TRT-4ª REGIÃO
Secretaria de Auditoria

JOSE CLAUDIO DA ROSA RICCARDI
03/12/2025 13:36

ADRIANO PRADO CAVALHEIRO
03/12/2025 13:40

DEBORA KATI DOS SANTOS SOUZA DARGEN
03/12/2025 14:19

CAROLINA FEUERHARMEL LITVIN
03/12/2025 14:40

FELIPE VIEGAS DA SILVA
19/12/2025 12:34

RELATÓRIO FINAL DE AUDITORIA

AUDITORIA EM GERENCIAMENTO DE INFRAESTRUTURA TECNOLÓGICA E SERVIÇOS EM NUVEM

DEZEMBRO/2025

TRT-4ª REGIÃO
Secretaria de Auditoria

DA AUDITORIA

Modalidade: conformidade

Relatório nº: 03/2025

PROAD nº: 5356/2025

Objeto da auditoria: Gerenciamento de infraestrutura de TIC e serviços em nuvem.

Objetivo da auditoria: Avaliar a implementação da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) do Tribunal, com foco no gerenciamento da infraestrutura tecnológica de TIC e nas estratégias e requisitos adotados em relação à prestação de serviços em nuvem.

Integrantes da auditoria: Adriano Prado Cavalheiro, Débora Kati dos Santos Souza Dargen, Felipe Viegas da Silva (Equipe de Auditoria)
José Cláudio da Rosa Riccardi (Auditor responsável)
Carolina Feuerharmel Litvin (Supervisora)

DA UNIDADE AUDITADA

Unidade auditada: **Secretaria-Geral de Tecnologia e Inovação (SGTI)**

Responsável pela unidade auditada:

Nome: Natacha Moraes de Oliveira
Função: Secretária-Geral de Tecnologia e Inovação
Período: desde 30.09.2025 (Portaria nº 2.223/2025)

SUMÁRIO EXECUTIVO

O QUE FOI AUDITADO?

A presente auditoria buscou avaliar a implementação da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) do Tribunal, com foco no gerenciamento da infraestrutura tecnológica de TIC. O escopo do trabalho, definido com base na análise dos riscos, compreendeu os seguintes processos: i) gestão de configuração e ativos de TIC; ii) gerenciamento da disponibilidade e da capacidade de TIC e iii) backup e recuperação de dados.

POR QUE ESTE TRABALHO FOI REALIZADO?

A seleção desta auditoria para compor o Plano Anual de Auditoria (PAA) – Exercício 2025 deu-se em virtude de sua classificação como quinto processo mais relevante e crítico a ser auditado dentre o universo de processos auditáveis disponíveis para o período. Este posicionamento reflete a importância estratégica do objeto para o Tribunal. O trabalho está alinhado ao Plano Estratégico Institucional 2021-2026, especialmente aos OE #6 – Garantir a Efetividade do Tratamento das Demandas Repetitivas, #7 – Fortalecer a Governança e a Gestão Estratégica e #10 – Aprimorar a Governança de Tecnologia da Informação e Comunicação – TIC e a Proteção de Dados. Ainda, contribui para o cumprimento da Estratégia Nacional do Poder Judiciário para o período 2021-2026, em relação ao macrodesafio "Fortalecimento da Estratégia Nacional de TIC e Proteção de Dados".

QUAIS FORAM AS CONCLUSÕES E AS PROPOSTAS DE ENCAMINHAMENTO?

A auditoria constatou que o processo de gerenciamento de infraestrutura tecnológica do TRT4, em geral, está em conformidade com a legislação adotada como critério para o trabalho e que a área técnica possui controles relevantes institucionalizados. Destaca-se que para a questão de auditoria referente ao processo de Gerenciamento da Disponibilidade e da Capacidade de TIC, não foram identificadas divergências em relação às normas e boas práticas aplicáveis. Após a realização das análises, a equipe de auditoria concluiu pela apresentação das seguintes propostas de encaminhamento:

R1. RECOMENDA-SE à Secretaria-Geral de Tecnologia e Inovação que, a fim de mitigar o risco de comprometimento da confiabilidade, precisão e rastreabilidade dos ativos de infraestrutura, assegure que os inventários operacionais do Banco de Dados do Gerenciamento da Configuração (BDGC) contemplem as informações mínimas estabelecidas em norma, em atendimento ao disposto na Resolução CNJ n° 370/2021, na Resolução CSJT nº 397/2024, na Portaria GP.TRT4 nº 6.371/2016, na Portaria CNJ n° 162/2021 (Anexo IV), na ABNT NBR ISO/IEC 27002:2022, na Norma Complementar nº 10/IN01/DSIC/GSIPR de 2012, no CIS Controls v8.1 e no COBIT 2019 – BAI10 – Managed Configuration.

R2. RECOMENDA-SE à Secretaria-Geral de Tecnologia e Inovação que, a fim de mitigar o risco de prejuízo à rastreabilidade e ao gerenciamento do ciclo de vida dos ativos de infraestrutura, realize a revisão e a compatibilização dos registros dos ativos constantes nos inventários operacionais com aqueles do sistema Patrimônio, de modo a atender ao disposto na Resolução CSJT nº 397/2024, na Portaria CNJ n° 162/2021 (Anexo IV), na Norma Complementar nº 10/IN01/DSIC/GSIPR de 2012, na ABNT NBR ISO/IEC 27002:2022.

R3. RECOMENDA-SE à Secretaria-Geral de Tecnologia e Inovação que, a fim de mitigar o risco de inviabilidade de recuperação de dados com informações críticas, e de forma a atender ao disposto na Portaria CNJ nº 162/2021, Anexo IV, na norma ABNT NBR ISO/IEC 27002:2022 e nas boas práticas previstas no COBIT 2019 e CIS Controls v8.1: (i) restabeleça os testes de recuperação de dados, bem como sua validação, para os grupos de backup dos arquivos armazenados em diretórios de rede da Capital e do interior; (ii) revise o quadro do item 7.2 do Anexo 4 da Portaria GP.TRT4 nº 4.772/2008 (NSI004 – Procedimentos de backup e recuperação de dados) de forma a atualizar e compatibilizar o normativo interno com as rotinas efetivamente praticadas para o grupo de backup de Dados dos Sistemas Armazenados no Banco de Dados da Capital; e (iii) ajuste seu processo de trabalho para que sejam devidamente gerados e retidos os registros (*logs*) dos testes de recuperação de dados dos backups realizados, bem como sejam expedidos os respectivos atestes por parte da equipe responsável.

S1. SUGERE-SE à Secretaria-Geral de Tecnologia e Inovação que, com o intuito de garantir maior alinhamento às boas práticas de governança e de segurança da informação, avalie a conveniência e a oportunidade de revisar a NSI004, contemplando: (i) a segregação entre a política de backup e recuperação de dados e os planos operacionais; e (ii) a adoção das boas práticas de controle recomendadas pelo Tribunal de Contas da União nos questionários de autoavaliação de controles internos relacionados à Política, aos planos e aos procedimentos de backup.

QUAIS OS PRÓXIMOS PASSOS?

Após a decisão da Presidência acerca deste Relatório, a Seaudi realizará o monitoramento das propostas de encaminhamento acolhidas.

LISTA DE SIGLAS E ABREVIATURAS

AIC	Atributo de Item de Configuração
BDGC	Banco de Dados do Gerenciamento da Configuração
CNJ	Conselho Nacional de Justiça
CIS	Center for Internet Security (Centro para Segurança na Internet)
COBIT	Control Objectives for Information and Related Technologies (Controle de Objetivos para Informação e Tecnologias Relacionadas)
CSJT	Conselho Superior da Justiça do Trabalho
DIRAUD-Jud	Diretrizes Técnicas das Atividades de Auditoria Interna Governamental do Poder Judiciário
ENTIC-JUD	Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário
IC	Item de Configuração
NSI	Norma de Segurança da Informação
PAA	Plano Anual de Auditoria
PALP	Plano de Auditoria de Longo Prazo
PEI	Plano Estratégico Institucional
PROAD-OUV	Sistema de Processo Administrativo Virtual e Ouvidoria Eletrônico
PSI	Política de Segurança da Informação
RDI	Requisição de Documentos e Informações
Seaudi	Secretaria de Auditoria
Seinfra	Secretaria de Infraestrutura de TIC
Setic	Secretaria de Tecnologia da Informação e Comunicações
SGTI	Secretaria-Geral de Tecnologia da Informação e Inovação
TCU	Tribunal de Contas da União
TIC	Tecnologia da Informação e Comunicação
TRT4	Tribunal Regional do Trabalho da 4ª Região

SUMÁRIO

1. INTRODUÇÃO

1.1. APRESENTAÇÃO

A presente auditoria foi incluída no item 1.4 do Plano Anual de Auditoria (PAA) – Exercício 2025 (PROAD nº 7001/2024), em atendimento ao Plano de Auditoria de Longo Prazo – Quadriênio 2022-2025. A ordem de prioridade dos processos auditáveis foi definida com base em critérios de criticidade e relevância, incluindo o grau de interesse da Alta Administração. O processo **Gestão de Infraestrutura e Serviços de Tecnologia da Informação e Comunicação (TIC)** ocupou o 5º lugar na ordem de classificação e foi selecionado para ser avaliado no presente exercício.

A realização deste trabalho apresenta relevância para a gestão administrativa do Tribunal e alinha-se ao Planejamento Estratégico Institucional (PEI 2021-2026), especialmente em relação aos seguintes objetivos estratégicos: #6 Garantir a Efetividade do Tratamento das Demandas Repetitivas, #7 Fortalecer a Governança e a Gestão Estratégica e #10 Aprimorar a Governança de Tecnologia da Informação e Comunicação – TIC e a Proteção de Dados. Além disso, a auditoria contribui para o cumprimento da Estratégia Nacional do Poder Judiciário para o período 2021-2026, em relação ao macrodesafio "Fortalecimento da Estratégia Nacional de TIC e Proteção de Dados".

Em consonância com esse macrodesafio, foi instituída a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), por meio da Resolução CNJ nº 370/2021. Essa norma tem como principal objetivo promover a melhoria da governança, da gestão e da colaboração tecnológica no Poder Judiciário, buscando eficiência, eficácia, efetividade e economicidade dos órgãos na utilização dos recursos e na entrega de resultados à sociedade. O presente trabalho está diretamente relacionado ao objetivo 8 da ENTIC-JUD – Promover Serviços de Infraestrutura e Soluções Corporativas.

Dessa forma, com o propósito de apoiar a Administração do TRT4 no alcance de seus objetivos estratégicos e no alinhamento com os macrodesafios do Poder Judiciário, esta auditoria tem como finalidade avaliar os procedimentos adotados por este Tribunal no gerenciamento de infraestrutura tecnológica, verificando sua

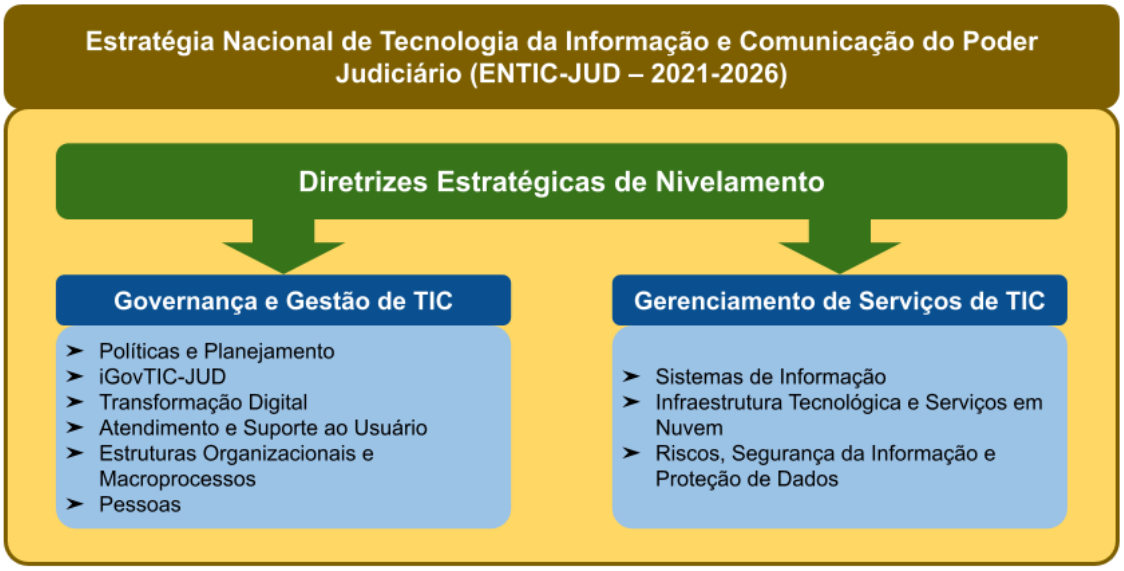
conformidade em relação à legislação vigente e às boas práticas de governança e gestão de TIC.

