir a efetividade do sistema e a conformidade com as normas e padrões estabelecidos.

Situação Encontrada

Atualmente, mesmo realizando alguns procedimentos de segurança, a SESAP não possui uma Política de Segurança da Informação (PSI) estruturada minimamente, aumentando o risco de quebras e controles sobre o sistema Regula RN. De acordo com as normas NBR ISO/IEC 27001, uma PSI é um instrumento imprescindível para que seja possível manter um Sistema de Gestão de Segurança da Informação capaz de assegurar os ativos de TI de uma instituição, como é o caso do Sistema Regula RN.

Dessa forma, a inexistência de uma PSI aumenta os riscos da instituição não tratar de ações necessárias para manter a integridade do sistema e seus dados, a disponibilidade do serviço digital que o sistema proporciona e sua confiabilidade.

Objetos nos quais o achado foi constatado

Sistema Regula RN

Evidências

Como evidências sobre este achado, é possível apresentar:

- Resposta da SESAP à ação de levantamento de governança de TI realizada em 2023 pelo TCE/RN (Processo n° 000927/2024-TC).

- Afirmação feita pela equipe da SESAP em entrevista realizada no prédio sede do TCE/RN no dia 05/08/2024.

Critérios

- NBR ISO/IEC 27001 versão 2022 (itens 4.4 e 5.2)

Causas e efeitos

Apresenta-se como principal causa deste achado a falta de priorização de ações estratégicas que visam a criação de uma política de segurança da informação, dado que essa atividade deve partir da gestão maior do órgão. Esta ação deverá se desdobrar em inúmeras outras necessárias à segurança dos ativos de TI, como é o caso do Regula RN. Então, deverá somar-se a esta ação as demais ações subsequentes e investimentos para que elas possam ser implantadas.

A falta de uma PSI tem como principais efeitos:

- Aumento considerável no risco de incidente de segurança da informação que venha a comprometer a execução dos protocolos estabelecidos para a Regulação de Leitos com o uso do Regula RN.

- Aumento considerável no risco de incidentes de segurança de informação que venham a comprometer a disponibilidade dos serviços de tecnologia necessários ao funcionamento do sistema Regula RN.

- Aumento considerável no risco de vazamento de informações sensíveis, infligindo a Lei Geral de Proteção à Dados, gerando problemas e possíveis danos aos usuários do sistema, pacientes e médicos que possuem dados cadastros, incluindo prontuários de diversos tipos.

Proposta de encaminhamento

Recomenda-se que a SESAP reforce seu Sistema de Gestão de Segurança da Informação desenvolvendo uma política de segurança da informação com base nas boas práticas atuais, como por exemplo, a NBR ISO/IEC 27001.

Benefícios esperados

Redução dos riscos apontados nos efeitos deste achado, além de muitos outros benefícios de segurança, não apenas para o sistema Regula RN, mas para os demais ativos de TI da Secretaria.

2.5. Da ausência de capacitação aos usuários sobre procedimentos de segurança da informação

Para garantir o uso adequado do sistema Regula RN, sem que haja riscos de quebra de integridade dos dados ou de vazamento de informações, convém que os seus usuários, especialmente aqueles que atuam no processo de regulação, recebam treinamento, educação e conscientização em segurança da informação apropriados e atualizações regulares da política de segurança da informação da organização, além da política e procedimentos específicos para o sistema Regula RN.

Situação Encontrada

Os usuários do sistema Regula RN lotados na unidade de regulação do Hospital Geral Dr. João Machado e na Central de Regulação não receberam capacitação necessária para assegurar que estejam cientes e cumpram suas responsabilidades de segurança da informação no uso do sistema. Ao questioná-los sobre procedimentos de segurança da informação, estes relataram que não haviam recebido instruções sobre tais procedimentos. Foi declarado também que ocorre compartilhamento de senhas, procedimento básico que aumenta o risco de incidentes de segurança da informação.

Objetos nos quais o achado foi constatado

Usuários do sistema Regula RN.

Evidências

Como evidências sobre este achado, é possível apresentar:

- Resposta da SESAP à ação de levantamento de governança de TI realizada em 2023 pelo TCE/RN (Processo n° 000927/2024-TC).

