MINISTÉRIO PÚBLICO DA UNIÃO

AUDITORIA INTERNA

RELATÓRIO PRELIMINAR DE AUDITORIA

BRASÍLIA

2018

Negócio

Controle interno da gestão dos recursos públicos destinados ao Ministério Público da União.

Missão

Fiscalizar a aplicação dos recursos públicos e contribuir para o aperfeiçoamento da gestão, em benefício da sociedade.

Visão

Ser reconhecido como Órgão de excelência no controle interno e que contribui efetivamente para o aperfeiçoamento da gestão das Unidades do Ministério Público da União.

Valores

Independência, ética, justiça, efetividade, respeito e profissionalismo.

MINISTÉRIO PÚBLICO DA UNIÃO

AUDITORIA INTERNA

SECRETARIA DE AUDITORIA

RELATÓRIO PRELIMINAR DE AUDITORIA N° 18/2018

BRASÍLIA

2018

Auditor-Chefe
Sebastião Gonçalves de Amorim

Secretaria de Auditoria
Eder Sardinha e Silva

Coordenadoria de Auditoria de Acompanhamento de Gestão
Josi Brandão Silva

Divisão de Planejamento de Auditoria e Pesquisa
Fernando de Andrade Moreira

Equipe de Auditoria
Coordenador de Equipe
Kamilla Turnes Lemos

Auditores
Ronaldo da Silva Pereira
Gustavo Pereira de Cuba

MINISTÉRIO PÚBLICO DA UNIÃO

RELATÓRIO PRELIMINAR DE AUDITORIA N° 18/2018	
Unidade auditada:	MINISTÉRIO PÚBLICO DO TRABALHO
Responsável:	Leomar Daroncho
Cargo:	Diretor-Geral
Período de realização da Auditoria:	Agosto a Outubro de 2018
Auditores:	1) Kamilla Turnes Lemos; 2) Ronaldo da Silva Pereira; e 3) Gustavo Pereira de Cuba

SUMÁRIO

1. INTRODUÇÃO

Em conformidade com o Plano Anual de Atividades de Auditoria Interna – PAINT 2018, no que se refere a área de Tecnologia da Informação, foi realizada auditoria em governança de TI baseada nas respostas da Unidade ao questionário do iGov, índice de Governança medido pelo Tribunal de Contas da União.

O foco principal do trabalho foi, a partir de um melhor entendimento de como funciona a governança em TI da unidade, auditar as respostas dadas aos levantamentos do iGov realizados em 2017 e 2018, bem como, o Plano Diretor de Tecnologia da Informação atualmente vigente na Procuradoria Geral do Trabalho (PDTI 2016-2018).

As etapas da auditoria compreenderam: (a) planejamento dos trabalhos; b) análise das respostas do iGov TI; (c) análise evolutiva da governança, considerando as respostas do iGov TI de 2017 e 2018; (d) análise do PDTI 2016-2018; (e) elaboração da Matriz de Procedimentos; (f) coleta e análise de informações; (g) reunião para esclarecimento de dúvidas; (h) elaboração do Relatório Preliminar de Auditoria.

Com base nos resultados das etapas acima mencionadas, foi realizado o diagnóstico de governança da unidade e os achados de auditoria foram detalhados neste relatório, a qual os gestores avaliarão a conveniência e oportunidade de aperfeiçoamento da gestão e apresentarão proposta inicial de plano de ação formalizada.

2. METODOLOGIA

Foi realizado coleta de informações e dados relativos à estrutura da Diretoria de Tecnologia da Informação, aos normativos vigentes (portarias e resoluções), ao PETI e PDTI vigentes e às respostas dos questionários iGov/TCU 2017 e 2018.

A partir das informações coletadas, procedeu-se à análise qualitativa dos documentos e entrevista com gestores para a realização do diagnóstico de governança de TI na PGT. Os resultados da auditoria encontram-se detalhadas na seção 3.4 deste relatório.

3. GOVERNANÇA DE TI

3.1. SOBRE A GOVERNANÇA DE TI

Segundo as Normas Internacionais para a Prática Profissional de Auditoria Interna (IPPF), a Governança de TI "consiste da liderança, estruturas organizacionais e processos que asseguram que a tecnologia da informação corporativa dá suporte às estratégias e aos objetivos da organização".

Ainda, conforme COBIT 5, ISACA, ela integra e institucionaliza boas práticas de forma a garantir que a TI forneça suporte aos objetivos da organização e potencializa o uso das informações de forma a maximizar benefícios e gerar vantagens competitivas.

Segundo o *IT Governance Institute* (ITGI), o escopo de governança de TI se encontra nas seguintes áreas de foco:

- Alinhamento estratégico da TI com o negócio da organização;
- Gerenciamento de riscos, envolvendo o apetite a riscos, conformidade, transparência, impacto de mudanças, entre outros;
- Gerenciamento de recursos, de forma a otimizar investimentos e recursos disponíveis de TI;
- Mensuração de desempenho, que consiste em monitorar recursos, implementação de estratégias, projetos, de forma a subsidiar ações futuras; e
- Entrega de valor, na qual os produtos de TI gerem valor à organização e auxiliem no alcance das estratégias estabelecidas.

3.2. OBJETIVOS DA AUDITORIA

O trabalho de Auditoria se concentrou nos seguintes objetivos:

- Conhecer a estrutura e organização da unidade de TI, considerando as respostas do questionário de iGov TI;
- Avaliar a evolução em TI na unidade, com base no comparativo de respostas dos questionários de 2017 e 2018;

- Averiguar se as respostas do questionário de 2018 condiz com a realidade da unidade;
- Averiguar se os planos de ação de 2017, considerando os prazos estabelecidos pelo MPT;
- Avaliar o alinhamento estratégico entre Governança, Segurança da Informação e objetivos organizacionais do MPT; e
- Avaliar o desempenho da governança por meio de indicadores de medição, monitoramento e reporte que garanta os objetivos;
- Avaliar os resultados obtidos com o ciclo PDTI 2016-2018, em comparação com o planejado.

3.3. ABRAGÊNCIA DA AUDITORIA

Considerando as especificidades de Auditoria de TI, bem como a expedição de relatórios anteriores estarem restritos a aspectos legais de contratação de soluções de tecnologia, optou-se por diagnosticar como se encontra a atual estrutura de governança de TI da unidade. Para realizar o diagnóstico a equipe se orientou pelas temáticas recentemente questionadas pelo TCU.

Foi elaborada análise prévia do das respostas do iGov 2017 e 2018, que consistiu em verificar como a unidade se avalia quanto à governança, o quanto ela evoluiu de um ano para outro e se as respostas e comprovações fornecidas ao TCU eram suficientes à equipe ou se necessitaria uma verificação mais aprofundada.

A análise do PDTI 2016/2018 consistiu em verificar como a unidade acompanha a execução das metas estabelecidas para o ciclo, considerando que o PDTI já está em fase final de vigência. Verificou-se, também, se a unidade procurou desenvolver processos relacionados aos temas presentes nos questionamentos do iGov e, daqueles que haviam metas previstas, qual foi o grau de execução.

Dos resultados obtidos, foi elaborada a Matriz de Procedimentos, de forma a orientar quais informações adicionais seriam necessárias coletar, bem como os pontos para esclarecimento de dúvidas que eventualmente surgiram.

O levantamento posterior de informações envolveu, além de consultas a documentos acima mencionados, reunião com gestores responsáveis pela Diretoria de Tecnologia da Informação, de forma a sanar as dúvidas persistentes.

As temáticas de governança abordadas foram as seguintes: (a) processo de planejamento e PDTI; (b) gestão de catálogo de serviços; (c) gestão de mudanças; (d) gestão de configuração e ativos de TI; (e) gestão de incidentes; (f) acordos de níveis de serviço; (g) gestão de riscos; (h) gestão de continuidade; (i) segurança da informação; (j) gestão de ativos de informação; e (k) gestão de softwares.

3.4. DIAGNÓSTICO DA UNIDADE

3.4.1. INDICE DE GOVERNANÇA – iGov TI

O índice de governança é o resultado de um levantamento realizado anualmente pelo Tribunal de Contas da União, de formar a mensurar a situação de órgãos e entidades integrantes da Administração Pública Federal relativa a governança pública, gestão de tecnologia da informação (TI), contratações, pessoas e resultados.

Em relação à TI nos órgãos e entidades da APF, o TCU, em seu Acórdão nº 518/2018 – Plenário, chegou à conclusão que, de modo geral, apesar da evolução considerável desde o primeiro levantamento (Acórdão 1603/2008 - Plenário), "a situação de governança e gestão de TI na APF está longe de ser aceitável, tendo em vista as várias deficiências detectadas no levantamento integrado".

Quanto à Procuradoria Geral do Trabalho, foi possível constatar que, apesar de haver ainda diversos pontos possíveis de melhoria, os gestores de TI envidam esforços para que haja contínua evolução no nível de governança. Ao se comparar a realidade da Diretoria e as respostas dadas ao iGov, percebe-se que, em geral, o nível de governança e gestão de TI no caso concreto condiz com o que foi reportado no iGov.

