PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO

PROAD 2483/2022

RELATÓRIO DA AÇÃO COORDENADA PELO CSJT PARA AVALIAR A GESTÃO DE SEGURANÇA DA INFORMAÇÃO

OUTUBRO/2022

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

RELATÓRIO DE AUDITORIA Nº 06/2022 - SAUD

1. INTRODUÇÃO

Em cumprimento ao disposto na Resolução do Conselho Nacional de Justiça (CNJ) n.º 309/2021, assim como ao previsto no subitem n.º 6 do item II do Anexo Único do Plano Anual de Auditoria para o exercício de 2022 (PAA-2022), aprovado pelo Ato nº 134/GP/TRT19ª, de 9 de dezembro de 2021, e alterado pelo Ato nº 23/GP/TRT19ª, de 23 de março de 2022, apresentam-se os resultados deste Tribunal Regional do Trabalho da 19ª Região em face da Ação Coordenada de Auditoria do CSJT para avaliar a Gestão da Segurança da Informação no âmbito da Justiça do Trabalho.

A fase de execução da auditoria teve início com o envio do Questionário desenvolvido pelo CSJT (documentos n.º 06 e 07), da Requisição de Documentos e Informações (RDI) n.º 06/2022 (documento n.º 11), os quais possibilitaram, juntamente com as observações realizadas em reunião, conforme Ata n.º 01/2022 (documento n.º 10), a coleta de informações para o diagnóstico da área auditada.

Os resultados da auditoria foram previamente apresentados à Diretoria Geral (DG), bem como à Secretaria de Tecnologia da Informação e Comunicações (SETIC), conforme Ata da Reunião n.º 06/2022 (documento n.º 20), para as discussões, esclarecimentos de eventuais dúvidas e prestação de informações adicionais.

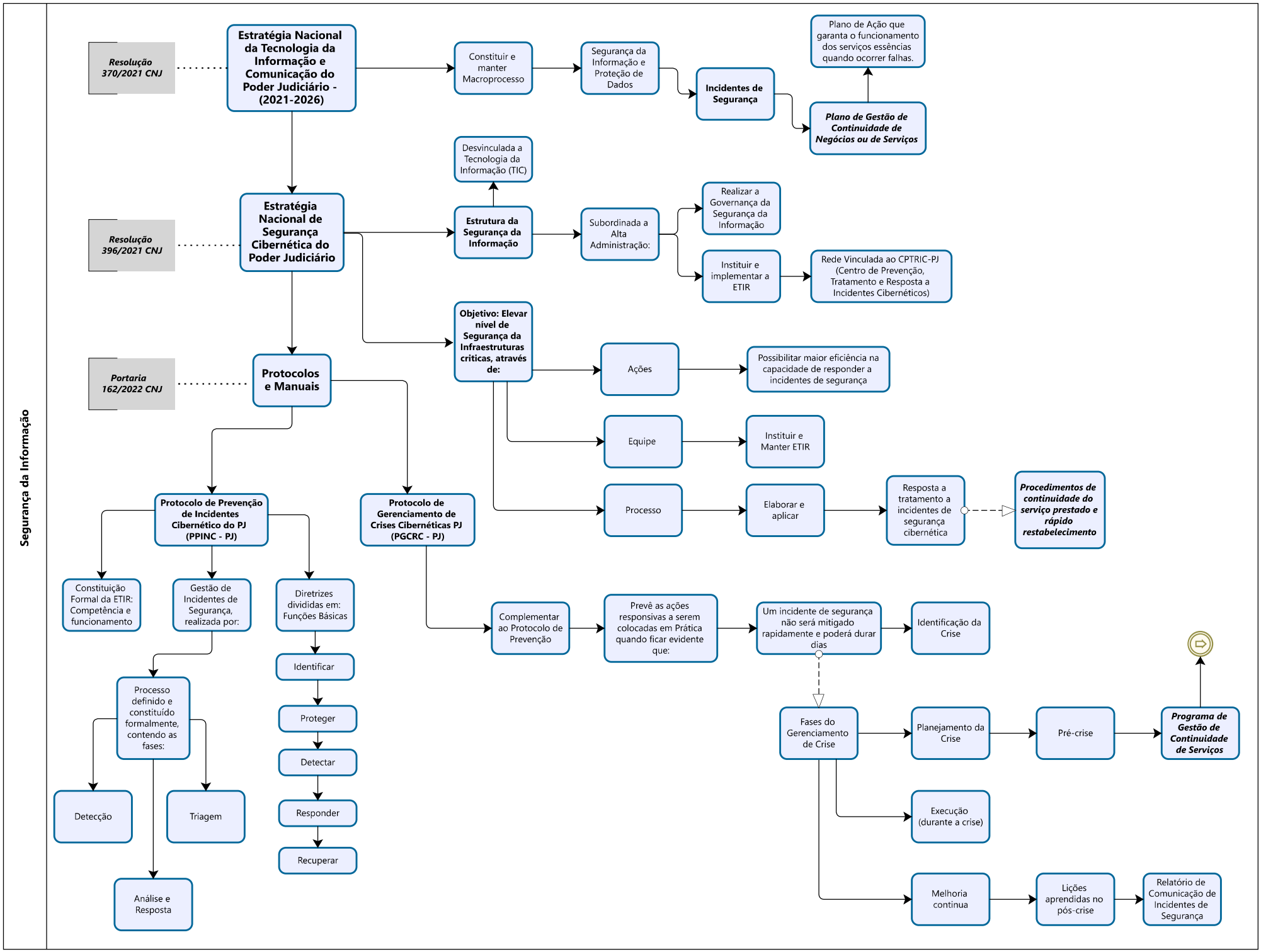
Assim, após os devidos ajustes e a apresentação das manifestações formais do auditado (documento n.º 18), a auditoria realizou sua análise e conclusão acerca dos achados de auditoria, nos quais embasou suas recomendações. Por conseguinte, os mapas dos achados (documento n.º 22) e a minuta de achados (documento n.º 23) foram enviados ao CSJT para consolidação dos resultados da auditoria no âmbito da justiça do trabalho.

Por fim, destaca-se que as inconformidades encontradas foram reunidas no Relatório de Fatos Apurados (documento n.º 21), para ciência, bem como para conferir à Secretaria de Tecnologia da Informação e Comunicações (SETIC) a oportunidade de se posicionar sobre as ocorrências identificadas e apresentar um Plano de Ação, com propostas de ações a serem tomadas a fim de dar cumprimento às recomendações indicadas, conforme os Achados de Auditoria identificados.

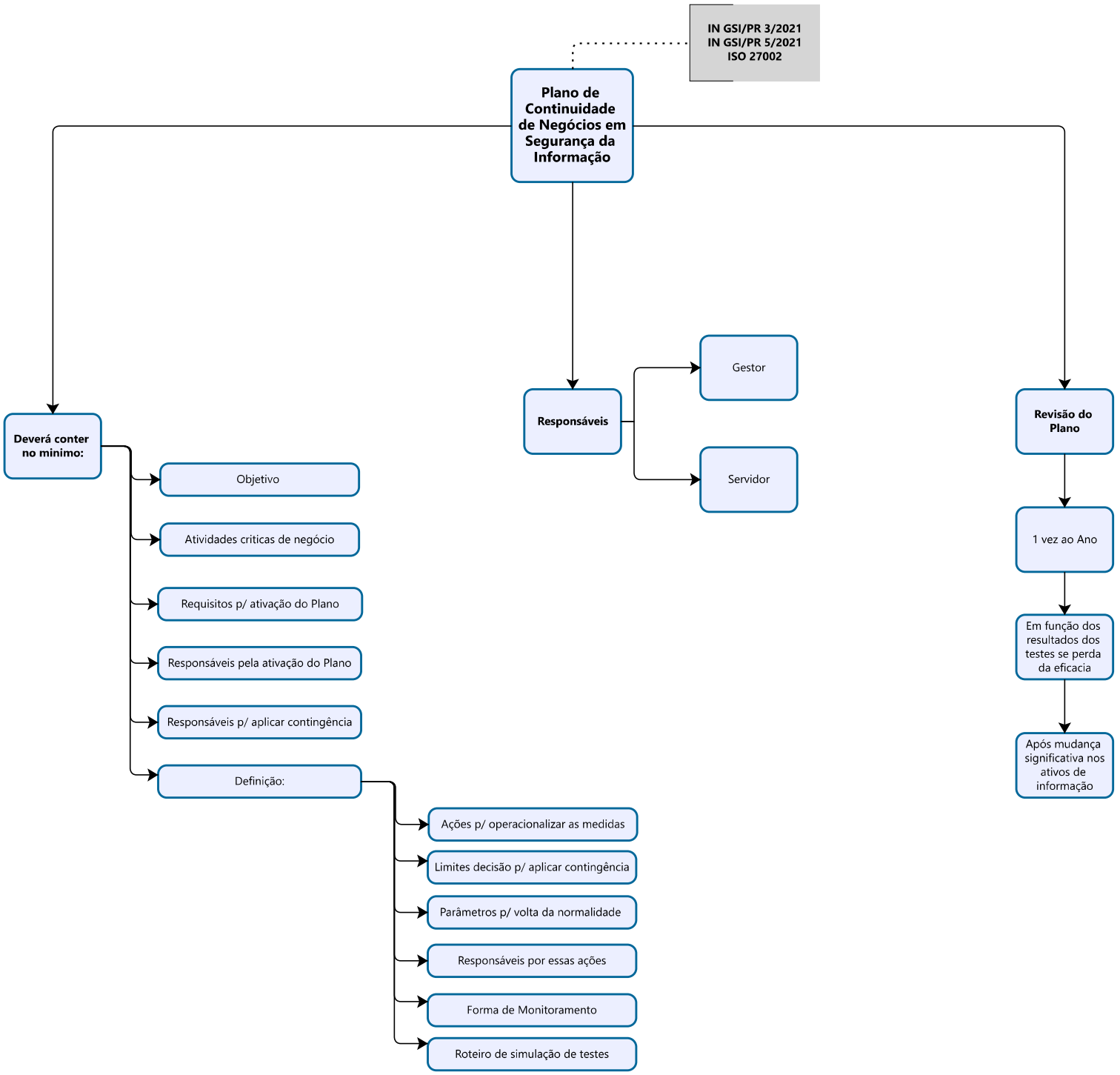
Ademais, torna-se importante ressaltar que no contexto em que há o predomínio dos recursos tecnológicos na execução das atividades finalísticas e administrativas, faz-se necessário ter um nível de segurança elevado, e para atingir tais fins são imprescindíveis processos bem estruturados, fundamentados em normativos e boas praticas para mitigar riscos e garantir a prestação dos serviços.

Em vista disso, a presente ação coordenada possibilitou observar se os controles relativos ao processo de segurança da informação, inerentes ao gerenciamento de incidentes cibernéticos e da gestão de continuidade dos serviços essenciais de tecnologia, estão sendo realizados conforme as diretrizes normativas, as quais podem ser compreendidas no contexto apresentado a seguir:

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br


Segurança da Informação
Resolução 370/2021 CNJ
Estratégia Nacional da Tecnologia da Informação e Comunicação do Poder Judiciário - (2021-2026)
Constituir e manter Macroprocesso
Segurança da Informação e Proteção de Dados
Incidentes de Segurança
Plano de Ação que garanta o funcionamento dos serviços essências quando ocorrer falhas.
Plano de Gestão de Continuidade de Negócios ou de Serviços
Resolução 396/2021 CNJ
Estratégia Nacional de Segurança Cibernética do Poder Judiciário
Desvinculada a Tecnologia da Informação (TIC)
Estrutura da Segurança da Informação
Subordinada a Alta Administração:
Realizar a Governança da Segurança da Informação
Instituir e implementar a ETIR
Rede Vinculada ao CPTRIC-PJ (Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos)
Portaria 162/2022 CNJ
Protocolos e Manuais
Objetivo: Elevar nível de Segurança da Infraestruturas criticas, através de:
Ações
Possibilitar maior eficiência na capacidade de responder a incidentes de segurança
Equipe
Instituir e Manter ETIR
Processo
Elaborar e aplicar
Resposta a tratamento a incidentes de segurança cibernética
Procedimentos de continuidade do serviço prestado e rápido restabelecimento
Protocolo de Prevenção de Incidentes Cibernético do PJ (PPINC - PJ)
Protocolo de Gerenciamento de Crises Cibernéticas PJ (PGCRC - PJ)
Constituição Formal da ETIR: Competência e funcionamento
Gestão de Incidentes de Segurança, realizada por:
Diretrizes divididas em: Funções Básicas
Processo definido e constituído formalmente, contendo as fases:
Detecção
Triagem
Análise e Resposta
Identificar
Proteger
Detectar
Responder
Recuperar
Complementar ao Protocolo de Prevenção
Prevê as ações responsivas a serem colocadas em Prática quando ficar evidente que:
Um incidente de segurança não será mitigado rapidamente e poderá durar dias
Identificação da Crise
Fases do Gerenciamento de Crise
Planejamento da Crise
Pré-crise
Programa de Gestão de Continuidade de Serviços
Execução (durante a crise)
Melhoria continua
Lições aprendidas no pós-crise
Relatório de Comunicação de Incidentes de Segurança

Segurança da Informação



2. OBJETIVO

Avaliar a Gestão da Segurança da Informação, no tocante ao processo de tratamento e resposta a incidentes cibernéticos e da gestão de continuidade dos serviços essenciais de Tecnologia da Informação, no Tribunal Regional do Trabalho da 19ª, a luz das normas vigentes adotadas no âmbito da Justiça do Trabalho.