- Afirmação feita pela equipe da SESAP em entrevista realizada no prédio sede do TCE/RN dia 05/08/2024.

Critérios

- NBR ISO/IEC 27001 versão 2022 (item 5.2 f)
- NBR ISO/IEC 27002 versão 2022 (item 6.3 - Conscientização, educação e treinamento em segurança da informação)

Causa

A ausência da Política de Segurança da Informação da SESAP e da Política de Segurança específica do Sistema Regula RN, bem como a ausência de um programa de conscientização, educação e treinamento em segurança da informação aos usuários do sistema que atuam no processo de regulação.

Efeito

- Vulnerabilidade dos usuários do Regula RN a ataques cibernéticos, tendo como exemplos os de engenharia social (*Phishing*[1], *Vishing*[2], *Smishing*[3], dentre outros), podendo comprometer a segurança do sistema e, consequentemente, a execução dos protocolos estabelecidos para a regulação.

- Aumento do risco de vazamento de informações pessoais sensíveis, em desacordo com a Lei Geral de Proteção de Dados Pessoais.

Proposta de encaminhamento

Recomenda-se que a SESAP estabeleça um programa continuado de conscientização, educação e treinamento em segurança da informação de acordo com a política de segurança da informação da organização, e procedimentos relevantes sobre segurança da informação.

[1] O criminoso envia um e-mail ou mensagem aparentemente confiável para obter informações sensíveis, como senhas, números de telefone, CPF ou CNPJ.
[2] O criminoso usa truques e técnicas semelhantes ao phishing, mas por telefone.
[3] O criminoso realiza o phishing por meio de mensagens de texto SMS.

Benefícios esperados

Redução dos riscos de vazamento de informações pessoais sensíveis e de ciberataques bem sucedidos, além de muitos outros benefícios de segurança, não apenas para o sistema Regula RN, mas para os demais ativos de TI da SESAP.

2.6. Da ausência de um processo definido para a gestão de incidentes de segurança

Conforme descrito pela NBR ISO/IEC 27002, convém que a organização planeje e se prepare para gerenciar incidentes de segurança da informação definindo, estabelecendo e comunicando processos, papéis e responsabilidades de gestão de incidentes de segurança da informação.

Situação Encontrada

Apesar de haver canais na SESAP que podem ser utilizados para registros de incidentes de segurança da informação (SI), a Secretaria não possui um processo definido de gestão de incidentes de SI. Os incidentes desse tipo, assim como demais incidentes envolvendo o sistema Regula RN, podem ser relatados por canais diversos como pela ouvidoria, e-mail e *WhatsApp*. O fluxo de resolução dos incidentes vai depender de quem se prontificar a resolver o problema e do canal usado, não sendo apresentada garantias mínimas de padrões ou processos usados para tratamento de cada tipo de incidente relatado.

Objetos nos quais o achado foi constatado

Gestão de incidentes de segurança da informação.

Evidências

- Afirmação feita pela equipe da SESAP em entrevista realizada no prédio sede do TCE/RN dia 05/08/2024.

- Afirmação feita pela equipe do LAIS em entrevista realizada no dia 17/05/2024 por videoconferência.

Critérios

- NBR ISO/IEC 27002 versão 2022 (item 5.24)

Causa

A ausência de um planejamento para gerenciar incidentes de segurança da informação definindo, estabelecendo e comunicando processos, papéis e responsabilidades de gestão de incidentes de segurança da informação.

Efeito

- Ausência de uma base de dados dos incidentes reportados, do tratamento realizado, das consequências, do resultado e boas práticas derivadas disso tudo.

- Demora na execução de ações corretivas ou de ajustes no sistema para deixá-lo resistente e resiliente aos efeitos negativos causados pelo tipo de incidente;

- Aumento do risco de adoção de ações inadequadas em resposta a um tipo de incidente de segurança da informação;

- Aumento do risco de comprometer a disponibilidade dos serviços de tecnologia necessários ao funcionamento do sistema Regula RN.

- Aumento do risco de manipulação indevida na base de dados.

- Aumento do risco de vazamento de informações pessoais sensíveis.

