ATOS DO COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO (CETI)

RESOLUÇÃO CETI/MPT Nº 16, DE 13 DE SETEMBRO DE 2017

Define modelo para planejamento e desenvolvimento dos Planos de Continuidade de Serviços de Tecnologia da Informação – PCSTI.

O **COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO (CETI)** do Ministério Público do Trabalho, no uso das atribuições que lhe confere a Portaria PGT nº 714, de 4 de maio de 2017;

CONSIDERANDO que, de acordo com a Resolução CNMP nº 70, compete ao CETI definir padrões de funcionamento, integração, qualidade e segurança dos serviços e sistemas de Tecnologia da Informação;

CONSIDERANDO a necessidade de aprimorar os padrões de governança em Tecnologia da Informação no Ministério Público do Trabalho;

CONSIDERANDO o artigo 26 da Resolução CETI nº 6, de 7 de março de 2016, que estabelece a estrutura para a gestão da Continuidade de Serviços de Tecnologia da Informação no Ministério Público do Trabalho. Resolve**:**

Art. 1º Definir o modelo para planejamento e desenvolvimento dos Planos de Continuidade de Serviços de Tecnologia da Informação – PCSTI, conforme as diretrizes da Política Nacional de Segurança de Tecnologia da Informação do MPT.

Art. 2º São pressupostos para o planejamento do PCSTI:

I. Basear-se, no que couber, na metodologia definida no macroprocesso de desenvolvimento de software no âmbito do MPT;
II. Adotar uma abordagem iterativa e incremental visando a melhoria contínua;
III. Fornecer uma documentação objetiva com foco nas atividades essenciais do PCSTI.

Art. 3º São objetivos do planejamento do PCSTI:

I. Qualificar o grau de criticidade dos serviços de TI do MPT;
II. Definir o escopo e objetivos específicos do PCSTI;
III. Qualificar os requisitos de segurança da informação conforme o escopo do planejamento do PCSTI;
IV. Quantificar os parâmetros objetivos de continuidade de serviço;
V. Considerar os resultados da análise de risco e impacto conforme o macroprocesso de gestão de risco;
VI. Descrever a plataforma operacional que suporta o serviço, principalmente o modelo de interação e a cadeia de dependência;
VII. Realizar o levantamento dos contatos técnicos e gerenciais;
VII. Mapear as habilidades e competências necessárias para operação do PCSTI;
VIII. Realizar o levantamento dos procedimentos ad hoc que porventura já são adotados para o serviço objeto do PCSTI.
Art. 4º O planejamento do PCSTI será realizado conforme roteiro anexo a esta resolução.

Parágrafo Único: O desenvolvimento e conclusão de cada PCSTI será o resultado da aplicação do roteiro de planejamento.

Art. 5º As situações não previstas serão resolvidas pelo CETI, em nota técnica, respeitados os parâmetros da Resolução CETI nº 2/2016.

Art. 6º Esta resolução entra em vigor na data de sua publicação.

LUIS FABIANO DE ASSIS
Procurador do Trabalho
Presidente do Comitê Estratégico de Tecnologia da Informação do MPT

ANEXO

ROTEIRO DO PLANEJAMENTO DO PCSTI

1. IDENTIFICAÇÃO DO SERVIÇO		
1.1	Nome do Serviço:	
1.2	Descrição:	
1.3	Gestor:	
1.4	Unidade Operacional	
Metodologias:		Entrevista via questionário estruturado.
Responsáveis:		Gestor do serviço.
Observações: 1) Conforme Art. 10, inc II da Resolução CETI nº 7, se o planejamento contemplar um conjunto de serviços, deverá ser designado um nome de serviço geral e, na descrição, a lista dos serviços específicos. 2) Unidade Operacional corresponde à unidade do MPT responsável pelo suporte operacional.		

2. ESCOPO E OBJETIVO DO PCSTI		
2.1	Escopo:	*Descrever o cenário atual do serviço considerando a interação do PCSTI e o nível de maturidade dos envolvidos no plano.*
2.2	Objetivos:	*Considerando um contexto com várias interações e melhorias dos PCSTI, deve-se, na primeira versão do plano, focar na indicação da escala do incidente do nível de risco a ser tratado.* *Nesse sentido, torna-se importante a realização de testes do plano a fim de identificar oportunidades de melhorias para as novas interações dos PCSTI.*
Metodologias:		Entrevista via questionário estruturado. Reunião.
Responsáveis:		Gestor do serviço. Equipe de TI.