3. ESCOPO

O escopo da auditoria contemplou a Divisão de Segurança da Informação e Processos de Tecnologia da Informação do Tribunal Regional do Trabalho da 19ª, e visou examinar a adoção de melhores práticas em segurança da informação referenciadas em normativos, com foco nas políticas, diretrizes, processos, pessoas, planejamento, riscos e controles da aludida área.

De acordo com a Matriz de Planejamento elaborada pela equipe de auditoria, que buscou avaliar os processos de gerenciamento de incidentes de segurança da informação e da gestão de continuidade dos serviços essenciais de TI, foram evidenciadas 2 (duas) macro questões de auditoria, a seguir descritas:

Q.1 O TRT19ª executa o processo de gerenciamento de incidentes de segurança da informação de acordo com os normativos vigentes e as boas práticas?

Q.2 O TRT19ª realiza a gestão da continuidade dos serviços essenciais de TIC de acordo com os normativos vigentes e as boas práticas?

No tocante a delimitação do que se buscou examinar, a auditoria restringiu-se ao *check list* formulado pelo CSJT e aplicado ao auditado, conforme disposto a seguir:

1.1.1 - Foi elaborado o processo de gerenciamento de incidentes de segurança da informação/cibernética?

1.1.2 - O processo de gerenciamento de incidentes de segurança da informação/cibernética foi instituído formalmente?

1.2.1 - Foi formalmente instituída Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação/Cibernética (ETIR)?

1.2.2 - O funcionamento da ETIR está formalmente regulamentado, descrevendo, no mínimo: a) definição da missão; b) público-alvo; c) modelo de implementação; d) nível de autonomia; e) designação de integrantes; f) canal de comunicação de incidentes de segurança; e g) serviços que serão prestados?

1.2.3 - Nos últimos 2 anos, foram realizadas ações para o desenvolvimento das competências, sobre Segurança da Informação/Cibernética, para os membros da ETIR? Informar as lacunas de competências apontadas pelo gestor que exigirão capacitação complementar, caso existam.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

1.2.4 - O processo de gerenciamento de incidentes de segurança da informação/cibernética prevê as fases de detecção, triagem, análise e resposta aos incidentes de segurança?

1.2.5 - A fase de detecção prevê interação com o monitoramento e gerenciamento de eventos (ou procedimentos equivalentes)?

1.2.6 - O processo de gerenciamento de incidentes de segurança da informação/cibernética prevê as ações responsivas a serem colocadas em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente (Identificação de crise cibernética)?

1.2.7 - O processo de gerenciamento de incidentes de segurança da informação/cibernética estabelece critérios para iniciar o gerenciamento de crise?

1.2.8 - O processo de gerenciamento de incidentes de segurança da informação/cibernética contempla incidentes ocorridos nos serviços em nuvem contratados pelo órgão (Ex.: Gsuite)?

1.2.9 - O processo prevê a comunicação de todos os incidentes graves ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ)?

1.2.10 - O processo contempla etapa de lições aprendidas pós-crise?

1.2.11 - O processo prevê a elaboração de Relatório de Comunicação de Incidente de Segurança da Informação/Cibernética, contendo a descrição e o detalhamento da crise e o plano de ação tomado?

1.2.12 - O processo de gerenciamento de incidentes de segurança da informação/cibernética está implantado?

2.1.1 - Foi estabelecido um programa de gestão da continuidade dos serviços essenciais de TI (Plano de Continuidade de TI) ?

2.2.1 - Foram definidos os papéis e responsabilidades dos profissionais envolvidos no programa de gestão de continuidade de serviços essenciais de TI, incluindo o agente responsável pela gestão de continuidade do serviços de TI no Órgão?

2.2.2 - O programa contém a definição das atividades críticas de negócio a serem contempladas, abarcando, no mínimo, os seguintes serviços: PJE-JT, SIGEP-JT (FOLHA + CADASTRO) ou sistema equivalente, Processo Administrativo, Portal Internet e solução de comunicação (EX: GOOGLE SUITE)?

2.2.3 - O programa prevê a identificação dos ativos de informação críticos, incluindo as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação?

2.2.4 - O programa prevê a capacitação para as pessoas envolvidas nos procedimentos e processos definidos? Em caso negativo, informar as lacunas de competências que exigirão capacitação complementar.

2.2.5 - Existe previsão de interação com o processo de gestão de riscos, com vistas a assegurar a avaliação contínua dos riscos a que as atividades críticas estão expostas e que possam impactar diretamente na continuidade do negócio?

2.2.6 - Há previsão de categorização dos incidentes e estabelecimento de procedimentos de resposta específicos (playbooks)?

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

2.2.7 - Há planos de contingência que detalham o monitoramento, o acompanhamento e o tratamento dos riscos de maior criticidade, em razão de possíveis cenários de crise?

2.2.8 - O programa de gestão da continuidade dos serviços essenciais de TI (Plano de Continuidade de TI) contém, no mínimo:

I - o objetivo;

II - as atividades críticas de negócio a serem contempladas no plano (contemplado PC 2.2.1);

III - os requisitos para ativação do plano, em especial, o tempo máximo aceitável de permanência da falha;

IV - o(s) responsável(is) pela ativação do plano, com seus respectivos dados de contato;

V - o(s) responsável(is) por aplicar as medidas de contingência definidas, tendo cada servidor responsabilidades formalmente definidas e nominalmente atribuídas, incluindo seus respectivos dados de contato; e

VI - a definição:

a) das ações necessárias para operacionalização das medidas cuja implementação dependa da aquisição de recursos físicos e/ou humanos;

b) dos limites de decisão para os responsáveis pela aplicação das medidas de contingência perante situações inesperadas;

c) dos parâmetros para encerramento do plano e para a volta à normalidade;

d) dos responsáveis por essas ações, incluindo seus dados de contato;

e) da forma de monitoramento desse processo; e

f) de um roteiro de simulação de teste de funcionamento e da forma de sua aplicação.

2.2.9 - Foram realizadas simulações e testes para validação dos planos e procedimentos que integram o programa?

2.2.10 - O programa estabelece critérios para sua revisão, como periodicidade (pelo menos anualmente), em função dos resultados dos testes de funcionamento realizados, uma vez comprovada a perda da validade e eficácia das medidas adotadas diante de novas situações; ou após mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes?

Assim, o escopo da auditoria ficou restrito a avaliação do gerenciamento de incidentes de segurança da informação e da gestão de continuidade dos serviços essenciais de tecnologia da informação, no tocante ao cumprimento das diretrizes normativas especificadas em questionário previamente formulado pelo CSJT.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

4. TÉCNICAS DE AUDITORIA

As investigações foram feitas mediante a aplicação das seguintes técnicas de auditoria:

4.1 Entrevista - Formulação de perguntas escritas, no formato de RDI, como também aplicação de questionário escrito, enviados ao responsável pela unidade auditada, para obtenção de dados e informações;

4.2 Análise Documental - Verificação de processos e documentos que conduziram à formação de evidências pela unidade auditada;

4.3 Exame dos registros - Verificação dos registros constantes de controles regulamentares, relatórios sistematizados, mapas e demonstrativos formalizados, elaborados de forma manual ou por sistemas informatizados e;

4.4 Correlação das Informações Obtidas - Correlação das informações obtidas nas respostas à RDI e Questionário aplicado, com as evidências colhidas *in loco* e enviadas pela unidade auditada.

Vale salientar que a equipe não encontrou qualquer dificuldade na aplicação dos procedimentos de auditoria inicialmente previstos, sendo prontamente atendida pela unidade auditada em todas as suas requisições.

5. PARÂMETROS NORMATIVOS E JURISPRUDENCIAIS

- Resolução 370-2021 - CNJ: Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).
- Resolução 396-2021 - CNJ: Institui a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ), no âmbito dos órgãos do Poder Judiciário, à exceção do Supremo Tribunal Federal (STF).
- Portaria 162-2021 - CNJ: Aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).
- Instrução Normativa - GSI/PR 3 – 2021: Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.
- Instrução Normativa - GSI/PR 5 – 2021: Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal
- Norma complementar 08/IN01/DSIC/GSIPR: Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal
- ISO 27002: Dispõe sobre controles de segurança da informação.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

6. ACHADOS DE AUDITORIA E RECOMENDAÇÕES

Seguindo as diretrizes prescritas pela Resolução CNJ nº 309/2020, foram encontrados os ACHADOS DE AUDITORIA, que são atos ou fatos em desconformidade com a legislação aplicada ao caso, dignos de serem reportados pelos auditores.

Para cada um desses Achados, são identificados os pontos abaixo:

- **SITUAÇÃO ENCONTRADA:** Situação existente, identificada e documentada durante a fase de execução do trabalho.
- **MANIFESTAÇÃO DO AUDITADO:** Comentários do auditado acerca dos achados encontrados.
- **ANÁLISE DA AUDITORIA:** Análise da Auditoria acerca dos achados encontrados e das considerações feitas pelo auditado em suas manifestações.
- **CRITÉRIO:** Legislação, jurisprudência, princípios ou, ainda, padrões e boas práticas que a equipe compara com a situação encontrada. Reflete como deveria ser a gestão.
- **EVIDÊNCIA:** Informações obtidas durante a execução dos trabalhos no intuito de documentar os achados e de respaldar as opiniões e conclusões da equipe, podendo ser classificadas como físicas, testemunhais, documentais e analíticas.
- **CAUSA:** O que, possivelmente, motivou a ocorrência do achado.
- **EFEITOS / RISCOS:** Consequências ou possíveis consequências do achado, que possam dificultar o alcance dos objetivos.
- **RECOMENDAÇÕES:** Providências indicadas pela Secretaria de Auditoria com o intuito de aperfeiçoar os controles internos da unidade auditada, com vistas a corrigir falhas detectadas, cuja gravidade possa repercutir em eventos futuros e evitar a sua repetição, demandando da Administração pronta ação ou correção.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

ACHADO 01: Falhas no processo de gerenciamento de incidentes de Segurança da Informação	
SITUAÇÃO ENCONTRADA (A1.1):	
No decurso dos trabalhos de auditoria, foi realizada observação acerca do atendimento, pelo TRT19ª, ao disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, em seu item 1.1, o qual menciona que: *1. Escopo* *1.1 O Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário é complementar ao Protocolo de Prevenção de Incidentes Cibernéticos e prevê as ações responsivas a serem colocadas em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente e poderá durar dias, semanas ou meses.* Assim, ao analisar os processos existentes no TRT19ª (ATO n.º 103/2019/GP/TRT19ª e ATO n.º 82/2019/GP/TRT19ª), em relação ao disposto no normativo supracitado, e, em consonância com a indagação realizada pelo CSJT, contida no item 1.2.6 do questionário aplicado, transcrita a seguir: *O processo de gerenciamento de incidentes de segurança da informação/cibernética prevê as ações responsivas a serem colocadas em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente (Identificação de crise cibernética)?* Concluiu-se, com amparo no exame dos normativos internos do TRT19ª e afirmações do auditado, extraídas do Questionário, Ata da Reunião, RDI n.º 06/2022, DOCS n.º 08, 10 e 14 do PROAD 2483/2022, que**:** **Não há previsão, no processo de gerenciamento de incidentes de segurança da informação, de ações responsivas a serem colocadas em prática quando ficar evidente que um incidente não será mitigado rapidamente.**	
MANIFESTAÇÃO DO AUDITADO:	
O processo de gerenciamento de incidentes de segurança da informação está sendo revisado para adequação às normas mais recentes. As ações responsivas serão incluídas na revisão, de acordo com o encaminhamento do Achado. Considerando a priorização e adequação de recursos da SETIC destinados a essa ação, a conclusão da revisão desse processo está prevista para novembro de 2022.	
ANÁLISE E CONCLUSÃO:	
A Secretaria de Auditoria (SAUD) ratifica o Achado. Dessa forma, a proposta de encaminhamento formulada subsiste.	
OBJETO(S):	- ATO n.º 103/2019/GP/TRT19ªe;