Proposta de encaminhamento

Recomenda-se que a SESAP:

- Estabeleça um método comum para relatar eventos de segurança da informação, incluindo ponto de contato;

- Estabeleça um processo de resposta a incidentes para fornecer à organização a capacidade de avaliar, responder e aprender com incidentes de segurança da informação;

- Permita apenas que o pessoal competente lide com as questões relacionadas à incidentes de segurança da informação dentro da organização e que esse pessoal seja provido com documentação do procedimento e treinamento periódico;

- Estabeleça um processo para identificar o treinamento, a certificação e o desenvolvimento profissional continuado, requeridos para o pessoal de resposta a incidentes.

Benefícios esperados

Assegurar uma resposta rápida, eficaz, consistente e ordenada aos incidentes de segurança da informação, incluindo a comunicação sobre eventos de segurança da informação, além da redução dos riscos apontados nos efeitos e criação de base de conhecimento para tratamento de futuros incidentes de SI.

2.7. Da ausência de uma política para tratamento da preservação da privacidade e proteção aos dados pessoais sensíveis

A Lei Geral de Proteção de Dados Pessoais (LGPD) é uma lei brasileira que estabelece regras para a recolha, tratamento, armazenamento e partilha de dados pessoais. Ela foi promulgada em 14 de agosto de 2018 e entrou em vigor em 18 de setembro de 2020 e foi inspirada na norma europeia de Proteção de Dados (GDPR – *General Data Protection Regulation*). O seu objetivo principal é proteger os direitos fundamentais à liberdade e à privacidade, e o livre desenvolvimento da personalidade de cada indivíduo.

Conforme a NBR ISO/IEC 27002, convém que a organização identifique e atenda aos requisitos relativos à preservação da privacidade e proteção de Dados Pessoais.

Situação Encontrada

A SESAP não possui uma política relacionada à LGPD ou específica para proteção dos dados pessoais no Regula RN. Também não foi identificada nenhuma instrução ou procedimento que trabalhe os cuidados necessários à proteção dos dados manipulados pelo Sistema Regula RN.

A base de dados com todas as informações contidas no sistema fica disponível para os integrantes do projeto que, mesmo tendo boa vontade e idoneidade, ficam de posse de dados sensíveis de pacientes e usuários do sistema de regulação, sem nenhum documento de resguardo (como um Acordo de Não-Divulgação) próprio, como é indicado pela LGPD.

Objetos

Dados Pessoais Sensíveis.

Evidências

- Afirmação feita pela equipe do LAIS em entrevista realizada no dia 17/05/2024 por videoconferência.

- Respostas submetidas pela SESAP ao questionário sobre implementação dos dispositivos da LGPD no âmbito de ação fiscalizatória (ID 4.00.2024.058.000 - PFA 2024/2025) realizada pelo TCE/RN.

- Ambiente de homologação do LAIS contendo os mesmos dados de produção sem anonimização dos registros.

- Liberação de acesso dos Auditores de Controle Externo aos dados não anonimizados, em ambiente de homologação, sem o devido Acordo de Não Divulgação (*Non Disclosure Agreement* - NDA) assinado.

Critérios

- NBR ISO/IEC 27002 versão 2022 (item 5.34)

Causa

Ausência de uma Política de Proteção de Dados Pessoais, que se desdobra na falta de procedimentos próprios e da instrução necessária às equipes participantes do projeto Regula RN, bem como aos usuários do próprio sistema.

Efeito

Aumento do risco de vazamento de informações pessoais sensíveis.

Proposta de encaminhamento

Recomenda-se que seja dada atenção à LGPD e que a SESAP tome as providências necessárias para se adequar a Lei.

Recomenda-se que a SESAP centre esforços para atender à LGPD, que defina procedimentos de segurança, instrumentos e treinamentos necessários para reforçar os cuidados com a privacidade dos dados pessoais tratados dentro do Sistema Regula RN.

Benefícios esperados

Assegurar o compliance dos requisitos legais, estatutários, regulamentares e contratuais relacionados aos aspectos de segurança da informação da proteção de DP.