3.4.1.1. ANÁLISE EVOLUTIVA – 2017/2018

As respostas fornecidas pela unidade encontram-se no quadro a seguir:

	2017	2018	Evolução
Planejamento de TI			
4211. A organização executa processo de planejamento de tecnologia da informação	Adota em maior parte ou totalmente	Adota em maior parte ou totalmente	
Visando explicitar melhor o grau de adoção do controle, marque uma ou mais opções que majoritariamente caracterizam sua organização	**a)** as áreas demandantes de soluções de TI participam do processo de planejamento de tecnologia da informação	**a)** as áreas demandantes de soluções de TI participam do processo de planejamento de tecnologia da informação **b)** o processo de planejamento de tecnologia da informação está formalizado na organização	
4212. A organização possui plano de tecnologia da informação vigente	Adota	Adota	
Visando explicitar melhor o grau de adoção do controle, marque uma ou mais opções que majoritariamente caracterizam sua organização	**a)** o plano de tecnologia da informação vigente foi aprovado pelo dirigente máximo da organização **c)** o plano de tecnologia da informação vigente fundamenta a proposta orçamentária da área	**a)** o plano de tecnologia da informação vigente foi aprovado pelo dirigente máximo da organização **c)** o plano de tecnologia da informação vigente fundamenta a proposta orçamentária da área	
Gestão de serviços de tecnologia da informação			
4221. A organização executa processo de gestão do catálogo de serviços	Adota em maior parte ou totalmente	Adota em maior parte ou totalmente	
Visando explicitar melhor o grau de adoção do controle, marque uma ou mais opções que majoritariamente caracterizam sua organização	**a)** o catálogo de serviços de tecnologia da informação está atualizado e está disponível aos seus usuários	**a)** o catálogo de serviços de tecnologia da informação está atualizado e está disponível aos seus usuários	
4222. A organização executa processo de gestão de mudanças	Não adota	Adota em menor parte	
4223. A organização executa processo de gestão de configuração e ativos (de serviços de tecnologia da informação)	Adota em menor parte	Adota em menor parte	
4224. A organização executa processo de gestão de incidentes	Adota parcialmente	Adota parcialmente	
4231. A área de gestão de tecnologia da informação acorda formalmente os níveis de serviço com as demais áreas de negócio internas à organização (Acordo de Nível de Serviço - ANS)	Há decisão formal ou plano aprovado para adotá-lo	Não adota	

	2017	2018	Evolução
4232. Os ANS incluem o grau de satisfação dos usuários como indicador de nível de serviço	Não adota	Não adota	
4233. A área de gestão de tecnologia da informação comunica às áreas de negócio o resultado do monitoramento em relação ao alcance dos níveis de serviço definidos com as referidas áreas	Não adota	Não adota	
4241. A organização gere os riscos de TI dos processos de negócio	Há decisão formal ou plano aprovado para adotá-lo	Há decisão formal ou plano aprovado para adotá-lo	
4242. A organização executa processo de gestão da continuidade dos serviços de tecnologia da informação	Há decisão formal ou plano aprovado para adotá-lo	Há decisão formal ou plano aprovado para adotá-lo	
4251. A organização dispõe de uma política de segurança da informação	Adota	Adota	
Visando explicitar melhor o grau de adoção do controle, marque uma ou mais opções que majoritariamente caracterizam sua organização	**a)** a política contempla orientações sobre gestão de riscos de segurança da informação **b)** a política abrange diretrizes para conscientização, treinamento e educação em segurança da informação	**a)** a política contempla orientações sobre gestão de riscos de segurança da informação **b)** a política abrange diretrizes para conscientização, treinamento e educação em segurança da informação	
4252. A organização dispõe de comitê de segurança da informação	Há decisão formal ou plano aprovado para adotá-lo	Adota	
Visando explicitar melhor o grau de adoção do controle, marque uma ou mais opções que majoritariamente caracterizam sua organização	(não marcou nenhuma)	a) o comitê de segurança da informação realiza as atividades previstas em seu ato constitutivo b) o comitê é responsável por formular diretrizes para a segurança da informação c) o comitê é responsável por propor a elaboração e a revisão de normas e de procedimentos inerentes à segurança da informação d) o comitê é composto por representantes de áreas relevantes da organização	
4253. A organização possui gestor de segurança da informação	Não adota	Não adota	
4254. A organização dispõe de política de controle de acesso à informação e aos recursos e serviços de tecnologia da informação	Há decisão formal ou plano aprovado para adotá-lo	Há decisão formal ou plano aprovado para adotá-lo	
4261. A organização executa processo de gestão de ativos associados à informação e ao processamento da informação	Não adota	Não adota	

	2017	2018	Evolução
4262. A organização executa processo para classificação e tratamento de informações	Não adota	Não adota	
4263. A organização executa processo de gestão de incidentes de segurança da informação	Não adota	Adota em menor parte	
4264. A organização realiza ações de conscientização, educação e treinamento em segurança da informação para seus colaboradores	Há decisão formal ou plano aprovado para adotá-lo	Há decisão formal ou plano aprovado para adotá-lo	
4271. A organização executa um processo de software	Há decisão formal ou plano aprovado para adotá-lo	Adota em maior parte ou totalmente	
Visando explicitar melhor o grau de adoção do controle, marque uma ou mais opções que majoritariamente caracterizam sua organização	(não marcou nenhuma)	**b)** a organização possui pessoal próprio capacitado para gerir o processo de software	
4281. A organização executa processo de gestão de projetos de tecnologia da informação	Adota parcialmente	Adota parcialmente	
Visando explicitar melhor o grau de adoção do controle, marque uma ou mais opções que majoritariamente caracterizam sua organização	**a)** a organização possui portfólio de projetos de tecnologia da informação	**a)** a organização possui portfólio de projetos de tecnologia da informação	

Legenda:

 Não houve alteração

 A unidade aperfeiçoou

 Houve retração

Considerando-se apenas as respostas dada pela unidade, observa-se que houve pouco aperfeiçoamento da governança de TI. Dos 21 questionamentos, apenas em quatro houve progresso. Nos 16 itens em que não houve alteração, em quatro a unidade afirma que adota totalmente ou em maior parte (nível ideal), a saber: processo de planejamento, PDTI formalizado, processo de gestão de catálogo de serviços e política de segurança da informação.

Nos quatro itens em que houve melhoria, em dois, conforme resposta, chegou-se ao nível ideal: existência do comitê de segurança da informação e execução de processo de software. Para os demais, apesar da evolução, todas as práticas ainda não são totalmente adotadas pela unidade.

O único item no qual houve retração foi o que se refere à adoção de acordos formais de níveis de serviços com as demais áreas da unidade, a PGT em 2017 afirmou que havia decisão formal/plano aprovado para adoção, porém em 2018 respondeu que não adota. No sistema Atena, os SLAs estão em formato padrão, ou seja, serviços muito complexos demandariam o mesmo tempo que serviços muito simples configurando que os acordos não teriam sido estabelecidos de forma coerente com a realidade.

Quanto aos processos e políticas que ainda não são totalmente executados (a saber: gestão de catálogo de serviços, gestão de mudanças, gestão de configuração e ativos de TI, gestão de incidentes, gestão de riscos, gestão de continuidade de serviços, segurança da informação, gestão de ativos associados à informação e gestão de softwares), percebe-se que, apesar de não haver processos estruturados, a unidade executa algumas ações e há planejamento em casos específicos que demandam mais tempo e recursos (exemplo: mudança de sistemas).

O detalhamento da situação real encontrada, separada por tópicos, está descrita na seção a seguir.

3.4.1.2. COMPARATIVO: RESPOSTAS iGov X REALIDADE DA UNIDADE

3.4.1.2.1. PROCESSO DE PLANEJAMENTO

Conforme resposta ao iGov, foi possível averiguar que a unidade realmente executa processo de planejamento e o resultado se materializa nos Planos Estratégicos e Planos Diretores de Tecnologia da Informação. Além disso, foram realizadas revisões periódicas do planejamento nas reuniões do Comitê Estratégico de TI (CETI), conforme atas das 19ª, 20ª e 22ª Reuniões de Avaliações Estratégicas. Os gestores acompanham a execução de ações e projetos, na qual os resultados alcançados são utilizados como insumo para as revisões e consequente priorização de ações para o período subsequente (que pode ser semestral ou anual). O acompanhamento das ações é realizado pelo JIRA (software de supervisão de projetos), que possui relação direta com o PDTI. Por fim, em entrevista com gestores, verificou-se que o processo de elaboração do novo PDTI encontra-se em fase inicial de execução e os resultados do PDTI 2016-2018 serão base para as novas estratégias e ações.

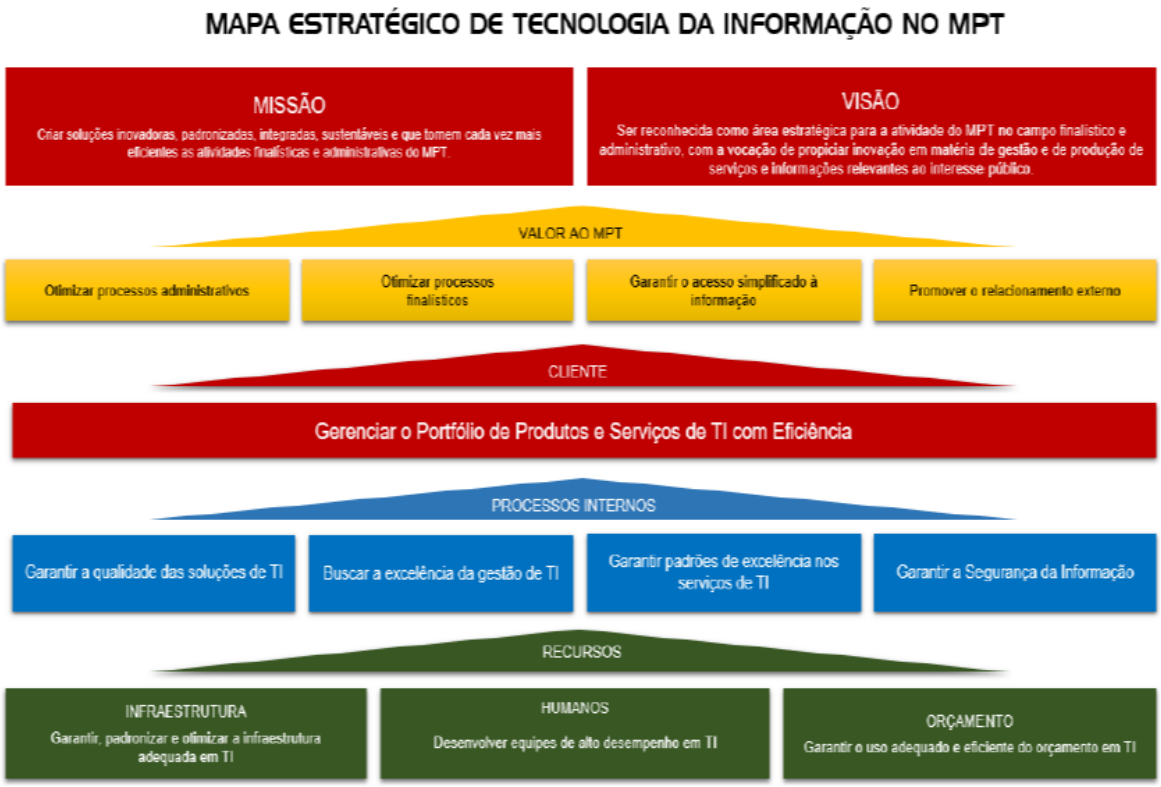
A análise detalhada do Plano Diretor vigente encontra-se a seguir.