1.2. VISÃO GERAL DO OBJETO

A Tecnologia da Informação e Comunicação constitui-se como elemento essencial para a consecução da missão institucional da Justiça do Trabalho, na medida em que viabiliza a execução célere, eficiente e transparente das atividades judiciais e administrativas. Nesse contexto, a adequada gestão da infraestrutura de TIC, pautada por boas práticas e pela conformidade normativa, torna-se imperativa para garantir que os serviços oferecidos atendam a padrões previamente acordados e alinhados aos objetivos institucionais.

No âmbito do Poder Judiciário, a ENTIC-JUD tem como principal objetivo, harmonizar as ações de tecnologia entre os tribunais, promovendo uma gestão mais eficiente e estratégica da TIC para elevar a qualidade da prestação jurisdicional. Para isso, essa norma atua como um guia para a modernização tecnológica, estabelecendo diretrizes, prioridades e metas que devem orientar o planejamento e a execução dos processos de TIC em todos os órgãos do Judiciário. Sua execução ocorre de maneira colaborativa e participativa, alinhada com as Diretrizes Estratégicas de Nivelamento. Essas diretrizes, por sua vez, são divididas em **dois domínios**: Governança e Gestão, e Gerenciamento de Serviços de TIC, conforme ilustrado pela figura abaixo:

Figura 1 – Diretrizes Estratégicas de Nivelamento da ENTIC-JUD



Fonte: elaboração própria.

O tema Infraestrutura Tecnológica e Serviços em Nuvem, escopo desta auditoria, está contido no domínio Gerenciamento de Serviços de TIC. Conforme preconizado pela Resolução CNJ nº 370/2021:

> Art. 34. Os itens de **infraestrutura tecnológica deverão atender as especificações, temporalidade de uso e obsolescência a serem regulados em instrumentos aplicáveis e específicos**.
> § 1º Deverão ser observadas as necessidades estratégicas dos órgãos do Poder Judiciário para que as especificações dos produtos constantes no parque tecnológico estejam adequadas e compatíveis.
> § 2º **A gestão dos ativos de infraestrutura tecnológica deverá ser realizada por meio da definição dos processos, visando o registro e monitoramento da localização de cada ativo**.
> § 3º A manutenção de documentos eletrônicos, incluindo o armazenamento e descarte, deverá seguir as diretrizes definidas na Recomendação CNJ n o 46/2013 e na Lei no 13.709/2018, e alterações posteriores.
> Art. 35. **Recomenda-se utilizar serviços em nuvem que simplificam a estrutura física**, viabilizam a integração, requisitos aceitáveis de segurança da informação, proteção de dados, disponibilidade e padronização do uso dessa tecnologia no Poder Judiciário. (grifo nosso).

De acordo com Laudon (2017 apud VARELLA, 2019)[1]:

> A infraestrutura de TI de uma empresa se refere aos equipamentos de hardware, como computadores, servidores, sistemas de armazenamento, sistemas de segurança, redes e comunicação, sistemas operacionais e diversos aplicativos cuja finalidade é atender às necessidades de negócios das organizações.

A infraestrutura de TIC pode ser implantada nas próprias instalações da organização (*on-premises*) ou utilizando computação em nuvem (*cloud computing*).

Considerando que a definição de infraestrutura de TIC é ampla, para este trabalho de auditoria adotou-se aquela prevista na Portaria GP.TRT4 nº 6.371/2016:

> Art. 3º Esta norma refere-se aos seguintes ativos de Tecnologia da Informação e Comunicações (TIC):
> [...]
> II – os equipamentos e soluções de **infraestrutura, tais como datacenters, geradores, equipamentos de armazenamento (storage), soluções de backup e de segurança, servidores, ativos de rede, nobreaks de datacenter**; (grifo nosso)

O quadro a seguir apresenta a definição desses ativos e soluções de infraestrutura de TIC:

[1] VARELLA, Walter Augusto. Infraestrutura de TI. São Paulo: Editora Senac São Paulo, 2019.

Quadro 1 – Equipamentos e soluções de infraestrutura (Portaria GP.TRT4 nº 6.371/2016)

Ativo	Definição resumida	Referência
Datacenter	A maior parte do hardware de infraestrutura de TIC está hospedada em datacenters. Um datacenter é um ambiente que inclui fonte de alimentação, refrigeração, prevenção e detecção de incêndio, racks de equipamentos e outras instalações necessárias para hospedar os componentes de infraestrutura instalados.	LAAN, Sjaak. IT *Infrastructure Architecture – Infrastructure Building Blocks and Concepts* (*4th Edition*). Editora Lulu Press Inc., 2023.
Geradores	Fornecer energia elétrica no caso de falha da rede elétrica. Um gerador de energia pode alimentar o datacenter por um período indefinido (desde que haja combustível disponível), até que o fornecimento de energia da concessionária seja restaurado.	LAAN, Sjaak. IT *Infrastructure Architecture – Infrastructure Building Blocks and Concepts* (*4th Edition*). Editora Lulu Press Inc., 2023.
Equipamento de armazenamento (storage)	O armazenamento storage, de uma forma geral, é um repositório onde estão centralizados os dados da rede local de uma organização, podendo funcionar como servidor de arquivos ou como backup, ou ainda uma área de compartilhamento de informações e colaboração.	VARELLA, Walter Augusto. Infraestrutura de TI. São Paulo: Editora Senac. São Paulo, 2019.
Soluções de backup e segurança	Backups são cópias de dados, usadas para restaurá-los a um estado anterior em caso de perda, corrupção ou situação de recuperação de desastre. Os backups são sempre o último recurso, usados apenas se tudo mais falhar, para salvaguardar uma organização em caso de desastre.	LAAN, Sjaak. IT *Infrastructure Architecture – Infrastructure Building Blocks and Concepts* (*4th Edition*). Editora Lulu Press Inc., 2023.
Servidores	Um servidor é um computador com um sistema operacional construído para armazenar dados, compartilhar recursos e atender à solicitação de diversos usuários. Por isso, em uma empresa, o servidor se torna um equipamento importante na infraestrutura de TIC, funcionando, de maneira colaborativa, como um repositório que armazena diversos tipos de arquivos.	VARELLA, Walter Augusto. Infraestrutura de TI. São Paulo: Editora Senac. São Paulo, 2019.
Ativos de rede	São usados para conectar os componentes da infraestrutura. São exemplos: roteadores, switches, firewalls.	LAAN, Sjaak. IT *Infrastructure Architecture – Infrastructure Building Blocks and Concepts* (*4th Edition*). Editora Lulu Press Inc., 2023.
Nobreaks de datacenter	Fornecer energia ao datacenter por um curto período de tempo, até que os geradores entrem em funcionamento.	LAAN, Sjaak. IT *Infrastructure Architecture – Infrastructure Building Blocks and Concepts* (*4th Edition*). Editora Lulu Press Inc., 2023.

No âmbito do TRT4, a área técnica responsável pela infraestrutura de TIC era a Secretaria de Tecnologia da Informação e Comunicações (atual Secretária-Geral de Tecnologia e Inovação) que, conforme artigo 1º da Portaria GP.TRT4 nº 486/2023:

> [...] É responsável pela prospecção de soluções, pelo desenvolvimento e implantação de sistemas e serviços, bem como pela **infraestrutura tecnológica apropriada às necessidades identificadas**, promovendo a inovação e adotando boas práticas de gestão de TI, com o objetivo de colaborar para o aprimoramento da prestação jurisdicional sob os aspectos da legalidade, da legitimidade, da economicidade, da eficiência e da eficácia. (grifo nosso)

Na antiga estrutura da Setic, a Coordenadoria de Infraestrutura Tecnológica (atual Secretaria de Infraestrutura e Serviços) era responsável por planejar, implementar, manter e aprimorar continuamente a infraestrutura de hardware, software e telecomunicações necessárias para a prestação dos serviços de Tecnologia da Informação e Comunicações, no âmbito do TRT4.

1.3. OBJETIVOS E ESCOPO DA AUDITORIA

O objetivo geral desta auditoria é o de avaliar a implementação da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) do Tribunal, com o foco no gerenciamento da infraestrutura tecnológica de TIC.

Inicialmente cabe destacar que o PAA – Exercício 2025 previu que os serviços em nuvem iriam compor o escopo desta auditoria. Entretanto, após a conclusão do estudo preliminar do objeto, e posterior realização de reunião com a área de Tecnologia da Informação e Comunicações do TRT4, em 12.09.2025, optou-se por excluir esse item do escopo da auditoria. Essa exclusão mostrou-se apropriada, considerando que este Tribunal não possui sua infraestrutura – ou mesmo parte dela – em nuvem. Atualmente, o TRT4 possui apenas a contratação de aplicativos em nuvem. Diante disso, concluiu-se que a abordagem mais adequada seria tratar o tema em uma auditoria específica voltada à gestão de contratos de TIC, o que caracterizaria um novo trabalho, a ser abordado futuramente. Da mesma forma, o datacenter foi retirado do escopo, uma vez que seus serviços também são prestados por empresas contratadas.

Quanto à relação entre os domínios da ENTIC-JUD e as auditorias previstas no Plano de Auditoria de Longo Prazo – 2022-2025 (PROAD nº 7490/2021), destaca-se que o domínio Governança e Gestão de TIC foi avaliado em 2023, enquanto o domínio Gerenciamento de Serviços de TIC foi dividido em três auditorias distintas: a primeira, relacionada à Gestão de Segurança da Informação e Proteção de Dados, realizada por meio de uma Ação Coordenada do Conselho Superior da Justiça do Trabalho (CSJT) em 2022; a segunda, relativa ao Gerenciamento dos Sistemas de TIC, realizada em 2024, e a presente auditoria, com foco em Gestão de Infraestrutura de TIC, conforme resumido no quadro 2, abaixo:

Quadro 2 – PALP 2022-2025 e ENTIC-JUD 2021-2026

Auditoria	Exercício	Domínio da ENTIC-JUD
Gestão de Segurança da Informação e Proteção de Dados **(realizada – PROAD nº 2861/2022)**	2022	Gerenciamento de Serviços de TIC (tema: Riscos, Segurança da Informação e Proteção de Dados)
Governança e Gestão de TIC **(realizada - PROAD nº 2572/2023)**	2023	Governança e Gestão de TIC
Gerenciamento dos Sistemas de TIC **(realizada - PROAD n° 304/2024)**	2024	Gerenciamento de Serviços de TIC (tema: Sistemas de Informação)
Gestão de Infraestrutura e Serviços de TI	2025	Gerenciamento de Serviços de TIC (tema: **Infraestrutura Tecnológica e Serviços em Nuvem**)

Para a delimitação do escopo deste trabalho, primeiramente, foi realizado o mapeamento do macroprocesso de Gerenciamento de infraestrutura de TIC, para que a equipe de auditoria formasse um entendimento sobre o objeto da auditoria. Assim, foram identificados três processos principais relacionados ao objeto desta auditoria:

P1. Gestão de Configuração e Ativos de TIC;

P2. Gerenciamento da Disponibilidade e Capacidade de TIC; e

P3. Backup e Recuperação de Dados.

Os dois primeiros processos foram mapeados pela área técnica e estão disponíveis no Portal da Governança de TIC. Já o processo referente ao backup e recuperação de dados foi mapeado com base na norma NSI004 – Procedimentos de backup e recuperação de dados. Esta norma é complementar às diretrizes gerais

definidas na Política de Segurança da Informação do TRT4, editada pela Portaria GP.TRT4 nº 4.772/2028.

Posteriormente, foram levantados os riscos associados às etapas de cada processo. Então, cada risco foi classificado em relação à probabilidade e ao impacto de sua ocorrência. Por fim, selecionaram-se os riscos inerentes mais significativos em cada um dos processos para compor o escopo do trabalho, ou seja, aqueles cuja classificação resultou em um nível de risco alto. Esses riscos nortearam a elaboração das questões de auditoria.

1.4. QUESTÕES DE AUDITORIA

As questões de auditoria, elaboradas pela equipe durante a fase de planejamento, foram as seguintes:

Q1. A Gestão de Configuração e Ativos de TIC, no âmbito do TRT4, segue as normas e boas práticas aplicáveis?

Q2. O Gerenciamento de Disponibilidade e Capacidade de TIC, no âmbito do TRT4, segue as normas e boas práticas aplicáveis?

Q3. A realização de backup e recuperação de dados, no âmbito do TRT4, atende ao disposto na Portaria GP.TRT4 nº 4.772/2008 e às boas práticas aplicáveis?

Para cada questão de auditoria foram elaboradas subquestões que avaliam os assuntos apresentados, conforme detalhado no quadro a seguir.