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

	- ATO n.º 82/2019/GP/TRT19ª.
CRITÉRIO(S):	- Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 1.1.
EVIDÊNCIA(S):	- DOC n.º 08 do PROAD 2483/2022 – Questionário; - DOC n.º 10 do PROAD 2483/2022 - Ata da Reunião e; - DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.
CAUSA(S):	- Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; - Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; - Ausência de atualização normativa pelo TRT19ª.
EFEITO(S)	- Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª; - Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª e; - Imprevisibilidade para mediação do problema.
PROPOSTA DE ENCAMINHAMENTO:	Recomenda-se: - Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: ✓ Atualização do ATO n.º 103/2019/GP/TRT19ª, para inclusão da etapa relativa às ações responsivas a serem colocadas em prática quando ficar evidente que um incidente não será mitigado rapidamente, conforme disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 1.1. ✓ Elaboração de manuais/protocolos, e/ou a construção do desenho do processo, contendo a aludida etapa, com a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos, bem como os modelos de documentos a serem utilizados nas etapas, conforme prevê o item 8.16 do ATO n.º 103/2019/GP/TRT19ª; como também, após a aprovação pela Presidência, posterior publicação no Portal de Governança de TI, **do que for cabível, observando os requisitos de segurança da informação quanto aos controles sigilosos**.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

ACHADO 01: Falhas no processo de gerenciamento de incidentes de Segurança da Informação
SITUAÇÃO ENCONTRADA (A1.2):
No decurso dos trabalhos de auditoria, foi realizada observação acerca do atendimento, pelo TRT19ª, ao disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, em seu item 2.2, o qual menciona que: *2. Identificação de Crise Cibernética* *2.2. O gerenciamento de crise se inicia quando:* *a)ficar caracterizado grave dano material ou de imagem;* *b)restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;* *c) o incidente impactar a atividade finalística ou o serviço crítico mantido pela organização; ou* *d) o incidente atrair grande atenção da mídia e da população em geral.* Assim, ao analisar os processos existentes no TRT19ª (ATO n.º 103/2019/GP/TRT19ª e ATO n.º 82/2019/GP/TRT19ª), em relação ao disposto no normativo supracitado, e, em consonância com a indagação realizada pelo CSJT, contida no item 1.2.7 do questionário aplicado, transcrita a seguir: *O processo de gerenciamento de incidentes de segurança da informação/cibernética estabelece critérios para iniciar o gerenciamento de crise?* Concluiu-se, com amparo no exame dos normativos internos do TRT19ª e afirmações do auditado, extraídas do Questionário, Ata da Reunião, RDI n.º 06/2022, DOCS n.º 08, 10 e 14 do PROAD 2483/2022, que**:** **Não há previsão, no processo de gerenciamento de incidentes de segurança da informação, de estabelecimento de critérios para iniciar o gerenciamento de crise.**
MANIFESTAÇÃO DO AUDITADO:
O processo de gerenciamento de incidentes de segurança da informação está sendo revisado para adequação às normas mais recentes. Os critérios para iniciar o gerenciamento de crise serão incluídos na revisão, de acordo com o encaminhamento do Achado. Considerando a priorização e adequação de recursos da SETIC destinados a essa ação, a conclusão desse processo está prevista para novembro de 2022.
ANÁLISE E CONCLUSÃO
A Secretaria de Auditoria (SAUD) ratifica o Achado. Dessa forma, a proposta de encaminhamento formulada subsiste.

OBJETO(S):	- ATO n.º 103/2019/GP/TRT19ª e; - ATO n.º 82/2019/GP/TRT19ª.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

CRITÉRIO(S):	- Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 2.2.
EVIDÊNCIA(S):	- DOC n.º 08 do PROAD 2483/2022 – Questionário; - DOC n.º 10 do PROAD 2483/2022 – Ata da Reunião e; - DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.
CAUSA(S):	- Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; - Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; - Ausência de atualização normativa pelo TRT19ª.
EFEITO(S)	- Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª; - Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª e; - Imprevisibilidade para mediação do problema.
PROPOSTA DE ENCAMINHAMENTO:	Recomenda-se: - Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: ✓ Atualização do ATO n.º 103/2019/GP/TRT19ª, para inclusão da etapa relativa a definição dos critérios para iniciar o gerenciamento de crise cibernética, conforme disposto na Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 2.2. ✓ Elaboração de manuais/protocolos, e/ou a construção do desenho do processo, contendo a aludida etapa, com a descrição das atividades, respectivos papeis e responsabilidades dos envolvidos, bem como os modelos de documentos a serem utilizados nas etapas, conforme prevê o item 8.16 do ATO n.º 103/2019/GP/TRT19ª; como também, após a aprovação pela Presidência, posterior publicação no Portal de Governança de TI, **do que for cabível, observando os requisitos de segurança da informação quanto aos controles sigilosos**.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

ACHADO 01: Falhas no processo de gerenciamento de incidentes de Segurança da Informação

SITUAÇÃO ENCONTRADA (A1.3):

No decurso dos trabalhos de auditoria, foi realizada observação acerca do atendimento, pelo TRT19ª, ao disposto na Instrução Normativa GSI/PR 5/2021, em seu artigo 16, inciso IV, o qual menciona que:
Art. 16. Em relação ao gerenciamento da nuvem, os órgãos ou as entidades deverão, no mínimo:
IV - elaborar um processo de tratamento de incidentes junto ao provedor de serviço de nuvem e comunicá-lo à equipe responsável pelo gerenciamento da nuvem.

Assim, ao analisar os processos existentes no TRT19ª (ATO n.º 103/2019/GP/TRT19ª), em relação ao disposto no normativo supracitado, e, em consonância com a indagação realizada pelo CSJT, contida no item 1.2.8 do questionário aplicado, transcrita a seguir:
O processo de gerenciamento de incidentes de segurança da informação/cibernética contempla incidentes ocorridos nos serviços em nuvem contratados pelo órgão (Ex.: Gsuite)?

Concluiu-se, com amparo no exame do normativo interno do TRT19ª, porém, em contraponto às afirmações do auditado, extraídas do Questionário, Ata da Reunião, RDI n.º 06/2022, DOCS n.º 08, 10 e 14 do PROAD 2483/2022, que:

Não há evidente previsão, no processo de gerenciamento de incidentes de segurança da informação, da contemplação dos incidentes que podem ocorrer nos serviços em nuvem contratados pelo órgão, a exemplo da plataforma Gsuite.

A conclusão decorre da compreensão, pela equipe de auditoria, de que, mesmo havendo controles internos oriundos da própria plataforma do provedor e previsão genérica nos processos existentes com referência a sistemas críticos, tal previsão poderia estar expressa de forma clara e especifica nos normativos instituídos, tendo em vista o caráter de relevância desses serviços, como também suas particularidades.

MANIFESTAÇÃO DO AUDITADO:

O único serviço em nuvem funcionando neste Tribunal é o Gsuite (conjunto de ferramentas tecnológicas da empresa Google), contratado a partir de Ata de Registro de Preços decorrente de licitação realizada pelo TRT8ª, da qual 11 tribunais foram participantes, inclusive o TRT19ª.
Atualmente, a equipe de Segurança da Informação da Setic recebe comunicados de eventos suspeitos ocorridos no Gsuite, o que se apresenta, na opinião desta Secretaria, como suficiente para mitigar eventuais riscos desse serviço.
O processo de gerenciamento de incidentes de segurança da informação está sendo revisado para atender as normas mais recentes e, se for o caso, para estender aos serviços em nuvem a

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

previsão já existente para os demais serviços.	
ANÁLISE E CONCLUSÃO	
A Secretaria de Auditoria (SAUD) analisou novamente o ATO n.º 103/2019/GP/TRT19ª, com vistas a reexaminar o Achado. Logo, concluiu que a situação encontrada permanece, tendo em vista que o normativo interno não trata de forma especifica de incidentes ocorridos nos serviços em nuvem e suas respectivas particulares. Dessa forma a SAUD ratifica o Achado e a proposta de encaminhamento formulada subsiste.	
OBJETO(S):	- ATO n.º 103/2019/GP/TRT19ª.
CRITÉRIO(S):	- Instrução Normativa GSI/PR 5/2021, Art. 16, inciso IV.
EVIDÊNCIA(S):	- DOC n.º 08 do PROAD 2483/2022 – Questionário; - DOC n.º 10 do PROAD 2483/2022 – Ata da Reunião e; - DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.
CAUSA(S):	- Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; - Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; - Ausência de atualização normativa pelo TRT19ª.
EFEITO(S)	- Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª; - Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª e; - Possível não atendimento às regulamentações contratuais com o provedor.
PROPOSTA DE ENCAMINHAMENTO:	Recomenda-se: - Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: ✓ Atualização do ATO n.º 103/2019/GP/TRT19ª, para inclusão da etapa relativa a contemplação dos incidentes ocorridos nos serviços em nuvem contratados pelo órgão, conforme disposto na Instrução Normativa GSI/PR 5/2021, Art. 16, inciso IV. ✓ Elaboração de manuais/protocolos, e/ou a construção do desenho do processo, contendo a aludida etapa, com a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos, bem como os modelos de documentos a serem utilizados nas etapas, conforme prevê o item 8.16 do ATO n.º 103/2019/GP/TRT19ª; como também, após a aprovação pela Presidência, posterior publicação no Portal de Governança de TI, **do que for cabível, observando os requisitos de segurança da informação quanto aos controles**

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

	sigilosos. - Por fim, adicionalmente, recomenda-se uma análise acerca das questões contratuais com os provedores dos serviços em nuvem, em relação a falta da referida previsão nos processos do TRT19ª, e seu reflexo quanto ao risco de quebra contratual e/ou não atendimento dos serviços, devido a possíveis infrações contratuais.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

ACHADO 01: Falhas no processo de gerenciamento de incidentes de Segurança da Informação	
SITUAÇÃO ENCONTRADA (A1.4):	
No decurso dos trabalhos de auditoria, foi realizada observação acerca do atendimento, pelo TRT19ª, ao disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, em seu item 5.9, o qual menciona que: *5. Execução (durante a crise)* *5.9 Todos os incidentes graves deverão ser comunicados ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça.* Assim, ao analisar os processos existentes no TRT19ª (ATO n.º 103/2019/GP/TRT19ª e ATO n.º 82/2019/GP/TRT19ª), em relação ao disposto no normativo supracitado, e, em consonância com a indagação realizada pelo CSJT, contida no item 1.2.9 do questionário aplicado, transcrita a seguir: *O processo prevê a comunicação de todos os incidentes graves ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ)?* Concluiu-se, com amparo no exame dos normativos internos do TRT19ª e afirmações do auditado, extraídas do Questionário, Ata da Reunião, RDI n.º 06/2022, DOCS n.º 08, 10 e 14 do PROAD 2483/2022, que**:** **Não há previsão, no processo, de etapa relativa à comunicação dos incidentes graves ao CPTRIC-PJ.**	
MANIFESTAÇÃO DO AUDITADO:	
O processo de gerenciamento de incidentes de segurança da informação está sendo revisado para atender as normas mais recentes e para incluir a comunicação de incidentes graves ao CPTRIC-PJ. Considerando a priorização e adequação de recursos da SETIC destinados a essa ação, a conclusão desse processo está prevista para novembro de 2022.	
ANÁLISE E CONCLUSÃO	
A Secretaria de Auditoria ratifica o Achado. Dessa forma, a proposta de encaminhamento formulada subsiste.	
OBJETO(S):	- ATO n.º 103/2019/GP/TRT19ª e; - ATO n.º 82/2019/GP/TRT19ª.
CRITÉRIO(S):	- Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 5.9.
EVIDÊNCIA(S):	- DOC n.º 08 do PROAD 2483/2022 – Questionário; - DOC n.º 10 do PROAD 2483/2022 – Ata da Reunião e;