3.4.1.2.1.1. PDTI 2016-2018

O Plano Diretor de Tecnologia da Informação em análise, com vigência entre 2º semestre de 2016 a 2º semestre de 2018, é o instrumento de gestão da área de TI do Ministério Público do Trabalho e possui abrangência nacional.

A metodologia adotada teve como referência o Modelo de Referência Guia Prático de Elaboração de PDTI v.2.0, proposto pelo Sistema de Administração de Recursos de Tecnologia de Informação (SISP) -STI/MPOG. Foram utilizados conceitos do *Balanced Scorecard* (BSC), COBIT, Analise SWOT e matriz GUT (gravidade, urgência e tendência).

O mapa estratégico, norteador das metas e ações estabelecidas, encontra-se na figura a seguir:



Fonte: PDTI 2016/2018 - MPT

No PDTI há também a avaliação do ambiente interno e externo, por meio da Matriz SWOT, na qual foram levantados seus pontos fortes e fracos, bem como as ameaças e oportunidades. A matriz está representada na tabela abaixo:

AMBIENTE INTERNO	
Forças (S)	
S1	Equipe altamente comprometida.
S2	Hardware de boa qualidade e atualizado.
S3	Planejamento Estratégico instituído.
S4	Processo de Software instituído.
S5	Competências da área de TI mapeadas.
S6	Apoio do CETI.
S7	Redundância para garantir a disponibilidade do acesso à Internet.
S8	Implantação dos escritórios de projetos.
S9	Implantação do Service Desk nacional.
S10	Implantação das Política de Segurança de TI.
S11	Implantação do escritório de Governança e Conformidade.
Fraquezas (W)	
W1	Quantitativo de pessoal de TI com habilidades específicas inferior a demanda.
W2	Pressão no trabalho inerente à atividade.
W3	Falta de definições de processos e controles de TI.
W4	Equipe com pouco conhecimento em governança de TI.
W5	Estrutura organizacional da TI não adequada às atribuições.
W6	Desmotivação e resistência dos servidores de TI provenientes das incertezas quanto a possíveis impactos negativos das mudanças organizacionais suscitadas.
W7	Baixa maturidade em governança de TI e em governança corporativa.
W8	Indefinição de padrões de arquitetura de Informação.
W9	Cultura de gestão de projetos de TI é muito recente e ainda não possui a desejada maturidade.
W10	Demora e inadequação de resposta do help-desk aos incidentes ou requisições, sobretudo em relação a alguns produtos e serviços.
W11	Necessidade de aprimoramento da usabilidade de produtos e serviços, de forma a mitigar a necessidade de capacitação dos usuários, que também precisa ser atendida.
W12	Não implementação de planos de segurança, risco e continuidade.

AMBIENTE EXTERNO	
Oportunidades (O)	
O1	Aprovação do novo plano de carreira.
O2	DataCenter e co-location externos.
O3	Intensificação do processo eletrônico do MPT.
O4	Nomeação de novos servidores.
O5	Queda na cotação do Dólar.
O6	Compartilhamento de recursos com outros ramos do MPU.
O7	Parcerias com outros órgãos da administração pública.
O8	Retomada do crescimento econômico do país e da estabilidade.
O9	Disponibilidade de soluções e ferramentas de mercado e Software público.
O10	Fortalecimento da TI como área estratégica.
Ameaças (T)	
T1	Restrições orçamentárias.
T2	Dificuldade de ampliação do quadro de pessoal de TI.
T3	Rotatividade dos servidores mais capacitados, devido a melhores salários oferecidos em outras carreiras públicas ou privadas.
T4	Dependência de serviços prestados por empresas de telecomunicações para o bom andamento da TI.
T5	Contingenciamento orçamentário dos gastos.
T6	Movimento sindical - períodos de greve podem dificultar a execução das atividades.
T7	Alta na cotação do dólar.
T8	Falência de fornecedores em função da instabilidade econômica.
T9	Falta de qualidade ou inexistência de fornecedores para prestação de serviços de TI em determinadas regiões do país. Ex.: locação de impressoras.
T10	Descontinuidade causada por mudanças de gestão.
T11	Incompatibilidade de prazos estabelecidos com a complexidade das demandas.
T12	Resistência à mudança dos Profissionais de TI.
T13	Aumento da imagem negativa da TI do MPT.
T14	Gestão inadequada da infraestrutura e dos serviços de TI.

Fonte: PDTI 2016/2018 - MPT

O Inventário de Necessidades (constante nas páginas 31 a 50 do PDTI), que define o que é necessário para o alcance dos objetivos organizacionais, foi alinhado aos objetivos estratégicos de TI (PETI 2016-2020) e a priorização ocorreu por meio da utilização da Matriz GUT (páginas 51 a 67 do PDTI).

As 206 necessidades estão agrupadas nos seguintes itens:

- Otimização da estrutura organizacional e orquestração da TI do MPT;
- Aprimoramento da governança de TI do MPT;
- Aprimoramento da gestão de projetos e a organização de portfólios;
- Aprimoramento da transparência e da comunicação interna e externa;
- Aprimoramento da gestão de contratos de TI;
- Implantação do plano de desenvolvimento de competências;
- Aprimoramento dos serviços públicos de TI prestados ao cidadão;
- Implantação de service desk nacional;
- Ampliação da padronização do funcionamento de recursos;
- Garantia da segurança da informação;
- Implantação da gestão de continuidade de negócio do MPT;
- Aprimoramento da gestão de riscos;
- Aprimoramento dos processos e dos padrões de desenvolvimento de soluções;
- Desenvolvimento de soluções;
- Refatoração e aprimoramento de soluções;
- Otimização e melhorias da infraestrutura;
- Acompanhamento da definição de padrões taxonômicos e de fluxo das atividades fim e meio consoantes definições do CNJ e do CNMP; e
- Aprimoramento do parque tecnológico;

A partir do levantamento de necessidades priorizadas e estratégias gerais de TI, foram definidos os planos de metas e de ações, que estão descritas no quadro a seguir. Os indicadores, recursos humanos e financeiros, prazos, área responsável e escopo estão detalhados no documento original, bem como o plano de gestão de pessoas e plano de riscos para o alcance dos objetivos propostos.

PLANO DE METAS E AÇÕES - PDTI 2016/2018 - MPT		
META 1	A1.1	Buscar garantir que a estrutura de TI do MPT e respectivas chefias sejam adequadas e compatíveis às necessidades institucionais e estratégicas do órgão

Estrutura Organizacional e Orquestração da TI do MPT	A1.2	Realizar avaliações periódicas para acompanhar a evolução da estratégia de TI do MPT, inclusive seus reflexos junto aos órgãos de controle
	A1.3	Efetivar dispositivos legais resultantes da Lei 13.316/2016
	A1.4	Implantar metodologia de avaliação de desempenho específica para TI
	A1.5	Acompanhar a satisfação e qualidade de vida no trabalho das equipes de TI do MPT
	A1.6	Acompanhar o atendimento aos níveis de serviços definidos no Catálogo de Serviços
	A1.7	Manter catálogo nacional de soluções de TI do MPT
	A1.8	Implementar plano de comunicação interna entre a comunidade de profissionais de TI do MPT
	A1.9	Formalizar e implantar o Plano Nacional de Estágio em TI
META 2 Governança de TI do MPT	A2.1	Instituir o Subcomitê de Governança em Tecnologia da Informação - SGTI
	A2.2	Promover a instituição de Subcomitês Diretivos de Tecnologia da Informação nas unidades regionais
	A2.3	Promover, acompanhar e monitorar, por meio dos SDTIs, a criação, implantação e execução de PDTI regionais
	A2.4	Formalizar e implantar processo de gestão estratégica de TI no MPT
	A2.5	Homologar e implantar solução para acompanhamento da estratégia de TI (indicadores)
META 3 Gestão de Projetos e Organização de Portfólios	A3.1	Formalizar e implantar processo de gestão do portfólio de projetos de TI do MPT
	A3.2	Universalizar o uso da metodologia SCRUM para projetos de TI no MPT
META 4 Transparência e Comunicação interna e externa	A4.1	Formalizar e implantar plano de comunicação interna e externa para promover a utilização correta e segura de recursos e serviços de TI do MPT
	A4.2	Formalizar e implantar plano de comunicação interna sobre a TI do MPT e seu papel na atuação institucional
	A4.3	Preparar e publicar *datasets* para divulgação de dados abertos à sociedade
META 5 Gestão de orçamentos, aquisições e contratos de TI	A5.1	Formalizar e implantar procedimentos para proposição, aprovação e realização de contratações de TI no âmbito do MPT
	A5.2	Formalizar e implantar procedimentos para gestão de contratos de TI no âmbito do MPT
	A5.3	Implantar catálogo nacional de aquisições, atas e contratos de TI do MPT
	A5.4	Formalizar e implantar procedimentos para gestão eficiente do Orçamento de TI do MPT
META 6 Plano de desenvolvimento de competências	A6.1	Formalizar e implantar Plano Nacional de Competências de TI do MPT
	A6.2	Implementar agenda continuada de transferência de conhecimento entre as equipes técnicas do MPT
META 7 Serviços públicos de TI prestados ao cidadão	A7.1	Formalizar e implantar procedimentos continuados para a otimização dos serviços públicos eletrônicos prestados pelo MPT ao cidadão
	A7.2	Formalizar e implantar procedimentos continuados para o estabelecimento e acompanhamento de níveis de serviço e satisfação por parte do cidadão perante serviços públicos eletrônicos prestados pelo MPT
META 8 Servic Desk Nacional	A8.1	Formalizar e implantar Service Desk unificado em âmbito nacional
	A8.2	Formalizar e implantar procedimentos continuados para a definição de uma Base de Conhecimentos, com objetivo de promover o autoatendimento

