TRT-8ª REGIÃO
Secretaria de Auditoria

# RELATÓRIO DE MONITORAMENTO DE AUDITORIA
## 08/2023

Monitoramento - Relatório de Auditoria nº 07/2022

Belém - Pará
Dezembro/2023

**Tribunal Regional do Trabalho da 8ª Região – TRT8**

**Secretaria de Auditoria**

**RELATÓRIO DE MONITORAMENTO**

Assunto: Avaliar a implementação das recomendações do Relatório de Auditoria nº 07/2022, que trata da avaliação do processo de tratamento e resposta a incidentes de segurança da informação e gestão de continuidade dos serviços de TI (Ação coordenada com o CSJT).

Responsável: Seção de Auditoria de Tecnologia de Informação

Processo Administrativo: PROAD 1113/2022

SUMÁRIO

**1. INTRODUÇÃO** **4**
**2. ANÁLISE DO ATENDIMENTO DAS RECOMENDAÇÕES** **4**
2.1 Recomendação R.1 4
2.2 Recomendação R.2 5
2.3 Recomendação R.3 6
**3. CONCLUSÃO** **7**
**4. PROPOSTA DE ENCAMINHAMENTO** **8**

## 1. INTRODUÇÃO

Apresenta-se neste relatório o resultado do 1º monitoramento realizado para verificar o cumprimento das recomendações de auditoria que avaliou os processos Tratamento e Resposta a Incidentes de Segurança da Informação e Gestão de Continuidade de Tecnologia da Informação, no âmbito do TRT8.

No ano de 2022, a SEAUD realizou, em Ação Coordenada do Conselho Superior da Justiça do Trabalho, auditoria para averiguar a aderência do TRT8 à implementação da ENSEC-PJ (Resolução CNJ nº 396/2021), no tocante a avaliação dos processos Tratamento e Resposta a Incidentes de Segurança da Informação. Os trabalhos foram concluídos em julho de 2022 com a emissão do Relatório de Auditoria (RA) nº 07/2021 (documento 42).

A conclusão dos trabalhos apresentou como resultado a necessidade de aprimoramento dos controles internos dos processos supracitados. A equipe de auditoria, então, definiu 3 (três) recomendações de auditoria, todas acolhidas pela Presidência (documento 44).

Diante disso, este 1º monitoramento buscou verificar se as recomendações, R.1, R.2 e R.3, mencionadas no RA como 7.1, 7.2 e 7.3, foram cumpridas.

Ressalta-se que a SEAUD adotou como categorização relativa ao *status* da recomendação aquela estabelecida pelo Manual de Auditoria do Poder Judiciário (seção 3.4.2), aprovado pelo Conselho Nacional de Justiça, conforme abaixo.

> **Implementada** - *A unidade auditada realizou as ações consideradas necessárias e suficientes pela auditoria interna para o atendimento da recomendação.*
>
> **Não Implementada** - *A unidade auditada não se manifestou, ou manifestou-se, de forma justificada, contrária à implementação da recomendação, porém, a auditoria interna não considerou razoáveis as justificativas apresentadas.*
>
> **Em Implementação** - *A unidade auditada iniciou a ação para atendimento da recomendação, porém, a solução não estava completa no momento da elaboração do relatório de monitoramento.*
>
> **Prejudicada** - *Recomendação que sofreu situações de mudança no seu contexto que inviabilizou ou tornou desnecessário o seu conteúdo. A recomendação perdeu seu objeto, não sendo possível seu atendimento pela unidade auditada.*

## 2. ANÁLISE DO ATENDIMENTO DAS RECOMENDAÇÕES

### 2.1 Recomendação R.1

***Recomendar à SETIN que inclua, quando da elaboração dos seus planos anuais de capacitação, previsões de ações para o desenvolvimento de competências dos membros da ETIR (ERITIC) do TRT8.***

2.1.1 Providência adotada pela área responsável

A Secretaria de Tecnologia da Informação e Comunicação (SETIN), através da Divisão de Riscos e Segurança da Informação (DISEG), apresentou em julho de 2023 um plano de ação (doc 54) no qual estabeleceu duas ações a serem cumpridas, em relação à recomendação em tela.