Redução no risco de vazamento de informações sensíveis, além de reforçar o cumprimento de leis como LGPD.

2.8. Da ausência de controles de direitos de acesso privilegiados

As boas práticas descritas pelas normas de segurança da informação reforçam a necessidade de restringir e gerenciar a atribuição e o uso de direitos de acessos privilegiados aos usuários. Assegurar que apenas usuários, componentes de software e serviços autorizados recebam direitos de acessos privilegiados, faz parte do processo de segurança da informação. Neste sentido, convém que a atribuição de direitos de acesso privilegiado seja controlada por meio de um processo de autorização de acordo com a política de controle de acessos.

Direitos de acesso privilegiados são direitos fornecidos a uma identidade, um papel ou um processo, que permitem a realização de atividades que usuários ou processos típicos não estão aptos a realizar. Os papéis de administrador do sistema normalmente exigem direitos de acesso privilegiados. O uso inadequado de privilégios de administrador do sistema é um dos principais fatores contribuintes para falhas ou violações de sistemas.

Assim, deve-se considerar que é preciso identificar usuários que precisem de direitos de acesso privilegiados para cada sistema ou processo e atribuir direitos de acesso privilegiado aos usuários conforme necessário e em um princípio de evento por evento, em consonância com a política de controle de acesso.

Situação Encontrada

Ao questionar a equipe de TI da SESAP, juntamente com a equipe do LAIS responsável pelo suporte ao “Regula RN”, sobre como é feito o processo de liberação de acessos aos usuários do sistema Regula RN, foi possível identificar que existe uma baixa formalização na gestão de atribuição de acessos privilegiados, relacionados ao “Regula RN”. A atribuição de acessos privilegiados ao banco de dados do sistema e dos repositórios de armazenamento do código fonte do sistema (*branchs* do *github*) ficam sob a responsabilidade de bolsistas do LAIS que não fazem parte do projeto.

Além de não haver um processo formalizado para os acessos aos dados ou código fonte do sistema, não existe o registro desses acessos, nem há a participação da SESAP nesse processo de autorização.

Objetos

Acessos privilegiados ao sistema Regula RN.

Evidências

- Afirmação feita pela equipe do LAIS em entrevista realizada no dia 17/05/2024 por videoconferência.

- Afirmação feita pela equipe da SESAP em entrevista realizada no prédio sede do TCE/RN dia 05/08/2024.

Critério

- NBR ISO/IEC 27002 versão 2022 (item 8.2 - Direitos de acessos privilegiados)

Causa

A falta de uma Política de Controle de Acesso (PCA) estabelecendo princípios, objetivos, diretrizes, principais atividades e responsabilidades relativas ao processo de controle de acesso surge como principal causa desse ponto abordado. Junta-se a isso, a falta de um processo de autorização de acessos privilegiados, em consonância com a PCA.

Efeito

Aumento do risco de uso inadequado de privilégios de administrador do sistema, podendo causar falhas ou violações de sistemas. Acessos indevidos podem ocasionar falhas, interrupções, mau funcionamento e vazamento de dados sensíveis.

Proposta de encaminhamento

Recomenda-se que a SESAP:

- Desenvolva e publique uma Política de Controle de Acesso (PCA) estabelecendo princípios, objetivos, diretrizes, principais atividades e responsabilidades relativos ao processo de controle de acesso do sistema Regula RN.

- Identifique as pessoas que precisam de direitos de acessos privilegiados (ex: administradores de banco de dados, branches de produção, sistema em si, etc.), mantenha um processo de autorização (ou seja, determinar quem pode aprovar direitos de acesso privilegiado, ou não conceder direitos de acesso privilegiado até que o processo de autorização seja concluído) e um registro de todos os privilégios alocados.

- Após qualquer mudança organizacional, analise criticamente os usuários trabalhando com direitos de acesso privilegiados, a fim de verificar se suas funções, papéis, responsabilidades e competências ainda os qualificam para trabalhar com direitos de acesso privilegiados.

- Registre todo o acesso privilegiado ao sistema para fins de auditoria.

- Não compartilhe ou vincule identidades com direitos de acesso privilegiados a várias pessoas, atribuindo a cada pessoa uma identidade separada que permita atribuir direitos específicos de acesso privilegiado.