	A8.3	Formalizar e implantar procedimentos continuados para o estabelecimento e manutenção do catálogo de serviços de TI do MPT
	A8.4	Aprimorar as rotinas de atendimento ao usuário de modo a integrar gerenciamento de problemas no Service Desk do MPT
	A8.5	Aprimorar as rotinas de atendimento ao usuário de modo a integrar gestão de Ativos de TI ao Service Desk do MPT
META 9 Infraestrutura Tecnológica	A9.1	Homologar e implantar serviço de streaming para publicar videoconferências e reuniões de órgãos superiores
	A9.2	Padronizar, em âmbito nacional, mecanismos unificados de autenticação em recursos e serviços de TI
	A9.3	Definir, implantar e manter Grupos Temáticos Nacionais para suporte à sustentação das tecnologias adotadas pelo MPT
	A9.4	Implantar gerência nacional de configuração para equipamentos Desktop no MPT
	A9.5	Formalizar e implantar procedimentos continuados para o monitoramento de recursos de TI, assim como planos de resposta a incidentes de capacidade ou disponibilidade
	A9.6	Formalizar e implantar procedimentos continuados para o gerenciamento de ativos TI e sua configuração, incluindo CMDB (Base Nacional de Ativos de TI)
	A9.7	Formalizar e implantar procedimentos continuados para o gerenciamento de liberações e implantação de serviços de TI
	A9.8	Homologar e implantar solução PaaS (Platform as a Service) para desenvolvimento de soluções de TI no MPT
	A9.9	Implantar programa de manutenção continuada das plataformas de produtos Microsoft (Exchange, AD, Skype e System Center)
	A9.10	Formalizar e implantar procedimentos continuados para o gerenciamento de mudanças em serviços de TI
	A9.11	Formalizar e implantar política nacional de uso dos recursos de impressão do MPT
META 10 Segurança da Informação	A10.1	Formalizar e implantar política nacional de Backup e Recovery
	A10.2	Implantação de solução unificada de Backup no âmbito de todo o MPT
	A10.3	Implantação de solução nacional de Segurança Lógica e Rede Suplementar de Acesso no MPT
	A10.4	Formalizar e implantar procedimentos de resposta a incidentes de segurança, incluindo designação e treinamento da equipe
	A10.5	Formalizar e implantar procedimentos para realização de auditorias periódicas em Soluções de TI
	A10.6	Formalizar e implantar Comitê de Segurança da Informação
	A10.7	Formalizar e implantar procedimentos para controle de acesso a recursos e serviços de TI do MPT
	A10.8	Formalizar e implantar programa de detecção, conscientização e mitigação de riscos inerentes à vulnerabilidades técnicas em serviços de TI
	A10.9	Implantar coleta e gerência centralizada de registros de auditoria (logs)
META 11 Gestão de continuidade dos serviços de TI	A11.1	Promover a elaboração e publicação do modelo e critérios para os Planos de Continuidade de Serviços de TI nas unidades do MPT
	A11.2	Elaborar e aprovar planos de continuidade para os principais serviços corporativos de TI do MPT
	A11.3	Acompanhar a execução dos Planos de Continuidade de Negócios de TI
META 12 Gestão de riscos	A12.1	Formalizar e implantar Gestão de Riscos de TI no MPT
META 13	A13.1	Implementar em âmbito nacional o Macroprocesso de Desenvolvimento de Software do MPT

Processos e padrões de desenvolvimento de soluções	A13.2	Homologar e formalizar arquitetura padrão para desenvolvimento de soluções de TI no MPT
META 14 Oferta de novas soluções de TI	A14.1	Implementar Portal Corporativo Único do MPT
	A14.2	Implantar e normatizar a utilização de solução de monitoramento do uso da telefonia
	A14.3	Implementar a Nova Intranet do MPT
	A14.4	Implantar o módulo PlanAssiste do COSMOS
	A14.5	Implantar o módulo Almoxarifado do COSMOS
	A14.6	Implantar o módulo Patrimônio (Compras) do COSMOS
	A14.7	Implantar o Processo Eletrônico Administrativo (MPT Digital) do COSMOS
	A14.8	Implantar o módulo de Diárias, Passagens e Transportes do COSMOS
	A14.9	Implantar o módulo de Orçamento e Finanças do COSMOS
	A14.10	Implantar o módulo de Suprimento de Fundos do COSMOS
	A14.11	Implantar o módulo de Contratos do COSMOS
	A14.12	Implantar o módulo de Compras, Registro de Preços e Licitações do COSMOS
	A14.13	Implantar o módulo de Estágio Acadêmico do COSMOS
	A14.14	Implantar o módulo de Convênios do COSMOS
	A14.15	Implantar o módulo de Biblioteca do COSMOS
	A14.16	Implantar novo Sistema de Eleições COSMOS
	A14.17	Implantar módulo de Enquetes do COSMOS
	A14.18	Implantar módulo de Recursos Humanos do COSMOS
	A14.19	Implantar módulo de Controle de Acesso do COSMOS
	A14.20	Implantar MPT Digital Administrativo no Conselho Superior do Ministério Público do Trabalho (e painel de julgamentos)
	A14.21	Implantar MPT Digital Administrativo na Corregedoria
	A14.22	Desenvolver Novo Portal da Transparência do MPT
	A14.23	Desenvolver Diário Eletrônico do MPT
	A14.24	Desenvolver aplicativo móvel "Inspetor MPT"
	A14.25	Desenvolver aplicativo móvel para suporte às comunicações relacionadas à procedimentos finalísticos (PELE)
	A14.26	Desenvolver aplicativo Móvel "Rede Aprendiz"
	A14.27	Desenvolver aplicativo Móvel Ouvidoria
	A14.28	Implantar sistema ATENA para Áreas Administrativas
	A14.29	Formalizar e implantar procedimentos para Administração de Banco de Dados, com abrangência nacional
META 15 Refatoração e aprimoramento de soluções de TI	A15.1	Ampliar mecanismos de Interoperabilidade com órgãos externos
	A15.2	Expandir oferta de serviços de TI já existentes através de interface Mobile
	A15.3	Implantar e aprimorar o Cadastro Nacional de Membros atrelado a solução nacional de cadastramento único de informações de membros e servidores
	A15.4	Manter e aprimorar sistema MPT Digital
	A15.5	Refatoração do MPT Digital
	A15.6	Aprimorar Interoperabilidade Pje/MPTD
	A15.7	Aprimorar e ampliar a utilização do serviço MPT Busca
	A15.8	Refatorar sistema Remoção de Membros
	A15.9	Integrar *datasets* a soluções de TI do MPT
	A15.10	Adequar rotinas de assinatura eletrônica do MPT à normativos e diretrizes do CNJ
	A15.11	Aprimoramento da infraestrutura de carimbo de tempo no MPT
META 16	A16.1	Implantar solução RFID no MPT
	A16.2	Implantar infraestrutura para Big Data na PGT

Otimização e melhoria da infraestrutura	A16.3	Implantar solução nacional de WiFi
	A16.4	Implantar a Acesso Remoto (VDI) e desativação da VPN
	A16.5	Implantar Teletrabalho
	A16.6	Estabelecer e executar diretrizes para a alocação de orçamento Administrativo para a padronização de ambientes técnicos de TI em PRT e PTM
	A16.7	Implementar ferramentas e melhores práticas para o gerenciamento da infraestrutura virtual do MPT, em âmbito nacional
	A16.8	Homologação e aquisição de equipamentos com capacidade adequada para processamento de grandes volumes de informação
META 17 Padrões taxonômicos e fluxos das atividades fim e meio consoante definições do CNJ e CNMP	A17.1	Aprimorar a implementação das tabelas unificadas do CNJ e CNMP no MPT Digital
	A17.2	Promover ajustes na interoperabilidade de forma a concentrar intimações do MPT ao redor do CNPJ
	A17.3	Implantação nacional da taxonomia administrativa do CNMP no âmbito dos sistemas do MPT
META 18 Manutenção do parque tecnológico de hardware e software	A18.1	Formalizar e implementar ciclos periódicos de avaliação tecnológica e definição de padrões mínimos para a infraestrutura de hardware e software do MPT
	A18.2	Realizar avaliações periódicas da infraestrutura atual de TI do MPT para identificar demandas de sustentação e modernização
	A18.3	Realizar avaliações periódicas do acervo de software atual do MPT para identificar demandas de atualização, descontinuidade ou aquisição
	A18.4	Executar e manter contratações para a sustentação da infraestrutura de comunicações do MPT
	A18.5	Executar e manter contratações para a sustentação da infraestrutura de técnica de Backend (Datacenter) do MPT
	A18.6	Executar aquisições periódicas de equipamentos para uniformizar e manter padrões mínimos em salas técnicas regionais
	A18.7	Executar aquisições periódicas de equipamentos para uniformizar e manter padrões mínimos em salas técnicas de PTM
	A18.8	Executar e manter contratações para a manutenção do acervo de licenças de software do MPT sob cobertura de manutenção, suporte técnico e atualização de versões
	A18.9	Executar aquisições periódicas de equipamentos para usuário final, buscando uniformizar e manter padrões mínimos, de acordo com necessidades institucionais
	A18.10	Executar aquisições periódicas de software utilitário básico, requerido para que usuários possam realizar suas atividades institucionais

A análise do PDTI permitiu averiguar como a unidade se percebe perante a instituição e o como ocorre o grau de alinhamento com a área estratégica da PGT. Foi possível constatar que a área de TI visualiza a essencialidade do seu papel para que o MPT atinja objetivos institucionais. Há uma coesão entre o que a organização almeja e o que a TI planeja para o futuro.