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

	- DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.
CAUSA(S):	- Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; - Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; - Ausência de atualização normativa pelo TRT19ª.
EFEITO(S)	- Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª; - Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª e; - Perda de colaboração com os órgãos superiores do Poder Judiciário.
PROPOSTA DE ENCAMINHAMENTO:	Recomenda-se: - Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: ✓ Atualização do ATO n.º 103/2019/GP/TRT19ª, para Inclusão de etapa relativa a comunicação dos incidentes graves ao CPTRIC-PJ, conforme disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 5.9. ✓ Elaboração de manuais/protocolos, e/ou a construção do desenho do processo, contendo a aludida etapa, com a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos, bem como os modelos de documentos a serem utilizados nas etapas, conforme prevê o item 8.16 do ATO n.º 103/2019/GP/TRT19ª; como também, após a aprovação pela Presidência, posterior publicação no Portal de Governança de TI, **do que for cabível, observando os requisitos de segurança da informação quanto aos controles sigilosos**.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

ACHADO 01: Falhas no processo de gerenciamento de incidentes de Segurança da Informação	
SITUAÇÃO ENCONTRADA (A1.5):	
No decurso dos trabalhos de auditoria, foi realizada observação acerca do atendimento, pelo TRT19ª, ao disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, em seu item 6.4, o qual menciona que: *6. Melhoria contínua (lições aprendidas no pós-crise)* *6.4 Deve ser elaborado Relatório de Comunicação de Incidente de Segurança Cibernética, que contenha a descrição e o detalhamento da crise, bem como o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados. Deve ser elaborado Relatório de Comunicação de Incidente de Segurança Cibernética, que contenha a descrição e o detalhamento da crise, e o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.* Assim, ao analisar os processos existentes no TRT19ª (ATO n.º 103/2019/GP/TRT19ª e ATO n.º 82/2019/GP/TRT19ª), em relação ao disposto no normativo supracitado, e, em consonância com a indagação realizada pelo CSJT, contida no item 1.2.11 do questionário aplicado, transcrita a seguir: *O processo prevê a elaboração de Relatório de Comunicação de Incidente de Segurança da Informação/Cibernética, contendo a descrição e o detalhamento da crise e o plano de ação tomado?* Concluiu-se, com amparo no exame dos normativos internos do TRT19ª e afirmações do auditado, extraídas do Questionário, Ata da Reunião, RDI n.º 06/2022, DOCS n.º 08, 10 e 14 do PROAD 2483/2022, que**:** **Não há previsão, no processo, da etapa relativa a elaboração de Relatório de Comunicação de Incidente de Segurança da Informação, contendo descrição e detalhamento da crise com plano de ação.**	
MANIFESTAÇÃO DO AUDITADO:	
O processo de gerenciamento de incidentes de segurança da informação está sendo revisado para atender as normas mais recentes e para incluir a etapa de elaboração do Relatório de Comunicação de Incidentes de Segurança da Informação. Considerando a priorização e adequação de recursos da SETIC destinados a essa ação, a conclusão desse processo está prevista para novembro de 2022.	
ANÁLISE E CONCLUSÃO	
A Secretaria de Auditoria (SAUD) ratifica o Achado. Dessa forma, a proposta de encaminhamento formulada subsiste.	
OBJETO(S):	- ATO n.º 103/2019/GP/TRT19ª e; - ATO n.º 82/2019/GP/TRT19ª.
CRITÉRIO(S):	- Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 6.4.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

EVIDÊNCIA(S):	- DOC n.º 08 do PROAD 2483/2022 – Questionário; - DOC n.º 10 do PROAD 2483/2022 – Ata da Reunião e; - DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.
CAUSA(S):	- Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; - Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; - Ausência de atualização normativa pelo TRT19ª.
EFEITO(S)	- Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª; - Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª e; - Comprometimento na gestão dos incidentes, por ausência de mecanismos capazes de auxiliar na gestão do problema.
PROPOSTA DE ENCAMINHAMENTO:	Recomenda-se: - Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: ✓ Atualização do ATO n.º 103/2019/GP/TRT19ª, para inclusão da etapa relativa a elaboração de Relatório de Comunicação de Incidente de Segurança da Informação, contendo descrição e detalhamento da crise com plano de ação, conforme disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 6.4. ✓ Elaboração de manuais/protocolos, e/ou a construção do desenho do processo, contendo a aludida etapa, com a descrição das atividades, respectivos papeis e responsabilidades dos envolvidos, bem como os modelos de documentos a serem utilizados nas etapas, conforme prevê o item 8.16 do ATO n.º 103/2019/GP/TRT19ª; como também, após a aprovação pela Presidência, posterior publicação no Portal de Governança de TI, **do que for cabível, observando os requisitos de segurança da informação quanto aos controles sigilosos**. - Elaboração do modelo de Relatório a ser utilizado, contendo a descrição e o detalhamento da crise e o plano de ação a ser tomado, quando da ocorrência dos eventos.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

ACHADO 01: Falhas no processo de gerenciamento de incidentes de Segurança da Informação	
SITUAÇÃO ENCONTRADA (A1.6):	
No decurso dos trabalhos de auditoria, foi realizada observação acerca do atendimento, pelo TRT19ª, ao disposto na Resolução CNJ n.º 396/2021, em seu artigo 11, incisos I e II; e seu artigo 21, § 2º, inciso IV, os quais mencionam que: *Art. 11 Para elevar o nível de segurança das infraestruturas críticas, deve-se:* *I – estabelecer todas as ações que possibilitem maior eficiência, ou seja, capacidade de responder de forma satisfatória a incidentes de segurança, permitindo a contínua prestação dos serviços essenciais a cada órgão;* *III – elaborar e aplicar processo de resposta e tratamento a incidentes de segurança cibernética que contenha, entre outros, procedimento de continuidade do serviço prestado e seu rápido restabelecimento, além de comunicação interna e externa;* *Art. 21 Cada órgão do Poder Judiciário, com exceção do STF, deverá constituir estrutura de segurança da informação, subordinada diretamente à alta administração do órgão e desvinculada da área de TIC.* *§ 2º O gestor de segurança da informação terá as seguintes atribuições:* *IV – implantar procedimento de tratamento e resposta a incidentes em segurança da informação;* Assim, ao analisar os processos existentes no TRT19ª (ATO n.º 103/2019/GP/TRT19ª), em relação ao disposto no normativo supracitado, e, em consonância com a indagação realizada pelo CSJT, contida no item 1.2.12 do questionário aplicado, transcrita a seguir: *O processo de gerenciamento de incidentes de segurança da informação/cibernética está implantado?* Concluiu-se, com amparo no exame do normativo interno do TRT19ª e afirmações do auditado, extraídas do Questionário, Ata da Reunião, RDI n.º 06/2022, DOCS n.º 08, 10 e 14 do PROAD 2483/2022, que**:** **O processo de gerenciamento de incidentes de segurança da informação está parcialmente implantado, pois encontra-se em fase de atualização, bem como, a etapa de Avaliação não está sendo devidamente executada.**	
MANIFESTAÇÃO DO AUDITADO:	
O processo está parcialmente implantado e a etapa de Avaliação está sendo parcialmente executada. Os eventos e incidentes de segurança da informação são registrados na ferramenta de gestão de demandas (Jira), que mantém o histórico das ocorrências. Os demais itens de avaliação serão contemplados quando da revisão do processo de gerenciamento de incidentes de segurança da informação. Considerando a priorização e adequação de recursos da SETIC destinados a essa ação, a conclusão desse processo está prevista para novembro de 2022.	
ANÁLISE E CONCLUSÃO	
A Secretaria de Auditoria (SAUD) ratifica o Achado. Dessa forma, a proposta de encaminhamento formulada subsiste.	
OBJETO(S):	- ATO n.º 103/2019/GP/TRT19ª.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

CRITÉRIO(S):	- Resolução CNJ n.º 396/2021, art. 11, incisos I e III; art. 21, § 2º, inciso IV.
EVIDÊNCIA(S):	- DOC n.º 08 do PROAD 2483/2022 – Questionário; - DOC n.º 10 do PROAD 2483/2022 – Ata da Reunião e; - DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.
CAUSA(S):	- Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; - Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; - Ausência de atualização normativa pelo TRT19ª.
EFEITO(S)	- Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª; - Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª e; - Comprometimento da gestão dos incidentes.
PROPOSTA DE ENCAMINHAMENTO:	Recomenda-se: - Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: ✓ Atualização do ATO n.º 103/2019/GP/TRT19ª conforme disposto na Resolução CNJ n.º 396/2021, art. 11, incisos I e III; art. 21, § 2º, inciso IV. ✓ Elaboração de manuais/protocolos, e/ou a construção do desenho do processo completo, com a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos, bem como os modelos de documentos a serem utilizados nas etapas, conforme prevê o item 8.16 do ATO n.º 103/2019/GP/TRT19ª; como também, após a aprovação pela Presidência, posterior publicação no Portal de Governança de TI, **do que for cabível, observando os requisitos de segurança da informação quanto aos controles sigilosos**. - Adoção de medidas necessárias para integração e amadurecimento da política de segurança da informação, tais como, realização de testes dos planos, estabelecimentos de controles, construção de relatórios por meio dos dados extraídos dos registros para melhor avaliação e analise dos incidentes, treinamento aos usuários do TRT19ª, melhor aproveitamento da ferramenta que registra os incidentes (Jira), com vistas a garantir a implantação integral do processo e sua efetividade.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

ACHADO 02: Falhas na gestão de continuidade dos serviços essenciais de Tecnologia da Informação

SITUAÇÃO ENCONTRADA (A2.1):

No decurso dos trabalhos de auditoria, foi realizada observação acerca do atendimento, pelo TRT19ª, ao disposto na Instrução Normativa n.º GSI/PR 3/2021, em seu artigo 25, o qual menciona que:

Art. 25. O gestor de segurança da informação coordenará o processo de gestão de continuidade de negócios em segurança da informação nos seus respectivos órgãos ou entidades, bem como designará um agente responsável pela referida gestão, dentre os servidores efetivos do órgão.

Como também, quanto o atendimento ao disposto na NBR ISO 27002, em seu item 17.1.2, o qual menciona que:

17.1.2 Implementando a continuidade da segurança da informação

Controle

Convém que a organização estabeleça, documente, implemente e mantenha processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa.

Diretrizes para implementação.

Convém que uma organização assegure-se de que:

a) uma estrutura de gerenciamento adequada está implementada para mitigar e responder a um evento de interrupção, usando pessoal com a necessária autoridade, experiência e competência;

Assim, ao analisar os processos existentes no TRT19ª (ATO n.º 82/2019/GP/TRT19ª, Planos de Continuidade Operacional e Planos de Recuperação de Desastres), em relação ao disposto nos normativos supracitados, e, em consonância com a indagação realizada pelo CSJT, contida no item 2.2.1 do questionário aplicado, transcrita a seguir:

Foram definidos os papéis e responsabilidades dos profissionais envolvidos no programa de gestão de continuidade de serviços essenciais de TI, incluindo o agente responsável pela gestão de continuidade dos serviços de TI no Órgão?

Concluiu-se, com amparo no exame do normativo interno do TRT19ª, na inspeção física realizada *in loco* nos Planos de Continuidade Operacional e Recuperação de Desastres, e nas afirmações do auditado, extraídas do Questionário, Ata da Reunião, RDI n.º 06/2022, DOCS n.º 08, 10 e 14 do PROAD 2483/2022, que**:**

Foram estabelecidos, os papéis e responsabilidades dos profissionais envolvidos no programa de gestão de continuidade de serviços essenciais de TI, incluindo o agente responsável pela gestão de continuidade dos serviços de TI no Órgão, somente nos Planos de Continuidade Operacional e Recuperação de Desastres relativos ao PJe e PROAD. Logo, concluiu-se que o atendimento da demanda é parcial.

MANIFESTAÇÃO DO AUDITADO:

Os responsáveis pelos ativos envolvidos estão definidos nos Planos de Continuidade Operacional e Planos de Recuperação de Desastres, os quais não são públicos por conterem informações sensíveis, estando à disposição da Auditoria para verificação e análise.