- Defina e implemente requisitos para o término dos direitos de acesso privilegiado;

Benefícios esperados

- Redução do risco de falhas e violações no sistema Regula RN.

- Redução no risco de vazamento de dados sensíveis ou dados pessoais de usuários da rede de regulação, mantendo a conformidade com as exigências dispostas na Lei Geral de Proteção da Dados Pessoais (LGPD).

- Redução do risco de interrupção do serviço disponibilizado pelo Sistema Regula RN para a população, gerando queda na qualidade da prestação do serviço de regulação fornecido pela SESAP.

2.9. Da ausência de um processo seguro para realização de backup e restauração de dados do Regula RN

Com o objetivo de permitir a recuperação da perda de dados ou sistemas, as normas de segurança da informação reforçam a necessidade de que cópias de *backup* de informações,

software e sistemas sejam mantidas e testadas regularmente de acordo com a política específica por tema acordada sobre *backup*.

Para atender aos requisitos mínimos de segurança da informação, no que tange a segurança dos dados do sistema Regula RN, convém que uma política sobre *backup* seja estabelecida e que instalações de *backup* adequadas sejam fornecidas para assegurar que todas as informações essenciais do sistema Regula RN possam ser recuperados após um incidente ou falha ou perda de mídia de armazenamento. Para tornar isso possível, convém que planos sejam desenvolvidos e implementados sobre como a organização fará cópia de segurança das informações, software e sistemas, para abordar a política sobre *backup*.

Ao projetar um plano de *backup*, convém que os seguintes itens sejam levados em consideração:

a) produção de registros precisos e completos das cópias de *backup* e procedimentos de restauração documentada;

b) armazenamento de *backup* em um local remoto e seguro, a uma distância suficiente para escapar de qualquer dano causado por um desastre no local principal;

c) fornecimento de informações de *backup* com um nível apropriado de proteção física e ambiental, consistente com as normas aplicadas no local principal;

d) teste regular de mídias de *backup* para assegurar que elas possam ser confiadas para uso emergencial, quando necessário. Teste da capacidade de restaurar dados apoiados em um sistema de teste, não substituindo a mídia de armazenamento original no caso de o processo de *backup* ou restauração falhar e causar danos ou perdas irreparáveis de dados;

e) proteção do *backup* por meio da criptografia, de acordo com os riscos identificados;

f) cuidado para assegurar que a perda inadvertida de dados seja detectada antes que a *backup* seja tomada.

Situação Encontrada

Ao questionar sobre como é feito o procedimento de *backup* do sistema Regula RN, verifica-se que, como ele está operando dentro da infraestrutura da UFRN, mesmo que sem previsão contratual conforme descrito no item 2.1, o *backup* é realizado pelo LAIS e a validação é feita de forma manual pelos bolsistas em suas máquinas locais.

Considerando que o sistema será migrado para o datacenter da SESAP, foi questionado a forma como o *backup* dos sistemas são realizados pela TI da SESAP. Estes informaram que o *backup* é realizado, mas não há um procedimento formal que defina esse processo, nem existe uma atividade para validar se o *backup* foi bem sucedido. Além disso, não existe

cópia espelho do *backup* em ambiente distante e seguro do *data center*. Além disso, não foi apresentada política formalizada ou escrita sobre os procedimentos de *backup*.

Objetos

Backup do sistema Regula RN.

Evidências

- Afirmação feita pela equipe do LAIS em entrevista realizada junto a equipe do LAIS e SESAP no dia 10/05/2024 presencialmente no TCE.
- Afirmação feita pela equipe do LAIS em entrevista realizada no dia 17/05/2024 por videoconferência.
- Afirmação feita pela equipe da SESAP em entrevista realizada no prédio sede do TCE/RN dia 05/08/2024.

Critério

- NBR ISO/IEC 27002 versão 2022 (item 8.13 - *Backup* das informações)

Causa

Falta de uma Política/Plano de *Backup* contendo os requisitos de retenção de dados e segurança da informação da organização, procedimentos de verificação e segurança física (distanciamento) dos *backups* e os dados.