Durante a reunião ocorrida no dia 10/10/2023, entre SEAUD e SETIN (cuja ata está registrada no doc 64), a unidade auditada manifestou a incidência de limitação orçamentária para

aplicação em capacitação de pessoal, e manifestou a concordância sobre a necessidade da reformulação do Plano de Ação para cumprimento da recomendação.

Em resposta a RDI SEAUD 14/2023 (registrada no doc 68), a parte auditada informou o status das ações definidas no plano de ação supracitado (documento 54), em relação à presente recomendação, não havendo reformulação nas ações anteriormente definidas. A definição da trilha de aprendizagem selecionada para os membros da ETIR foi realizada pela própria parte auditada, e apresentada na reunião da ETIR ocorrida em 23 de novembro de 2023, conforme ata (doc 4 do PROAD 6650/2023).

2.1.2 Análise da equipe de auditoria

Diante das ações determinadas pelo plano de ação fornecido pela SETIN / DISEG, a SEAUD/ SeATI a efetividade das mesmas com relação ao cumprimento da presente recomendação. Observou-se que não houve, dentre as ações estabelecidas pela parte auditada, o acréscimo da previsão de que a trilha de capacitação definida seja formalizada nos planos anuais de capacitação da SETIN, referenciando os membros da ETIR.

A SEAUD verificou que, em pese a realização das ações constantes no plano de ação estabelecido, apesar de ter sido definida pela parte auditada uma trilha de qualificação para os membros da ETIR, a recomendação não foi cumprida, uma vez que não há evidência da inclusão da trilha de capacitação da ETIR nos planos anuais de capacitação da SETIN, com o objetivo de que a própria unidade auditada possa fazer o acompanhamento da efetiva execução da trilha de capacitação pelos membros da ETIR. Dessa forma, conclui-se que a recomendação R.1 está em implementação pela unidade.

2.1.3 Status da Recomendação

Recomendação **EM IMPLEMENTAÇÃO**

## 2.2 Recomendação R.2

***Recomendar às equipes responsáveis pelos preenchimentos dos relatórios envolvendo incidentes de segurança da informação (em especial da Seção de Infraestrutura e Redes/COINS - atual Coordenadoria de Infraestrutura Tecnológica - COINT), sempre que ocorrerem incidentes dessa natureza, que elaborem relatórios técnicos relativos às ocorrências, devendo, a Assistência de Segurança da Informação (atual Divisão de Riscos e Segurança da Informação - DISEG), acompanhar as equipes, no sentido de certificar-se acerca do efetivo preenchimento desses relatórios.***

2.2.1 Providência adotada pela área responsável

A SETIN apresentou, através da DISEG, em julho de 2023 um plano de ação (doc 54) no qual estabeleceu quatro ações a serem cumpridas, em relação à recomendação em tela. As ações citadas no plano de ação foram: (i) a criação de um questionário sintético e relatório analítico (detalhado) para registro de incidentes; (ii) da Reunião da Equipe da ETIR, a fim de formalizar questionário simplificado e relatório analítico e processo para preenchimento e acompanhamento; (iii) a revisão do Processo de Gerenciamento de Incidentes; e (iv) Autuação de PROAD para registro e acompanhamento das atividades da ETIR.

Em resposta a RDI SEAUD 14/2023 (registrada no doc 68), a unidade informou o status das ações em questão, disponibilizando o link para o formulário elaborado para o registro de incidentes, e a ata de reunião onde o assunto foi levado à apreciação da ETIR (doc 4 do PROAD 6650/2023). A ata não

deixa explícita a informação de que o formulário foi aprovado pelo colegiado, registrando somente que foi apresentado para homologação.