ANÁLISE E CONCLUSÃO

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

A Secretaria de Auditoria ratifica o Achado. Dessa forma, a proposta de encaminhamento formulada subsiste, considerando que atualmente o TRT19ª tem contemplado nos Planos de Continuidade Operacional e de Recuperação de Desastres somente o PJe e PROAD. Assim sendo, o atendimento é parcial, tendo em vista que outros serviços essências de TI, tais como SIGEP, não foram contemplados, e consequentemente os papéis e responsabilidades dos profissionais envolvidos.	
OBJETO(S):	- ATO n.º 82/2019/GP/TRT19ª; - Plano de Continuidade Operacional – PJE; - Plano de Continuidade Operacional – PROAD e; - Planos de Recuperação de Desastres.
CRITÉRIO(S):	- Instrução Normativa GSI/PR 3/2021, art. 25. - NBR ISO 27002, item 17.1.2.
EVIDÊNCIA(S):	- DOC n.º 08 do PROAD 2483/2022 – Questionário; - DOC n.º 10 do PROAD 2483/2022 – Ata da Reunião e; - DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.
CAUSA(S):	- Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; - Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; - Ausência de atualização normativa pelo TRT19ª.
EFEITO(S)	- Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª e; - Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª.
PROPOSTA DE ENCAMINHAMENTO:	Recomenda-se: - Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: ✓ Atualização do ATO n.º 82/2019/GP/TRT19ª, para inclusão da menção relativa a definição dos papéis e responsabilidades dos profissionais envolvidos no programa de gestão de continuidade de serviços essenciais de TI, incluindo o agente responsável pela gestão de continuidade dos serviços de TI no Órgão, conforme disposto na Instrução Normativa GSI/PR n.º 3/2021, art. 25 e NBR ISO 27002, item 17.1.2. ✓ Elaboração dos protocolos, manuais e/ou processos, que ainda não estão mapeados, com a inclusão da descrição das atividades, respectivos papeis e responsabilidades dos envolvidos e responsáveis pelo programa de gestão de continuidade de serviços essenciais de TI.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

ACHADO 02: Falhas na gestão de continuidade dos serviços essenciais de Tecnologia da Informação

SITUAÇÃO ENCONTRADA (A2.2):

No decurso dos trabalhos de auditoria, foi realizada observação acerca do atendimento, pelo TRT19ª, ao disposto na Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, em seu item 4.1, alínea "b" o qual menciona que:

4. Planejamento da Crise (pré-crise)

4.1 Para melhor lidar com uma crise cibernética, é necessário prévia e adequada preparação, sendo fundamental que os órgãos do Poder Judiciário estabeleçam um Programa de Gestão da Continuidade de Serviços que contemple as seguintes atividades:

b) definir as atividades críticas que são fundamentais para a atividade finalística do órgão;

Assim, ao analisar os processos existentes no TRT19ª (ATO n.º 82/2019/GP/TRT19ª, Planos de Continuidade Operacional e Planos de Recuperação de Desastres), em relação ao disposto no normativo supracitado, e, em consonância com a indagação realizada pelo CSJT, contida no item 2.2.2 do questionário aplicado, transcrita a seguir:

O programa contém a definição das atividades críticas de negócio a serem contempladas, abarcando, no mínimo, os seguintes serviços: PJE-JT, SIGEP-JT (FOLHA + CADASTRO) ou sistema equivalente, Processo Administrativo, Portal Internet e solução de comunicação (EX: GOOGLE SUITE)?

Concluiu-se, com amparo no exame do normativo interno do TRT19ª, na inspeção física realizada *in loco* nos Planos de Continuidade Operacional e Recuperação de Desastres, e nas afirmações do auditado, extraídas do Questionário, Ata da Reunião, RDI n.º 06/2022, DOCS n.º 08, 10 e 14 do PROAD 2483/2022, que**:**

Não há, no programa de gestão de continuidade de serviços de TI, a definição das atividades críticas de negócio a serem contempladas, em especial, quanto aos serviços relativos ao Portal SIGEP, Processo Administrativo e Google.

MANIFESTAÇÃO DO AUDITADO:

Segundo o Glossário do anexo na Portaria n.º 162/2021: Atividades críticas são "atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão, de maneira que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo".

A SETIC contemplou nos Planos de Continuidade Operacional e de Recuperação de Desastres os ativos de infraestrutura os sistemas de processo administrativo (PROAD) e de processo judicial (PJe).

Na atualização do processo de continuidade, os demais serviços definidos como críticos pelo CSJT (SIGEP e Google Suíte) serão incluídos.

Considerando a priorização e adequação de recursos da SETIC destinados a essa ação, a conclusão desse processo está prevista para dezembro de 2024.

ANÁLISE E CONCLUSÃO

A Secretaria de Auditoria (SAUD) ratifica o Achado. Dessa forma, a proposta de encaminhamento formulada subsiste, considerando que atualmente o TRT19ª tem contemplado nos Planos de Continuidade Operacional e de Recuperação de Desastres somente o PJe e PROAD. Assim sendo, o atendimento é parcial, tendo em vista que outras atividades críticas de

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

negócio não foram contempladas.	
OBJETO(S):	- ATO n.º 82/2019/GP/TRT19ª; - Plano de Continuidade Operacional – PJE; - Plano de Continuidade Operacional – PROAD e; - Planos de Recuperação de Desastres.
CRITÉRIO(S):	- Portaria CNJ n.º162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea b.
EVIDÊNCIA(S):	- DOC n.º 08 do PROAD 2483/2022 – Questionário; - DOC n.º 10 do PROAD 2483/2022 – Ata da Reunião e; - DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.
CAUSA(S):	- Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; - Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; - Ausência de atualização normativa pelo TRT19ª.
EFEITO(S)	- Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª e; - Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª.
PROPOSTA DE ENCAMINHAMENTO:	Recomenda-se: - Definição, junto à Alta Administração do TRT19ª, das atividades críticas de negócio a serem contempladas no programa de gestão de continuidade de serviços de TI. - Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: ✓ Atualização do ATO n.º 82/2019/GP/TRT19ª, para inclusão da menção relativa a definição das atividades críticas de negócio a serem contempladas no programa de gestão de continuidade de serviços de TI, conforme disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea b. ✓ Elaboração dos protocolos, manuais e/ou processos relativos as atividades críticas, que ainda não estão mapeados, com a descrição das atividades, respectivos papeis e responsabilidades dos envolvidos.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

ACHADO 02: Falhas na gestão de continuidade dos serviços essenciais de Tecnologia da Informação	
SITUAÇÃO ENCONTRADA (A2.3):	
No decurso dos trabalhos de auditoria, foi realizada observação acerca do atendimento, pelo TRT19ª, ao disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, em seu item 4.1, alínea "c", o qual menciona que: *4. Planejamento da Crise (pré-crise)* *4.1 Para melhor lidar com uma crise cibernética, é necessário prévia e adequada preparação, sendo fundamental que os órgãos do Poder Judiciário estabeleçam um Programa de Gestão da Continuidade de Serviços que contemple as seguintes atividades:* *c) identificar os ativos de informação críticos, ou seja, aqueles que suportam as atividades primordiais, incluindo as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação;* Assim, ao analisar os processos existentes no TRT19ª (ATO n.º 82/2019/GP/TRT19ª, Planos de Continuidade Operacional e Planos de Recuperação de Desastres), em relação ao disposto no normativo supracitado, e, em consonância com a indagação realizada pelo CSJT, contida no item 2.2.3 do questionário aplicado, transcrita a seguir: *O programa prevê a identificação dos ativos de informação críticos, incluindo as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação?* Concluiu-se, com amparo no exame do normativo interno do TRT19ª, na inspeção física realizada *in loco* nos Planos de Continuidade Operacional e Recuperação de Desastres, porém, em contraponto as afirmações do auditado, extraídas do Questionário, Ata da Reunião, RDI n.º 06/2022, DOCS n.º 08, 10 e 14 do PROAD 2483/2022, que não encontraram respaldo quando da confrontação com o processo instituído e formalizado, que**:** **Há previsão, no programa de gestão de continuidade de serviços de TI, da identificação dos ativos de informação críticos, incluindo as pessoas, a infraestrutura e os recursos de tecnologia, somente nos Planos de Continuidade Operacional e Recuperação de Desastres relativos ao PJe e PROAD. Logo, concluiu-se que o atendimento da demanda é parcial.**	
MANIFESTAÇÃO DO AUDITADO:	
A SETIC contemplou nos Planos de Continuidade Operacional e de Recuperação de Desastres os ativos de infraestrutura os sistemas de processo administrativo (PROAD) e de processo judicial (PJe). Na atualização do processo de continuidade, os demais serviços definidos como críticos pelo CSJT (SIGEP e Google Suíte) serão incluídos. Considerando a priorização e adequação de recursos da SETIC destinados a essa ação, a conclusão desse processo está prevista para dezembro de 2024.	
ANÁLISE E CONCLUSÃO	
A Secretaria de Auditoria (SAUD) ratifica o Achado. Dessa forma, a proposta de encaminhamento formulada subsiste, considerando que atualmente o TRT19ª tem contemplado nos Planos de Continuidade Operacional e de Recuperação de Desastres somente o PJe e PROAD. Assim sendo, o atendimento é parcial, tendo em vista que outras atividades críticas de negócio não foram contempladas.	
OBJETO(S):	- ATO n.º 82/2019/GP/TRT19ª;

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

	- Plano de Continuidade Operacional – PJE; - Plano de Continuidade Operacional – PROAD e; - Planos de Recuperação de Desastres.
CRITÉRIO(S):	- Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea c.
EVIDÊNCIA(S):	- DOC n.º 08 do PROAD 2483/2022 – Questionário; - DOC n.º 10 do PROAD 2483/2022 – Ata da Reunião; - DOC n.º 13 do PROAD 2483/2022 – Declaração e; - DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.
CAUSA(S):	- Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; - Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; - Ausência de atualização normativa pelo TRT19ª.
EFEITO(S)	- Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª e; - Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª.
PROPOSTA DE ENCAMINHAMENTO:	- Recomenda-se: - Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: ✓ Atualização do ATO n.º 82/2019/GP/TRT19ª, para inclusão da menção relativa a identificação dos ativos de informação críticos, incluindo as pessoas, a infraestrutura e os recursos de tecnologia, respeitando os requisitos de segurança da informação e as exigências dos normativos em vigor, conforme disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea c. ✓ Elaboração dos protocolos, manuais e/ou processos relativos as atividades críticas, que ainda não estão mapeados, com a identificação dos ativos de informação críticos, incluindo as pessoas, a infraestrutura e os recursos de tecnologia.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

ACHADO 02: Falhas na gestão de continuidade dos serviços essenciais de Tecnologia da Informação

SITUAÇÃO ENCONTRADA (A2.4):

No decurso dos trabalhos de auditoria, foi realizada observação acerca do atendimento, pelo TRT19ª, ao disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, em seu item 4.1, alínea "e" e "f", o qual menciona que:
4. Planejamento da Crise (pré-crise)
4.1 Para melhor lidar com uma crise cibernética, é necessário prévia e adequada preparação, sendo fundamental que os órgãos do Poder Judiciário estabeleçam um Programa de Gestão da Continuidade de Serviços que contemple as seguintes atividades:
e) categorizar os incidentes e estabelecer procedimentos de resposta específicos (playbooks) para cada tipo de incidente, de forma a apoiar equipes técnicas e de liderança em casos de incidentes cibernéticos;
f) priorizar o monitoramento, acompanhamento e tratamento dos riscos de maior criticidade. Tais atividades deverão ser detalhadas e consolidadas em um plano de contingência que contemple diversos setores, em razão de possíveis cenários de crise, a fim de se contrapor à escalada de uma eventual crise e com o objetivo de manter os serviços prestados pela organização; e

Assim, ao analisar os processos existentes no TRT19ª (ATO n.º 82/2019/GP/TRT19ª, Planos de Continuidade Operacional e Planos de Recuperação de Desastres), em relação ao disposto no normativo supracitado, e, em consonância com a indagação realizada pelo CSJT, contida no item 2.2.6 do questionário aplicado, transcrita a seguir:
Há previsão de categorização dos incidentes e estabelecimento de procedimentos de resposta específicos (playbooks)?

Concluiu-se, com amparo no exame do normativo interno do TRT19ª, na inspeção física realizada *in loco* nos Planos de Continuidade Operacional e Recuperação de Desastres, e nas afirmações do auditado, extraídas do Questionário, Ata da Reunião, RDI n.º 06/2022, DOCS n.º 08, 10 e 14 do PROAD 2483/2022, que**:**

Não há previsão, no programa de gestão de continuidade dos serviços de TI, de protocolos, processos, manuais para categorização dos incidentes e estabelecimento de procedimentos de resposta específicos (*playbooks*).

MANIFESTAÇÃO DO AUDITADO:

O processo de gestão de continuidade de serviços de TI será revisado para atender as normas mais recentes e para ajustar de acordo com o encaminhamento adotado pela Auditoria.
Considerando a priorização e adequação de recursos da SETIC destinados a essa ação, a conclusão desse processo está prevista para dezembro de 2024.

