MINISTÉRIO PÚBLICO DO TRABALHO
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO – CETI
SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

Resolução CETI/MPT n.º 8, de 3 de maio de 2016

Institui a Política e o Macroprocesso de Gerenciamento de Riscos de TI no Ministério Público do Trabalho.

O Comitê Estratégico de Tecnologia da Informação (CETI) do Ministério Público do Trabalho, no uso das atribuições que lhe conferem a Portaria n.º 723, de 9 de setembro de 2015;

CONSIDERANDO que, de acordo com a Resolução CNMP n. 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 conjunto de boas práticas de governança corporativa de Tecnologia da Informação previstas no framework COBIT (*Control Objectives for Information and Related Techonogy*), a incluir suas diretrizes de gerenciamento de riscos (*RiskIT - Framework for Management of IT Related Business Risks*);

RESOLVE:

Art. 1º Instituir a Política e o Processo de Gerenciamento de Riscos de Tecnologia da Informação do Ministério Público do Trabalho.

Art. 2º Para os efeitos desta resolução e das notas técnicas a serem produzidas em consonância com as diretrizes ora estabelecidas, consideram-se as seguintes definições:

I. Risco: evento possível cuja ocorrência incidente sobre determinado objeto culmina em um impacto negativo ou positivo;

II. Risco de Tecnologia da Informação: é um risco associado a um serviço, ativo ou projeto de Tecnologia da Informação (TI);

III. Processo de Gerenciamento de Riscos de TI (PGRTI): conjunto de procedimentos, organizados consoante princípios e com a consideração das relações entre diferentes atores, destinado a identificar, analisar, acompanhar e planejar respostas aos riscos de TI;

IV. Vulnerabilidade: qualidade ou estado de fraqueza associado a um ativo ou a um processo de sistemas de informação;

V. Oportunidade: risco de impacto positivo, caso ocorra;

VI. Registro de Risco: conjunto de informações relacionadas ao risco levantado, como impacto, probabilidade e plano de respostas;

VII. Apetite por Riscos: grau de exposição a riscos, característica do órgão ou unidade organizacional;

VIII. Indicadores de Risco:

a) Indicadores-chave de riscos (KRI): como tendência, indicam a iminência do evento ao qual o risco está associado – considera, como pressuposto, que todos os riscos sejam mensurados para definir o quanto o perfil de riscos está se alterando e, assim, para perceber se o risco, em sua probabilidade ou impacto, vai se agravar;

b) Indicadores-chave de performance (KPI): medem a performance dos serviços sobre os quais incidem os riscos, de forma a monitorar atividades ou entes cujo mal funcionamento possam provocar prejuízos ou perdas;

c) Indicadores-chave de Resultado (KGI): aferem o resultado dos serviços, de forma a indicar possibilidade de ocorrência de um sinistro quando confrontado com o que ordinariamente acontece ou se espera – tendem a estar no PETI, sobretudo para serviços estratégicos.

IX. Sinistro: evento de um risco quando concretizado;

X. Resposta ao Risco: coordenação de ações preventivas visando a reduzir o impacto ou a probabilidade de ocorrência do sinistro. Não se confunde com resposta a incidente ou evento, que é iniciada pelo disparo de um gatilho (sinistro) no plano fático;

XI. Estratégias de Resposta a Risco: proposta de curso de ações diante da avaliação do risco:

a) Aceitar: não promover qualquer ação preventiva, de modo que só se mobilizem recursos quando da ocorrência do sinistro;

b) Transferir: atribuir a terceiros a responsabilidade pela resposta ao risco;

c) Mitigar: promover conjunto de ações preventivas que reduzam o risco a níveis aceitáveis de probabilidade e impacto;

d) Evitar: modificar ou cancelar o objeto (escopo do projeto ou desenho do serviço) de forma que o cenário se torne inviável.

XII. Ameaça: ação intencional ou acidental que, ao explorar vulnerabilidades, podem causar impactos negativos

XIII. Risco Residual: nível de risco remanescente após a etapa de tratamento de risco.

Art. 3º Os papéis envolvidos no Processo de Gerenciamento de Riscos de TI são:

I. Dono do Risco: colaborador da área de negócio exposta ao risco – em geral, são os usuários dos serviços;

II. Gestor de Riscos: responsável pela compilação dos perfis de risco e pelo acompanhamento de KRI e KPI no MPT;

III. Analista de Risco: pratica as atividades de identificação, análise e planejamento de resposta aos riscos.

a) Gerente de Projeto ou Dono do Produto: além de atuar, responsável pela condução do projeto ou evolução de um produto, no papel de analista de risco do projeto, do produto ou do serviço; promove ajustes na sensibilidade dos KRI para evitar acionamentos desnecessários de planos de resposta a eventos

b) Gerente de Serviço de TI: como responsável pela operação de um serviço de TI, atua naturalmente como analista de risco de operações;

CAPÍTULO I - DA IDENTIFICAÇÃO DE RISCOS

Art. 4º A abordagem para identificação de riscos, conforme o contexto, poderá ser:

I. Descendente (top-down): apropriada a análises estratégicas e consistente na compreensão do negócio e da aptidão de um evento de prejudicar seus objetivos.

