PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
SECRETARIA DE AUDITORIA INTERNA

EDSON FURTADO ALVES JUNIOR
16/01/2026 08:57

WHANDER JEFFSON DA SILVA COSTA
16/01/2026 09:44

RELATÓRIO FINAL DE AUDITORIA

Auditoria de Avaliação da Gestão de Banco de Dados de Tecnologia da Informação e Comunicação

Secretaria de Auditoria Interna - SEAUDI

Porto Velho/RO, janeiro de 2026

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
SECRETARIA DE AUDITORIA INTERNA

Sumário

1. APRESENTAÇÃO

O presente Relatório Final de Auditoria decorre dos trabalhos de avaliação da Gestão de Banco de Dados de Tecnologia da Informação e Comunicação (TIC) do Tribunal Regional do Trabalho da 14ª Região, realizados em conformidade com o Plano Anual de Auditoria (PAA) 2024 e com as diretrizes estabelecidas na Resolução CNJ nº 309/2020 e no Manual de Auditoria do Poder Judiciário.

A auditoria teve como foco a conformidade normativa, a eficiência, a eficácia e a efetividade dos controles internos administrativos relacionados à gestão de bancos de dados, considerando os exercícios de 2023, 2024 e 2025.

2. OBJETIVO DA AUDITORIA

Avaliar a existência, a eficiência e a eficácia dos controles internos administrativos na Gestão de Banco de Dados de TIC, à luz das diretrizes estabelecidas nos atos normativos elencados no item 9 deste Plano, especificamente com o objetivo de contribuir para:

- A conformidade legal da gestão de banco de dados de TIC com os objetivos institucionais e estratégicos do Poder Judiciário e Institucional;
- O alinhamento e a adequação dos controles internos com as políticas de institucionais e com as boas práticas da área de Tecnologia;
- A melhoria da eficiência operacional dos controles internos administrativos da Gestão de Banco de Dados;
- A melhoria e a implantação dos processos de trabalhos referentes à área de Banco de Dados.

3. ESCOPO DA AUDITORIA

O escopo da Auditoria da Gestão de Banco de Dados de Tecnologia da Informação e Comunicação incluiu:

- A avaliação da aplicação das políticas de segurança da informação e de cópias (*backups*) de segurança relacionadas a área de Banco de Dados informatizados;
- A verificação dos procedimentos utilizados para salvaguarda, segurança, monitoramento e otimização das consultas ao Banco de Dados realizadas por meio dos sistemas utilizados pelo Tribunal;
- A análise dos controles internos administrativos existentes no Tribunal, sobretudo na Secretaria de Tecnologia da Informação e Comunicação - SETIC, referente ao gerenciamento dos dados registrados em Bancos de Dados.

4. METODOLOGIA

Os trabalhos foram desenvolvidos mediante abordagem baseada em riscos e envolveram testes de controles e de procedimentos substantivos, ou seja, a análise dos sistemas de controles internos, documental, diligências, entrevistas com gestores e responsáveis, além de observações *in loco* e revisão analítica dos registros e controles internos, com a utilização dos seguintes procedimentos e papéis de trabalhos:

- Informações Requeridas: Coleta de informações sobre processos e procedimentos que evidenciem o planejamento, a execução e o monitoramento das ações referentes aos serviços de Banco de Dados. Os procedimentos serão realizados.
- Fontes de Informação: Documentação relacionada à Política de Segurança da Informação, de Backup, ao Plano Estratégico Institucional, às Resoluções do CNJ e do CSJT, e outros normativos.
- Procedimentos: Verificação do cumprimento dos normativos e regulamentações; análise da padronização de atividades e rotinas; avaliação do uso racional e produtivo da força de trabalho.
- Técnicas de Auditoria: Análise documental, entrevistas, diligências, exame dos registros, observação *in loco*, revisão analítica.