Quadro 3 – Principais pontos avaliados nas subquestões de auditoria

Questão	Principais Pontos Avaliados nas Subquestões de Auditoria
Q1	• Cadastro dos Itens de Configuração (IC) no Banco de Dados do Gerenciamento da Configuração (BDGC) com seus respectivos atributos (AIC) e responsáveis; • Atualização do BDGC, tanto da desativação de ICs quanto da atualização de AICs, de forma a refletir a realidade e necessidades específicas do TRT4.
Q2	• Realização de monitoramento da capacidade de uso e disponibilidade dos serviços de infraestrutura; • Adoção de medidas para corrigir as eventuais inconformidades apontadas na etapa de monitoramento da capacidade e disponibilidade das soluções de infraestrutura.
Q3	• Execução dos procedimentos de backup em conformidade com a política do TRT4 e boas práticas identificadas; • Realização dos testes periódicos de recuperação de dados, com a frequência e abrangência definidas na política interna e boas práticas identificadas; • Documentação dos resultados dos testes de recuperação de dados.

1.5. METODOLOGIA UTILIZADA E LIMITAÇÕES À AUDITORIA

Os trabalhos foram realizados em conformidade com a Resolução CNJ nº 309/2020, que aprova as Diretrizes Técnicas das Atividades de Auditoria Interna Governamental do Poder Judiciário – DIRAUD-Jud e dá outras providências, e com a Portaria GP.TRT4 nº 3.215/2024, que regulamenta a atividade de auditoria desenvolvida pela Secretaria de Auditoria do Tribunal Regional do Trabalho da 4ª Região.

As técnicas de auditoria utilizadas pela equipe para obtenção das informações necessárias à análise do objeto foram: (i) análise documental de documentos compartilhados pela área cliente; (ii) exame de registros, por meio de consulta às informações constantes no sistema PATRIMÔNIO – Sistema de Controle Patrimonial do TRT da 4ª Região e no sítio eletrônico do Portal da Governança de TIC do TRT4; (ii) aplicação de checklists e *benchmarking* com outros Tribunais; (iii) aplicação de questionário, por meio de Requisição de Documentos e Informações (RDI), e (iv) realização de entrevistas com a área técnica para o entendimento dos processos relacionados ao objeto deste trabalho e esclarecimento das dúvidas da equipe.

Não foram verificadas dificuldades ou restrições na aplicação dos procedimentos de auditoria, sendo que a equipe de auditoria foi prontamente atendida pela área de TIC em todas as requisições formuladas.

Todos os procedimentos encontram-se documentados nos papéis de trabalho da auditoria, e a metodologia adotada é detalhada a seguir.

1.5.1. Estudo Preliminar

A partir do estudo de normativos, de trabalhos de auditoria anteriormente realizados por esta Secretaria, por outros Tribunais do Trabalho e pelo Conselho Superior da Justiça do Trabalho, bem como da jurisprudência do Tribunal de Contas da União, normas técnicas e *frameworks* de governança e gestão de tecnologia da informação, a equipe de auditoria levantou os possíveis critérios para o trabalho. Também foi realizada, em 12.09.2025, a primeira reunião entre a Secretaria de Auditoria (Seaudi) e a SGTI para troca de informações e alinhamento de expectativas em relação ao trabalho (documento nº 4). Nessa oportunidade ocorreu: (i) a validação dos critérios legais aplicáveis ao objeto da auditoria, por parte da área

técnica; (ii) o entendimento dos processo internos relacionados à infraestrutura; e (iii) a compreensão dos principais desafios e limitações enfrentados pela área, em relação ao objeto do presente trabalho.

Após, a equipe elaborou a matriz de avaliação de riscos da auditoria, atividade que demandou: (i) o entendimento dos processos auditados, englobando seus objetivos e respectivas etapas; (ii) a análise e validação do mapeamento dos processos de Gestão de Configuração e Ativos de TIC e de Gerenciamento da Disponibilidade e Capacidade de TIC realizado pela SGTI; (iii) o mapeamento do processo de Backup e Recuperação de Dados; (iv) a avaliação dos riscos genéricos e detalhados; (v) a classificação da probabilidade e do impacto de cada risco identificado para a obtenção dos riscos inerentes; e (vi) o levantamento dos controles existentes para obtenção dos riscos residuais, referentes aos riscos significativos. Em 08.10.2025, foi realizada a segunda reunião entre Seaudi e SGTI (documento nº 10) para validação dos controles identificados pela equipe de auditoria para os riscos inerentes mais significativos de cada processo.

Com base nessa matriz, considerando o custo-benefício de se avaliar todos os riscos identificados, a equipe de auditoria priorizou aqueles classificados como alto. Diante dessa análise, foi definido o escopo do trabalho e foram elaboradas as questões de auditoria.

1.5.2. Programa de Auditoria

Após o levantamento preliminar, a equipe de trabalho elaborou o Programa de Auditoria, que apresentou os critérios aplicáveis, o objetivo geral, as questões de auditoria e o detalhamento dos procedimentos e dos testes a serem aplicados na fase de execução do trabalho, bem como a estimativa de custos, os recursos humanos necessários e o cronograma do trabalho. O Programa foi compartilhado com a unidade auditada para ciência sobre as diretrizes e os critérios legais que embasam a execução do trabalho (documento nº 7).

Na sequência, em 17.10.2025, foi realizada reunião de abertura da auditoria com a participação da gestora da unidade auditada e dos integrantes das equipes da SGTI responsáveis pelos processos auditados, com o intuito de apresentar as principais informações sobre a auditoria e esclarecer alguns pontos sobre o objeto

(documentos nºs 11 e 12). Na ocasião, foi oportunizada à área auditada a inclusão de algum item no escopo do trabalho, conforme preconizado no parágrafo único artigo 9º da Portaria GP.TRT4 nº 3.215/2024.

Tendo em vista que não houve manifestação da unidade envolvida acerca da alteração do escopo, foi consolidado o Programa de Auditoria.

1.5.3. Coleta de Dados

Para a coleta dos dados necessários ao alcance do objetivo do trabalho, a equipe analisou os documentos compartilhados pela SGTI. Também foram coletadas informações dos scripts, elaborados pela área técnica para as rotinas de backup e dos respectivos *logs*, gerados pelos sistemas responsáveis pela execução das cópias de segurança. Além disso, foram extraídos dados do sistema PATRIMÔNIO.

1.5.4. Análise

Na sequência, a equipe reuniu e examinou todas as informações coletadas sob a perspectiva das questões de auditoria e dos critérios adotados como referência para o presente trabalho.

1.5.5. Elaboração da Matriz de Achados e do Relatório Preliminar

Com base nos resultados obtidos, foi elaborada a Matriz de Achados, que reuniu as informações relacionadas aos achados de auditoria e às eventuais oportunidades de melhoria. Após aprovação da supervisora, foram consolidados os achados que compõem o presente relatório.

A equipe designada para o trabalho realizou reunião para apresentação dos achados às equipes técnicas responsáveis pelos processos auditados, em 14.11.2025 (documento nº 17), a fim de promover o diálogo sobre as constatações do trabalho, as possíveis soluções para os problemas identificados e as propostas de encaminhamento preliminares. Na sequência, foi realizada nova reunião para apresentação dos resultados da auditoria à gestora da SGTI e à Presidência, em 18.11.2025 (documento nº 19). Após a reunião, foi encaminhado o Relatório Preliminar com a consolidação dessas informações à unidade auditada.

1.5.6. Manifestação da área responsável

O relatório preliminar foi submetido à manifestação da área responsável, oportunidade em que foram apresentados esclarecimentos adicionais sobre atos e fatos administrativos sob sua responsabilidade.

1.5.7. Elaboração do Relatório Final

Por fim, recebidas e analisadas as manifestações, foram consolidadas as propostas de encaminhamento da equipe de auditoria no presente relatório.

1.6. CRITÉRIOS DE AUDITORIA

Todos os critérios considerados para este trabalho foram apresentados no Programa de Auditoria (documento nº 7), dos quais se destacam os seguintes:

- Resolução CNJ nº 370/2021 – Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Resolução CNJ n° 162/2021 – Anexo IV – Proteção de Infraestruturas Críticas de TIC – Aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
- Resolução CSJT nº 397/2024 – Institui a Política de Gerenciamento de Serviços de Tecnologia da Informação e Comunicação no âmbito da Justiça do Trabalho;
- Portaria GP.TRT4 nº 4772/2008 – Norma NSI004 – Procedimentos de backup e recuperação de dados;
- Norma Complementar nº 10/IN01/DSIC/GSIPR de 2012, que estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações, dos órgãos e entidades da Administração Pública Federal, direta e indireta;
- COBIT 2019 – Modelo Corporativo para Governança e Gestão de TIC da Organização, elaborado pela ISACA;
- ABNT NBR ISO/IEC 27002:2022 – Fornece um conjunto de referência de controles genéricos de segurança da informação, incluindo orientação para implementação;

- CIS *Controls* v8.1 – Fornece as diretrizes para a implementação de controles de segurança cibernética, desenvolvido pelo *Center for Internet Security* (CIS);

1.7. BENEFÍCIOS ESTIMADOS

Entre os benefícios estimados desta auditoria estão: (i) o fortalecimento da governança e da gestão da área técnica, pela aderência de seus procedimentos às normas e boas práticas; (ii) a manutenção de inventário de ativos de infraestrutura atualizado e contendo as informações mínimas exigidas em normas; (iii) a melhoria do controle e da rastreabilidade dos ativos de infraestrutura tecnológica, por meio da conciliação das informações do Banco de Dados do Gerenciamento da Configuração (BDGC) com o sistema patrimonial do TRT4; (iv) o aumento da efetividade da recuperação de dados, caso o Tribunal precise restaurá-los a partir das cópias de backup; e (v) o aperfeiçoamento da Política de Segurança da Informação, especialmente quanto aos procedimentos de backup e recuperação de dados.

2. RESULTADOS DA AUDITORIA

Este capítulo apresenta os resultados de auditoria obtidos a partir dos procedimentos realizados para responder às três questões propostas neste trabalho. De modo geral, a auditoria constatou que os procedimentos adotados pela Secretaria-Geral de Tecnologia e Inovação estão em conformidade com a legislação adotada como critério para o trabalho. Destaca-se que na questão 2 – referente ao processo de Gerenciamento da Disponibilidade e da Capacidade de TIC – não foram identificadas divergências em relação às normas e boas práticas aplicáveis. Esse resultado evidencia o comprometimento e a maturidade da equipe da Secretaria de Infraestrutura e Serviços (Seinfra) na condução das atividades de gerenciamento da disponibilidade e da capacidade de TIC.

Contudo, considerando o papel da auditoria interna de agregar valor e contribuir para o aprimoramento das atividades da gestão, são apresentados, a seguir, dois achados de auditoria e, no capítulo 3, é apresentada uma oportunidade

de melhoria. O objetivo é fortalecer a governança e a gestão da SGTI, além de aperfeiçoar o processo de Gerenciamento de Configuração e Ativos de TIC, bem como a política e os procedimentos de backup e recuperação de dados deste Tribunal.

A1. A manutenção de inventário de ativos de infraestrutura com informações mínimas, atualizado e integrado ao processo de gestão patrimonial fortalece o controle, a rastreabilidade e a segurança dos recursos tecnológicos do órgão.

Situação encontrada

A Resolução CNJ n° 370/2021, em relação à infraestrutura tecnológica, estabelece que:

> Art. 34. Os itens de infraestrutura tecnológica **deverão atender as especificações, temporalidade de uso e obsolescência a serem regulados em instrumentos aplicáveis e específicos**.
> § 1º Deverão ser observadas as necessidades estratégicas dos órgãos do Poder Judiciário para que as especificações dos produtos constantes no parque tecnológico estejam adequadas e compatíveis.
> § 2º A gestão dos ativos de infraestrutura tecnológica deverá ser realizada por meio da **definição dos processos, visando o registro e monitoramento da localização de cada ativo**. (grifo nosso).

No âmbito da Justiça do Trabalho, a Resolução CSJT nº 397/2024, que institui a Política de Gerenciamento de Serviços de Tecnologia da Informação e Comunicação, dispõe em seu artigo 5º, inciso IX, que:

> Art. 5º Na implementação das práticas obrigatórias de Gerenciamento de Serviços de TIC, os Tribunais Regionais do Trabalho observarão as seguintes diretrizes: [...]
> IX – Gerenciamento de Ativos de TIC
> No Gerenciamento de Ativos de TIC, observar-se-ão:
> a) **a interação com o processo institucional de gestão patrimonial, com escopo de atuação detalhado, a fim de evitar sobreposição**; e
> b) **a sincronização com as movimentações dos ativos de TIC realizadas por meio de outras práticas ou processos de gestão patrimonial do órgão**.
> **Os ativos de infraestrutura deverão conter informações mínimas, tais como: tipo, localização, responsável técnico e cópia de segurança**. (grifo nosso)

No âmbito deste Tribunal, a Portaria GP.TRT4 nº 6.371/2016, que estabelece as diretrizes para a Gestão de Ativos de Tecnologia da Informação e Comunicações e institui o processo de Gestão de Configuração e Ativos de TIC no TRT4, dispõe em seu artigo 15 e §1º que:

> Art. 15. O **inventário de ativos** será realizado utilizando todas as ferramentas e meios disponíveis, conjugando os resultados emitidos pelos sistemas corporativos e outros documentos de controle.