II. Ascendente (bottom-up): emergente de ambientes operacionais, em que os riscos apontem eventos potencialmente incidentes em situações específicas, de forma a conduzir a avaliação do seu impacto sobre os objetivos do negócio.

Art. 5º A identificação do risco deverá ser documentada por meio do Termo de Registro de Risco (Anexo I), do qual deverá constar, no mínimo:

I. Declaração do Risco: breve descrição do risco, necessária para identificar seus elementos fundamentais como o evento, o agente, os ativos envolvidos e o impacto;

II. Dono do Risco: responsável por determinar as respostas a um risco, com base no apetite por risco da organização, mediante análise de custo-benefício dos controles e medidas de combate aos sinistros;

III. Data da formulação identificação ou revisão para atualização;

IV. Data prevista da próxima revisão para atualização;

V. Categoria do Risco: estratégico, de projeto ou de operação;

VI. Descrição do Risco: detalhamento da declaração do risco, necessária a analises aprofundadas;

VII. Cenário: Composição hipotética detalhada de variáveis, que conduziriam à concretização do evento descrito no risco, como motivação e habilidade do agente, ameaças, vulnerabilidades, ativos correlatos;

VIII. Declaração do Cenário;

IX. Detalhamento do Cenário: agente, tipo de ameaça, evento, ativo e fatores temporais;

X. Informações complementares.

Art. 6º Os processos de desenho de serviços e de gerenciamento de projetos devem prever ritos para identificação de riscos.

Parágrafo Único. Os riscos de operação identificados no decorrer da execução de um projeto devem ser imediatamente registrados e submetidos à respectiva área de operações para análise e avaliação, na forma da resolução CETI n. 2/2016.

CAPÍTULO II - DA ANÁLISE DE RISCOS

Art. 7º A responsabilidade pela realização da análise de riscos incumbe:

I. Ao gerente do projeto (dono do produto) ou ao membro da equipe por ele designado, no caso dos riscos do projeto;

II. Ao gerente do serviço ou ao membro da equipe por ele designado, no caso dos riscos de operação.

Parágrafo Único. Os critérios para a análise de riscos específicos deverão ser propostos durante sua identificação.

Art. 8 A construção do catálogo de riscos estratégicos e a avaliação do perfil de riscos da organização serão elaborados e atualizados com periodicidade anual pelo Escritório de Governança, na figura do Gestor de Riscos.

Parágrafo único. A avaliação do perfil de risco da organização será documentada com um conjunto de critérios globais de análise de impacto e probabilidade que servirão de diretrizes a elaboração de critérios específicos, quando necessário.

Art. 9 A taxonomia do registro de riscos deverá ser aprovada pelo CETI, mediante parecer do Escritório de Governança.

Art. 10. A análise de riscos deve compreender, pelas perspectivas quantitativa e qualitativa:

I. A avaliação das funções críticas para a manutenção das atividades estratégicas da organização no cenário desenhado para o risco;

II. A ponderação sobre o impacto de eventual sinistro sobre o serviço, considerando o nível de criticidade a ele atribuído;

III. O exame da probabilidade de ocorrência, considerando, no mínimo, a natureza da ameaça, a motivação do agente e a habilidade deste;

IV. A avaliação da aptidão controles existentes, com propostas de aprimoramentos, sempre que necessário, de modo que se considerem variáveis de custo em confronto com o valor dos ativos expostos ao risco.

§1º O registro do histórico do monitoramento do risco deverá engendrar a utilização de modelos probabilísticos.

§2º A análise deverá ser realizada mediante critérios globais e específicos pré-estabelecidos ou por critérios complementares necessários à manutenção da qualidade da avaliação e das respostas aos riscos.

CAPÍTULO III - DA AVALIAÇÃO DE RISCOS

Art. 11 Realizada a análise e com base no apetite por riscos, a resposta será elaborada com os seguintes elementos fundamentais:

I. Estratégia de resposta, consistente em aceitar, transferir, mitigar ou evitar;

II. Plano de Resposta, consistente em ações para reduzir o impacto ou a probabilidade de sinistro a um nível aceitável.

§ 1º As ações do plano de resposta serão detalhadas individualmente com as seguintes informações mínimas:

I. Breve descrição da ação;

II. Responsável por sua execução;

III. Prazo de sua conclusão;

IV. Custo estimado de implementação.

§ 1º O plano de resposta será submetido ao dono do risco para aprovação mediante exame da relação entre o custo da implementação e a expectativa de impacto do sinistro.