Além disso, há a integração a nível tático e operacional de TI, na qual as metas e planos de ação estão alinhados com as necessidades e objetivos estratégicos, que, por sua vez, estão coerentes com a missão e visão da Diretoria de Tecnologia da Informação.

Observa-se também que há grau de alinhamento do PDTI com os temas abordados pelo iGov. Algumas metas e ações previstas envolvem, direta ou indiretamente, os pontos questionados pelo iGov. Quanto às necessidades, há uma necessidade especifica levantada somente para o iGov, a saber N.032. Comunicação:

> Divulgação na intranet, em área específica intitulada "Governança de TI" o programa de implementação do modelo de governança, evolução histórica das respostas aos questionários dos levantamentos de governança de TI realizados pelo TCU e relatórios de feedback, informações aderentes aos princípios dos "Dados Abertos Governamentais". A área deve ser mantida pelo Escritório de Governança. Os produtos que devem ser transferidos para a gestão devem, no entanto, ser publicados na área de Gestão de TI.

Diante do exposto, conclui-se que a unidade conta com um processo bem delineado de planejamento em Tecnologia da Informação.

3.4.1.2.2. GESTÃO DE CATÁLOGO DE SERVIÇOS E ACORDOS DE NÍVEIS DE SERVIÇOS

No iGov, a unidade respondeu que executa a gestão de catálogo de serviços e foi possível constatar a existência do processo. Há um sistema que gere o portfólio de serviços no Ministério Público do Trabalho, denominado Atena, e ele é gerenciado a nível nacional por uma equipe denominada *Gestão e Desenvolvimento Atena* (composta por um servidor da PGT e dois servidores da PRT 9° Região). Esse sistema é continuamente melhorado, possui níveis de acesso distintos e equipes diversas integrando grupos de atendimento (direcionado a assuntos específicos, como segurança da informação, sistemas internos, banco de dados, escritório de projetos, entre outros). Os gestores do Atena são os únicos com permissão para alteração do sistema, porém recebem e acatam, quando oportuno, as demandas recebidas, bem como a inclusão de novos serviços no catálogo.

Quanto aos níveis de serviço (ANS), conforme resposta ao iGov, não há acordo formal estabelecido com os demais setores. Atualmente, há ANS padrões para os serviços ofertados

pelo Atena, que são os mesmo para todos os serviços prestados, porém há previsão para que as unidades adequem os ANS conforme a realidade (aumentando ou diminuindo o tempo para atendimento de chamado, por exemplo). O sistema também possui um Observatório, em fase de aperfeiçoamento, que visa demonstrar o grau de atingimento dos ANS e objetiva aumentar a eficiência das unidades e setores. Em relação aos Acordos de Níveis de Serviço de contratos de TI, estes são averiguados e atestados pelos respectivos fiscais de contrato. Ainda sobre os ANS, a unidade relatou que:

> *O nível de maturidade na disciplina 'Nível de Serviço' é considerada "Nível 1 - Inicial". O ANS foi implantado no 2º semestre de 2017, ainda é preciso discutir este processo e treinar pessoas neste framework, para inclusive criar um plano de ação. Sobre a satisfação dos usuários, o Sistema Atena permite que os usuários avaliem os chamados quando finalizado, dando as seguintes opções: (1) Ruim, (2) Regular, (3) Bom, (4), Muito bom e (5) Excelente.*

Conforme situação exposta, nota-se que a unidade possui processo de gestão de catálogo de serviços, que é continuamente aprimorado.

3.4.1.2.3. GESTÃO DE MUDANÇAS

A unidade adota em menor parte a gestão de mudanças, conforme iGov. Ao ser questionada sobre o processo, os gestores responderam que:

> *Apesar desta disciplina estar prevista no PDTI 2016-2018, considerando o grande volume de projetos e demais ações do plano, não foi possível envidar esforços para sua implementação. Como resultado, no momento não há portaria para gestão de mudanças nem processo definido, sendo que esta matéria está prevista para inclusão no próximo PDTI.*

Em entrevista, os gestores relataram que, apesar de não haver processo estruturado, a migração de sistemas é feita de forma planejada, em que se avalia os melhores caminhos para não haver interrupção dos serviços fornecidos e perda de dados.

3.4.1.2.4. GESTÃO DE CONFIGURAÇÃO E ATIVOS DE TI

Conforme iGov, a unidade adota, também em menor parte, a gestão de configuração e ativos de TI. Ao ser questionada sobre o processo, os gestores responderam que:

> *Apesar desta disciplina estar prevista no PDTI 2016-2018, considerando o grande volume de projetos e demais ações do plano, não foi possível envidar esforços para sua implementação. Contudo, ações ad-hoc para gerenciamento de configuração e ativos de TI estão sendo implementadas a partir de 2018 de forma centralizada através da ferramenta Microsoft System Center (para ambiente do usuário final) e VMware VOperations (para ambiente de backend). Como resultado, no momento não há portaria para gestão de configuração nem processo definido, sendo que esta matéria está prevista para inclusão no próximo PDTI.*

Sobre os sistemas citados, em entrevista, os gestores relataram que o VOperations monitora a saúde do Data Center e o Microsoft System Center gerencia os hardwares e softwares existentes em nível nacional, por meio do qual é possível identificar ativos que estão em uso ou não, o que está obsoleto e precisa ser renovado, consumo elétrico, além de auxiliar no inventário do parque tecnológico, mapeamento de necessidades (como realocação de ativos entre unidades do MPT) e verificação de uso de softwares e licenças de alto valor.

Quanto à gestão de configuração e ativos, apesar de incipiente, a unidade envida esforços para o seu aperfeiçoamento.

3.4.1.2.5. GESTÃO DE INCIDENTES

De acordo com resposta ao iGov 2018, a PGT adota parcialmente a gestão de incidentes. Quando questionada sobre documentação relativa ao processo, a unidade respondeu que:

> *O processo geral de gestão de incidentes foi estabelecido pela Resolução CETI nº 2, de 7 de março de 2016, publicada no BS ESPECIAL 04-A 2016, que segue anexo. Nesse sentido, o Atena é o sistema que operacionaliza todas as diretrizes dessa resolução.*

Em relação à priorização no atendimento de incidentes, os gestores relataram que a ordem dos chamados é realizada automaticamente no sistema Atena, exceto os incidentes de rede, que são monitorados pelo sistema Zabbix. Entretanto, a DTI planeja a integração do Zabbix ao Atena. Por fim, ao ser questionada sobre incidente simulado, os gestores afirmaram que ainda não há rotina estabelecida, porem estão implantando os incidentes de segurança.

Dessa maneira, assim como a gestão de configuração e ativos, a unidade busca constante aperfeiçoamento do processo.

3.4.1.2.6. GESTÃO DE RISCOS

Para a gestão de riscos, segundo resposta ao iGov, há "decisão formal ou plano aprovado para adotá-lo". Quando questionada sobre o processo, os gestores responderam que:

> *O processo geral para gestão de riscos está descrito na Resolução CETI nº 8, de 3 de maio de 2016, publicada no BS ESPECIAL 05-F 2016, que segue anexo. Até o presente momento, a única iniciativa formal decorrente das diretrizes da gestão de risco foi concretizada por meio da Resolução CETI nº 14, de 8 de junho de 2017, publicada na página 2, do BS ESPECIAL 6-C 2017, que segue anexo, estabelecendo medidas complementares a serem adotadas pelos Subcomitês Diretivos de Tecnologia da Informação (nas Procuradorias Regionais do Trabalho) quanto ao mapeamento de riscos em datacenters e instalações computacionais.*

Em entrevista, os gestores reafirmaram que ainda não obtiveram êxito em implantar a gestão de riscos devido à complexidade do tema.

3.4.1.2.7. GESTÃO DE CONTINUIDADE DE SERVIÇOS

Assim como gestão de riscos, no iGov a gestão de continuidade de serviços consta apenas como "decisão formal ou plano aprovado para adotá-lo". Após questionamento, a unidade informou que:

> *O processo geral para gestão da continuidade de serviços de TI está descrito na Resolução CETI nº 6, de 07 de março de 2016, publicada na página 13 do BS ESPECIAL 04-A 201. [...] Adicionalmente, o Modelo para Planejamento e Desenvolvimento dos Planos de Continuidade de Serviços de TI está definido na Resolução CETI nº 16, de 13 de setembro de 2017, publicada na página 2, do BS ESPECIAL 9-D 2017.*

Na auditoria *in loco*, os gestores relataram que algumas unidades já possuem planos de continuidade de serviços, mas como em outras ainda não houve a migração completa dos sistemas, seria improdutivo montar planos de continuidade para essas unidades em transição.