> § 1º **Na identificação do ativo deverá constar, no mínimo, sua descrição, configurações de hardware, versões de software, localização** e, quando pertinente, sua criticidade ou relevância, considerando os serviços e sistemas que ele suporta. (grifo nosso)

Alinhando-se a essas diretrizes, a Portaria CNJ n° 162/2021, que aprova os protocolos e manuais criados pela Resolução CNJ nº 396/2021, apresenta em seu Anexo IV o Manual de Referência – Proteção de Infraestruturas Críticas de TIC. Esse documento "[...] baseia-se em um **conjunto de controles mínimos exigidos compreendidos como pertinentes e condizentes com a realidade do Judiciário**.". Um dos controles apresentados, no tópico "Inventário e controle de ativos de hardware" é:

> 1.3 **Manter inventário atualizado e preciso de todos os ativos de tecnologia** que detenham o potencial de armazenamento ou processamento de informações. Esse inventário deve incluir ativos de hardware, conectados ou não à rede da organização.

Adicionalmente, a Norma Complementar nº 10/IN01/DSIC/GSIPR de 2012, que estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações, dos órgãos e entidades da Administração Pública Federal, direta e indireta, preconiza que:

> 4.4 O processo de Inventário e Mapeamento de Ativos de Informação tem como objetivo prover o órgão ou entidade da APF: de um **entendimento comum, consistente e inequívoco de seus ativos de informação; da identificação clara de seu(s) responsável(eis)** – proprietário(s) e custodiante(s); de um conjunto completo de informações básicas sobre os requisitos de segurança da informação e comunicações de cada ativo de informação; de uma descrição do contêiner de cada ativo de informação; e da identificação do valor que o ativo de informação representa para o negócio do órgão ou entidade da APF;
> [...]
> 4.6 O processo de Inventário e Mapeamento de Ativos de Informação, deve ser **dinâmico, periódico e estruturado, para manter a Base de Dados de Ativos de Informação atualizada** e conseqüentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação e Comunicações. (grifo nosso).

A ABNT NBR ISO/IEC 27002:2022, norma de referência para controles de segurança da informação, estabelece, em seu item 5.9, orientações essenciais com o intuito de garantir a identificação das informações relativas aos ativos das organizações:

> Convém que o inventário de informações e outros ativos associados seja preciso, atualizado, consistente e alinhado com outros inventários. As opções para assegurar a exatidão de um inventário de informações e outros ativos associados incluem:

> a) **conduzir análises críticas regulares de informações identificadas e outros ativos associados contra o inventário de ativos**;
> b) **impor automaticamente uma atualização de inventário no processo de instalação, alteração ou remoção de um ativo**.
> **Convém que a localização de um ativo seja incluída no inventário conforme apropriado**.
> O inventário **não precisa ser uma única lista** de informações e outros ativos associados. Convém que **o inventário seja mantido pelas funções relevantes**, que pode ser visto como **um conjunto de inventários dinâmicos**, como inventários de ativos de informação, hardware, software, máquinas virtuais (VM), instalações, pessoal, competências, capacidades e registros. (grifo nosso).

No âmbito das referências internacionais de segurança cibernética, o *CIS Controls* v8.1, por meio do controle 1 que trata do inventário e controle de ativos empresariais (*Control 1 – Inventory and Control of Enterprise Assets*), reforça a necessidade de detalhamento no controle dos recursos. A salvaguarda específica, *1.1 – Establish and Maintain Detailed Enterprise Asset Inventory*, recomenda que **o inventário de ativos seja preciso e atualizado**, abrangendo uma vasta gama de dispositivos, incluindo servidores e dispositivos de rede. Além disso, a norma prescreve que este inventário deve registrar informações específicas como endereço de rede, nome da máquina, proprietário do ativo de dados, departamento e status de aprovação de conexão, destacando a abrangência de dados requerida pelas boas práticas de gestão de ativos de segurança.

A necessidade de detalhamento e manutenção do repositório é corroborada pelo COBIT 2019, por meio do processo *BAI10 – Managed Configuration*, que visa manter um repositório atualizado de itens de configuração (ICs), preenchendo **todas as alterações de configuração**.

Assim, percebe-se a ênfase que os normativos e as boas práticas apresentadas atribuem ao gerenciamento dos ativos de tecnologia da informação. A manutenção de um ou mais inventários dos recursos tecnológicos de forma completa e atualizada possibilita à organização monitorar seus ativos, registrando as informações mínimas pertinentes a cada um deles, bem como as eventuais alterações. Além disso, destaca-se a importância de **conciliar as informações presentes nos inventários de ativos de TIC com o sistema patrimonial** da instituição, viabilizando a rastreabilidade e o controle efetivo dos recursos tecnológicos do órgão.

Em resposta à RDI Seaudi n° 08/2025 (documento n° 2), quando questionada sobre os artefatos utilizados para a gestão de configuração e dos ativos de infraestrutura, a Secretaria-Geral de Tecnologia e Inovação manifestou-se nos seguintes termos (documento n° 3):

> A Planilha "Plano de Renovação de Infraestrutura" **centraliza informações relevantes**, a fim de fornecer subsídios para manter a infraestrutura de TIC do TRT4 atualizada.
> [...]
> Os links para **acesso aos artefatos de inventário estão contidos no Plano de Renovação de Infraestrutura, na coluna "Inventário Operacional"**.
> A coluna aponta para o controle de inventário específico de cada ativo de infraestrutura. Pode ser uma lista de equipamentos ou o manual de instalação e manutenção de um software, conforme o tipo de ativo. (grifo nosso).

Em análise ao documento Plano de Renovação de Infraestrutura, verificou-se que o processo de Gestão e Configuração de Ativos de TIC vem sendo executado pela área técnica. Entretanto, identificaram-se pontos de aprimoramento nos inventários de controle utilizados, conforme descrito a seguir.

a) Informações mínimas presentes nos inventários de ativos de infraestrutura tecnológica

Pela análise dos documentos de inventário, associados ao Plano de Renovação de Infraestrutura, inicialmente verificou-se que esses não são padronizados. Essa característica não representa necessariamente um problema, visto que cada inventário foi elaborado em função das características dos bens nele contidos, bem como das necessidades específicas de cada equipe responsável pelos ativos. Entretanto, conforme mencionado anteriormente, a Resolução CSJT nº 397/2024 e a Portaria GP.TRT4 nº 6.371/2016 apresentam, cada uma, um rol de informações mínimas para identificação de um ativo. Assim, entende-se que os inventários deveriam possuir um conjunto de informações mínimas, além das demais informações específicas relacionadas a cada tipo de ativo.

A título exemplificativo, uma das informações mínimas elencadas na Resolução CSJT nº 397/2024 é o responsável técnico. Para as planilhas de inventário abaixo, não foi localizado campo próprio para preenchimento dessa informação:

- Inventário – Wireless Cisco (Access Points, Controladoras e WLANs);
- Inventário – Wireless Alcatel (Access Points e WLANs);
- Inventário – Switches - Seriais e Patrimônio (abas “Alcatel”, “Huawei” e “Topologia Huawei”);
- No-Breaks Interior;
- Inventário Servidores DIRT.

Já no documento Inventario – serviços, ativos, hardware, software, apesar de existir uma coluna para identificação da seção responsável, em consulta realizada em 10.11.2025, identificou-se que 26 dos 163 itens listados (aproximadamente 16% do total) não possuíam responsável técnico designado.

Outro exemplo diz respeito ao tipo ou descrição do ativo, conforme previsto tanto na Resolução CSJT nº 397/2024, quanto na Portaria GP.TRT4 nº 6.371/2016. No Inventário – Switches – Seriais e Patrimônio, aba "Alcatel", verificou-se que os itens com "Sysname" cadastrados como "Enviados previamente" e "Sem definição (DAC 40G)", possuíam apenas a coluna “CAB-PN”, preenchida. As demais colunas (Pav, Rack, Chassis, Modelo, Patrimônio, *MAC Address* e *Serial Number*) não estavam preenchidas. Durante a reunião realizada com a equipe da Seinfra, em 23.10.2025, esclareceu-se que esses itens se tratavam de cabos *stack*.

b) Alinhamento entre os inventários para os ativos de infraestrutura tecnológica e o Sistema de Patrimônio

Ao analisar as informações dos ativos de informática cadastrados no Sistema de Patrimônio do Tribunal, comparando-as com as informações dos ativos de infraestrutura relacionados nos inventários mantidos pela Secretaria de Infraestrutura e Serviços, observaram-se algumas situações de desalinhamento parcial.

A título de exemplo, compararam-se as informações de localização de alguns ativos de rede dos inventários da Seinfra com o sistema Patrimônio. De forma amostral, foi elaborada uma relação de itens com localização divergente entre os dois controles. Essa relação foi apresentada à área técnica em reunião realizada no dia 23.10.2025, que apresentou, posteriormente, manifestação, conforme consta no documento nº 16. Pela análise da manifestação da área técnica, verificou-se que,

em alguns casos, a informação correta era aquela presente nos inventários da Seinfra; em outros, porém, o sistema de Patrimônio era quem continha a informação correta.

Em outra situação, localizou-se, no sistema Patrimônio, dois equipamentos nobreaks de data center, identificados pelos patrimônios nº 02.165.03033 e nº 02.165.03034. Entretanto, esses itens não foram localizados nos inventários mantidos pela área técnica.

Critérios de auditoria

- Resolução CNJ n° 370/2021, artigo 34, §§1º e 2º;
- Portaria CNJ nº 162/2021 – Anexo IV (Manual de Referência – Proteção de Infraestruturas Críticas de TIC), item 8: Inventário e controle de ativos de hardware;
- Resolução CSJT nº 397/2024, artigo 5º, inciso IX;
- Portaria GP.TRT4 nº 6.371/2016, artigo 15, §1º;
- ABNT NBR ISO/IEC 27002:2022, item 5.9;
- COBIT 2019, BAI10 – *Managed Configuration*;
- CIS *Controls* v8.1, *Control 1 – Inventory and Control of Enterprise Assets*.

Evidências

- RDI Seaudi nº 08/2025 (documento n° 3);
- Localização de ativos de infraestrutura tecnológica (documento n° 16);
- Plano de Renovação de Infraestrutura;
- Inventário – Wireless Cisco (Access Points, Controladoras e WLANs);
- Inventário – Wireless Alcatel (Access Points e WLANs);
- Inventário – Switches - Seriais e Patrimônio (abas “Alcatel”, “Huawei” e “Topologia Huawei”);
- Inventario – serviços, ativos, hardware, software;
- No-Breaks Interior;
- Inventário Servidores DIRT;
- Processo de Gestão de Configuração e Ativos de TIC.

Possíveis causas

- Falha ou insuficiência na coleta e/ou inserção dos dados de itens de configuração (ICs) e seus respectivos atributos;
- Informações não registradas no inventário por já serem de conhecimento dos(as) servidores(as) da Seinfra;
- Ausência de rotina periódica de conferência das informações inseridas nos inventários operacionais e no sistema Patrimônio;
- Ausência de etapa de compatibilização entre as informações do inventário de infraestrutura tecnológica e sistema de patrimônio no Processo de Gestão de Configuração e Ativos de TIC.

Efeitos

- Desconhecimento dos ativos críticos da organização, podendo comprometer a rastreabilidade e a segurança das informações patrimoniais e operacionais;
- Dificuldade para planejar renovações, acompanhar o ciclo de vida e avaliar a obsolescência dos ativos de infraestrutura;
- Comprometimento da completude e da confiabilidade dos registros pela ausência de informações mínimas exigidas pelas normas.

Manifestação do Auditado

A Secretaria-Geral de Tecnologia e Inovação não manifestou discordância pela situação encontrada neste achado (documento nº 23):

> [...] venho manifestar que esta área técnica está de acordo com o novo processo participativo promovido pela SEAUDI nesta auditoria, onde o relatório preliminar reflete os achados e propostas de encaminhamento discutidos junto a esta unidade auditada.
> Considerando a inexistência de ações corretivas antecipadas para as recomendações e oportunidades de melhoria contidos no relatório, informo que esta Secretaria-Geral irá apresentar o devido Plano de Ações para tais propostas de encaminhamento, no prazo de 60 dias previsto no plano de auditoria.