ANÁLISE E CONCLUSÃO

A Secretaria de Auditoria (SAUD) ratifica o Achado. Dessa forma, a proposta de

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

encaminhamento formulada subsiste.	
OBJETO(S):	- ATO n.º 82/2019/GP/TRT19ª; - Plano de Continuidade Operacional – PJE; - Plano de Continuidade Operacional – PROAD e; - Planos de Recuperação de Desastres.
CRITÉRIO(S):	- Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea 'e' e 'f'.
EVIDÊNCIA(S):	- DOC n.º 08 do PROAD 2483/2022 – Questionário; - DOC n.º 10 do PROAD 2483/2022 – Ata da Reunião e; - DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.
CAUSA(S):	- Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; - Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; - Ausência de atualização normativa pelo TRT19ª.
EFEITO(S)	- Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª e; - Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª.
PROPOSTA DE ENCAMINHAMENTO:	Recomenda-se: - Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: ✓ Atualização do ATO n.º 82/2019/GP/TRT19ª, para inclusão da menção relativa a previsão de protocolos, processos, ou manuais para categorização dos incidentes e estabelecimento de procedimentos de resposta específicos (*playbooks*), conforme disposto na Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea 'e' e 'f'. ✓ Elaboração dos manuais ou protocolos específicos *(playbooks)*, contendo os procedimentos necessários para atendimento da demanda, no tocante a categorização dos incidentes e estabelecimento de procedimentos de resposta específicos.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

ACHADO 02: Falhas na gestão de continuidade dos serviços essenciais de Tecnologia da Informação

SITUAÇÃO ENCONTRADA (A2.5):

No decurso dos trabalhos de auditoria, foi realizada observação acerca do atendimento, pelo TRT19ª, ao disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, em seu item 4.1, alínea "e" e "f", o qual menciona que:
4. Planejamento da Crise (pré-crise)
4.1 Para melhor lidar com uma crise cibernética, é necessário prévia e adequada preparação, sendo fundamental que os órgãos do Poder Judiciário estabeleçam um Programa de Gestão da Continuidade de Serviços que contemple as seguintes atividades:
e) categorizar os incidentes e estabelecer procedimentos de resposta específicos (playbooks) para cada tipo de incidente, de forma a apoiar equipes técnicas e de liderança em casos de incidentes cibernéticos;
f) priorizar o monitoramento, acompanhamento e tratamento dos riscos de maior criticidade. Tais atividades deverão ser detalhadas e consolidadas em um plano de contingência que contemple diversos setores, em razão de possíveis cenários de crise, a fim de se contrapor à escalada de uma eventual crise e com o objetivo de manter os serviços prestados pela organização; e

Assim, ao analisar os processos existentes no TRT19ª (ATO n.º 82/2019/GP/TRT19ª, ATO n.º 22/2022/GP/TRT19ª, Planos de Continuidade Operacional e Planos de Recuperação de Desastres), em relação ao disposto no normativo supracitado, e, em consonância com a indagação realizada pelo CSJT, contida no item 2.2.7 do questionário aplicado, transcrita a seguir:
Há planos de contingência que detalham o monitoramento, o acompanhamento e o tratamento dos riscos de maior criticidade, em razão de possíveis cenários de crise?

Concluiu-se, com amparo no exame dos normativos internos do TRT19ª, na inspeção física realizada *in loco* nos Planos de Continuidade Operacional e Recuperação de Desastres, e nas afirmações do auditado, extraídas do Questionário, Ata da Reunião, RDI n.º 06/2022, DOCS n.º 08, 10 e 14 do PROAD 2483/2022, que**:**

Não há previsão, no programa de gestão de continuidade dos serviços de TI, de planos de contingência que detalham o monitoramento, o acompanhamento e o tratamento dos riscos de maior criticidade, em razão de possíveis cenários de crise.

MANIFESTAÇÃO DO AUDITADO:

Estão parcialmente contemplados nos Planos de Continuidade Operacional e Planos de Recuperação de Desastres.

ANÁLISE E CONCLUSÃO

A Secretaria de Auditoria ratifica o Achado, tendo em vista que, na inspeção física realizada nos planos de continuidade operacional e recuperação de desastres existentes, não restou

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

evidente a referida previsão, como também, em razão da ausência de outros planos relativos a serviços críticos, e consequentemente, a falta de previsão do plano de contingência. Dessa forma, a proposta de encaminhamento formulada subsiste.	
OBJETO(S):	- ATO n.º 82/2019/GP/TRT19ª; - ATO n.º 22/2022/GP/TRT19ª; - Plano de Continuidade Operacional – PJE; - Plano de Continuidade Operacional – PROAD e; - Planos de Recuperação de Desastres.
CRITÉRIO(S):	- Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea 'e' e 'f'.
EVIDÊNCIA(S):	- DOC n.º 08 do PROAD 2483/2022 – Questionário; - DOC n.º 10 do PROAD 2483/2022 – Ata da Reunião e; - DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.
CAUSA(S):	- Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; - Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; - Ausência de atualização normativa pelo TRT19ª.
EFEITO(S)	- Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª e; - Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª.
PROPOSTA DE ENCAMINHAMENTO:	Recomenda-se: - Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: ✓ Atualização do ATO n.º 82/2019/GP/TRT19ª para inclusão da menção relativa aos planos de contingência que detalham o monitoramento, o acompanhamento e o tratamento dos riscos de maior criticidade, em razão de possíveis cenários de crise, conforme disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea 'e' e 'f'. ✓ Elaboração dos planos de contingência, com detalhamento do monitoramento, acompanhamento e tratamento dos riscos de maior criticidade, em razão de possíveis cenários de crise.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

ACHADO 02: Falhas na gestão de continuidade dos serviços essenciais de Tecnologia da Informação

SITUAÇÃO ENCONTRADA (A2.6):

No decurso dos trabalhos de auditoria, foi realizada observação acerca do atendimento, pelo TRT19ª, ao disposto na Instrução Normativa GSI/PR n.º 3/2021, em seu artigo 23, o qual menciona que:

Art. 23. O plano de continuidade de negócios em segurança da informação deverá conter, no mínimo:
I - o objetivo;
II - as atividades críticas de negócio a serem contempladas no plano;
III - os requisitos para ativação do plano, em especial, o tempo máximo aceitável de permanência da falha;
IV - o(s) responsável(is) pela ativação do plano, com seus respectivos dados de contato;
V - o(s) responsável(is) por aplicar as medidas de contingência definidas, tendo cada servidor responsabilidades formalmente definidas e nominalmente atribuídas, incluindo seus respectivos dados de contato; e
VI - a definição:
a) das ações necessárias para operacionalização das medidas cuja implementação dependa da aquisição de recursos físicos e/ou humanos;
b) dos limites de decisão para os responsáveis pela aplicação das medidas de contingência perante situações inesperadas;
c) dos parâmetros para encerramento do plano e para a volta à normalidade;
d) dos responsáveis por essas ações, incluindo seus dados de contato;
e) da forma de monitoramento desse processo; e
f) de um roteiro de simulação de teste de funcionamento e da forma de sua aplicação.
Parágrafo único. O plano de continuidade de negócios deverá ser testado regularmente, com intuito de que seus resultados sejam documentados e possam garantir a sua efetividade em caso de necessidade de ativação.

Assim, ao analisar os processos existentes no TRT19ª (ATO n.º 82/2019/GP/TRT19ª, Planos de Continuidade Operacional e Planos de Recuperação de Desastres), em relação ao disposto no normativo supracitado, e, em consonância com a indagação realizada pelo CSJT, contida no item 2.2.8 do questionário aplicado, transcrita a seguir:

O programa de gestão da continuidade dos serviços essenciais de TI (Plano de Continuidade de TI) contém, no mínimo:
I - o objetivo;
II - as atividades críticas de negócio a serem contempladas no plano (contemplado PC 2.2.1);
III - os requisitos para ativação do plano, em especial, o tempo máximo aceitável de permanência da falha;
IV - o(s) responsável(is) pela ativação do plano, com seus respectivos dados de contato;
V - o(s) responsável(is) por aplicar as medidas de contingência definidas, tendo cada

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

servidor responsabilidades formalmente definidas e nominalmente atribuídas, incluindo seus respectivos dados de contato; e
VI - a definição:
a) das ações necessárias para operacionalização das medidas cuja implementação dependa da aquisição de recursos físicos e/ou humanos;
b) dos limites de decisão para os responsáveis pela aplicação das medidas de contingência perante situações inesperadas;
c) dos parâmetros para encerramento do plano e para a volta à normalidade;
d) dos responsáveis por essas ações, incluindo seus dados de contato;
e) da forma de monitoramento desse processo; e
f) de um roteiro de simulação de teste de funcionamento e da forma de sua aplicação.

Concluiu-se, com amparo no exame do normativo interno do TRT19ª, na inspeção física realizada *in loco* nos Planos de Continuidade Operacional e Recuperação de Desastres, e nas afirmações do auditado, extraídas do Questionário, Ata da Reunião, RDI n.º 06/2022, DOCS n.º 08, 10 e 14 do PROAD 2483/2022, que**:**

O programa de gestão de continuidade contém parcialmente os requisitos dispostos na referida norma, sendo que, não há previsão:

- ✓ **Das atividades críticas de negócio;**
  (item II do Art. 23 - IN GSI/PR 3/2021)

- ✓ **Da definição:**
  - **Das ações necessárias para operacionalização das medidas cuja implementação dependa da aquisição de recursos físicos e/ou humanos,**
  - **Dos limites de decisão para os responsáveis pela aplicação das medidas de contingência perante situações inesperadas**
  - **Dos parâmetros para encerramento do plano e para a volta à normalidade,**
  - **De um roteiro de simulação de teste de funcionamento e da forma de sua aplicação.**

  (item VI, a, b, c e f, respectivamente, do Art. 23 - IN GSI/PR 3/2021)

MANIFESTAÇÃO DO AUDITADO:
O processo de gestão de continuidade de serviços de TI será revisado para atender as normas mais recentes e para ajustar de acordo com o encaminhamento adotado pela Auditoria. Considerando a priorização e adequação de recursos da SETIC destinados a essa ação, a conclusão desse processo está prevista para dezembro de 2024.
ANÁLISE E CONCLUSÃO
A Secretaria de Auditoria ratifica o Achado. Dessa forma, a proposta de encaminhamento formulada subsiste.

OBJETO(S):	- ATO n.º 82/2019/GP/TRT19ª.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

	- Plano de Continuidade Operacional – PJE; - Plano de Continuidade Operacional – PROAD e; - Planos de Recuperação de Desastres.
CRITÉRIO(S):	- Instrução Normativa GSI/PR 3/2021, art. 23.
EVIDÊNCIA(S):	- DOC n.º 08 do PROAD 2483/2022 – Questionário; - DOC n.º 10 do PROAD 2483/2022 – Ata da Reunião e; - DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.
CAUSA(S):	- Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; - Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; - Ausência de atualização normativa pelo TRT19ª.
EFEITO(S)	- Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª e; - Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª.
PROPOSTA DE ENCAMINHAMENTO:	Recomenda-se: - Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: ✓ Atualização do ATO n.º 82/2019/GP/TRT19ª, para inclusão da menção relativa a especificação dos itens II e VI, a, b, c e f, do Art. 23 da IN GSI/PR n.º 3/2021. ✓ Revisão nos protocolos já existentes e inclusão nos novos, das atividades críticas a serem elaborados, das seguintes etapas: • Ações necessárias para operacionalização das medidas cuja implementação dependa da aquisição de recursos físicos e/ou humanos; • Limites de decisão para os responsáveis pela aplicação das medidas de contingência perante situações inesperadas; • Parâmetros para encerramento do plano e para a volta à normalidade; • Roteiro de simulação de teste de funcionamento e da forma de sua aplicação.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

ACHADO 02: Falhas na gestão de continuidade dos serviços essenciais de Tecnologia da Informação

SITUAÇÃO ENCONTRADA (A2.7):

No decurso dos trabalhos de auditoria, foi realizada observação acerca do atendimento, pelo TRT19ª, ao disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, em seu item 4.1, alínea "g", o qual menciona que:
4. Planejamento da Crise (pré-crise)
4.1 Para melhor lidar com uma crise cibernética, é necessário prévia e adequada preparação, sendo fundamental que os órgãos do Poder Judiciário estabeleçam um Programa de Gestão da Continuidade de Serviços que contemple as seguintes atividades:
g) realizar simulações e testes para validação dos planos e procedimentos.