	ASTI/DTI/PGT.
Observações:	

3. CRITICIDADE			
Parâmetro		**Escore**	
3.1	Requisito de Disponibilidade:	( ) 4 – Altíssima > 99,72% ( ) 3 – 99,72 ≥ Alta > 99,44% ( ) 2- 99,44% ≥ Média > 98,98% ( ) 1- Baixa ≤ 98,89%	
3.2	Abrangência:	( ) 4 - Nacional ( ) 2 - Regional	
3.3	Finalidade:	( ) 4 - Finalístico ( ) 2 - Administrativo	
3.4	Regime de Operação:	( ) 4 - 24x7 ( ) 2 - 8x5	
3.5	Impacto em Caso de Incidente (conforme Perfil de Risco – Resolução CETI nº 8):	( ) 4 - Altíssimo ( ) 3 - Alto ( ) 2 - Médio ( ) 1 - Baixo	
3.6	Classificação do Risco (conforme Perfil de Risco – Resolução CETI nº 8):	( ) 4 - Altíssimo ( ) 3 - Alto ( ) 2 - Médio ( ) 1 - Baixo	
3.7	Público:	( ) 3 - Externo ( ) 1 - Interno	
3.8	Requisito Legal	( ) 3 – Sim ( ) 1 - Não	
CRITICIDADE		Altíssima: 30 - 27 Alta: 26 – 22 Médio: 21 – 16 Baixo: 15 – 11	
Metodologias:		Entrevista via questionário estruturado. Pesquisa em outros documentos (análise de risco). Reunião.	
Responsáveis:		Gestor do Serviço. Equipe de TI. ASTI/DTI/PGT.	
Observações: Os itens 2.6 e 2.7 dependem dos resultados da análise de risco. Dessa forma, se no momento de planejamento do PCSTI ainda não houver a conclusão da análise de risco, os respectivos itens deverão ser marcados como ALTO.			

4. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO		
4.1	Confidencialidade:	Identificar as informações classificas e como são criadas, armazenadas, transmitidas, manipuladas e descartadas. O principal mecanismo para a garantia da confidencialidade é a criptografia.
4.2	Autenticidade:	Identificar os mecanismos de garantia de autenticidade, principalmente de certificação digital de AC interna. Os principais mecanismos para a garantia da autenticidade são códigos de autenticação de mensagens (MAC) e assinaturas digitais.
4.3	Integridade:	Identificar os mecanismos de garantia de integridade.
4.4	Não-repúdio:	Identificar mecanismos de autenticidade que exigem certificação digital pública.
Metodologias:		Reunião.
Responsáveis:		Gestor do Serviço. Equipe de TI. ASTI/DTI/PGT.
Observações:		

5. PARÂMETROS OBJETIVOS PARA CONTINUIDADE DE SERVIÇO		
5.1	RPO – Ponto Pretendido de Recuperação	Tempo máximo aceitável para a perda de informação. O RPO deverá ser utilizado nas configurações das rotinas de cópias de segurança ou em mecanismos de redundância.
5.2	RTO – Tempo Pretendido para Recuperação	Tempo entre o início da indisponibilidade e o retorno da operação do serviço.
5.3	WRT – Tempo para Recuperação Plena	Após atingir o RTO, o WRT é tempo necessário para a restauração de cópias de segurança ou para a replicação de base de dados, considerada a meta de operação em consonância com os níveis de qualidade de serviço acordados.
5.4	MTD – Tempo Máximo Tolerável	Tempo máximo de indisponibilidade do serviço. Deve ser a soma do RTO com WRT.
Metodologias:		Reunião.
Responsáveis:		Gestor do Serviço. Equipe de TI. ASTI/DTI/PGT.

Observações:
1) Na primeira interação do PCSTI, esses valores serão totalmente empíricos e baseados em decisões subjetivas. Dessa forma, o teste do PCSTI fornecerá informações objetivas para ajustes desses valores.
2) Se não houver base de dados a ser restaurada ou replicada, RTO = WRT.
3) No caso de serviços complexos, pode-se definir um RTO para cada atividade distinta a fim de permitir uma melhor visibilidade do andamento da recuperação total.