Conclusão da Equipe de Auditoria

Esta equipe de auditoria entende pertinente manter as duas propostas de encaminhamento para o achado A1, considerando que não houve discordância da Secretaria-Geral de Tecnologia e Inovação para a situação encontrada neste achado. As propostas de encaminhamento tem como objetivo aprimorar a

integridade e a precisão do Banco de Dados do Gerenciamento da Configuração e de formalizar a sincronização com o sistema de gestão patrimonial.

Proposta de Encaminhamento

R1. RECOMENDA-SE à Secretaria-Geral de Tecnologia e Inovação que, a fim de mitigar o risco de comprometimento da confiabilidade, precisão e rastreabilidade dos ativos de infraestrutura, assegure que os inventários operacionais do Banco de Dados do Gerenciamento da Configuração (BDGC) contemplem as informações mínimas estabelecidas em norma, em atendimento ao disposto na Resolução CNJ n° 370/2021, na Resolução CSJT nº 397/2024, na Portaria GP.TRT4 nº 6.371/2016, na Portaria CNJ n° 162/2021 (Anexo IV), na ABNT NBR ISO/IEC 27002:2022, na Norma Complementar nº 10/IN01/DSIC/GSIPR de 2012, no *CIS Controls* v8.1 e no COBIT 2019 – *BAI10 – Managed Configuration*.

R2. RECOMENDA-SE à Secretaria-Geral de Tecnologia e Inovação que, a fim de mitigar o risco de prejuízo à rastreabilidade e ao gerenciamento do ciclo de vida dos ativos de infraestrutura, realize a revisão e a compatibilização dos registros dos ativos constantes nos inventários operacionais com aqueles do sistema Patrimônio, de modo a atender ao disposto na Resolução CSJT nº 397/2024, na Portaria CNJ n° 162/2021 (Anexo IV), na Norma Complementar nº 10/IN01/DSIC/GSIPR de 2012, na ABNT NBR ISO/IEC 27002:2022.

A2. A realização, validação e registro (*logs*) periódicos dos testes de recuperação dos backups fortalecem a efetividade da recuperação de dados quando necessário.

Situação encontrada

A Portaria GP.TRT4 nº 4.772/2008 institui a Política de Segurança da Informação (PSI) no âmbito do TRT4. Em seu Anexo 4 é apresentada a Norma de Segurança da Informação NSI004 – Procedimentos de backup e recuperação de dados. Nessa norma são apresentadas as diretrizes e os padrões para os procedimentos de backup, além dos testes de recuperação de dados, conforme definidos no item 7:

> 7. Testes de recuperação de dados
> 7.1. **Periodicamente serão realizados testes de recuperação de dados**.
> 7.2. Os testes serão baseados em dados pré-selecionados que garantam a efetividade, eficiência e confiabilidade do procedimento, na periodicidade e forma estabelecidas no quadro que segue:
> [...]
> 7.3. Os resultados dos testes **serão validados, de forma documentada**, pelas equipes identificadas no quadro anterior.
> 7.4. **Se restaurações de dados forem realizadas em períodos iguais ou menores que os definidos para os testes**, a equipe responsável pela execução dos testes poderá, a partir dos resultados obtidos, **considerar que tais ações têm validade como teste naquele período**. (grifo nosso)

O item 7.2 apresenta um quadro que define, para cada grupo de backup, as equipes responsáveis pela recuperação, a periodicidade, o tipo de recuperação, a equipe responsável pela validação e a metodologia a ser utilizada para que seja atestada a validação dos dados recuperados nos testes.

A realização de testes de recuperação de dados é uma ação amplamente recomendada, tanto por resoluções do Poder Judiciário, quanto por normas e *frameworks* destinados à gestão e ao gerenciamento das tecnologias da informação. Nesse sentido, cita-se novamente o Manual de Referência – Proteção de Infraestruturas Críticas de TIC, presente no Anexo IV da Portaria CNJ nº 162/2021. No tópico “Capacidade de recuperação de dados” é apresentado o seguinte controle:

> 9.3 **Testar a integridade dos dados nas mídias das cópias de segurança de forma regular**, por meio da realização de um processo de restauração dos dados, de forma a garantir que o processo de cópia de segurança (backup) esteja sendo executado de forma apropriada. (grifo nosso)

Da mesma maneira, a norma ABNT NBR ISO/IEC 27002:2022 estabelece em seu item 8.13:

> 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**;
> [...]
> e) **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. (grifo nosso).

Cita-se também o COBIT 2019, referência internacional de boas práticas. Em sua prática DSS04.07, que trata do gerenciamento dos arranjos de backup, é

sugerido, na atividade nº 3, que **os dados das cópias de segurança do tipo backup e archive sejam testados e atualizados periodicamente**.

Outra referência internacional, o CIS *Controls* v8.1, no Controle 11, dedicado à recuperação de dados, sugere que a cada trimestre (ou sempre que um novo processo ou tecnologia de backup for introduzido), uma equipe de testes deve avaliar uma amostra aleatória de backups e tentar restaurá-los em um ambiente de teste. Os backups restaurados devem ser verificados para garantir que o sistema operacional, o aplicativo e os dados do backup estejam intactos e funcionais. A salvaguarda *11.1: Establish and Maintain a Data Recovery Process*, **recomenda que se estabeleça e mantenha um processo documentado de recuperação de dados**. Que nesse processo, seja abordado o escopo das atividades de recuperação de dados, a priorização da recuperação e a segurança dos dados de backup. Além de proceder a revisão e atualização da documentação anualmente ou sempre que ocorrerem mudanças significativas na empresa que possam impactar essa salvaguarda.

Em sua manifestação à RDI Seaudi nº 11/2025 (documento nº 13), quanto à execução dos testes de recuperação e respectivo documento de validação dos resultados, a Secretaria-Geral de Tecnologia e Inovação informou que (documento nº 14):

> Desde 2014, os registros das execuções de recuperações solicitadas, bem como os testes realizados, são armazenados na planilha Backup/Recover – Testes de Recuperação de Dados.
> **Em todos os incidentes (chamados) em que se fez necessária a restauração de arquivos, o conteúdo se mostrou aproveitável**. Os registros desses restores podem ser encontrados na mesma planilha dos testes.
> Quando falamos de resultados de testes rotineiros de recuperação, no escopo proposto (arquivos capital/interior, BD capital e PJe), **nossa atuação oscila**:
>
> - **Arquivos armazenados em diretórios de rede na Capital**: Testes rotineiros de recuperação não foram retomados após a volta da pandemia;
> - **Arquivos armazenados em diretórios de rede do interior**: Testes rotineiros de recuperação não foram retomados após a volta da pandemia;
> - **Dados dos sistemas armazenados no Banco de Dados da Capital**: Há uma rotina de recuperação semanal que valida a saúde do backup e consistência dos dados, mas ela difere da lista de sistemas especificado na PSI e no momento não retém logs;
> - **Banco de dados do PJe-JT**: na planilha Backup/Recover – Testes de Recuperação de Dados encontram-se os registros dos testes e respectivos logs. (grifo nosso)

A partir da análise da planilha compartilhada pela área técnica com esta equipe de auditoria (Backup/Recover – Testes de Recuperação de Dados) verificaram-se as informações prestadas pela SGTI em sua manifestação. No quadro 4 é apresentada a situação de cada grupo de backup conforme a informação da área técnica e a análise documental executada pela Seaudi. Os grupos de backup do quadro 4 são os mesmos constantes do item 7.2 da NSI004.

Quadro 4 – Análise da execução dos testes de recuperação em função dos grupos de backup

Grupo de Backup	Análise da Seaudi
Arquivos armazenados em diretórios de rede na Capital	**Não estão sendo realizados**, conforme manifestação da SGTI.
Arquivos armazenados em diretórios de rede do interior	
Dados do inFOR do interior	**Realizados**. Testado por *restore* real dos dados, conforme Backup/Recover – Testes de Recuperação de Dados: ● 2022/1: Bagé ● 2022/2: Bento Gonçalves; ● 2023/1: São Borja ● 2023/2: Cachoeira do Sul; ● 2024/1: Novo Hamburgo - Centralização; ● 2024/2: Vacaria - Centralização; ● 2025/1: Camaquã.
Dados dos sistemas armazenados no Banco de Dados da Capital (inFOR, NovaJus4, Folha, RH, PJ4, System)	**Realizados parcialmente**. Conforme manifestação "Há uma rotina de recuperação semanal que valida a saúde do backup e consistência dos dados, mas ela difere da lista de sistemas especificados na PSI e no momento não retém logs". Em análise à planilha compartilhada (Backup/Recover – Testes de Recuperação de Dados), verifica-se também que foram realizados os seguintes restore dos dados: ● 2022: Sigabugfix 19C; ● 2023: Sigabugfix 19C (14/01 e 08/07); ● 2024: Sigabugfix 19C (13/01 e 06/07); ● 2025: Novajus4 (criação do banco PRDHML 19c), em 02/06 e NovaJus4, em 14/10.
PJe/Banco de dados	**Realizados**. Em análise à planilha compartilhada Backup/Recover – Testes de Recuperação de Dados, verificaram-se os seguintes testes: ● 2015: backup de produção + WALs testados mensalmente, com exceção de fev e jul; ● 2016: backup de produção + WALs testados mensalmente, com exceção de abril em que foi testado o archive de produção e out e nov em que não foram realizados testes; ● 2017: backup de produção + WALs testados em mar, jun e set;

	• 2018: backup de produção + WALs testados em mar, jun, set e dez; • 2019: backup de produção + WALs testados em fev, abr, set e dez; • 2020: backup de produção testado em fev, abr, set e dez; • 2021: backup de produção testado em fev, jun, ago e nov; • 2022: backup de produção testado mensalmente; • 2023: backup de produção testado em jan, fev, mar, abr, maio, jun. De julho em diante não foi testado por falta de espaço no storage; • 2024: backup de produção testado em dezembro. Nos demais meses não foram testados por falta de espaço no storage; • 2025: backup de produção testado mensalmente.

Assim, a **ausência de realização dos testes em todos os grupos de backup** representa uma lacuna em relação aos requisitos previstos no item 7.2 da NSI004. Da mesma forma, a carência de **registro para a devida documentação da validação** dos testes realizados prejudica o fiel atendimento do item 7.3 da NSI004. Essas duas situações evidenciam oportunidades de aprimoramento nos procedimentos adotados pela área técnica com as boas práticas, as quais preconizam que a realização periódica de testes de recuperação de dados (restore) dos backups – bem como seu registro e validação – aumenta a garantia de que, em situações reais em que a organização precise recuperar algum sistema e/ou dados a partir das cópias armazenadas, essa operação seja executada com sucesso.

Nesse contexto, a SGTI em resposta à RDI Seaudi nº 11/2025 demonstrou proatividade ao apresentar propostas que buscam solucionar as situações encontradas e reforçar a gestão da continuidade (documento nº 14):

> Considerando nossa defasagem em relação a PSI, incluímos aqui algumas propostas de ações por parte da SGTI que talvez possam ser analisadas durante a auditoria:
>
> - Para o grupo "**Arquivos em diretórios de rede na Capital**" e "**Arquivos armazenados em diretórios de rede do interior**": **Propomos automatizar os testes e validação de arquivos recuperados**. Adicionalmente, acelerar a migração desses arquivos de usuários para o Google Workspace, que possui mecanismos próprios de backup e já é amplamente utilizado (em grande parte porque arquivos em diretórios não podem ser utilizados no teletrabalho);
> - Dados dos **sistemas armazenados no Banco de Dados da Capital**: A rotina que recria semanalmente a base "Bugfix" **valida as mesmas etapas necessárias para a recuperação dos demais sistemas que constam na PSI (InFOR, NovaJus4, ADMEletrônico, RH e Folha)**. Todos esses sistemas fazem backup com o mesmo software (RMAN), para as mesmas mídias, através do mesmo hardware e são restaurados para o mesmo SGBD (Oracle). Assim, **propomos um**

> **ajuste na PSI para refletir a rotina já praticada e somente ela. Adicionalmente, ajustaremos o processo para que fiquem registrados os logs dessas recuperações e o ateste por parte da CDS que o sistema restaurado ficou operacional**. (grifo nosso)

Em análise às proposições da área de TIC, identificou-se um ponto de atenção, no que se refere à migração dos dados dos diretórios de rede da capital e do interior para o Google Workspace. Assim, no caso da transferência de dados para a nuvem, é necessário ponderar os riscos envolvidos nesse processo e as formas de mitigação, bem como as salvaguardas oferecidas para o backup e a recuperação desses dados. Essa avaliação deve assegurar que os requisitos de segurança sejam adequadamente cumpridos por parte dos provedores de nuvem pública. Além disso, essa migração de dados para a nuvem não exime a área técnica de efetuar as cópias de segurança para os arquivos que eventualmente permanecerem nos diretórios da Capital e interior.