2.2.2 Análise da equipe de auditoria

Diante das ações determinadas pelo plano de ação fornecido pela SETIN / DISEG, a SEAUD / SeATI analisou a efetividade das ações com relação ao cumprimento da presente recomendação. Avalia-se como positiva a elaboração do formulário padronizado para o registro de incidentes pelas unidades técnicas da SETIN, e a submissão do mesmo à apreciação da ETIR. Contudo, para que a recomendação seja cumprida, é necessário que a ação de revisão do processo Gerenciamento de Incidentes, prevista no plano de ação da DISEG, seja feita com o objetivo de prever o preenchimento do formulário pelas equipes quando houver a ocorrência de incidentes de segurança da informação. Ademais, é necessário que a unidade estabeleça ações que garantam o preenchimento do formulário, de forma a garantir a efetividade do registro de incidentes, assim como a possibilidade de acompanhamento pela DISEG, que deve monitorar e orientar as equipes em relação ao correto registro das informações pertinentes. Portanto, ainda não há evidências que permitam atestar o cumprimento do objetivo da presente recomendação.

2.2.3 Status da Recomendação

Recomendação **EM IMPLEMENTAÇÃO.**

### 2.3 Recomendação R.3

***Recomendar à SETIN que realize os testes de continuidade dos serviços essenciais de TI, bem como produza a documentação correlata, de forma regular e anual, a começar no corrente ano de 2022.***

2.3.1 Providência adotada pela área responsável

A Secretaria de Tecnologia da Informação e Comunicação (SETIN), através da Divisão de Riscos e Segurança da Informação (DISEG), apresentou em julho de 2023 um plano de ação (doc 54) no qual estabeleceu cinco ações a serem cumpridas, em relação à recomendação em tela.

Durante a reunião ocorrida no dia 11/10/2023, entre SEAUD e SETIN (cuja ata está registrada no doc 65), a DISEG manifestou-se de forma a explicitar as razões pelas quais a execução dos testes de continuidade em relação aos sistemas essenciais não foram realizados em sua totalidade. Dentre os problemas levantados figuraram: (i) a não definição pela Alta Administração dos serviços essenciais do TRT8; (ii) A não possibilidade da atualização do rol de sistemas e serviços essenciais de TIC, frente ao Subcomitê Gestor de TIC, pois tal atualização depende da definição pela Alta Administração dos serviços essenciais; (iii) Alterações no ambiente tecnológico do Tribunal, em especial a migração do PJe para a nuvem da AWS, que fez o teste já em execução em relação a esse sistema perder o objeto.

Em resposta a RDI SEAUD 14/2023 (registrada no doc 68), a parte auditada informou status das ações definidas no plano de ação supracitado (documento 54), em relação à presente recomendação, não havendo reformulação nas ações, mas apenas a atualização dos prazos estabelecidos. As ações estabelecidas pela parte auditada foram: (i) Participação na Oficina de Design Thinking que definirá os serviços essenciais do TRT8; (ii) a formalização, junto ao Subcomitê Gestor de TIC, de proposta para atualização do rol dos sistemas e serviços essenciais de TIC; (iii) a atualização do Processo de Continuidade de Serviços Essenciais de TIC, a fim de contemplar todos os serviços essenciais formalizados; (iv) a criação de um Plano de Testes referente ao Processo de Continuidade de Serviços

Essenciais de TIC atualizado; e (v) a execução do Plano de Testes de Continuidade dos Serviços Continuados de TIC. Destaca-se que a unidade auditada informou que não há previsão para realização da Oficina para definição dos serviços essenciais.

2.3.2 Análise da equipe de auditoria

Diante das ações determinadas pelo plano de ação fornecido pela SETIN / DISEG, a SeATI / SEAUD analisou a efetividade das ações com relação ao cumprimento da presente recomendação.

Em que pese a DISEG ter elaborado um plano de ação que define ações para implementar a recomendação, a conclusão dos testes está prevista para julho de 2024. Cabe ressaltar que a recomendação foi formalizada no Relatório de Auditoria nº 07/2022, publicado em julho de 2022, sendo a ciência da unidade auditada registrada no PROAD em agosto de 2022. Dessa forma, foi recomendado que os testes de continuidade fossem realizados a partir do ano de 2022. Alerta-se para o risco inerente de descontinuidade dos serviços essenciais de TIC que a administração está assumindo ao postergar tais testes.