5. QUESTÕES DE AUDITORIA

Os trabalhos de auditoria foram orientados por questões de auditoria previamente definidas, elaboradas com base no objetivo do trabalho, na análise de riscos e nos critérios normativos e técnicos aplicáveis à gestão de bancos de dados de Tecnologia da Informação e Comunicação (TIC), tendo sido aplicadas as seguintes questões de auditoria:

- 1. Há um **Gerenciamento Contínuo dos Dados** registrados em bancos de dados informatizado, de acordo com as normas institucionais e as boas práticas na área de tecnologia?;
- 2. Foi realizada a **Gestão de Riscos sobre os dados** registrados em Banco de Dados?;
- 3. A **Política de Cópia de Segurança (*Backup*)** do banco de dados vem sendo aplicada de forma contínua?;
- 4. Os **controles internos sobre os usuários de Sistemas** de Banco de Dados - BD são adequados?;
- 5. Os **mecanismos para monitorar, otimizar e atualizar o Banco de Dados** vem sendo aplicados periodicamente?;

- 6. Foram implementadas **medidas efetivas para reduzir o risco de Violação ou Adulteração de Dados** registrados?;
- 7. O **Processo de Gerenciamento da Capacidade** vem sendo aplicado para o banco de dados?;
- 8. A Gestão de Banco de Dados vem automatizando processos por meio da implantação de ferramentas de **Business Intelligence (BI) ou da implementação de Inteligência Artificial (IA)** no Tribunal?.

As respostas às questões de auditoria foram obtidas por meio da análise documental, da aplicação de questionário de auditoria às unidades envolvidas e da avaliação das evidências apresentadas pelas áreas auditadas, permitindo à equipe de auditoria formar juízo técnico acerca da conformidade, da efetividade dos controles internos e do nível de maturidade da gestão de banco de dados do Tribunal.

Os resultados decorrentes da análise das questões de auditoria fundamentaram a identificação dos achados, o reconhecimento das boas práticas existentes e a formulação das recomendações apresentadas neste Relatório Final, assegurando a rastreabilidade entre o planejamento, a execução dos trabalhos e as conclusões alcançadas.

6. CRITÉRIOS DE AUDITORIA

Os critérios de auditoria incluíram as normas institucionais, regulamentações, e boas práticas aplicáveis à gestão de dados registrados em banco de dados, que visam propiciar a melhoria dos processos de trabalhos, com o objetivo de identificar eventuais fragilidades acerca dos controles internos existentes no âmbito do Poder Judiciário e do TRT da 14º Região, conforme quadro abaixo:

Normas	Assunto
Resolução CNJ n. 325, de 29 de junho de 2020	Estratégia Nacional do Poder Judiciário 2021/2026.
Resolução CNJ n. 370, de 28 de janeiro de 2021	Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o sexênio 2021-2026.
Planejamento Estratégico Participativo - PEP	Plano Estratégico Participativo do Tribunal Regional do Trabalho da 14ª Região (PEP 2021-2026).
Manual de Auditoria do Poder Judiciário (2023)	Procedimentos de auditoria necessários para execução dos diversos tipos de trabalhos de avaliação e consultoria no âmbito do Poder Judiciário.

Resolução Administrativa TRT14 n. 82/2022	Política de Governança de Tecnologia da Informação e Comunicação - TIC no âmbito do TRT da 14ª Região.
Resolução Administrativa TRT14 n. 66/2021	Política de Privacidade e Proteção de Dados Pessoais no âmbito do TRT da 14ª Região.
Portaria GP Nº 581, de 29 de maio de 2024	Política de Segurança da Informação no âmbito do TRT da 14ª Região.
Portaria GP Nº 988, de 1º de agosto de 2023.	Política de *Backup* (cópias de segurança) das informações eletrônicas no âmbito do TRT da 14ª Região.
Processos de Trabalho	Mapeamento dos Processos de Gerenciamento da Gestão de Configuração e Ativos de TIC, da Capacidade, de Disponibilidade, de Cópias de Segurança e Restauração de Dados e de Níveis de Serviços de TIC instituídos pelo TRT da 14ª Região.