Como também, quanto o atendimento ao disposto na Instrução Normativa GSI/PR n.º 3/2021, em seu artigo 23, parágrafo único, o qual menciona que:
Art. 23. O plano de continuidade de negócios em segurança da informação deverá conter, no mínimo:
Parágrafo único. O plano de continuidade de negócios deverá ser testado regularmente, com intuito de que seus resultados sejam documentados e possam garantir a sua efetividade em caso de necessidade de ativação.

Assim, ao analisar os processos existentes no TRT19ª (ATO n.º 82/2019/GP/TRT19ª, Planos de Continuidade Operacional e Planos de Recuperação de Desastres), em relação ao disposto no normativo supracitado, e, em consonância com a indagação realizada pelo CSJT, contida no item 2.2.9 do questionário aplicado, transcrita a seguir:
Foram realizadas simulações e testes para validação dos planos e procedimentos que integram o programa?

Concluiu-se, com amparo no exame do normativo interno do TRT19ª, na inspeção física realizada *in loco* nos Planos de Continuidade Operacional e Recuperação de Desastres, e nas afirmações do auditado, extraídas do Questionário, Ata da Reunião, RDI n.º 06/2022, DOCS n.º 08, 10 e 14 do PROAD 2483/2022, que**:**

Não foram realizadas simulações e testes para validação dos planos e processos que integram o programa de gestão de continuidade dos serviços de TI.

MANIFESTAÇÃO DO AUDITADO:

O processo de gestão de continuidade de serviços de TI será revisado para atender as normas mais recentes e para ajustar de acordo com o encaminhamento adotado pela Auditoria.
Considerando a priorização e adequação de recursos da SETIC destinados a essa ação, a conclusão desse processo está prevista para dezembro de 2024.

ANÁLISE E CONCLUSÃO

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

A Secretaria de Auditoria (SAUD) ratifica o Achado. Dessa forma, a proposta de encaminhamento formulada subsiste.	
OBJETO(S):	- ATO n.º 82/2019/GP/TRT19ª. - Plano de Continuidade Operacional – PJE; - Plano de Continuidade Operacional – PROAD e; - Planos de Recuperação de Desastres.
CRITÉRIO(S):	- Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea g; - Instrução Normativa GSI/PR n.º 3/2021, art. 23, parágrafo único.
EVIDÊNCIA(S):	- DOC n.º 08 do PROAD 2483/2022 – Questionário; - DOC n.º 10 do PROAD 2483/2022 – Ata da Reunião e; - DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.
CAUSA(S):	- Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; - Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; - Ausência de atualização normativa pelo TRT19ª.
EFEITO(S)	- Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª; - Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª e; - Risco do programa, processos e protocolos implantados não atenderem as demandas do TRT19ª.
PROPOSTA DE ENCAMINHAMENTO:	Recomenda-se: - Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: ✓ Atualização do ATO n.º 82/2019/GP/TRT19ª, para inclusão da etapa relativa a rotina de realização das simulações e testes para validação dos planos e processos que integram o programa de gestão de continuidade dos serviços de TI, conforme disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea g; e na Instrução Normativa GSI/PR 3/2021, art. 23, parágrafo único. ✓ Elaboração de manuais/protocolos, e/ou a construção do desenho do processo, contendo a aludida etapa, com a descrição das atividades, respectivos papeis e responsabilidades dos envolvidos, bem como os modelos

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

	de documentos e indicadores, conforme prevê o item 6.2 do ATO n.º 82/2019/GP/TRT19ª; como também, após a aprovação pela Presidência, posterior publicação no Portal de Governança de TI, **do que for cabível, observando os requisitos de segurança da informação quanto aos controles sigilosos**. - Estabelecimento da rotina de simulações e testes contínuos, na implantação e continuidade dos processos que integram o programa de gestão de continuidade dos serviços de TI.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

MINUTA DOS ACHADOS - TRT19ª

Tema	Achado	Descrição do achado	Situação encontrada	Objetos	Evidência	Critério	Possíveis Causas	Possíveis Efeitos	Encaminhamento
Gerenciamento de incidentes de segurança da informação	**A1**	Falhas no processo de gerenciamento de incidentes de segurança da informação	**A1.1** - Não há previsão, no processo de gerenciamento de incidentes de segurança da informação, de ações responsivas a serem colocadas em prática quando ficar evidente que um incidente não será mitigado rapidamente. **A1.2** - Não há previsão, no processo de gerenciamento de incidentes de segurança da informação, de estabelecimento de critérios para iniciar o gerenciamento de crise. **A1.3** - Não há evidente previsão, no processo de gerenciamento de incidentes de segurança da informação, da contemplação dos incidentes que podem ocorrer nos serviços em nuvem contratados pelo órgão, a exemplo da plataforma Gsuite. **A1.4** - Não há previsão, no processo, de etapa relativa à comunicação dos incidentes graves ao CPTRIC-PJ. **A1.5** - Não há previsão, no processo, da etapa relativa a elaboração de Relatório de Comunicação de Incidente de Segurança da Informação, contendo descrição e detalhamento da crise com plano de ação. **A1.6** - O processo de gerenciamento de incidentes de segurança da informação está parcialmente implantado, pois encontra-se em fase de atualização, bem como, a etapa de Avaliação não está sendo devidamente executada	• ATO n.º 103/2019/GP/TRT19ª • ATO n.º 82/2019/GP/TRT19ª.	• DOC n.º 08 do PROAD 2483/2022 – Questionário; • DOC n.º 10 do PROAD 2483/2022 - Ata da Reunião e; • DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.	• Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 1.1; • Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 2.2; • Instrução Normativa GSI/PR 5/2021, art. 16, inciso IV.; • Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 5.9; • Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 6.4; • Resolução CNJ 396/2021, art. 11, incisos I e III; art. 21, § 2º, inciso IV	• Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; • Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; • Ausência de atualização normativa pelo TRT19ª.	• Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª; • Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª e; • Imprevisibilidade para mediação do problema. • Possível não atendimento às regulamentações contratuais com o provedor. • Perda de colaboração com os órgãos superiores do Poder Judiciário. • Comprometimento na gestão dos incidentes, por ausência de mecanismos capazes de auxiliar na gestão do problema. • Comprometimento da gestão dos incidentes.	**Recomenda-se:** Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: • Atualização do ATO n.º 103/2019/GP/TRT19ª, para inclusão das etapas não previstas. • Elaboração de manuais/protocolos, e/ou a construção do desenho do processo, contendo as aludidas etapas, com a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos, bem como os modelos de documentos a serem utilizados nas etapas, conforme prevê o item 8.16 do ATO n.º 103/2019/GP/TRT19ª; como também, após a aprovação pela Presidência, posterior publicação no Portal de Governança de TI, *do que for cabível, observando os requisitos de segurança da informação quanto aos controles sigilosos.* • Análise acerca das questões contratuais com os provedores dos serviços em nuvem, em relação a falta da referida previsão nos processos do TRT19ª, e seu reflexo quanto ao risco de quebra contratual e/ou não atendimento dos serviços, devido a possíveis infrações contratuais. • Elaboração do modelo de Relatório de Comunicação de Incidentes de Segurança da Informação, a ser utilizado, contendo a descrição e o detalhamento da crise e o plano de ação a ser tomado, quando da ocorrência dos eventos. • Adoção de medidas necessárias para integração e amadurecimento da política de segurança da informação, tais como, realização de testes dos planos, estabelecimentos de controles, construção de relatórios por meio dos dados extraídos dos registros para melhor avaliação e analise dos incidentes, treinamento aos usuários do TRT19ª, melhor aproveitamento da ferramenta que registra os incidentes (Jira), com vistas a garantir a implantação integral do processo e sua efetividade.
Gestão da continuidade dos serviços de TI	**A2**	Falhas na gestão de continuidade dos serviços essenciais de TI	**A2.1** - Foram estabelecidos, os papéis e responsabilidades dos profissionais envolvidos no programa de gestão de continuidade de serviços essenciais de TI, incluindo o agente responsável pela gestão de continuidade dos serviços de TI no Órgão, somente nos Planos de Continuidade Operacional e Recuperação de Desastres relativos ao PJe e PROAD. Logo, concluiu-se que o atendimento da demanda é parcial. **A2.2** - Não há, no programa de gestão de continuidade de serviços de TI, a definição das atividades críticas de negócio a serem contempladas, em especial, quanto aos serviços relativos ao Portal SIGEP, Processo Administrativo e Google. **A2.3** - Há previsão, no programa de gestão de continuidade de serviços de TI, da identificação dos ativos de informação críticos, incluindo as pessoas, a infraestrutura e os recursos de tecnologia, somente nos Planos de Continuidade Operacional e Recuperação de Desastres relativos ao PJe e PROAD. Logo, concluiu-se que o atendimento da demanda é parcial. **A2.4** - Não há previsão, no programa de gestão de continuidade dos serviços de TI, de protocolos, processos, manuais para categorização dos incidentes e estabelecimento de procedimentos de resposta específicos (playbooks). **A2.5** - Não há previsão, no programa de gestão de continuidade dos serviços de TI, de planos de contingência que detalham o monitoramento, o acompanhamento e o tratamento dos riscos de maior criticidade, em razão de possíveis cenários de crise. **A2.6** - O programa de gestão de continuidade contém parcialmente os requisitos dispostos na referida norma, sendo que, não há previsão: - Das atividades críticas de negócio; (item II do Art. 23 - IN GSI/PR 3/2021) - Da definição: • Das ações necessárias para operacionalização das medidas cuja implementação dependa da aquisição de recursos físicos e/ou humanos, • Dos limites de decisão para os responsáveis pela aplicação das medidas de contingência perante situações inesperadas • Dos parâmetros para encerramento do plano e para a volta à normalidade, • De um roteiro de simulação de teste de funcionamento e da forma de sua aplicação. (item VI, a, b, c e f, respectivamente, do Art. 23 - IN GSI/PR 3/2021) **A2.7** - Não foram realizadas simulações e testes para validação dos planos e processos que integram o programa de gestão de continuidade dos serviços de TI.	• ATO n.º 82/2019/GP/TRT19ª; • ATO n.º 22/2022/GP/TRT19ª; • Plano de Continuidade Operacional – PJE; • Plano de Continuidade Operacional – PROAD e; • Planos de Recuperação de Desastres.	• DOC n.º 08 do PROAD 2483/2022 – Questionário; • DOC n.º 10 do PROAD 2483/2022 – Ata da Reunião; • DOC n.º 13 do PROAD 2483/2022 – Declaração e; • DOC n.º 14 do PROAD 2483/2022 – RDI n.º 06/2022.	• Instrução Normativa GSI/PR 3/2021, art. 25; • NBR ISO 27002, item 17.1.2 - Implementando a continuidade da segurança da informação, alínea a; • Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea b; • Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea c; • Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea 'e' e 'f'; • Instrução Normativa GSI/PR 3/2021, art. 23; • Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea g; • Instrução Normativa GSI/PR 3/2021, art. 23, parágrafo único	• Incipiência na implantação e manutenção dos processos e sistemas de gestão de segurança da informação; • Limitações de estrutura, quadro de pessoal, e alta demanda da área de TI no TRT19ª e; • Ausência de atualização normativa pelo TRT19ª.	• Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT19ª e; • Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT19ª. • Risco do programa, processos e protocolos implantados não atenderem as demandas do TRT19ª.	**Recomenda-se:** Atualização e aprimoramento dos processos, das normas internas do TRT19ª, com vistas a refletir as exigências normativas contemporâneas relativas à segurança da informação. Posto isto, sugere-se: • Atualização do ATO n.º 82/2019/GP/TRT19ª, para inclusão das etapas não previstas. • Elaboração dos protocolos, manuais e/ou processos: - Relativos as atividades criticas, que ainda não estão mapeados, com a inclusão da descrição das atividades, respectivos papeis e responsabilidades dos envolvidos e responsáveis pelo programa de gestão de continuidade de serviços essenciais de TI. - Relativos as atividades críticas, que ainda não estão mapeados, com a identificação dos ativos de informação críticos, incluindo as pessoas, a infraestrutura e os recursos de tecnologia. - Contendo a categorização dos incidentes e estabelecimento de procedimentos de resposta especificos. • Elaboração dos planos de contingência, com detalhamento do monitoramento, acompanhamento e tratamento dos riscos de maior criticidade, em razão de possíveis cenários de crise. • Revisão nos protocolos já existentes e inclusão nos novos, das atividades críticas a serem elaborados, das seguintes etapas: - Ações necessárias para operacionalização das medidas cuja implementação dependa da aquisição de recursos físicos e/ou humanos; - Limites de decisão para os responsáveis pela aplicação das medidas de contingência perante situações inesperadas; - Parâmetros para encerramento do plano e para a volta à normalidade; - Roteiro de simulação de teste de funcionamento e da forma de sua aplicação. • Estabelecimento da rotina de simulações e testes contínuos, na implantação e continuidade dos processos que integram o programa de gestão de continuidade dos serviços de TI. • Definição, junto à Alta Administração do TRT19ª, das atividades críticas de negócio a serem contempladas no programa de gestão de continuidade de serviços de TI.