Critérios de auditoria

- Portaria GP.TRT4 nº 4.772/2008, Anexo 4 (NSI004 – Procedimentos de backup e recuperação de dados), item 7;
- Portaria CNJ nº 162/2021 – Anexo IV (Manual de Referência – Proteção de Infraestruturas Críticas de TIC), item 8: Capacidades de recuperação de dados;
- COBIT 2019, DSS04 – *Managed Continuity*, DSS04.07 – *Manage backup arrangements*;
- ABNT NBR ISO/IEC 27002:2022, item 8.13;
- CIS *Controls* v8.1, *Control 11 – Data Recovery*.

Evidências

- RDI Seaudi nº 11/2025;
- Backup/Recover – Teste de Recuperação de Dados.

Possíveis causas

- Quantitativo insuficiente de servidores nas equipes responsáveis pela recuperação e validação dos testes;
- Eventual indisponibilidade de espaço de armazenamento para realização dos backups;

- Ferramentas utilizadas não retém os registros (*logs*) dos testes realizados.

Efeitos

- Possível insegurança quanto à integridade e à confiabilidade dos arquivos e dados dos backups realizados.
- Dificuldade para recuperação de dados, em especial informações críticas à instituição;
- Comprometimento da rastreabilidade, não sendo possível comprovar a realização dos testes, bem como a validade dos resultados pelas equipes competentes.

Manifestação do Auditado

A Secretaria-Geral de Tecnologia e Inovação não manifestou discordância pela situação encontrada neste achado (documento nº 23).

Conclusão da Equipe de Auditoria

Esta equipe de auditoria entende pertinente manter a proposta de encaminhamento para o achado A2, considerando que não houve discordância da Secretaria-Geral de Tecnologia e Inovação para a situação encontrada neste achado. Destaca-se que a proposta de encaminhamento está alinhada às propostas de ação apresentadas pela SGTI e tem como objetivo alinhar as práticas operacionais da área ao normativo interno e assegurar que a recuperação dos dados do Tribunal a partir das cópias de segurança funcione adequadamente quando necessária.

Proposta de Encaminhamento

R3. RECOMENDA-SE à Secretaria-Geral de Tecnologia e Inovação que, a fim de mitigar o risco de inviabilidade de recuperação de dados com informações críticas, e de forma a atender ao disposto na Portaria CNJ nº 162/2021, Anexo IV, na norma ABNT NBR ISO/IEC 27002:2022 e nas boas práticas previstas no COBIT 2019 e CIS *Controls* v8.1:

(i) restabeleça os testes de recuperação de dados, bem como sua validação, para os grupos de backup dos arquivos armazenados em diretórios de rede da Capital e do interior;

(ii) revise o quadro do item 7.2 do Anexo 4 da Portaria GP.TRT4 nº 4.772/2008 (NSI004 – Procedimentos de backup e recuperação de dados) de forma a atualizar e compatibilizar o normativo interno com as rotinas efetivamente praticadas para o grupo de backup de Dados dos Sistemas Armazenados no Banco de Dados da Capital;

(iii) ajuste seu processo de trabalho para que sejam devidamente gerados e retidos os registros (*logs*) dos testes de recuperação de dados dos backups realizados, bem como sejam expedidos os respectivos atestes por parte da equipe responsável.

3. OPORTUNIDADES DE MELHORIA

OM1. Oportunidade de revisão e aprimoramento da Norma NSI004 – Procedimentos de backup e recuperação de dados.

Situação encontrada

A partir da análise dos documentos compartilhados pela Secretaria-Geral de Tecnologia e Inovação, referentes aos procedimentos de backup executados pelo Tribunal, bem como sua manifestação à RDI Seaudi nº 11/2025 (documento nº 14), observou-se que a área técnica atua de forma consistente para atender ao objetivo definido na NSI004 – Procedimentos de backup e recuperação de dados (Anexo 4 da Portaria GP.TRT4 nº 4.772/2008):

> 1.1. Estabelecer diretrizes e padrões para os procedimentos de backup, testes e recuperação de dados realizados pela Secretaria de Tecnologia da Informação e Comunicações, no âmbito do Tribunal Regional do Trabalho da 4ª Região.

Dessa forma, a SGTI vem garantindo a salvaguarda dos dados, o que é essencial para a continuidade dos serviços prestados pelo Tribunal. Essa atuação está em consonância com as motivações contidas no item 2 da referida norma:

> 2.1. Alinhamento às normas, regulamentações e melhores práticas, relacionadas à matéria.
> 2.2. Garantia de que a salvaguarda das informações seja realizada de forma otimizada, atendendo às necessidades do Tribunal.

A partir da análise da NSI004, a equipe de auditoria verificou que seu conteúdo é adequado, pois dispõe sobre aspectos essenciais ao processo de

backup e aos testes de recuperação de dados (*restore*). Todavia, foram identificadas oportunidades de aprimoramento que podem tornar o documento mais abrangente e alinhado às normas e boas práticas nacionais e internacionais.

Assim, com base na análise dos questionários de autoavaliação de controles elaborados pelo Tribunal de Contas da União (TCU), bem como de políticas de backup adotadas por outros órgãos públicos, foram identificados **dois pontos que podem ser avaliados pela Secretaria-Geral de Tecnologia e Inovação para o aprimoramento da norma interna**.

O primeiro ponto diz respeito à **segregação entre a política e os planos operacionais**. A NSI004 reúne, em um único documento, tanto a política geral de backup e recuperação de dados quanto os planos operacionais. Essa abordagem contrasta com a recomendação de segregação desses instrumentos, conforme disposto na ABNT NBR ISO/IEC 27002:2022 (item 8.13):

> Convém que **uma política específica de tema sobre backup seja estabelecida** para atender aos requisitos de retenção de dados e segurança da informação da organização.
> [...]
> Convém que **planos sejam desenvolvidos e implementados** sobre como a organização fará cópia de segurança das informações, software e sistemas, para abordar a política específica por tema sobre backup. (grifo nosso).

Na mesma linha, o Modelo de Política de Backup da Secretaria de Governo Digital[2] sugere que:

> [...] é uma prática recomendada abrigar políticas e procedimentos em documentos separados para manter o conteúdo focado e reduzir o número de vezes que a política deve ser reaprovada pela alta administração.

Tal orientação também está presente na jurisprudência relativa ao tema, conforme Acórdão TCU nº 1109/2021 – Plenário (item 9.1):

> 9.1 recomendar ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), ao **Conselho Nacional de Justiça (CNJ)** e ao Conselho Nacional do Ministério Público (CNMP), com fundamento no art. 11 da Resolução - TCU 315/2020, que editem normativos para, cada um no seu âmbito de governança, **orientar os gestores e regulamentar a obrigatoriedade de que as entidades e órgãos públicos aprovem formalmente e mantenham atualizadas políticas gerais e planos específicos de backup (para suas bases de dados e sistemas críticos, por exemplo)** [...]. (grifo nosso)

[2] BRASIL. Secretaria de Governo Digital. **Modelo de Política de Backup**. Versão 2.0. Brasília, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modelo_politica_backup.pdf. Acesso em: 4 nov. 2025.

O Acórdão TCU nº 1109/2021 – Plenário também apresenta, como parte integrante da decisão, o relatório de fiscalização elaborado pela Secretaria de Fiscalização de Tecnologia da Informação que oferece o seguinte conceito:

> Em linhas gerais, essa **política consiste num acordo de alto nível entre as áreas de negócio ("dona" dos dados e/ou sistemas) e de TI da organização** para documentar de quais dados serão feitos os backups, as suas respectivas periodicidades, tipos, quantidades de cópias, locais de armazenamento, tempos de retenção e outros requisitos de segurança. Esses requisitos podem variar de acordo com cada base de dados ou sistema da organização, sendo que, para as bases de dados/arquivos/sistemas/aplicativos/servidores mais críticos, **eles podem ser detalhados em documentos específicos, chamados planos (ou procedimentos/roteiros/scripts) de backup**. (grifo nosso)

Verificou-se que o TRT2 (Ato GP nº 07/2015, artigo 8º-A), o TRT9 (Política nº 86/2024, artigo 6º) e o TRT12 (Portaria PRESI nº 235/2021, artigo 15) são exemplos de Tribunais que adotaram a prática de ter uma política de backup separada de seus planos operacionais, possibilitando que as revisões dos procedimentos operacionais sejam realizadas de forma ágil proporcionando maior capacidade de resposta às mudanças no ambiente de negócio da organização.

O segundo ponto refere-se às **boas práticas de controles recomendados pelo Tribunal de Contas da União** que poderiam estar contemplados na NSI004. Nesta auditoria, também foi utilizado, de forma simplificada, os Questionários de Avaliação de Controles Internos, QACI 01 – Avaliação da política de backup e QACI 02 – Planos e procedimentos, elaborados pelo TCU. Esses instrumentos têm como objetivo a autoavaliação dos controles internos "[...] **por meio do qual os próprios gestores avaliam seus controles e riscos**"[3]. Para cada item do questionário é atribuída uma nota, seguindo uma tabela de pontuação e, posteriormente, é calculado o percentual de implementação da boa prática. A partir desse mapeamento é sugerido a elaboração de um plano de ação indicando qual tratamento será efetuado para os eventuais controles deficitários. No contexto desta auditoria, os questionários serviram como referência para identificar temas e controles relevantes que poderiam ser incorporados ou reforçados na NSI004. As constatações da equipe de auditoria estão presentes no Apêndice A deste relatório.

[3] BRASIL. Tribunal de Contas da União. QACI 01 Avaliação da política de backup. Brasilia, 2025. Disponível em: https://portal.tcu.gov.br/uploads/QACI_01_Avaliacao_da_politica_de_backup_998ea9c6af.docx. Acesso em 07 nov. 2025.

O Quadro 5, a seguir, resume exemplos de controles presentes em normas de outros órgãos do Poder Judiciário, alinhados às boas práticas destacadas pelo TCU.

Quadro 5 – Controles elencados nos questionários do TCU presentes em outros Tribunais

Controles presentes nos questionários QACI 01 e QACI 02	Exemplos de órgãos que adotam
A política estabelece que sejam disponibilizados recursos adequados para a gestão e operacionalização dos procedimentos relativos a cópias de segurança/restauração.	**TRT2** (Ato GP nº 07/2015, artigo 9º); **TRT8** (Portaria PRESI nº 147/2017, artigo 43); **TRT18** (Portaria GP/SGGOVE nº 1094/2020, artigo 8º).
A política estabelece diretrizes para o descarte de mídias.	**CNJ** (Portaria CNJ nº 197/2023, artigo 25); **TRT2** (Ato GP nº 07/2015, artigo 14); **TRT3** (Portaria GP Nº 134/2019, item 3.6 do Anexo IX); **TRT7** (Ato GP nº 88/2020, item 10.3); **TRT8** (Portaria PRESI nº 147/2017, artigo 12); **TRF1** (Portaria PRESI 10264108, artigo 28).
Os requisitos de negócios são levados em consideração nos planos/procedimentos.	**CNJ** (Portaria CNJ nº 197/2023, artigo 4º); **TRT8** (Portaria PRESI nº 147/2017, artigo 34); **TRT12** (Portaria PRESI nº 235/2021, inciso III do artigo 6º); **TRT18** (Portaria GP/SGGOVE nº 1097/2020, item b, do inciso I do artigo 12).
Os planos/procedimentos definem requisitos específicos de segurança da informação (criptografia, imutabilidade, isolamento etc.).	**TRT2** (Ato GP nº 07/2015, alínea "i" do artigo 11); **TRT6** (Ato GP nº 411/2022, item 5.1.9 do Anexo I); **TRT9** (Política nº 86/2024, §7º do artigo 4º); **TRT14** (Portaria GP nº 988/2023, inciso IV do artigo 11); **TRT18** (Portaria GP/SGGOVE nº 1097/2020, artigo 4º).
A execução dos backups e restores realizados contêm registros (*logs*) precisos e completos e procedimentos de restauração documentada.	**TRT7** (Ato GP nº 88/2020, item 12); **TRT8** (Portaria PRESI nº 147/2017, incisos XV e XVI do artigo 37); **TRT9** (Política nº 86/2024, artigo 8º e Parágrafo Único do artigo 9º); **TRT18** (Portaria GP/SGGOVE nº 1097/2020, artigo 13).
O monitoramento periódico da execução dos backups e eventuais restaurações, de modo a permitir a detecção tempestiva de eventuais falhas.	**TRT6** (Ato GP nº 411/2022), item 13 do Anexo VIII); **TRT14** (Portaria GP nº 988/2023), alínea "a" do inciso II, do artigo 10); **TRT18** (Portaria GP/SGGOVE nº 1097/2020, artigos 14 e 15).

Benefícios estimados

- Fortalecimento da governança de TIC e da segurança da informação no âmbito do TRT4;
- Manter o normativo interno alinhado e em conformidade com as boas práticas recomendadas pelo TCU e pelas normas nacionais.
- Facilitar a consulta e a manutenção dos documentos de backup, otimizando os procedimentos e a gestão de rotinas da área técnica.