3.4.1.2.8. SEGURANÇA DA INFORMAÇÃO

Quanto aos questionamentos relativos a segurança da informação, as respostas do MPT condizem com a realidade encontrada. A gestão de segurança da informação segue a ABNT NBR ISO/IEC 27001 e possui a seguinte normatização, segundo informação da unidade:

- Em vigor:
  - Resolução CETI nº 4, de 7 de março de 2016, publicada na página 7 do BS ESPECIAL 04-A 2016, que institui a Política Nacional de Segurança da Informação, constitui a única normatização no nível estratégico.
  - Resolução CETI nº 5, de 7 de março de 2016, publicada na página 10 do BS ESPECIAL 04-A 2016, que disciplina o uso de recursos de Tecnologia da Informação no Ministério Público do Trabalho conforme diretrizes da Política Nacional de Segurança da Informação.
  - Resolução CETI nº6, de 7 07 de março de 2016, publicada na página 13 do BS ESPECIAL 04-A 2016, que estabelece metas e estrutura para a gestão da Continuidade de Serviços de Tecnologia da Informação no Ministério Público do Trabalho conforme diretrizes da Política Nacional de Segurança da Informação.
  - Resolução CETI nº 8, de 3 de maio de 2016, publicada no BS ESPECIAL 05-F 2016, que institui a política e macroprocesso de gerenciamento de riscos TI do Ministério Público do Trabalho.
  - Resolução CETI nº 14, de 8 de junho de 2017, publicada na página 2, do BS ESPECIAL 6-C 2017, estabelecendo medidas complementares a serem adotadas pelos Subcomitês Diretivos de Tecnologia da Informação quanto ao mapeamento de riscos em datacenters e instalações computacionais.
  - Resolução CETI nº 16, de 13 de setembro de 2017, publicada na página 2, do BS ESPECIAL 9-D 2017, definindo modelo para planejamento e desenvolvimento dos Planos de Continuidade de Serviços de Tecnologia da Informação.
- Em revisão ou fase de minuta:

- Revisão da Política Nacional de Segurança de Tecnologia da Informação: aguardado aprovação.
- Revisão da Norma de Uso de Recursos de TI: aguardado aprovação.
- Minuta de Norma de Controle de Acesso: aguardando aprovação.

Ao ser questionada sobre o Comitê de Segurança da Informação e não existência de Gestor de Segurança da Informação, a unidade justificou que:

> *O Conselho Nacional do Ministério Público publicou a Resolução CNMP nº 156, de 13 de dezembro de 2016, que Instituiu a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público. Nessa resolução, há a Subseção IV, do Capítulo II, que trata da segurança da informação nos meios de tecnologia da informação, nos seguintes termos, com grifo nosso:*
>
> > *"Art. 7º A segurança da informação compreende o conjunto de medidas voltadas para proteger dados e informações sensíveis ou sigilosas, cujo acesso ou divulgação não autorizadas possa acarretar prejuízos de qualquer natureza ao Ministério Público ou proporcionar vantagem a atores antagônicos.*
> >
> > *...*
> >
> > *§2ºA segurança da informação, pela sua relevância e complexidade, desdobra-se nos seguintes subgrupos:*
> >
> > *I – segurança da informação nos meios de tecnologia da informação; "*
>
> *A Portaria nº 739, de 5 de dezembro de 2016, alterada pela Portaria nº1418, de 19 de setembro de 2017, ambas do Procurador-Geral do Trabalho, instituiu o Sistema Integrado de Governança da Gestão Estratégico do Ministério Público do Trabalho – SIGGE. Nesse sistema, além de ratificar as atribuições do Comitê Estratégico de Tecnologia da Informação – CETI, criou outros comitês dentre eles o Comitê Estratégico de Segurança Institucional – CESI.*
>
> *Nesse contexto do SIGGE, são atribuições do CESI e CETI:*
>
> > *Art. 18. Cabe ao CESI:*
> >
> > *I – orientar a gestão estratégica da segurança institucional, bem como elaborar estudos para o respectivo desenvolvimento;*
> >
> > *II – propor ao Procurador-Geral do Trabalho alterações na Política de Segurança Institucional;*
> >
> > *III – propor projetos, iniciativas e ações de fortalecimento da segurança institucional, bem como parcerias estratégicas correlatas;*
> >
> > *IV – interagir com as Unidades e os Órgãos do Ministério Público do Trabalho, bem como com os diversos segmentos administrativos, visando à consecução dos projetos, iniciativas e ações de segurança institucional;*
> >
> > *V – exercer outras atribuições compatíveis com os propósitos da sua criação.*

...

Art. 22. Cabe ao CETI:

I – estabelecer políticas e diretrizes de tecnologia de informação (TI), alinhadas aos objetivos institucionais estratégicos;

II – propor o Plano Diretor Nacional de Tecnologia da Informação – PDNTI;

III – definir prioridades de investimentos em tecnologia da informação;

IV – estabelecer prioridades na execução de projetos de tecnologia da informação;

V – definir padrões de funcionamento, integração, qualidade e segurança dos serviços e sistemas de tecnologia da informação;

VI – propor, nos limites das suas atribuições, políticas de gestão de pessoas e de padronização da estrutura;

VII – exercer outras atribuições compatíveis com os propósitos da sua criação.

Em 27 de agosto de 2018, o Procurador-Geral do Trabalho institui a Política de Segurança Institucional do Ministério Público do Trabalho – PSI-MPT, por meio da Portaria nº 1213, publicada no BS ESPECIAL 08-I 2018, que segue anexa. Basicamente a PSI-MPT é a internalização da Resolução CNMP nº 156, de 13 de dezembro de 2016, no MPT. Entretanto, vale destacar:

"Art. 1º

§4º Compete ao Comitê Estratégico de Segurança Institucional (CESI) propor as medidas de governança específicas da Segurança Institucional."

...

Art. 3º A segurança institucional compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações de qualquer natureza que constituam ameaças à salvaguarda da Instituição e de seus integrantes, inclusive à imagem e reputação.

§1º As medidas a que se reportam o caput compreendem a segurança orgânica e a segurança ativa.

§2º A segurança orgânica é composta pelos seguintes grupos de medidas:

...

IV..segurança da informação.

...

Art 7º

§2º A segurança da informação desdobra-se nos seguintes subgrupos:

I. segurança da informação nos meios de tecnologia da informação;

...

§7º As medidas de segurança da informação deverão ser observadas, em especial e sem prejuízo das demais unidades do Ministério Público do Trabalho, pelas áreas de comunicação social e de tecnologia da informação.

> *No PDTI 2016-2018 está prevista a ação A10.6 "Formalizar e implantar Comitê de Segurança da Informação". Entretanto, diante dos atos normativos supracitados, surgiu a dúvida sobre qual contexto esse comitê de segurança deveria se encaixar e, consequentemente, do gestor de segurança da informação.*
> *Diante desse cenário, o CETI vem exercendo o papel de comitê de segurança da informação quando se trata da "segurança em meios de tecnologia da informação". Nesse caso, o gestor de segurança é o próprio CETI.*
> *Vale ressaltar que no art. 213 do Regimento Administrativo do MPT, existe a Assessoria de Governança, Segurança e Conformidade em Tecnologia da Informação que presta assessoramento ao Diretor de Tecnologia da Informação da PGT. Entretanto, não consta nas atribuições dessa assessoria, atuar como gestor de segurança da informação.*

Na auditoria *in loco*, os gestores complementaram a informação acima relatando que o CESI é comitê ligado a segurança institucional, portanto ainda não está definido como será tratado e por quem, considerando que engloba atribuições de diferentes áreas da PGT. Atualmente a área de TI está cuidando da segurança de tecnologia da informação, porém não é normatizado.

Quanto as ações de conscientização, educação e treinamento em Segurança da Informação, os gestores relataram que:

> *No Núcleo de Referência de Segurança da Informação, constituído conforme 20ª Reunião de Avaliação Estratégica do CETI/MPT, tem por atribuição executar as ações de conscientização, educação e treinamento em segurança da informação.*
> *Na intranet, há um espaço para divulgação das ações de segurança: https://intranet.mpt.mp.br/pgt/seguranca-em-ti.*
> *Nesse sentido, a principal campanha que tem sido desenvolvida, em conjunto com a ASCOM/PGT é como identificar e agir diante de mensagens de correio falsas que buscam coletar informações pessoais. Segue o link na intranet sobre esses alertas: https://intranet.mpt.mp.br/pgt/noticias-mpt/usuarios-da-rede-do-mpt-devem-se-proteger-de-fraudes-na-internet. Outra campanha foi sobre os cuidados com a senha: https://intranet.mpt.mp.br/pgt/noticias-mpt/usuarios-da-rede-mpt-devem-ficar-atentos-para-a-importancia-das-senhas.*
> *Além das orientações acima, em casos de maior recebimento de mensagens falsas, há envio de notificações por e-mail.*

Em complemento às informações acima, foi relatado que as equipes de TI estão em constante capacitação em segurança da informação.

3.4.1.2.9. GESTÃO DE ATIVOS ASSOCIADOS À INFORMAÇÃO

Em conformidade com a resposta ao iGov, a unidade não possui gestão de ativos associados à informação. Em entrevista os gestores relataram a dificuldade em definir quais ativos são voltados para informação e seu processamento. Atualmente estão trabalhando na formação do banco de configuração de dados, porém não está bem regulamentado.

3.4.1.2.10. GESTÃO DE SOFTWARES

A unidade executa, de fato, a gestão de softwares, conforme afirmado no iGov. O estabelecimento do Macroprocesso de Software encontra-se na Resolução CETI n° 003/2016. O gerenciamento é realizado pelo Escritório de Projetos e o desenvolvimento é realizado por equipe exclusiva, sendo vedado o desenvolvimento regional de sistemas.