Os critérios acima reportados são de natureza institucional, normativa e regulatória, focando na conformidade legal, eficiência, eficácia e integração dos processos da gestão de banco de dados, em especial com os objetivos estratégicos do TRT da 14ª Região.

7. ACHADO DE AUDITORIA

Achado: Falhas na Gestão de Controle de Acesso dos Usuários aos Sistemas

Objeto: Privilégios de usuários de Banco de Dados.

Situação Encontrada: Verificou-se a inexistência de processo de trabalho formalmente mapeado e sistematizado para a concessão e revogação de privilégios de usuários de sistemas de banco de dados. Embora a Política de Segurança da Informação estabeleça diretrizes gerais sobre o tema e a SETIC execute ações de bloqueio e revogação de acessos, tais medidas não garantem, de forma plena, a retirada tempestiva e integral de todas as permissões dos usuários desligados da Instituição.

Critérios:
- Portaria TRT14 n. 581, de 29/05/2024 (Política de Segurança da Informação);
- Boas Práticas de TIC para Banco de Dados.

Evidência:
- Respostas às questões 4.1 e 4.2 do questionário de auditoria.

Causas Prováveis:
- Inexistência de estudo de caso;

- Limitações em relação aos sistemas não desenvolvidos pelo TRT14.

Efeitos/Riscos:

- Risco de acessos indevidos;
- Possibilidade de violação, adulteração ou vazamento de dados;
- Comprometimento da integridade, confidencialidade e disponibilidade das informações.

Recomendação inicial

Recomendamos que a Secretaria de Tecnologia da Informação e Comunicação (SETIC) faça uma análise, em conjunto, com a Secretaria de Governança e Gestão Estratégica (SEGGEST) e a Secretaria de Gestão de Pessoas (SGEP), com a finalidade de verificar uma solução sistemática para a melhoria da gestão das permissões dos usuários de sistemas de informação, mapeando a referida solução por meio de Método Operacional Padronizado (MOP), a fim de evitar riscos à segurança da informação.

8. MANIFESTAÇÃO DA UNIDADE AUDITADA

A unidade auditada informou, por meio do Documento nº 36 do PROAD nº 8317/2024, que, em atenção ao item constante do Quadro de Resultados Preliminares (Doc. nº 27), referente à desativação de usuários nos sistemas informatizados com credenciais de acesso geridas pela SETIC, que embora ainda não haja um Método Operacional Padronizado (MOP) específico sobre a matéria, a Portaria GP nº 0581/2024, especialmente o seu Anexo III, estabeleceu diretrizes claras acerca da gestão de identidades, acessos e privilégios, bem como define as atribuições da SETIC, das chefias imediatas e da Secretaria de Gestão de Pessoas (SGEP) quanto à criação, alteração e desativação de credenciais de acesso aos sistemas institucionais.

Informou ainda que, no âmbito da Secretaria de Tecnologia da Informação e Comunicação (SETIC), o tema é tratado de forma contínua em fórum permanente mantido no Google Chat, dedicado à avaliação de credenciais, procedimentos de desativação e automação de rotinas sempre que possível e que nessa instância, aplica-se a abordagem mais restritiva e que ofereça maior garantia de segurança ao acesso e à preservação dos dados, estendendo-se não apenas aos sistemas sob gestão direta da SETIC, mas também a outras soluções informatizadas.

Ademais, informou que foi implantado um serviço de auditoria de acessos, que diariamente gera alertas sobre possíveis inconsistências, permitindo pronta atuação das áreas de banco de dados, sistemas, infraestrutura e segurança, como exemplo, notificações de situações em que usuários inativos no SIGEP ainda permanecem cadastrados no PJe, possibilitando correções tempestivas.