Manifestação do Auditado

A Secretaria-Geral de Tecnologia e Inovação não manifestou discordância pela situação encontrada (documento nº 23).

Conclusão da Equipe de Auditoria

Esta equipe de auditoria entende pertinente manter a proposta de encaminhamento para a presente oportunidade de melhoria, uma vez que não houve discordância da Secretaria-Geral de Tecnologia e Inovação para a situação descrita. A proposta de encaminhamento tem como objetivo o aprimoramento da NSI004, de forma a incorporar as boas práticas apresentadas neste relatório.

Proposta de Encaminhamento

S1. SUGERE-SE à Secretaria-Geral de Tecnologia e Inovação que, com o intuito de garantir maior alinhamento às boas práticas de governança e de segurança da informação, avalie a conveniência e a oportunidade de revisar a NSI004, contemplando:

(i) a segregação entre a política de backup e recuperação de dados e os planos operacionais; e

(ii) a adoção das boas práticas de controle recomendadas pelo Tribunal de Contas da União nos questionários de autoavaliação de controles internos relacionados à Política, aos planos e aos procedimentos de backup.

4. CONCLUSÃO

O presente trabalho teve como objetivo principal avaliar a implementação da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário no TRT4, com foco no gerenciamento da infraestrutura tecnológica de TIC. Inicialmente, o escopo também previa a análise de estratégias e requisitos relativos à prestação de serviços em nuvem. Contudo, este item foi excluído, uma vez que o Tribunal atualmente não possui sua infraestrutura, ou parte dela, em nuvem, limitando-se à contratação de aplicativos externos.

O escopo da auditoria envolveu três processos principais: P1. Gestão de Configuração e Ativos de TIC; P2. Gerenciamento da Disponibilidade e Capacidade de TIC; e P3. Backup e Recuperação de Dados. Para esses processos foram propostas três questões de auditoria, as quais foram divididas em oito subquestões de auditoria.

Quanto às duas subquestões da Questão 1, a auditoria verificou que a Seinfra utiliza planilhas de apoio para o controle e o gerenciamento dos ativos de infraestrutura tecnológica. Entretanto, foram observados pontos de atenção referentes ao preenchimento das informações mínimas desses ativos, bem como à sincronização e atualização dos respectivos inventários com o sistema de patrimônio (Achado A1).

Para às duas subquestões da Questão 2, referente ao processo de Gerenciamento da Disponibilidade e da Capacidade de TIC, não foram identificadas divergências em relação às normas e boas práticas aplicáveis.

Com relação às três subquestões da Questão 3, constatou-se, para a primeira delas, que os procedimentos de backup são executados conforme a política interna. No entanto, ao confrontar essa política com as normas de outros tribunais do trabalho, bem como com os Questionários de Avaliação de Controles Internos (QACI) propostos pelo TCU (Apêndice A), identificou-se uma oportunidade de melhoria a ser avaliada pela Secretaria-Geral de Tecnologia e Inovação (Oportunidade de Melhoria 1). Para as outras duas subquestões, esta equipe de auditoria observou aspectos a serem desenvolvidos e aprimorados quanto à

realização de testes periódicos de recuperação de dados e à respectiva validação desses testes (Achado A2).

Ao final, foram consolidadas quatro propostas de encaminhamento para este trabalho, as quais objetivam contribuir para o aperfeiçoamento do gerenciamento de infraestrutura tecnológica do TRT4. Destaca-se que a SGTI não manifestou discordância quanto aos apontamentos da equipe de auditoria. Além disso, a própria área técnica sugeriu ações corretivas ainda durante a auditoria para as situações observadas no achado A2, que foram incorporadas à recomendação final.

Assim, este trabalho reforça o compromisso da Secretaria de Auditoria com o cumprimento das normas, o aperfeiçoamento das rotinas internas e a melhoria contínua da governança e da gestão de TIC do Tribunal.

5. ENCAMINHAMENTO

Em consonância com o papel da auditoria interna estabelecido na Resolução CNJ nº 309/2020, na Resolução CSJT nº 282/2021 e na Resolução Administrativa TRT4 nº 03/2021, levamos à consideração de Vossa Excelência o resultado desta auditoria, sugerindo que seja determinada à área auditada a elaboração de um **plano de ação** para tratar as inconformidades identificadas neste trabalho de auditoria, nos termos do § 1º do artigo 21 da Portaria GP.TRT4 nº 3.215/2024.

Em 03 de dezembro de 2025.

Documento assinado digitalmente
ADRIANO PRADO CAVALHEIRO
Equipe de Auditoria
Divisão de Auditoria de Contratações

Documento assinado digitalmente
DÉBORA KATI DOS S.S. DARGEN
Equipe de Auditoria
Seção de Auditoria de Gestão de Pessoas

Documento assinado digitalmente
FELIPE VIEGAS DA SILVA
Equipe de Auditoria
Divisão de Auditoria de Contratações

Documento assinado digitalmente
JOSÉ CLÁUDIO DA ROSA RICCARDI
Auditor responsável
Divisão de Auditoria de Contratações

Documento assinado digitalmente
CAROLINA FEUERHARMEL LITVIN
Supervisora
Diretora da Secretaria de Auditoria

APÊNDICE A – Aplicação dos Questionários de Avaliação de Controles Internos (QACI) propostos pelo TCU[4]

Gestão de cópias de segurança (backups)			
QACI 01 – Avaliação da política de backup			
Controle	**Critério**	**Avaliação da Seaudi**	**Evidência**
Existe uma política de backup (ou instrumento normativo equivalente com os requisitos da organização relativos às cópias de segurança das informações) formalmente estabelecida?	ABNT NBR ISO/IEC 27002: 2022 item 8.13	**Sim**	Norma NSI004 - Procedimentos de backup e recuperação de dados (Anexo 4 da Portaria GP.TRT4 nº 4.772/2008). Entretanto, a NSI 004 é tanto política quanto plano.
A política foi publicada/comunicada para as partes interessadas (ex: titulares dos dados, usuários e gestores dos sistemas etc.)?	ABNT NBR ISO/IEC 27002: 2022, item 5.1	**Sim**	A norma NSI004 é parte integrante da Portaria GP.TRT4 nº 4.772/2008, publicada em 23.09.2008 e está disponível no Portal da Governança de TIC.
A política estabelece o escopo de alcance? (ex: quais sistemas a política se aplica, agentes públicos e colaboradores necessários e o que não está no escopo)	Modelo de Política de Backup/SGD, v2	**Sim**	Quadros dos itens 5.6 e 5.7, além do item 5.8 da norma NSI004.
Há um processo de revisão e atualização da política de backup? Qual a frequência? Quando foi revista e atualizada?	ABNT NBR ISO/IEC 27002: 2022, item 5.1 NIST SP 800-209: DP-SS-R3	**Sim**	Item 8 da norma NSI004.
Existe um processo de análise de impacto nos negócios (BIA), análise de riscos ou priorização dos ativos críticos? A política utiliza o resultado da BIA, análise de riscos ou priorização dos ativos críticos para determinar os requisitos de RTO e RPO?	NIST SP 800-209: DP-SS-R1 e DP-SS-R2 ABNT NBR ISO/IEC 27002: 2022, item 8.13	**Parcialmente**	Existe um processo de análise de riscos de TIC. É a norma NSI006 - Gestão de Riscos de TIC (Anexo 6 da Portaria GP.TRT4 nº 4.772/2008). Ela se aplica a todas as unidades pertencentes à Secretaria de Tecnologia da Informação e Comunicações, responsáveis por gerenciar, manipular e operar informações, projetos,

[4] Fiscalização de Segurança da Informação e Cibersegurança.

			processos, produtos e serviços relacionados à área de TIC no âmbito do TRT da 4ª Região. Entretanto, **não há evidências de que essa análise de riscos foi utilizada para determinar os RTOs e RPOs**.
A política define ou estabelece que os planos/procedimentos de backup devem definir requisitos específicos de segurança da informação (1) paras as cópias de segurança realizadas (ex.: controles de acesso lógico, criptografia, armazenamento em local seguro, armazenamento em local remoto seguro diferente do local original, imutabilidade e bloqueio, arquivamento, localização, distribuição geográfica, número mínimo de cópias etc.)	ABNT NBR ISO/IEC 27002: 2022, item 8.13, diretrizes para implementação - alínea “b” NIST SP 800-209: DP-SS-R1	**Parcialmente**	Na NSI004 são definidos requisitos para armazenamento em local distinto (itens 3.15 e 5.5) e transporte (item 5.9) das cópias de segurança.
A política estabelece responsabilidades e competências pela definição dos requisitos mínimos de cópia de segurança?	Modelo de Política de Backup/SGD, v2 ABNT NBR ISO/IEC 27002: 2022, item 5.1,	**Sim**	Item 5.1 da norma NSI004.
A política estabelece diretrizes para cópias dos ativos críticos?	Modelo de Política de Backup/SGD, v2	**Sim**	Quadros dos itens 5.6 e 5.7 da norma NSI004.
A política estabelece que os planos/procedimentos de backup devem definir a abrangência / escopo das cópias de segurança de dados e de sistemas (2)	Modelo de Política de Backup/SGD, v2	**Sim**	Quadros dos itens 5.6 e 5.7 da norma NSI004.
A política estabelece que os planos/procedimentos de backup devem definir os tipos de cópias a serem realizadas (completa/full, incremental ou diferencial)	ABNT NBR ISO/IEC 27002: 2022, item 8.13, diretrizes para implementação - alínea “b” NIST SP 800-209: DP-SS-R1	**Sim**	Quadros dos itens 5.6 e 5.7 da norma NSI004.

A política estabelece que os planos/procedimentos de backup devem definir a frequência de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.)	ABNT NBR ISO/IEC 27002: 2022, item 8.13, diretrizes para implementação - alínea “b” NIST SP 800-209: DP-SS-R1	**Sim**	Quadros dos itens 5.6 e 5.7 da norma NSI004.
A política estabelece os tipos de mídias (disco rígido, ssd, fitas de backup, nuvem etc) que podem ser utilizados na gestão de cópias de segurança?	Modelo de Política de Backup/SGD, v2 NIST SP 800-209: DP-SS-R1	**Parcialmente**	Apenas para o item 5.7 da norma NSI004.
A política estabelece que os planos/procedimentos de backup devem definir o RTO e RPO das cópias de segurança?	Modelo de Política de Backup/SGD, v2 NIST SP 800-209: DP-SS-R1	**Sim**	Quadros dos itens 5.6 e 5.7 da norma NSI004.
A política estabelece que os planos /procedimentos /roteiros de backup devem definir o tempo de retenção das cópias de segurança.	ABNT NBR ISO/IEC 27002: 2022, item 8.13	**Sim**	Quadros dos itens 5.6 e 5.7 da norma NSI004.
A política estabelece que as cópias de segurança devem ser testadas regularmente (pelo menos mensalmente para ativos críticos) por meio de testes de recuperação/restauração (restore), a fim de verificar sua integridade e capacidade de restauração?	ABNT NBR ISO/IEC 27002: 2022, item 8.13, diretrizes para implementação - alínea “e” NIST SP 800-209: DP-SS-R3	**Sim**	Item 7 da norma NSI004.
A política estabelece que a geração das cópias de segurança e eventual restauração sejam monitoradas de modo a permitir a detecção tempestiva de eventuais falhas	ABNT NBR ISO/IEC 27002: 2022, item 8.13	**Parcialmente**	**Não há previsão para monitoramento da geração das cópias de segurança**. Para a restauração, há previsão nos itens 7.3 e 7.4 da norma NSI004.
A política estabelece que sejam disponibilizados recursos adequados para a gestão e operacionalização dos procedimentos relativos	Modelo de Política de Backup/SGD, v2 NIST SP 800-209: DP-SS-R1	**Não**	-x-

a cópias de segurança/restauração?			
A política estabelece diretrizes para realizar a recuperação/restauração (restore) das cópias de segurança quando necessário?	ABNT NBR ISO/IEC 27002: 2022, item 8.13, diretrizes para implementação – alínea "e"	**Sim**	Item 6 da norma NSI004.
A política estabelece diretrizes para definição do período de janela de backup (ex: Com base na análise de impacto de uso de rede e outros fatores internos)?	Modelo de Política de Backup/SGD, v2	**Sim**	Itens 5.3, 5.6 e 5.7 da norma NSI004.
A política estabelece diretrizes para transporte e armazenamento dos backups?	Modelo de Política de Backup/SGD, v2	**Sim**	Itens 5.9 da norma NSI004.
A política estabelece diretrizes para o descarte de mídias?	Modelo de Política de Backup/SGD, v2 NIST SP 800-88 v1	**Não**	-x-
A política estabelece diretrizes para proteção dos dados armazenados nas mídias? Por exemplo, atualizar dados antigos, em risco ou que não são mais suportados na mídia copiando para uma nova etc.)	NIST SP 800-209: DP-SS-R3	**Não**	-x-

1. Requisitos de segurança da informação referem-se, em especial, à confidencialidade, à integridade e à disponibilidade das informações. Porém, como esses termos podem não ser citados na política, é preciso focar nos exemplos citados no item 4 acima ou checar se a política registra a necessidade de os controles serem compatíveis com a segurança das informações ou com a classificação das informações.