Efeito

A não observância dos requisitos da Política/Plano de *Backup* pode inviabilizar a recuperação de dados ou sistema, após um incidente ou falha ou perda de mídia de armazenamento. Isso pode aumentar de forma considerável o risco de interrupção do sistema Regula RN para a sociedade por tempo indeterminado, em caso de falhas nos sistemas de armazenamento.

Proposta de encaminhamento

Recomenda-se que a SESAP desenvolva, publique e operacionalize uma Política/Plano de *Backup* estabelecendo os procedimentos e responsabilidades para que a geração das cópias de *backup* de dados e sistema sejam mantidas e testadas regularmente.

Benefícios esperados

Permitir a recuperação da perda de dados ou sistema, mesmo após um incidente ou falha ou perda de mídia de armazenamento, reduzindo o risco de interrupções do serviço de regulação por um período prejudicial ao sistema de regulação.

2.10. Da ausência de instrumentos de proteção para o encerramento do contrato com o LAIS

Convém que as responsabilidades e funções de segurança da informação permaneçam válidas após o encerramento ou mudança da contratação sejam definidos, aplicados e comunicados a todas as partes interessadas pertinentes ao projeto Regula RN. Essa orientação objetiva proteger os interesses da SESAP como parte do processo de mudança ou encerramento da contratação.

Situação Encontrada

Ao questionar os integrantes do projeto Regula RN e colaboradores da SESAP envolvidos no projeto, verificou-se que a SESAP não possui instrumentos de proteção para o encerramento do contrato com o LAIS, definindo responsabilidades e funções válidas de segurança após a mudança ou encerramento do contrato, como termo de confidencialidade, propriedade intelectual, além das responsabilidades e o período de vigência dessas obrigações.

Nas entrevistas realizadas e avaliando o instrumento contratual que regulamenta as ações do projeto entre a SESAP e o LAIS, verificou-se que não existe plano de projeto, plano de encerramento do projeto, acordos sobre a propriedade intelectual do sistema e suas informações, vigência dos Acordos de Não Divulgação ou algo do tipo.

Objetos

Instrumento Contratual entre SESAP e LAIS.

Evidências

- Afirmação feita pela equipe do LAIS em entrevista realizada no dia 17/05/2024 por videoconferência.
- Afirmação feita pela equipe da SESAP em entrevista realizada no prédio sede do TCE/RN dia 05/08/2024.
- Contrato entre SESAP e Fundação de Apoio à Educação e ao Desenvolvimento Tecnológico (FUNCERN).

Critérios

- NBR ISO/IEC 27002 versão 2022 (item 6.5 - Responsabilidades após encerramento ou mudança da contratação).

Causa

A falta de um plano de projeto, um plano de encerramento de projeto, ou procedimentos que cuidam do encerramento de um projeto aparecem como causas geradoras da situação encontrada. Como causas primárias, apresentam-se a falta de instrumentos contratuais e Acordos de Não Divulgação que tratam diretamente os cuidados necessários para que o encerramento do projeto Regula RN não gere riscos de uso indevido de dados, propriedade intelectual ou até mesmo parada do serviço.

Efeito

- Aumento do risco de incidentes de segurança de informação que envolvam a quebra de sigilo sobre dados pessoais sensíveis;

- Aumento do risco de ocorrência de problemas jurídicos quanto ao uso indevido dos dados ou do código fonte do sistema desenvolvido, tanto por parte da SESAP quanto do LAIS.

Proposta de encaminhamento

Recomenda-se que a SESAP elabore um plano de encerramento de projeto, ou procedimentos próprios para tratar esse risco.

Recomenda-se, também, que a SESAP elabore termos de rescisão contratual que envolvam o uso das tecnologias disponibilizadas, direitos autorais e o sigilo de dados sensíveis, mesmo com o contrato encerrado (período de carência).

Benefícios esperados

Proteção aos interesses da SESAP como parte do processo de mudança ou encerramento do contrato com a FUNCERN.

Redução do risco de vazamento de informações pessoais sensíveis.

Redução no risco de embates jurídicos sobre o uso do sistema Regula RN por parte dos atores envolvidos.