Mas reconheceu que, em relação a sistemas externos administrados por unidades negociais, a SETIC identificou que, ao menos aparentemente, não há gestão regular quanto à desativação de contas.

Assim, a SETIC entende que há necessidade de que tais unidades sejam formalmente oficiadas para implementar rotinas periódicas de revisão e desativação de acessos e que por questões de segurança da informação, não encaminham os registros das discussões mantidas no grupo interno de Google Chat “Desativação de usuários inativos”.

Entendeu também que, caso seja necessário, poderá ser concedido acesso controlado ao auditor responsável pelo sistema, e que, ainda sem um MOP publicado, a SETIC adota medidas técnicas e administrativas adequadas e contínuas para coibir acessos indevidos e preservar a segurança dos dados.

Nesse contexto, a SETIC manifestou o entendimento de que a elaboração de um Método Operacional Padronizado (MOP) específico poderia resultar na divulgação indevida de informações sensíveis, com potencial risco à segurança da informação, motivo pelo qual solicitou o cancelamento da parte da determinação que determina a elaboração do MOP.

9. AVALIAÇÃO DA AUDITORIA INTERNA

A equipe de auditoria reconhece as iniciativas adotadas pela Secretaria de Tecnologia da Informação e Comunicação na área de segurança dos , ressaltando que a recomendação apresentada visa ao fortalecimento da governança e à mitigação de riscos, sem prejuízo das práticas atualmente implementadas.

Considera, ainda, que a elaboração de um Método Operacional Padronizado (MOP) excessivamente detalhado poderia, de fato, resultar na divulgação indevida de informações sensíveis relativas aos acessos dos usuários aos sistemas informatizados.

Não obstante, esta equipe de auditoria entende que as unidades envolvidas necessitam avaliar e implementar uma solução sistemática para a melhoria da gestão das permissões dos usuários de sistemas de informação, a fim de mitigar riscos e fortalecer os controles internos, sem exposição de informações sensíveis.

10. RECOMENDAÇÃO

Recomendamos que a Secretaria de Tecnologia da Informação e Comunicação (SETIC) faça uma análise, em conjunto, com a Secretaria de Governança e Gestão Estratégica (SEGGEST) e a Secretaria de Gestão de Pessoas (SGEP), com a finalidade de **verificar uma solução sistemática para a melhoria da gestão das permissões dos usuários de sistemas de informação utilizados pelo TRT da 14ª Região**, a fim de evitar riscos à segurança da informação.

11. CONCLUSÃO

A presente auditoria evidenciou que o TRT da 14ª Região dispõe de controles internos, políticas e práticas aderentes às diretrizes normativas e às boas práticas aplicáveis à Gestão de Bancos de Dados de Tecnologia da Informação e Comunicação (TIC), apresentando nível de maturidade satisfatório na área auditada. Constatou-se, nesse contexto, a existência de políticas institucionais atualizadas de segurança da informação, bem como de mecanismos de monitoramento de acessos, com geração de alertas para identificação de inconsistências.

Em conclusão, esta equipe de auditoria entende que o achado identificado no item 7 não compromete, de forma significativa, o conjunto da gestão, mas evidencia oportunidade de aprimoramento da governança de acessos, com vistas ao fortalecimento da segurança da informação e à mitigação de riscos residuais.

12. ENCAMINHAMENTO

Diante do exposto, submetem-se os autos à consideração superior, com fundamento no art. 51 da Resolução CNJ nº 309/2020, para apreciação e aprovação da recomendação de auditoria constante do item 10 deste Relatório Final de Auditoria, propondo-se à Presidência do Tribunal a adoção das providências cabíveis ao atendimento da recomendação apresentada.

Porto Velho/RO, 16 de janeiro de 2026.

(assinado digitalmente) WHANDER JEFFSON DA SILVA COSTA Assistente	(assinado digitalmente) EDSON FURTADO ALVES JÚNIOR Secretário de Auditoria Interna