6. GESTÃO DE RISCO E DE IMPACTO AOS SERVIÇOS	
Deve-se incluir o Perfil de Riscos conforme Art. 18 da Resolução CETI nº8 que trata da gestão de riscos.	
Responsáveis:	Gestor do serviço. ASTI/DTI/PGT
Observações: Caso se disponha da análise de risco, deve-se estimar, de forma *ad hoc*, as principais ameaças, vulnerabilidades e impacto.	

7. DESCRIÇÃO DA PLATAFORMA OPERACIONAL DO SERVIÇO		
7.1	Descrição técnica do sistema ou serviço.	
7.2	Modelo de Arquitetura e Interação	Modelo de arquitetura (cliente/servidor, P2P, webservices). Camadas e principais entidades em cada camada. Modelo de interação entre essas entidades.
7.3	Plataforma lógica	Servidor de Aplicação. Banco de Dados. Sistema Operacional.
7.4	Plataforma física	Processamento. Memória Primária. Armazenamento. Físico ou virtual.
7.5	Informações de Rede	Endereço. Nome. Localização.
7.6	Cadeia de Dependência	Identificar outros serviços e sistemas que dão suporte ao serviço objeto do PCSTI.
Metodologias:		Reunião.
Responsáveis:		Gestor do Serviço. Equipe de TI. ASTI/DTI/PGT.
Observações: 1) O preenchimento deste tópico não necessita ser detalhado. As informações devem ser suficientes para os objetivos do PCSTI. 2) Entretanto, deve-se dar atenção para o modelo de interação entre as entidades do serviço e para a cadeia de dependência com outros serviços.		

8. MAPEAMENTO DE PROCEDIMENTOS *ad hoc*.	
Incluir qualquer documentação ou procedimento ad hoc relacionados à continuidade do serviço.	
Responsáveis:	Equipe de TI.
Observações: 1) Identificar os possíveis valores ad hoc para RPO. 2) Identificar como os dados são armazenados e como funcionam os mecanismo de cópia de segurança. 3) Identificar o histórico de incidentes. Mesmo que não estejam documentados, colher depoimentos com a equipe técnica.	

9. CRITÉRIOS PARA ATIVAÇÃO DO PCSTI	
9.1 Avaliação inicial sobre o incidente.	
9.2 Potencial de agravamento.	
9.3 Ações de contorno.	
9.4 Ativação total ou parcial do plano.	
Metodologia:	Reunião.
Responsáveis:	Gestor Equipe de TI.
Observações:	

10. ESTRUTURA DO PLANO DE RECUPERAÇÃO DE SERVIÇO DE TI – PRSTI.		
10.1	Alternativas imediatas para solução de contorno em caso de incidente.	
10.2	Lista das atividades conhecidas para a solução da causa raiz.	
10.3	Lista das atividades conhecidas para recuperação do serviço.	
10.4	Procedimento atual de restauração de cópias de segurança.	
10.5	Identificar as dependências entre as atividades de recuperação.	
10.6	Identificar as dependências do fornecimento de serviços de terceiros.	
10.7	Se ainda não disponível a análise de riscos, identificar os controles atuais que possam reduzir a ocorrência de incidentes.	
Metodologias:	Reunião.	
Responsáveis:	Equipe de TI. ASTI/DTI/PGT.	
Observações:		

11. MAPEAMENTO DAS HABILIDADES	
Procedimento/Atividade do PRSTI	**Habilidade**
Metodologias:	Entrevista via questionário estruturado.
Responsáveis:	Equipe de TI. ASTI/DTI/PGT.
Observações: 1) Incluir informações de treinamentos formais. 2) Deve-se identificar a concentração de habilidades em uma única pessoa da equipe. 3) Identificar as habilidades que, embora não estejam fisicamente na equipe de TI, possam contribuir para o PRSTI.	

12. PLANO DE COMUNICAÇÃO		
Atividade	**Nome**	**Contato**
Metodologias:	Entrevista via questionário estruturado. Reunião.	
Responsáveis:	Gestor Equipe de TI. ASTI/DTI/PGT.	
Observações:		