O plano de ação apresentado estabelece uma relação de dependência entre os testes de continuidade e a definição, pela Oficina de Design Thinking, dos serviços essenciais, o que inviabilizou, segundo a unidade, o planejamento e execução dos mesmos até o presente momento. A SEAUD sugere que a estratégia que envolve essa ação seja revista, a fim de se avaliar a efetividade da mesma em relação a definição dos serviços essenciais pela alta administração, ou a possibilidade de se estabelecer uma ação alternativa que possa ser resolvida de forma mais rápida e previsível, dada a necessidade de mitigação do risco envolvido.

A análise da equipe de auditoria reconhece a importância da intenção da unidade em priorizar os testes de continuidade necessários em relação ao PJe, enfatizando, contudo, que a resposta da DISEG à RDI SEAUD 14/2023 não deixa claro se os prazos estabelecidos para as ações de criação e execução do Plano de Testes dos Serviços Continuados de TIC, se referem ao teste de continuidade do PJe especificamente. Contudo, cabe destacar que a recomendação só será efetivamente cumprida com a realização dos testes de continuidade de todos os serviços essenciais do Tribunal.

2.2.3 Status da Recomendação

Recomendação **EM IMPLEMENTAÇÃO.**

## 3. CONCLUSÃO

O monitoramento de recomendações é etapa fundamental do trabalho de auditoria. O monitoramento consiste na adoção de ações pela SEAUD para verificar se as unidades auditadas cumpriram, implementaram, as recomendações emitidas pela Auditoria e se as medidas adotadas foram suficientes para solucionar a situação apontada pela Auditoria.

A responsabilidade de atendimento às recomendações emitidas pela Secretaria de Auditoria compete, inicialmente, aos gestores das unidades auditadas. À SEAUD cabe estabelecer e realizar o processo de monitoramento da implementação das recomendações, verificando a efetividade de suas recomendações.

No tocante ao atendimento das recomendações presentes no Relatório de Auditoria nº 07/2022, verificou-se que as 3 recomendações encontram-se ainda em fase de implementação pela

SETIN/DISEG. A análise da SEAUD é de que as ações definidas no plano de ação da unidade não são suficientes para garantir o cumprimento das recomendações.

Em relação à recomendação R.3, alerta-se para o risco inerente de descontinuidade dos serviços essenciais de TIC que a administração assume quando decide postergar tais testes, dada a dependência estabelecida pela parte auditada em relação à realização da Oficina de Design Thinking para a definição dos serviços essenciais, que segundo a unidade não tem prazo definido para conclusão. Ressalta-se ainda que o cumprimento da recomendação encontra-se pendente desde a publicação do Relatório de Auditoria nº 07/2022, que já previa a necessidade da realização dos testes a partir de 2022.

## 4. PROPOSTA DE ENCAMINHAMENTO

Ante o exposto, submete-se o presente relatório à Presidência do TRT da 8ª Região, conforme disposto no artigo 52, da Resolução CNJ nº 309/2020, para conhecimento dos resultados obtidos no 1º monitoramento das recomendações expedidas no Relatório de Auditoria nº 07/2022.

Por oportuno, a Secretaria de Auditoria propõe a continuidade do monitoramento e, ainda, que a SETIN/DISEG **reformule o plano de ação no prazo de 30 dias**, submetendo o documento para avaliação da SEAUD neste prazo. O plano de ação deve conter pelo menos: (i) objetivo geral que se pretende alcançar por meio das ações; (ii) ações que serão realizadas; (iii) objetivo de cada uma das ações; (iv) cronograma para desenvolvimento das ações; e (v) responsável pela execução de cada ação.

Belém, 14 de dezembro de 2023.

MARCIO MAGALHAES DE ANDRADE SILVA:30883091

Assinado de forma digital por MARCIO MAGALHAES DE ANDRADE SILVA:30883091
Dados: 2023.12.14 15:38:10 -03'00'

Márcio Magalhães de Andrade Silva
Chefe da Seção de Auditoria de Tecnologia da Informação - SeATI

LUCIANA KELLY MAIA CORREIA:30882557

Assinado de forma digital por LUCIANA KELLY MAIA CORREIA:30882557
Dados: 2023.12.14 15:42:45 -03'00'

Luciana Correia
Diretora da SEAUD