2. Ou seja, aquilo que deve ser copiado: quais pastas/folders de dados, quais arquivos de dados, quais arquivos de sistemas, quais bases de dados, quais tabelas de dados etc.

QACI 02 – Planos e procedimentos

Controle	Critério		Avaliação da Seaudi
Existe(m) planos/procedimentos de backup desenvolvidos e implementados?	ABNT NBR ISO/IEC 27002: 2022, item 8.13	**Sim**	Norma NSI004 - Procedimentos de backup e recuperação de dados

			(Anexo 4 da Portaria GP.TRT4 nº 4.772/2008). Entretanto, a NSI 004 é tanto política quanto plano.
O plano/procedimento foi aprovado pelas partes interessadas e responsáveis pela definição dos requisitos mínimos de cópia de segurança?	ABNT NBR ISO/IEC 27002: 2022, item 5.1	**Sim**	Item 5.1 da norma NSI004.
Durante a elaboração dos planos/procedimentos, os requisitos de negócios são levados em consideração?	ABNT NBR ISO/IEC 27002: 2022, 8.13: diretrizes para implementação, alínea “b”	**Não**	Não há evidências.
Os dados são submetidos a classificação prévia para verificar o tratamento e armazenamento adequado?	Modelo de contratação de software e de serviços de computação em nuvem/SGD, item 5.3	**Sim**	Item 5.1 da norma NSI004.
A organização estabelece um inventário (CMDB ou ITAM) dos ativos de informação críticos a fim de evitar o “shadow IT”?	ITIL 4 IT Asset Management	**Sim**	O sistema Oraculum é o repositório “[...] que visa centralizar as informações dos ativos de configuração e seus relacionamentos com os produtos e serviços de tecnologia que sustentam a prestação jurisdicional”[5]. Entretanto, não há referência expressa na NSI004.
Há plano de recuperação de desastres (PDR), ou plano de continuidade dos negócios (PCN) desenvolvido e revisado periodicamente? Se existir, estabelece os recursos, pessoas, mapeamento de processos, fluxo e testes?	NIST SP 800-209: RA-SS-R10 ABNT NBR ISO/IEC 27002: 2022, item 5.30 ABNT NBR ISO/IEC 27031: 2022, item 7.4.3 e) vi)	**Sim**	Os planos PDR e PCN foram definidos no item 7 da norma NSI010 – Gestão da Continuidade de TIC (Anexo 10 da Portaria GP.TRT4 nº 4.772/2008).

[5] Conforme informação prestada pelo TRT4 à Secretaria de Auditoria do CSJT no Relatório de Auditoria da auditoria sistêmica para levantamento e avaliação da gestão de serviços de tecnologia da informação na Justiça do Trabalho. Disponível em: https://www.csjt.jus.br/documents/955023/10030873/1.+Relatorio+de+Auditoria.pdf/2aeb9d93-7eb4-e5c3-db00-dd45fc7e9a49?version=1.0&t=1645201717163

Os planos/procedimentos de backups são revisados para refletir as mudanças nos requisitos de negócios? Se não, existe alguma periodicidade definida?	ABNT NBR ISO/IEC 27002: 2022, 8.13: diretrizes para implementação, alínea “b” NIST SP 800-209: DP-SS-R3	**Sim**	Item 8 da norma NSI004.
Os planos/procedimentos definem requisitos específicos de segurança da informação (criptografia, imutabilidade, isolamento etc.)?	ABNT NBR ISO/IEC 27002: 2022, item 8.13, diretrizes para implementação - alínea “b”	**Parcialmente**	Apenas para o item 5.5 da norma NSI004.
A implantação de requisitos específicos de segurança da informação é definida com base em análise de risco/gestão de risco?	ABNT NBR ISO/IEC 27002: 2022	**Sim**	A norma NSI006 - Gestão de Riscos de TIC (Anexo 6 da Portaria GP.TRT4 nº 4.772/2008), tem como motivação a necessidade de um processo sistemático para gerenciar riscos referentes à Segurança da Informação e Comunicações (SIC), projetos e processos de TIC, provendo insumos para aumentar a proteção contra eventos indesejados.
Há planos/procedimentos de backup dos ativos críticos de informação? Todos esses são protegidos (backup) e retidos adequadamente?	Modelo de Política de Backup/SGD, v2 NIST SP 800-209: DP-SS-R2	**Sim**	Quadros dos itens 5.6 e 5.7 da norma NSI004.
Os planos/procedimentos de backup estabelecem a abrangência/escopo das cópias de segurança de dados, sistemas, aplicativos, banco de dados etc. (1)?	Modelo de Política de Backup/SGD, v2	**Sim**	Quadros dos itens 5.6 e 5.7 da norma NSI004.
Os planos/procedimentos de backup estabelecem os tipos de cópias a serem realizadas (completa/full, incremental ou diferencial)?	ABNT NBR ISO/IEC 27002: 2022, item 8.13, diretrizes para implementação - alínea “b”	**Sim**	Quadros dos itens 5.6 e 5.7 da norma NSI004.
Os planos/procedimentos estabelecem a frequência de realização das cópias de segurança (ex.: diária,	ABNT NBR ISO/IEC 27002: 2022, item 8.13, diretrizes para	**Sim**	Quadros dos itens 5.6 e 5.7 da norma NSI004.

semanal, mensal, anual etc.)?	implementação - alínea “b”		
Os planos/procedimentos preveem a utilização de diferentes tipos de mídias para armazenar o backup (storage de disco rígido, cloud, fita magnética etc.)?	NIST SP 800-209: DP-SS-R1	**Parcialmente**	A NSI004 define os tipos de mídias, no item 3 – Conceitos e definições. Entretanto, a previsão de utilização é apresentada apenas no quadro do item 5.7. No quadro do item 5.6 não há previsão de quais mídias serão utilizadas para cada tipo de cópia de segurança.
Os planos/procedimentos estabelecem o tempo de retenção das cópias de segurança? (de cada ativo, ativos de informação críticos e não críticos) Os backups são excluídos após o tempo de retenção?	ABNT NBR isso/IEC 27002: 2022, item 8.13	**Parcialmente**	Quadros dos itens 5.6 e 5.7 da norma NSI004. Entretanto, **não há previsão para exclusão das cópias de segurança após o tempo de retenção**.
Os planos/procedimentos estabelecem que as mídias de backup sejam sanitizados ou descartadas seguramente? Como é o ciclo de vida das mídias?	NIST SP 800-88 Rev1	**Não**	-x-
Os planos/procedimentos de backup estabelecem o RTO e RPO das cópias de segurança? Eles são estabelecidos juntamente com a área de negócio (cliente)?	Modelo de Política de Backup/SGD, v2 NIST SP 800-53 Rev5 CP-9	**Sim**	Quadros dos itens 5.6 e 5.7 da norma NSI004.
Os planos/procedimentos determinam qual conjunto de arquivos de backup e outras informações precisam ser protegidos offline em um site remoto ou isolado do principal? (senhas, certificados digitais, chaves de criptografia e outras informações necessárias para restabelecer rapidamente as operações)	NIST SP 800-53 Rev5 CP-2, CP-9	**Sim**	Item 5.5 da norma NSI004.
Os planos/procedimentos de backup estabelecem testes de restauração periódicos (pelo menos mensalmente	ABNT NBR ISO/IEC 27002: 2022, item 8.13, diretrizes para	**Sim**	Item 7 da norma NSI004.

para ativos de informação críticos), a fim de verificar sua integridade e capacidade de restauração?	implementação - alínea “e” NIST SP 800-209 DP-SS-R3		
Os planos/procedimentos definem período de janela de backup com base na análise de impacto de uso de rede, carga de trabalho e outros fatores internos?	Modelo de Política de Backup/SGD, v2	**Sim**	Itens 5.2, 5.3 e quadros dos itens 5.6 e 5.7 da norma NSI004.
A execução dos backups e restores realizados contêm registros (*logs*) precisos e completos dos procedimentos realizados?	ABNT NBR ISO/IEC 27002: 2022, item 8.13, diretrizes para implementação - alínea “a”	**Não**	-x-
Os planos/procedimentos prevêem que os backups e restores sejam executados de forma automatizada, ou possuem algum procedimento manual? Quem sãos os responsáveis pelos procedimentos manuais?	Framework PPSI/SGD 11.3	**Sim**	Item 5.2 e quadro do item 7.2.
Se utilizado serviços/recursos em nuvens, há ato normativo que regule o uso de recursos em nuvem?	Instrução Normativa - GSI/PR nº 3/2021: Art. 4, 5, 6.	**Sim**	Item 5.3 da NSI003 – Uso de Recursos de Tecnologia da Informação e Controle de Acesso (Anexo 3 da Portaria GP.TRT4 nº 4.772/2008). Quanto à cópia de segurança dos serviços armazenados em nuvem, cita-se o item 5.8 da NSI004.
Pelo menos uma cópia atualizada de segurança é mantida em território brasileiro?	Instrução Normativa - GSI/PR nº 5/2021: Art. 18.	**Não**	-x-
Os dados, metadados, informações e conhecimentos sensíveis produzidos ou custodiados pelo órgão ou pela entidade, transferidos para o provedor de serviço de nuvem, são hospedados em território brasileiro?	Instrução Normativa - GSI/PR nº 5/2021: Art. 18	**Não**	-x-

A organização possui um plano/procedimento de resposta a incidente para o caso de um ataque de ransomware ou de desastre que comprometa a operação dos ativos de informação críticos?	NIST SP 800-209: IR-SS-R1	N/A	N/A
Se existir, o plano/procedimento de resposta foi elaborado com base em uma análise de risco? Ele prevê aspectos como isolamento, preparação, prevenção, detecção, remediação, recuperação e procedimentos de teste?	NIST SP 800-209: IR-SS-R1 Artigo Lessons Learned: Recovering from Ransomware (Rubrik)	N/A	N/A
Se existir, o plano/procedimento de resposta considera o comprometimento dos componentes de backup (armazenamento, software, inventário, *logs*, fitoteca, mídias etc.), inclusive do backup offsite em local remoto?	NIST SP 800-209: IR-SS-R1	N/A	N/A
Se existir, o plano/procedimento prevê a recuperação priorizada dos ativos? Por exemplo, os serviços básicos necessários para a funcionalidade principal, incluindo DHCP, autenticação e DNS, sejam executados restaurados primeiro.	Artigo - Noções básicas e 6 práticas recomendadas essenciais (Netapp)	N/A	N/A
Se existir, o plano/procedimento prevê que a recuperação dos dados é iniciada em um ambiente isolado e após a neutralização do ransomware?	Artigo - Noções básicas e 6 práticas recomendadas essenciais (Netapp)	N/A	N/A
Se existir, o plano/procedimento prevê que a operação de recuperação inclui a identificação e a correção da causa raiz do ataque? Ao	Artigo - Noções básicas e 6 práticas recomendadas essenciais (Netapp)	N/A	N/A

restaurar um sistema, você retorna a um ponto em que provavelmente ainda possui a vulnerabilidade explorada pelos invasores			
Existem planos/procedimentos para realizar verificação, com uso de ferramentas de anti-malware, por exemplo, nas cópias de segurança (incluindo backup, replicação, cópias pontuais, snapshots etc.) a fim de verificar cópias comprometidas?	NIST SP 800-209: DP-SS-R3	N/A	N/A
A estratégia de backup 3-2-1 ou 3-2-1-1 é utilizada nos ativos de informação críticos da organização? (3 cópias dos dados, em 2 diferentes tipos de mídias, com 1 offsite e 1 offline, imutável ou air-gapped)	NIST SP 800-209: DP-SS-R3	**Não**	Não há previsão expressa.
Existem planos para monitorar periodicamente a execução dos backups e eventuais restaurações, de modo a permitir a detecção tempestiva de eventuais falhas?	NIST SP 800-209: DP-SS-R3 ABNT NBR ISO/IEC 27002: 2022, item 8.13	**Parcialmente**	**Não há previsão para monitoramento da geração das cópias de segurança**. Para a restauração, há previsão nos itens 7.3 e 7.4 da norma NSI004.

1 Ou seja, aquilo que deve ser copiado: quais pastas/folders de dados, quais arquivos de dados, quais arquivos de sistemas, quais bases de dados, quais tabelas de dados etc.

N/A – Não avaliado no escopo desta auditoria.