Assegurar o compliance dos requisitos legais, estatutários, regulamentares e contratuais relacionados aos aspectos de segurança da informação da proteção de dados pessoais.

3. CONCLUSÃO

A auditoria realizada no Sistema de Regulação de Leitos do Estado do Rio Grande do Norte - Regula RN constatou que a plataforma é um recurso essencial para a administração pública estadual e para a otimização do serviço de regulação de leitos no SUS. A análise destacou aspectos positivos relacionados à automação dos protocolos de regulação e ao impacto significativo na melhoria da gestão hospitalar e na transparência das informações disponibilizadas. Entretanto, também foram identificadas fragilidades que requerem atenção prioritária para assegurar a continuidade e a eficácia do sistema.

Os achados de auditoria indicam a necessidade de aprimorar a segurança da informação, planejar a sustentabilidade do sistema e formalizar contratos e processos relacionados à sua operação e manutenção. A ausência de uma política estruturada de segurança da informação, de processos definidos para gestão de incidentes e de controles de acesso privilegiados compromete a robustez do sistema. Além disso, a falta de capacitação dos usuários em práticas de segurança e de planejamento para garantir a continuidade da sustentação da plataforma após o encerramento dos contratos atuais representa riscos operacionais e jurídicos significativos.

Os resultados também apontam para a necessidade de maior alinhamento às boas práticas internacionais, como as normas ISO/IEC 27001 e 27002, além de um fortalecimento do compliance com a Lei Geral de Proteção de Dados Pessoais (LGPD). Essa adequação é crucial para a proteção de dados sensíveis e para a confiabilidade do serviço prestado.

A versão preliminar deste relatório foi encaminhada por meio de ofício protocolado no sistema SEI (Recibo Eletrônico de Protocolo - 30084235), para que o gestor responsável pudesse avaliar os pontos, e ter a possibilidade de se manifestar previamente a respeito das informações apontadas, como orienta a NBASP 4000. Foi previsto o prazo de 15 dias para manifestação do gestor (ou seu representante) mas, até o momento da finalização deste relatório, não houve retorno oficial por parte do ente auditado.

Sendo assim, avaliando todos os aspectos do sistema Regula RN e seu contexto de uso, fica clara a existência dos benefícios inegáveis proporcionados pelo sistema Regula RN à sociedade. Mas há uma urgência em implementar medidas corretivas e preventivas que mitiguem os riscos identificados. A adoção das recomendações apresentadas neste relatório contribuirá para garantir que o sistema continue a cumprir seu papel estratégico de forma segura, eficiente e em conformidade com os marcos regulatórios aplicáveis.

4. PROPOSTA DE ENCAMINHAMENTO

Com base nos achados apresentados e considerando a relevância estratégica do Sistema Regula RN para a gestão da saúde pública no Estado do Rio Grande do Norte, a equipe de auditoria propõe que este Tribunal de Contas emita recomendação no sentido de que a SESAP adote um conjunto de ações prioritárias, estruturadas nas seguintes frentes:

4.1. Regularização Contratual e Sustentação do Sistema

- **Formalização Contratual:** Promover a formalização de um contrato específico para a operação e manutenção do Regula RN, contemplando os serviços necessários para sua hospedagem, suporte técnico e atualizações.
- **Plano de Sustentação:** Elaborar um plano de médio e longo prazo para assegurar a continuidade do sistema, considerando alternativas como infraestrutura própria ou contratação de serviços em nuvem.

4.2. Segurança da Informação e Proteção de Dados

- **Política de Segurança da Informação:** Desenvolver e implementar uma política abrangente, alinhada às boas práticas internacionais, como a norma ISO/IEC 27001.
- **Gestão de Acessos Privilegiados:** Estabelecer controles rigorosos para a atribuição, registro e monitoramento de acessos privilegiados, restringindo o uso desses direitos apenas a pessoal autorizado.
- **Capacitação de Usuários:** Implantar um programa contínuo de conscientização e treinamento sobre segurança da informação, abrangendo boas práticas de uso e proteção de dados sensíveis.
- **LGPD:** Implementar medidas específicas para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD), incluindo a adoção de políticas de privacidade e tratamento de dados pessoais.