§ 2º As ações que demandarem abertura inicial ou superveniente de projeto devem ser registradas no Funil de Serviços e avaliadas pelo CETI de acordo com o processo de gerenciamento do portfólio (Resolução CETI n.º 2/2016).

§ 3º O plano de resposta deverá prever data da nova análise e de avaliação do risco, que poderá ser atualizada em função de mudanças no objeto ou de ocorrência de eventos, conforme procedimentos de monitoração.

CAPÍTULO IV - DO TRATAMENTO DE RISCOS

Art. 12 O analista do risco deverá acompanhar o andamento do plano de resposta e de suas ações de forma a atualizar o registro do risco com descrição de impedimentos e informações sobre as ações, concluídas ou programadas.

§ 1º Inclui-se, no escopo do acompanhamento, o desenvolvimento dos projetos referidos no §2º, supra.

§ 2º O andamento do plano de resposta deverá ser informado ao dono do risco e ao Escritório de Governança.

CAPÍTULO V - DO MONITORAMENTO DE RISCOS

Art. 13 Os indicadores associados ao registro do risco devem ser monitorados pela área responsável pela operação do serviço ou pela condução do projeto.

Art. 14 O acompanhamento de indicadores será realizado de forma unificada em ferramenta eletrônica com gatilhos de notificação aos interessados, consoante diretrizes da política de comunicação.

Art. 15 Em caso de ocorrência de sinistro, de evento-gatilho ou de elevação do indicador a determinado nível, serão notificados:

I. Os gerentes dos serviços, donos de produto ou gerentes de projetos que podem ser afetados pelo evento, conforme Registros de Riscos;

II. Os Analistas dos Riscos associados ao indicador;

III. O Gestor de Riscos, no Escritório de Governança;

IV. Os Donos dos Riscos, conforme Registros de Riscos relacionados ao indicador;

V. Demais partes interessadas, conforme políticas de segurança, planos de continuidade e recuperação e processos de gerenciamento de eventos.

§ 1º As ações de contingência devem respeitar regramento específico de gerenciamento de incidentes, de projetos ou de segurança da informação.

§ 2º Os analistas de risco notificados deverão:

I. Avaliar ou reavaliar a sensibilidade dos indicadores, promovendo, conforme o caso, ajustes nos níveis de alerta;

II. Reportar a ocorrência do sinistro no registro do risco, juntamente com a ação de contingência adotada.

§ 3º Os níveis de tolerância serão baseados nos instrumentos de governança existentes e no parecer de todos os envolvidos em sua configuração.

CAPÍTULO VI - DO PERFIL DE RISCOS

Art. 16 Os indicadores devem ser auditados anualmente ou sempre que identificados problemas em sua aptidão de diagnóstico.

Art. 17 São responsabilidades do gestor de riscos, quanto ao delineamento e ao acompanhamento do Perfil de Riscos do MPT:

I. Revisar periodicamente os registros de riscos em busca de padrões de vulnerabilidade e oportunidades de melhoria, de forma a fornecer subsídios para um Perfil de Riscos de TI do MPT.

II. Manter uma matriz dos riscos de TI, assessorando o CETI e as áreas operacionais sobre o grau de exposição dos serviços aos riscos mapeados;

III. Auxiliar os gerentes de projetos e de serviços de TI na identificação e na análise de riscos de projeto e de operação, respectivamente;

IV. Elencar as mudanças necessárias para garantir a eficácia do processo de gerenciamento de riscos;

V. Fomentar ajustes na sensibilidade dos KRI para evitar acionamentos desnecessários de planos de resposta a eventos.

§ 2º A compilação dos registros de risco será mantida de forma sumarizada, sob a forma de perfil de riscos.

Art. 18 O Perfil de Riscos deverá conter:

I. Catálogo dos Registros de Risco;

II. Critérios Globais para Análise de Risco;

III. Catálogo de Indicadores, preferencialmente com os valores da leitura mais recente, data da leitura, referencial e sinalização de situação e tendência;

IV. Apetite por Riscos corrente, apontando critérios para adoção de estratégias de resposta a riscos;

V. Relatórios de risco, contendo o Perfil de Riscos ao final de um período de avaliação, determinado pelo CETI, e uma análise crítica;

Art. 19 O Perfil de Riscos deve ser acessível a todos os colaboradores de TI do MPT, aos Donos de Risco e ao CETI;

Art. 20 O relatório de risco deve ser apresentado ao CETI com periodicidade mínima semestral.

Parágrafo único. Todas as propostas de melhoria deverão ser registradas no Funil de Serviços, na forma de Resolução CETI n.º 2/2016.