Quanto ao desenvolvimento de softwares, a equipe informou que:

> *Esse macroprocesso é baseado em uma metodologia de desenvolvimento ágil chamada Scrum (https://www.scrum.org/about). Assim, são criadas equipes para o desenvolvimento de cada sistema onde há um líder do projeto específico. Nesse contexto, a disciplina de escritório de projetos é realizada pela Assessoria de Gestão de Projetos Estratégicos de Tecnologia da Informação, cujas atribuições estão no art. 212 do Regimento Interno Administrativo do MPT. (https://intranet.mpt.mp.br/pgt/comunicacao/publicacoes/regimento-interno-administrativo_web.pdf).*

3.5. ACHADOS

3.5.1. ACHADO – Não implantação de processos do iGov previstos no PDTI 2016-2018

Os processos de gestão de mudanças e gestão de continuidade de serviços de TI, ambos questionados no iGov e com implantação prevista no PDTI 2016-2018, não possuem todas as ações concluídas.

Em relação à gestão de mudanças, a unidade adota apenas ações pontuais e, no caso da gestão da continuidade de serviços, há apenas plano formal. Apesar da realidade estar em conformidade com o respondido no levantamento do TCU, era prevista sua implantação e esta não ocorreu em sua totalidade. O cruzamento de dados encontra-se a seguir:

PDTI			iGov TI	
	Ação	**Status**	**Questionamento**	**Resposta**
Gestão de Mudanças	A9.10 Formalizar e implantar procedimentos continuados para o gerenciamento de mudanças em serviços de TI.	Não iniciada	4222. A organização executa processo de gestão de mudanças	Adota em menor parte
Gestão de continuidade de serviços de TI	A11.1 Promover a elaboração e publicação do modelo e critérios para os Planos de Continuidade de Serviços de TI nas unidades do MPT.	Concluída	4242. A organização executa processo de gestão da continuidade dos serviços de tecnologia da informação	Há decisão formal ou plano aprovado para adotá-lo
	A11.2 Elaborar e aprovar planos de continuidade para os principais serviços corporativos de TI do MPT.	Não iniciada		
	A11.3 Acompanhar a execução dos Planos de Continuidade de Negócios de TI.	Não iniciada		

Obs.: foram inseridas somente as respostas em que a PGT afirmou não adotar ou que há apenas plano ou decisão formal para adoção, em casos que há correlação com as ações do PDTI

Segundo o ITIL (*Information Technology Infraestructure Library*), guia de boas práticas para gestão de serviços de TI, o gerenciamento de mudança é "o processo responsável pelo controle do ciclo de vida de todas as mudanças, permitindo que mudanças benéficas sejam feitas com o mínimo de interrupção aos serviços de TI". Nesse contexto, mudança é definida como "O acréscimo, modificação ou remoção de qualquer coisa que possa afetar serviços de TI. O escopo deve incluir mudanças a todos os processos, arquiteturas, ferramentas, métricas e documentação, além de mudanças em serviços de TI e outros itens de configuração".

Em relação à gestão de continuidade, conforme Norma ABNT NBR ISO 22313:2015, que orienta gestores sobre a continuidade do negócio, aplicável aos serviços de tecnologia da informação:

> A continuidade de negócios é a capacidade que uma organização tem de continuar a entrega de produtos ou serviços em níveis aceitáveis pré-definidos após um incidente de interrupção. A gestão de continuidade de negócios (GCN) é o processo de alcançar a continuidade do negócio e é sobre a preparação de uma organização para lidar com incidentes de interrupção que poderiam impedi-la de atingir seus objetivos. Colocar a GCN dentro de uma

> estrutura e disciplinas de um sistema de gestão cria um sistema que permite que a GCN possa ser controlada, avaliada e melhorada continuamente.
> Um sistema de gestão de continuidade de negócios (SCGN) enfatiza a importância de: i) compreender as necessidades da organização e a necessidade de estabelecer uma política e objetivos de continuidade de negócios; ii) implementar e operar controles e medidas para a gestão da capacidade geral de uma organização para gerenciar incidentes de interrupção; iii) monitorar e analisar criticamente o desempenho e a eficácia do SGCN; e iv) melhorar continuamente, com base em medições objetivas.

Mais especificamente sobre gerenciamento de continuidade de serviços de TI, o ITIL o define como:

> O processo responsável pelo gerenciamento de riscos que podem impactar seriamente os serviços de TI. O gerenciamento de continuidade de serviço de TI garante que o provedor de serviço de TI pode sempre prover o mínimo nível de serviço acordado, através da redução do risco a um nível aceitável e planejamento da recuperação dos serviços de TI. O gerenciamento de continuidade de serviço de TI suporta o gerenciamento de continuidade de negócio.

Além disso, a Resolução CNMP n° 171/2017, em seu artigo 18, inciso IV, determinou a regulamentação do macroprocesso de gestão de continuidade de serviços de TI em todos os ramos e unidades do Ministério Público.

Por fim, o modelo de referência de processo do COBIT 5.0 (guia de boas práticas de governança de TI amplamente utilizado), que trata de 32 processos de gestão, inclui, entre eles, o Gerenciamento de Mudanças (BAI06) e Gerenciamento de Continuidade (DSS04).

A partir do exposto, depreende-se a necessidade de processos de gestão de mudanças e de continuidade de negócios bem estruturados na organização, considerando a importância para a entrega eficiente de serviços de TI no MPT.

3.5.1.1. *RECOMENDAÇÕES*

Para o próximo PDTI, propor, além de ações ligadas a instituição da gestão da continuidade de serviços e gestão de mudanças, asserções para a sua viabilização. Caso a Unidade julgue não ser possível desenvolver de forma completa os processos de gestão de mudanças e de continuidade de serviços de TI, utilizar critérios objetivos de priorização, de forma que justifique o enfoque no desenvolvimento de um processo em detrimento do outro naquele momento, e assim desenvolver as ações de maneira gradativa e programada.

3.5.2. ACHADO - Não implantação do processo de gestão de riscos

Apesar da unidade dispor de uma Resolução (CETI n° 08/2016), que institui a Política e Gerenciamento de Riscos em TI no Ministério Público do Trabalho, e ação prevista no PDTI 2016-2018 (A12.1), não houve o desenvolvimento do processo de gestão de riscos. À exceção das medidas complementares de mapeamento de riscos em datacenters e instalações computacionais, dispostas na Resolução CETI n° 14/2017, a serem adotadas pelos Subcomitês Diretivos de Tecnologia da Informação nas Procuradorias Regionais do Trabalho.

A Resolução CNMP n° 171/2017 institui que:

> Art. 18 A unidades e os ramos do Ministério Público deverão regulamentar a gestão dos seguintes macroprocesso de TI:
> [...]
> II- Riscos de TI

Conforme Art. 7° da Portaria PGR/MPU n° 78/2017, que institui a Política de Gestão de Riscos do MPU:

> Art. 7° Os ramos do MPU e a ESMPU deverão estabelecer a unidade responsável por coordenar a implementação da política de gestão de riscos e **monitorar sua execução.** (grifo nosso)

Por fim, a Resolução CETI n° 14/2017 resolve:

> Art. 1° Instituir a Política e **o Processo de Gerenciamento de Riscos** de Tecnologia da Informação do Ministério Público do Trabalho. (grifo nosso)

O ITIL conceitua gerenciamento de riscos como o processo responsável pela identificação, avaliação e controle de riscos. Riscos, no mesmo guia, é definido como:

> Um evento possível que pode causar perdas ou danos, ou afetar a habilidade de atingir objetivos. Um risco é calculado pela probabilidade de uma determinada ameaça ocorrer, pela vulnerabilidade do ativo a essa ameaça e pelo impacto gerado caso ela tivesse ocorrido. O risco também pode ser definido como incerteza do resultado e pode ser usado no contexto da medição da probabilidade de resultados positivos ou de resultados negativos.

A Norma ABNT NBR ISO 31000:2018 afirma que gerenciar riscos é iterativo e auxilia as organizações em suas estratégias, alcance dos objetivos e tomada de decisões fundamentais, sendo parte da governança e liderança, fundamental para a governança e liderança,

contribuindo para a melhoria dos sistemas de gestão. O propósito da gestão de riscos é criar e proteger valor, melhorando o desempenho, promovendo a inovação e alcance dos objetivos.

Uma gestão de riscos adequada minimiza os impactos da ocorrência dos riscos detectados, caso o evento se concretize, auxiliando, assim, no atingimento dos objetivos organizacionais e geração de valor para a unidade.

3.5.2.1. *RECOMENDAÇÕES*

Priorizar, no próximo PDTI, rotinas ligadas à estruturação do processo de gestão de riscos em conformidade com o estabelecido na Resolução CETI nº 08/2016 e normas pertinentes

3.5.3. ACHADO – Não há acompanhamento de resultados das orientações emitidas pelo CETI aos Subcomitês Diretivos

Os resultados das medidas emitidas por meio das Resoluções do CETI aos Subcomitês Diretivos de TI (nas Procuradorias Regionais) não são monitoradas. Conforme entrevista com os gestores, como não há relação de subordinação entre o CETI e os Subcomitês, não há ferramentas para uma cobrança mais incisiva.

Os exemplos de medidas que, a princípio, não foram monitoradas são:

a) Modelo para Planejamento e Desenvolvimento dos Planos de Continuidade de Serviços de TI, estabelecido na Resolução CETI n° 16/2017 (nas unidades que já migraram para os novos sistemas);
b) Mapeamento de riscos em datacenters e instalações computacionais, estabelecido na Resolução CETI n° 14/2017.

Quanto aos planos de continuidade, há, inclusive, ação prevista no PDTI 2016-2018 de acompanhamento da execução desses planos: "A11.3 Acompanhar a execução dos Planos de Continuidade de Negócios de TI". Conforme informação fornecida pelos gestores, essa ação não foi iniciada no ciclo vigente.