4.3. Continuidade Operacional e Gestão de Riscos

- **Plano de Gestão de Incidentes:** Definir e documentar um processo estruturado para gestão de incidentes de segurança, abrangendo identificação, resposta, recuperação e análise pós-incidente.
- **Backup e Recuperação de Dados:** Criar uma política robusta de backup e recuperação de dados, com testes regulares e armazenamento seguro em local remoto.
- **Infraestrutura Física:** Adequar as instalações do datacenter da SESAP para atender aos requisitos de segurança física e ambiental necessários à hospedagem do sistema.

4.4. Planejamento e Gestão do Encerramento do Contrato

- **Plano de Transição:** Desenvolver um plano de encerramento de projeto e transferência de tecnologia que assegure a preservação da continuidade operacional, da propriedade intelectual e da confidencialidade dos dados.
- **Acordos de Não-Divulgação:** Formalizar instrumentos jurídicos que garantam a proteção das informações sensíveis após o término da parceria com o LAIS.

4.5. Monitoramento e Avaliação Contínua

- **Auditorias Periódicas:** Instituir ciclos regulares de auditoria para monitorar a implementação das recomendações e identificar novas áreas de melhoria.

- **Indicadores de Desempenho:** Estabelecer métricas para avaliar a eficácia das ações adotadas, como tempo médio de resposta a incidentes, conformidade com protocolos de segurança e índices de capacitação dos usuários.

Essas medidas, quando implementadas, visam mitigar os riscos identificados, fortalecer a governança do sistema e assegurar a continuidade e a qualidade do serviço prestado à população. O sucesso da execução dependerá do comprometimento da SESAP e de seus parceiros em priorizar essas ações no planejamento estratégico e operacional do órgão.

Natal/RN, 17 de dezembro de 2024

gov.br
Documento assinado digitalmente
EDUARDO PEREIRA LIMA
Data: 17/12/2024 17:36:05-0300
Verifique em https://validar.iti.gov.br

Eduardo Pereira Lima,
Auditor de Controle Externo, Matrícula 9.874-4.

ALEXANDRE LUIZ GALVAO DAMASCENO:02544087455

Digitally signed by ALEXANDRE LUIZ GALVAO DAMASCENO:02544087455
DN: C=BR, O=ICP-Brasil, OU=AC SOLUTI Multipla v5, OU=09461647000195, OU=Presencial, OU=Certificado PF A3, CN=ALEXANDRE LUIZ GALVAO DAMASCENO:02544087455
Reason: I am the author of this document
Location:
Date: 2024.12.17 17:26:45-03'00'
Foxit PDF Reader Version: 12.1.0

Alexandre Luiz Galvão Damasceno,
Auditor de Controle Externo, Matrícula 9.988-0

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ISO Guia 27001:2022**. Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ISO Guia 27002:2022.** Rio de Janeiro, 2022.

Secretaria de Estado da Saúde Pública do Estado do Rio Grande do Norte. **Protocolo de Regulação para Acesso a Leitos Clínicos**. Rio Grande do Norte, 2021.

Secretaria de Estado da Saúde Pública do Estado do Rio Grande do Norte. **Protocolo de Regulação para Acesso a Leitos em Unidade de UTI Geral**. Rio Grande do Norte, 2021.

Secretaria de Estado da Saúde Pública do Estado do Rio Grande do Norte. **Protocolo de Regulação para Acesso a Leitos em Unidade de Terapia Intensiva Pediátrica (UTIP)**. Rio Grande do Norte, 2021.

Secretaria de Estado da Saúde Pública do Estado do Rio Grande do Norte. **Protocolo de Regulação para Acesso a Leitos em Unidade de Terapia Intensiva Neonatal (UTIN)**. Rio Grande do Norte, 2021.

Secretaria de Estado da Saúde Pública do Estado do Rio Grande do Norte. **Protocolo de Acesso aos Cuidados Vasculares de Urgência**. Rio Grande do Norte, 2021.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado, 1988.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Brasília, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 23 out. 2024.

Tribunal de Contas da União. **Padrões de Auditoria de Conformidade**. Brasília, 2009a.