Art. 21 Os casos omissos serão resolvidos pelo CETI, em Nota Técnica, ouvidos os interessados.

Art. 22 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

MINISTÉRIO PÚBLICO DO TRABALHO
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO – CETI
SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

ANEXO I - PERFIL DE RISCO

Todos os Registros de Risco devem ser registrados neste espaço, usando o modelo, também disposto nesta área.

Critérios Globais:

Critério	Parâmetro	Tipo	Faixa	Referência
<sigla - nome>	***<parâmetro de medição>***	**IMPACTO PROBABILIDADE**	**0**	
			1	
			2	
			3	
			4	
			5	

MINISTÉRIO PÚBLICO DO TRABALHO
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO – CETI
SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

Os Riscos de TI

<Tipo de Ameaça>

Risco	Categoria	Classificação	Probabilidade	Impacto	Indicadores	Resposta
<Denominação>	OPERAÇÃO PROJETO ESTRATÉGICO	ALTÍSSIMA ALTA MÉDIA BAIXA	ALTÍSSIMA ALTA MÉDIA BAIXA	ALTÍSSIMO ALTO MÉDIO BAIXO	*<sigla>*	ACEITAR TRANSFEIR MITIGAR EVITAR

MINISTÉRIO PÚBLICO DO TRABALHO
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO – CETI
SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

Apetite por Riscos:

		Probabilidade					
		0	**1**	**2**	**3**	**4**	**5**
Impacto	**0**	ACEITAR	ACEITAR	TRANSFERIR	TRANSFERIR	MITIGAR	MITIGAR
	1	ACEITAR	TRANSFERIR	TRANSFERIR	MITIGAR	MITIGAR	MITIGAR
	2	TRANSFERIR	TRANSFERIR	MITIGAR	MITIGAR	MITIGAR	MITIGAR
	3	TRANSFERIR	MITIGAR	MITIGAR	MITIGAR	MITIGAR	EVITAR
	4	MITIGAR	MITIGAR	MITIGAR	MITIGAR	EVITAR	EVITAR
	5	MITIGAR	MITIGAR	MITIGAR	EVITAR	EVITAR	EVITAR

MINISTÉRIO PÚBLICO DO TRABALHO
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO – CETI
SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

Indicadores:

Indicador	Tipo	Data da Leitura	Valor	Referencial	Situação	Tendência
<Sigla> - <Nome>	KRI KPI KGI				ALERTA AVISO CONFORME	ESCALADA AUMENTO CONTROLE REDUÇÃO

MINISTÉRIO PÚBLICO DO TRABALHO
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO – CETI
SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

ANEXO II - MODELO DE REGISTRO DE RISCO

I. Resumo

Declaração do Risco		ID
Dono do Risco		ID
Última Avaliação		ID AVR
Próxima Avaliação		ID AVR
Categoria do Risco	OPERAÇÃO PROJETO ESTRATÉGICO	ID
Classificação do Risco	ALTÍSSIMO ALTO MÉDIO BAIXO	ANR
Resposta ao Risco	ACEITAR TRANSFERIR MITIGAR EVITAR	AVR

Quando preencher - legenda
ID - Identificação de Risco
ANR - Análise de Risco
AVR - Avaliação de Risco
OC - Observação Constante

II .Descrição do Risco

Descrição			ID
Cenário			ID
Componentes do Cenário	**Agente**		ID
	Tipo de Ameaça		ID
	Evento		ID
	Ativo		ID
	Fatores Temporais		ID
Informações Complementares			ID
Critérios Globais Adotados			ID
Critérios Específicos			ID ANR

III - Resultado da Análise

Probabilidade	*Usar escala prevista nos critérios*	ANR
Observações sobre a Probabilidade		ANR
Impacto (por critério)	*Usar escala prevista nos critérios*	ANR
Observações sobre o Impacto (por critério)		ANR
Impacto Global		ANR
Observações sobre o Impacto Global	ALTÍSSIMO ALTO MÉDIO BAIXO	ANR

IV - Plano de Respostas

Resposta ao Risco	ACEITAR TRANSFERIR MITIGAR EVITAR	AVR
Justificativa		AVR
Plano de Ação	**Ação** / **Custo** / **Responsável** / **Prazo** / **Status** / **Concluído em**	AVR
Situação Geral do Plano de Ação		OC
Impedimentos ao Plano de Ação		OC
Situação da Ações Concluídas		OC
Problemas nas Ações Concluídas		OC

V - Indicadores ANR

Indicador	**Tipo**
	KRI KPI KGI

VI - Sinistralidade OC

Data do Sinistro	**Duração**	**Impacto**	**Tempo de Resposta/Recuperação**	**Observação**