7. CONSIDERAÇÕES EM FACE DA RESPOSTA DA UNIDADE AUDITADA

Inicialmente, esclarece-se que a auditoria desenvolvida por esta Secretaria de Auditoria seguiu o rito processual estabelecido no Anexo Único do Ato GP/TRT19ª nº 62/2021, o qual prevê a etapa de envio do Relatório de Fatos Apurados à unidade auditada para manifestações, esclarecimentos, elucidações de erros, elaboração de um Plano de Ação, dentre outras possibilidades, além da etapa de realização da Reunião Expositiva dos Fatos Apurados com a unidade auditada e a Diretoria Geral deste TRT19ª. Somente após a avaliação das respostas encaminhadas pela(s) unidade(s) auditada(s), é elaborado o Relatório Final de Auditoria e encaminhado à Presidência do Tribunal, para avaliação e determinação do cumprimento das recomendações acatadas.

Nesse contexto, após a SETIC tomar conhecimento dos levantamentos inseridos no Relatório Preliminar para Manifestações do Auditado (documento n.º 16), no qual constaram 2 (dois) macro Achados, desmembrados em 13 situações, foi realizada a Reunião Expositiva com os representantes daquela unidade e da Diretoria Geral, registrada em Ata de Reunião n.º 06/2022 (documento n.º 20). Em seguida, a unidade auditada apresentou suas manifestações por escrito (documento 18) e seu Plano de Ação (documento n.º 26).

Apesar dos esclarecimentos apresentados pela unidade auditada, todos os Achados foram mantidos, visando o cumprimento das recomendações firmadas, a fim de que se possa aperfeiçoar a qualidade e suficiência dos controles internos relativos a segurança da informação, instituídos pela SETIC.

Por fim, destaca-se que tais achados e consequentes recomendações serão objeto de monitoramento posterior, em momento oportuno, conforme os prazos estabelecidos no plano de ação.

8. RECOMENDAÇÕES

Quanto ao processo de gerenciamento de incidentes de segurança da informação:

8.1 Recomenda-se a atualização do ATO n.º 103/2019/GP/TRT19ª para inclusão da etapa relativa às ações responsivas a serem colocadas em prática, quando ficar evidente que um incidente não será mitigado rapidamente, conforme disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 1.1. **(A1.1)**

8.2 Recomenda-se a atualização do ATO n.º 103/2019/GP/TRT19ª para inclusão da etapa relativa à definição dos critérios para iniciar o gerenciamento de crise cibernética, conforme disposto na Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 2.2. **(A1.2)**

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

8.3 Recomenda-se a atualização do ATO n.º 103/2019/GP/TRT19ª para inclusão da etapa relativa à contemplação dos incidentes ocorridos nos serviços em nuvem contratados pelo órgão, conforme disposto na Instrução Normativa GSI/PR 5/2021, Art. 16, inciso IV. **(A1.3)**

8.4 Recomenda-se a atualização do ATO n.º 103/2019/GP/TRT19ª para inclusão de etapa relativa à comunicação dos incidentes graves ao CPTRIC-PJ, conforme disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 5.9. **(A1.4)**

8.5 Recomenda-se a atualização do ATO n.º 103/2019/GP/TRT19ª para inclusão da etapa relativa à elaboração de Relatório de Comunicação de Incidente de Segurança da Informação, contendo descrição e detalhamento da crise com plano de ação, conforme disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 6.4. **(A1.5)**

8.6 Recomenda-se a atualização do ATO n.º 103/2019/GP/TRT19ª para certificação do cumprimento das disposições previstas na Resolução CNJ 396/2021, em seu Art. 11, incisos I e III e Art. 21, § 2º, inciso IV. **(A1.6)**

8.7 Recomenda-se, adicionalmente a atualização do ATO n.º 103/2019/GP/TRT19ª, conforme previsão no item 8.16 deste regulamento, a elaboração de controles internos (manuais/protocolos/processos), contendo o detalhamento da execução das etapas do processo de gerenciamento de incidentes de segurança da informação, que ainda não estão mapeados, com a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos, bem como os modelos de documentos a serem utilizados nessas etapas, tais como a confecção do Relatório previsto na recomendação 8.1.5. **(A1.1; A1.2; A1.3; A1.4; A1.5; A1.6)**

8.8 Recomenda-se a adoção de medidas necessárias para integração e amadurecimento da política de segurança da informação, com vistas a garantir a implantação integral do processo e sua efetividade, tais quais: **(A1.6)**

8.8.1 Realização de testes dos planos relativos ao gerenciamento dos incidentes;

8.8.2 Melhor aproveitamento da ferramenta que registra os incidentes (Jira), no sentido de extrair dados para construção de indicadores, com finalidade de melhorar a análise dos incidentes; e

8.8.3 Treinamento aos usuários do TRT19ª no tocante aos protocolos a serem seguidos relativos à segurança da informação.

Quanto à gestão da continuidade dos serviços essenciais de tecnologia da informação:

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

8.9 Recomenda-se a atualização do ATO n.º 82/2019/GP/TRT19ª para inclusão da etapa relativa à definição dos papéis e responsabilidades dos profissionais envolvidos no programa de gestão de continuidade de serviços essenciais de TI, incluindo o agente responsável pela gestão de continuidade dos serviços de TI no Órgão, conforme disposto na Instrução Normativa GSI/PR n.º 3/2021, art. 25 e NBR ISO 27002, item 17.1.2. **(A2.1)**

8.10 Recomenda-se a atualização do ATO n.º 82/2019/GP/TRT19ª para inclusão da etapa relativa à definição das atividades críticas de negócio a serem contempladas no programa de gestão de continuidade de serviços de TI, conforme disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea b. **(A2.2)**

8.11 Recomenda-se a atualização do ATO n.º 82/2019/GP/TRT19ª para inclusão da etapa relativa à identificação dos ativos de informação críticos, incluindo as pessoas, a infraestrutura e os recursos de tecnologia, respeitando os requisitos de segurança da informação e as exigências dos normativos em vigor, conforme disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea c. **(A2.3)**

8.12 Recomenda-se a atualização do ATO n.º 82/2019/GP/TRT19ª para inclusão da etapa relativa à previsão de protocolos, processos, ou manuais para categorização dos incidentes e estabelecimento de procedimentos de resposta específicos (*playbooks*), conforme disposto na Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea 'e' e 'f'. **(A2.4)**

8.13 Recomenda-se a atualização do ATO n.º 82/2019/GP/TRT19ª para inclusão da etapa relativa aos planos de contingência que detalham o monitoramento, o acompanhamento e o tratamento dos riscos de maior criticidade, em razão de possíveis cenários de crise, conforme disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea 'e' e 'f'. **(A2.5)**

8.14 Recomenda-se a atualização do ATO n.º 82/2019/GP/TRT19ª para inclusão da etapa relativa à especificação dos itens II e VI, a, b, c e f, do Art. 23 da IN GSI/PR n.º 3/2021. **(A2.6)**

8.15 Recomenda-se a atualização do ATO n.º 82/2019/GP/TRT19ª para inclusão da etapa relativa à rotina de realização das simulações e testes para validação dos planos e processos que integram o programa de gestão de continuidade dos serviços de TI, conforme disposto na Portaria CNJ n.º 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea g; e na Instrução Normativa GSI/PR 3/2021, art. 23, parágrafo único. **(A2.7)**

8.16 Recomenda-se, adicionalmente a atualização do ATO n.º 82/2019/GP/TRT19ª, conforme previsão no item 6.2 deste regulamento, a elaboração de controles internos (manuais/protocolos/processos) contendo o detalhamento da execução das etapas do programa de gestão de continuidade de serviços essenciais de TI, incluindo a construção dos protocolos de

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

gerenciamento de crises cibernéticas, com a descrição das atividades, respectivos papeis e responsabilidades dos envolvidos, bem como os modelos de documentos e indicadores a serem utilizados. **(A2.1; A2.2; A2.3; A2.4; A2.5; A2.6; A2.7)**

8.17 Recomenda-se a inclusão nos protocolos já existentes, como também nos novos que surgirem, das seguintes etapas: **(A2.6)**

8.17.1 Ações necessárias para operacionalização das medidas cuja implementação dependa da aquisição de recursos físicos e/ou humanos;

8.17.2 Limites de decisão para os responsáveis pela aplicação das medidas de contingência perante situações inesperadas;

8.17.3 Parâmetros para encerramento do plano e para a volta à normalidade;

8.17.4 Roteiro de simulação de teste de funcionamento e da forma de sua aplicação.

8.18 Recomenda-se definição, junto à Alta Administração do TRT19ª, das atividades críticas de negócio a serem contempladas no programa de gestão de continuidade de serviços de TI. **(A2.2)**

8.19 Recomenda-se a implantação da rotina de simulações e testes contínuos, na implantação e continuidade dos processos que integram o programa de gestão de continuidade dos serviços essenciais de Tecnologia da Informação. **(A2.7)**

9. CONCLUSÃO

A presente auditoria visou avaliar a Gestão da Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 19ª, especificamente, quanto aos controles internos relativos ao gerenciamento de incidentes cibernéticos e a gestão de continuidade dos serviços essenciais de Tecnologia da Informação.

Os resultados da presente Auditoria demonstram a necessidade deste Tribunal atualizar seus regulamentos internos, com vistas a refletir as exigências normativas contemporâneas, que primam pela adoção de boas práticas na gestão da segurança da informação; como também, corroboram para a necessidade de estabelecimento e aprimoramento de controles internos específicos, principalmente quanto aos serviços críticos, tais quais: PJe, PROAD, SIGEP, Portal Internet, Google Suíte, para mitigar os riscos inerentes a instabilidades cibernéticas, com foco na prevenção e na qualidade da administração das ocorrências que possam vir a surgir, com fins de possibilitar uma resposta rápida, segura e eficiente, minimizando prejuízos aos serviços prestados por este Tribunal.

A auditoria também evidenciou a ausência de uma rotina de testes e simulações dos protocolos e a subutilização da ferramenta que registra os incidentes cibernéticos (Jira), uma vez que este controle poderia ser melhor aproveitado na extração de dados para construção de indicadores e relatórios, com fins de promover uma melhor avaliação e analise dos incidentes ocorridos.

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br

Ademais, restou evidenciada a necessidade de elaboração dos protocolos de gerenciamento de crises cibernéticas para garantir a continuidade dos serviços essenciais de tecnologia da informação.

Assim, as constatações apontadas nos Achados de Auditoria respaldam as aludidas conclusões, e as recomendações propostas objetivam o aprimoramento do gerenciamento de incidentes de segurança da informação e da gestão de continuidade dos serviços essenciais de Tecnologia da Informação, quanto ao cumprimento das diretrizes normativas adotadas no âmbito da Justiça do Trabalho, que buscam a adoção de boas práticas em segurança da informação.

Maceió, 04 de novembro de 2022.

Fábia Fernanda Curvelo Marques
Líder da Equipe de Auditoria

Bráulio Clementino M. M. Soares
Supervisor da Equipe de Auditoria

10. PROPOSTA DE ENCAMINHAMENTO

Ante o exposto, considerando o papel da auditoria interna preconizado pelo artigo 74 da Constituição Federal, e com o intuito de auxiliar a Administração deste Regional no controle, na eficiência e legalidade dos procedimentos da gestão, submete-se o presente Relatório de Auditoria ao Exmo. Senhor Desembargador Presidente do Tribunal Regional do Trabalho da 19ª Região, a fim de que possa deliberar acerca dos resultados da presente Auditoria, realizada com o intuito de avaliar a Gestão da Segurança da Informação no âmbito da Justiça do Trabalho.

Maceió, 04 de novembro de 2022.

BRÁULIO CLEMENTINO M. M. SOARES
Secretário de Auditoria

SECRETARIA DE AUDITORIA
Avenida da Paz, 2076 – 7º andar – Centro.
Maceió/AL – CEP: 57020-440
Telefone: (82) 2121.8267 / 8297 / 8224
Email audtoria@trt19.jus.br