O risco do não acompanhamento é de possível não implementação das medidas estabelecidas pelo Conselho Estratégico de TI do MPT.

3.5.3.1. *RECOMENDAÇÕES*

Estabelecer controles de monitoramento e reporte das unidades em relação as resoluções do CETI, a exemplo do realizado pela unidade em relação à Resolução CETI nº 05/2016, na qual foi emitido o Ofício CETI n° 04/2018 para desinstalação e retirada de equipamentos obsoletos e posterior acompanhamento do progresso via sistema.

3.5.4. ACHADO – Acordos de Níveis de Serviços padronizados para diferentes tipos de serviços ofertados pelo Atena

No sistema Atena, os acordos de níveis de serviços (SLAs) são os mesmos para os diferentes tipos de serviços ofertados pela Unidade, ou seja, serviços mais complexos e que demandam mais tempo estão equiparados àqueles de maior facilidade de execução em relação ao atendimento.

Segundo a Resolução CNMP n° 171/2017:

> Art. 23. A regulamentação da gestão de serviços de TI contemplará:
> I – gestão do Catálogo de Serviços, incluindo a **dos Acordos de Níveis de Serviço** (grifo nosso)
> Art. 2° Para os fins desta Resolução, considera-se:
> I – Acordo de Nível de Serviço (ANS): acordo definido entre a unidade de TI e os usuários da instituição que descreve condições e garantias na prestação dos serviços de TI, além de documentar metas de qualidade e especificar as responsabilidades da unidade de TI e dos usuários

Conforme Norma ABNT NBR ISO/IEC 20000-1:2011:

> Para cada serviço fornecido, um ou mais acordos de nível de serviço (ANS) devem ser acordados com o cliente. Quando for criado um ANS, o provedor de serviço deve considerar os requisitos do serviço. Os ANS devem incluir metas de serviço, características da carga de trabalho e exceções. O provedor de serviço, em intervalos planejados, deve analisar criticamente com o cliente os serviços e os ANS.

Apesar dos níveis de serviços estarem em fase inicial de execução, caso a falta de correção perdure no tempo, poderá refletir no Observatório Atena, que será responsável por demonstrar o grau de atingimento dos SLAs de setores e unidades. Essa padronização pode gerar conclusão inadequada sobre a eficiência das unidades.

3.5.4.1. *RECOMENDAÇÕES*

Estabelecer rotinas visando reavaliar, junto às unidades e setores responsáveis, os SLAs em casos constatados que os níveis estabelecidos não condizem com a realidade de execução.

3.5.5. ACHADO – Comitê de Segurança da Informação não implementado

Devido ao conflito de atribuições do Comitê Estratégico de Segurança Institucional (CESI) e Comitê Estratégico de Tecnologia da Informação (CETI) em relação à Segurança da Informação (relatado no item 3.4.1.2.8), não há a normatização das atribuições relativas ao tema na área de TI e, consequentemente, não há gestor de segurança da informação nomeado.

As ações relativas ao tema atualmente são realizadas pelo CETI, com assessoramento informal da Assessoria de Governança e Conformidade em Tecnologia da Informação. Cabe ressaltar que há ação prevista no PDTI 23016-2018 para instauração de comitê responsável: A10.6 Formalizar e implantar Comitê de Segurança da Informação.

Segundo a Resolução CNMP n° 171/2017:

> Art. 18 A unidades e os ramos do Ministério Público deverão regulamentar a gestão dos seguintes macroprocesso de TI:
> [...]
> VII- Segurança da informação dos ativos de TI
> [...]
> Art. 19. As unidades e os ramos do Ministério Público deverão **instituir comitê gestor e designar gestor** para, respectivamente, governar e gerir os macroprocessos de TI previstos no artigo anterior. (grifo nosso)

A Norma ABNT NBR ISO/IEC 27002:2013, que trata sobre código de prática para controles de segurança da informação, no item 6.1.1, orienta sobre responsabilidade e papeis pela segurança da informação:

> Controle
>
> **Convém que todas as responsabilidades pela segurança da informação sejam definidas e atribuídas.**
>
> Diretrizes para implementação
> Convém que a atribuição das responsabilidades pela segurança da informação seja feita em conformidade com as políticas de segurança da informação. **Convém que as responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de segurança da informação específicos**

> **sejam claramente definidas**. Convém que as responsabilidades pelas atividades do gerenciamento dos riscos de segurança da informação e, em particular, pela aceitação dos riscos residuais sejam definidas. Convém que as responsabilidades sejam complementadas, onde necessário, com orientações mais detalhadas para locais específicos e recursos de processamento da informação. Convém que as responsabilidades locais para a proteção dos ativos e para realizar processos de segurança da informação específicos sejam definidas.
> Indivíduos que receberam responsabilidades de segurança da informação podem delegar tarefas de segurança da informação para outros. Todavia, convém que eles permaneçam responsáveis e determinem se quaisquer tarefas delegadas tenham sido corretamente executadas.
> **Convém que as áreas pelas quais as pessoas sejam responsáveis estejam claramente definidas**; em particular, recomenda-se que os seguintes itens sejam cumpridos:
> a) convém que os ativos e os processos de segurança da informação sejam identificados e claramente definidos;
> b) convém que a entidade responsável por cada ativo ou processo de segurança da informação seja determinada e os detalhes dessa responsabilidade sejam documentados (ver 8.1.2);
> c) convém que os níveis de autorização sejam claramente definidos e documentados;
> d) convém que as pessoas indicadas sejam competentes e capazes de cumprir com as responsabilidades pela segurança da informação e a elas seja dada a oportunidade de manter-se atualizada com os desenvolvimentos;
> e) convém que a coordenação e a visão global dos aspectos de segurança da informação na cadeia de suprimento sejam identificadas e documentadas.
> (grifo nosso)

Com as atribuições definidas para cada Comitê, há a possibilidade de controles mais eficientes para ações de Segurança da Informação, dada a sua importância para manutenção da confidencialidade, integridade e disponibilidade das informações existentes, e preservar seus respectivos valores para Ministério Público do Trabalho. Sem as atribuições definidas, há o risco de aspectos de segurança da informação serem negligenciados.

3.5.5.1. *RECOMENDAÇÕES*

Avaliar a necessidade de definir, em conjunto com o CESI, quais são as atribuições da área de TI relativas à segurança da informação para posterior implementação do comitê e definição do gestor de segurança de informação responsável.

4. CONCLUSÕES

Diante do exposto, conclui-se que a unidade envida esforços para o contínuo aprimoramento da Governança em Tecnologia da Informação.

O processo de planejamento em TI da unidade é bem estruturado e desenvolvido, e os processos de gestão de catálogo de serviços, segurança da informação e gestão de softwares já possuem um grau maior de maturidade.

Quanto aos processos de gestão de configuração e ativos de TI, gestão de incidentes, gestão de mudanças, gestão de riscos, gestão de continuidade de serviços e gestão de ativos associados à informação, ou possuem decisão formal para adoção ou estão em fase inicial de planejamento e desenvolvimento.

Para todos os processos listados nas quais a auditoria identificou oportunidades de melhoria foram exaradas recomendações à unidade.

Por fim, em face das recomendações da Audin-MPU, solicitamos que a unidade apresente plano de ação apontando, para cada achado de auditoria, **a providência que será adotada**, **o responsável pela implementação da providência** e o **prazo de implementação**, ou **justificativa para manter a situação observada assumindo os riscos decorrentes.**

Para elaboração do plano de ação, poderá ser adotada como modelo a tabela sugerida a seguir:

Situação observada	Providências para sanar a situação observada	Prazo para implementação das providências	Responsável pela implementação das providências	Justificativa para manutenção da situação observada*

*Caso a unidade opte por manter a situação observada

Poderá ser agendada reunião, por iniciativa da Auditoria Interna ou da Unidade, para tratar de eventuais esclarecimentos a respeito dos achados e sobre a elaboração do plano de ações, preferencialmente no prazo de 15 dias a contar do recebimento deste relatório.

É o Relatório Preliminar.

Brasília, 29 de novembro de 2018.

KAMILLA TURNES LEMOS
Coordenador

RONALDO DA SILVA PEREIRA
Membro da Equipe

GUSTAVO PEREIRA DE CUBA
Membro da Equipe

De acordo.
Encaminhe-se ao Senhor Secretário de Auditoria.

JÔSI BRANDÃO SILVA
Coordenadora de Auditoria de Acompanhamento de Gestão

De acordo.
À consideração do Senhor Auditor-Chefe.

EDER SARDINHA E SILVA
Secretário de Auditoria

Aprovo.
Encaminhe-se à Direção-Geral do Ministério Público do Trabalho, para ciência.

SEBASTIÃO GONÇALVES DE AMORIM
Auditor-Chefe

MINISTÉRIO PÚBLICO FEDERAL

Assinatura/Certificação do documento **AUDIN-MPU-00002889/2018 RELATÓRIO**

Signatário(a): **JOSI BRANDAO SILVA**
Data e Hora: **29/11/2018 16:05:30**
Assinado com login e senha

Signatário(a): **KAMILLA TURNES LEMOS**
Data e Hora: **29/11/2018 16:12:25**
Assinado com login e senha

Signatário(a): **GUSTAVO PEREIRA DE CUBA**
Data e Hora: **29/11/2018 16:06:07**
Assinado com login e senha

Signatário(a): **EDER SARDINHA E SILVA**
Data e Hora: **29/11/2018 16:04:57**
Assinado com login e senha

Signatário(a): **RONALDO DA SILVA PEREIRA**
Data e Hora: **29/11/2018 16:11:33**
Assinado com login e senha

Signatário(a): **SEBASTIAO GONCALVES DE AMORIM**
Data e Hora: **29/11/2018 16:18:49**
Assinado com certificado digital